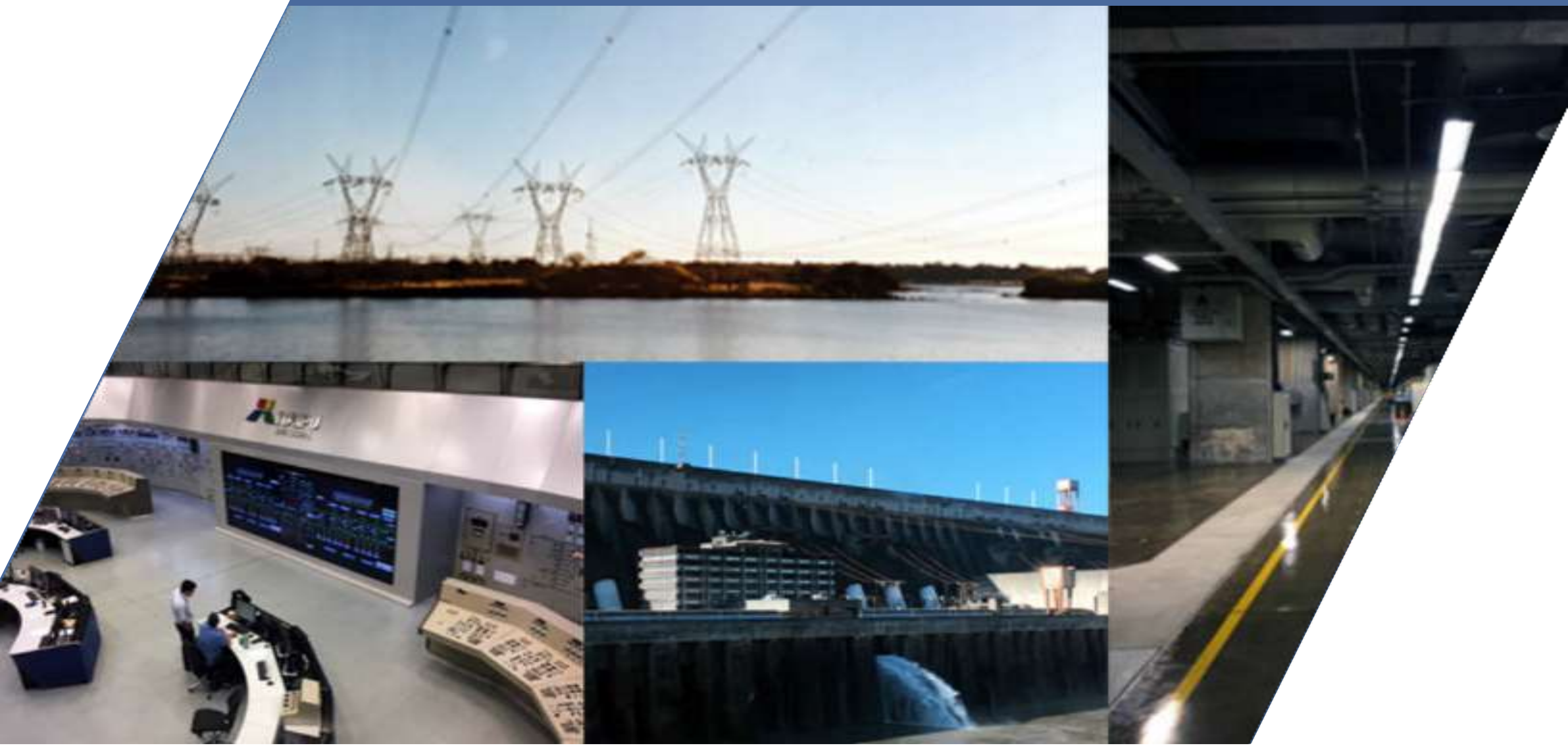
UNITED NATIONS
OFFICE OF COUNTER-TERRORISM
UN Counter-Terrorism Centre

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

INTERPOL

The protection of critical infrastructures against terrorist attacks: Compendium of good practices



Compiled by CTED and UNOCT in 2018

THE PROTECTION OF CRITICAL INFRASTRUCTURES AGAINST TERRORIST ATTACKS:

COMPENDIUM OF GOOD PRACTICES

TABLE OF CONTENTS

PREFACE

On 17 February 2017, the United Nations Security Council unanimously adopted Resolution 2341 on Protection of Critical Infrastructures and Enhancement of States' Capacities to Prevent Attacks against Critical Infrastructure and called upon Member States to address the danger of terrorist attacks against critical infrastructure. The resolution invites Member States to consider possible preventive measures in developing national strategies and policies.

In the UN Global Counter-Terrorism Strategy, under Pillar II on "Measures to Combating and Preventing 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".

Security Council Resolution 1373 (2001) had already called on Member States to "take the necessary steps to prevent the commission of terrorist acts, including by provision of early warning to other States by exchange of information". Security Council Resolution 1566 (2004) also had called upon States to prevent criminal acts, including against civilians, committed with the purpose to provoke a state of terror in the general public or in a group of persons, intimidate a population, or compel a Government or an international organization to do or to abstain from doing any act. The physical protection of critical infrastructure can prevent the commission of high-impact terrorist attacks. Moreover, the immediate response to a terrorist attack against critical infrastructure can prevent the "cascading" effects frequently associated with such attacks.

Security Council Resolution 2341 (2017) directs the Counter-Terrorism Committee (CTC), with the support of the Counter-Terrorism Committee Executive Directorate (CTED), "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." This CTED mandate contributes to the production of assessment and to develop analysis, including on counter-terrorism trends, which will be shared within the context of this important project[1].

Resolution 1373 also mandates the Counter-Terrorism Implementation Task Force (CTITF), under the Office on Counter-Terrorism (OCT), the CTITF Working Group on the Protection of Critical Infrastructure including Vulnerable Targets, Internet and Tourism Security, and the CTC (with the support of CTED) to continue to work together in the facilitation of technical assistance and capacity building, as well in raising awareness in the field of critical infrastructure protection (CIP) from terrorist

[1] The CTC held two open briefings on these matters: (i) an open briefing on "Protection of Critical Infrastructure in Tourism", held on 12 June 2014 and (ii) an open briefing on "Strengthening Emergency Responses in the Aftermath of Terrorist Incidents", held on 16 June 2015. On 21 November 2016, the Security Council held an "Arria Formula" meeting on the "Protection of Critical Infrastructure against Terrorist Attacks", at which Member States presented their concerns and views on key aspects of this topic.

attacks, in particular by means of: strengthening their dialogue with States and international and regional organizations (IROs) and working with technical assistance providers, including by sharing information.

In the UN Global Counter-Terrorism Strategy, under Pillar II on measures to combating and preventing Terrorism, Member States also resolved "to work with the United Nations with due regard to confidentiality, respecting human rights and in compliance with other obligations under international law, to explore ways and means to Coordinate efforts at the international and regional levels to counter terrorism in all its forms and manifestations on the Internet; Use the Internet as a tool for countering the spread of terrorism, while recognizing that States may require assistance in this regard."

Under the chairmanship of INTERPOL and UNOCT, the CTITF Working Group on "Protection of Critical Infrastructure including Vulnerable Targets, Internet and Tourism Security" decided to develop a Compendium of good practices for the protection of critical infrastructures against terrorist attacks. The Compendium has been elaborated under a "One UN approach". It does contribute to raising awareness on the requirements of Resolution 2341 (2017). The Compendium offers Member states and IROs guidelines and compiles good practices on the_Protection of Critical Infrastructures from Terrorist Attacks (with indicators, standards, risk assessment measures, recommendations, good practices, and *etc*.). It also provides Member States with reference material on the development of strategies for reducing risks to Critical Infrastructure from terrorist attacks. While keeping in mind the differences in the conceptual and normative frameworks applicable to "soft targets" and Critical Infrastructures, the Compendium highlights possible element of synergies, considering that very often the same public agencies have institutional and operational responsibilities in both areas. Moreover, it provides Member States as well as IRO with clear guidance on how to develop and strengthen such strategies. References and indicators address prevention, preparedness, mitigation, investigation, response, recovery and other relevant concepts in CIP.

In addition to the requirements of Security Council resolution 2341 (2017), the implementation of the different elements included in the Compendium is taking place in the context of the General Assembly resolution on the Sixth Review of the United Nations Global Counter-Terrorism Strategy (A/RES/72/284), which "[e]ncourages all Member States to collaborate with the United Nations Counter-Terrorism Centre and to contribute to the implementation of its activities within the Counter-Terrorism Implementation Task Force (Global Counter-Terrorism Coordination Compact entities), including through the development, funding and implementation of capacity-building projects in order to mobilize a stronger and more systematic response to terrorism at the national, regional and global levels."

This Compendium was compiled and developed with the assistance of Mr. Stefano Betti, Senior Criminal Justice and Policy Expert, under the guidance of CTED. The project was made possible through a generous grant from the UN Counter-Terrorism Centre.

Vladimir Voronkov
Under-Secretary-General
United Nations Office of Counter-Terrorism
Executive Director
United Nations Counter-Terrorism Centre

Michèle Coninsx
Assistant-Secretary General
Executive Director
Counter-Terrorism Committee Executive Directorate

THE PROTECTION OF CRITICAL INFRASTRUCTURES AGAINST TERRORISM ATTACKS – THE PERSPECTIVE OF INTERPOL

*Introductory remarks by INTERPOL – **Chair of the CTITF Working Group on** "Protection of Critical **Infrastructure including Vulnerable Targets, Internet and Tourism Security"***

Critical infrastructure acts as the life support system of our everyday existence. Our societies are sustained by a highly complex and sophisticated network of infrastructure systems. Our citizens expect and rely upon functioning institutions and services for their health, safety, security and economic well-being.

This life support system has become more efficient and productive due to technological advances, the interchanges of globalisation, and the demands of an increasingly urban population. The advent of *life 3.0* - the overlapping of the digital and physical world – allowed us to monitor and even control infrastructure from anywhere in the world.

However, with heavy reliance and real-time connectivity comes vulnerability to threats. The interdependence of our infrastructure through sectors and industries, between cyber and physical areas, and across national boundaries, means that the consequences of an attack could be far-reaching.

One attack on a single point of failure could lead to the disruption or destruction of multiple vital systems in the country directly affected, and a ripple effect worldwide. This creates an appealing target to those intending to harm us. And as our cities and infrastructure evolve, so do their weapons.

Conflict zone tactics - such as simultaneous active shooter events; armoured vehicle-borne improvised explosive devices (VBIED); home-made explosive vests; hacking attacks; or portable Unmanned Aerial Systems with explosive payloads – could be honed for use in our city streets and against key facilities.

So how can we protect the vital organs of our life support system against this ever-adapting threat?

The short answer: by getting all relevant actors able to prepare; prevent; and respond to such attacks.

These imperatives are at the core of INTERPOL's efforts to promote intelligence sharing, capacity building and resilience in some crucial areas.

First, we focus on strengthening critical site security with emergency preparedness standards and procedures.

For instance, INTERPOL's Vulnerable Targets team has been working with our member countries in West Africa to enhance the physical security of laboratories hosting dangerous pathogens and protect them from terrorist attacks. Generously funded by the Canadian government, this project seeks to build biosecurity action plans through joint inter-agency action.

Second, we continue to urge countries to protect their borders and counter terrorist mobility.

Between January 2017 and April 2018 INTERPOL observed a more than 200 per cent increase in the number of profiles of foreign terrorist fighters accessible in real time through its criminal information system and a 750 per cent increase in the sharing of information by member countries through its channels.

This is simply unprecedented in such a sensitive area – the call issued by the Security Council created a watershed.

Third, it is essential to remain vigilant and increase efforts to interdict materials and tools before they become the next weapon.

In this context, INTERPOL works closely with the IAEA on mitigating the illicit trafficking of radiological and nuclear materials, through training in monitoring and detection, and cross-border operations.

Lastly, and above all, INTERPOL encourages inter-agency and international collaboration, as a force multiplier. The exchange of information, urgent threats detected, and best practices on identifying vulnerabilities, methodologies, and lessons learned is crucial.

In law enforcement, we are keenly aware of the tragic paradox: a terrorist incident is often among the best opportunity for learning and improving. Sharing these lessons across borders means reaping the benefits, without paying that cost. It's a win-win scenario.

Together, we can build a global infrastructure security toolkit, and incident response mechanisms based on real-life operational experience. In parallel, we can test ourselves with plausible scenarios we may have to face in the future.

To this end, INTERPOL organises events for experts from all involved stakeholders. Our Digital Security Challenges, together with private sector specialists, is an example of how we are working with member countries and donors to prepare, prevent and respond to threats – be they physical, digital, or both.

In an interconnected world, we will not succeed in protecting national infrastructure in isolation. This is why global initiatives supported by the United Nations and INTERPOL - and the steps that will be taken as a result by the international community - are essential.

LIST OF ABBREVIATIONS

CBRN	Chemical, Biological, Radiological and Nuclear
CI	Critical Infrastructure
CII	Critical Information Infrastructure
CIP	Critical Infrastructure Protection
CIPRNet	Critical Infrastructure Preparedness and Resilience Research Network
DHS	Department of Homeland Security
EOS	European Organization for Security
ICAO	International Civil Aviation Organization
ICS	Industrial Control System
ICT	Information and Communication Technology
IMO	International Maritime Organization
ISPS Code	International Ship and Port Facility Security Code
ITU	International Telecommunication Union
DoS Attack	Denial-of-Service Attack
IED	Improvised Explosive Devise
ISIL	Islamic State of Iraq and the Levant
ISO	International Organization for Standardization
MANPADS	Man-Portable Air-Defense Systems
NIPC	National Infrastructure Protection Center
OPCW	Organization for the Prevention of Chemical Weapons
OSCE	Organization for Security and Cooperation in Europe
PPP	Public-Private Partnership
UNICRI	United Nations Interregional Crime and Justice Research Institute
UNISDR	United Nations Office for Disaster Risk Reduction
UNOCT	United Nations Office of Counter Terrorism

INDEX OF TABLES

INDEX OF CASE STUDIES

CONTEXT, OBJECTIVES AND METHODOLOGY

This Compendium addresses a topic that is still, to a good extent, in its infancy. The pace with which modern economies have become inextricably interconnected over the past two decades, especially through the great strides made by Information and Communication Technologies, has exposed our societies to a set of unprecedented threats and vulnerabilities. Many of these come from terrorist groups that seek to de-stabilize communities and create widespread panic by interfering in those very assets and processes from which our societies depend for their survival. These assets and processes are central nodes known as "critical infrastructures" (CIs).

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. Still, recent attacks on transportation systems, repeated acts of sabotage against dams, oil pipelines, bridges, etc., by Al-Qaida and ISIL have acted as fresh reminders of the continued interest of terrorist groups in CI disruption.

It is in this context that Security Council resolution 2341(2017) has been adopted as the first ever global instrument entirely devoted to the protection of CIs against terrorist attacks. Its provisions reflect renewed willingness on the part of the international community to elaborate and upgrade mechanisms needed to minimize risks to CIs caused by terrorist attacks and to adequately respond to and recover from such attacks.

This Compendium is born as a tool to support a wide range of actors (from policy makers to law enforcement authorities and private-sector stakeholders) who have responsibilities for designing, improving or implementing policies and measures to protect CIs against terrorist attacks in compliance with the Resolution.

It is arranged in thematic blocks which broadly follow the structure of the Resolution. Each chapter is introduced by one or more of its Operative Paragraphs and by a background analysis to the subject(s) 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 "Critical Infrastructure Protection" is a relatively new acquisition 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 adopted by specific Governments and organizations. The pragmatic approach followed by the Compendium is illustrated by the wealth of case studies that provide concrete examples and implementation options. A number of tables have been added to allow countries to quickly compare measures adopted by other countries and ultimately help them shape those that would best fit their own institutional context within the framework set by the Resolution.

Although the Compendium focuses on the protection of CIs from terrorist attacks, it recognizes that a number of countries have chosen to adopt broad and integrated strategies that take into account the need to enhance CI resilience against all hazards, whether man-made or natural. The Compendium thus provides the conceptual tools to enable countries to adopt, if so they wish, all-encompassing strategies with a special attention to the terrorist threat and related assessment and mitigation mechanisms.

In line with Resolution 2341(2017), the Compendium deals with CIP without focusing on any specific infrastructure type. The transversal approach seeks to highlight common principles, processes and methodologies that countries are encouraged to translate into concrete strategies, actions plans and measures touching on specific areas. At the same time, examples of sector-specific mitigation measures are offered throughout the document. Additionally, Chapter 9 provides an overview of the main initiatives taken by leading international agencies in selected sectors.

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

1. UNDERSTANDING THE CHALLENGE

Security Council Resolution 2341(2017)
Operative Paragraph 2

> *The Security Council […]*
>
> *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 infrastructures.*

1.1 Terrorism as a distinctive threat to CIs

While CIs are exposed to multiple types of hazards, including natural events, human error, technical failure and criminal acts in a broad sense, the birth of CI protection as a distinctive policy area was a direct consequence of the 9/11 events.

Over the past few decades, terrorists have undoubtedly shown interest in CIs as potential targets to advance their goals. Already in 2002, there were clear indications that Al Qaeda was seeking to exploiting vulnerabilities in US public and private utilities. The discovery in Afghanistan of a computer containing structural analysis programs for dams prompted the US National Infrastructure Protection Center to issue a Warning Information Bulletin (NIPC 2002).

Crucially, hardly any sector has escaped from terrorist activity or at least focused attention on the part of terrorist groups. Examples abound. In the transport sector, recent events include the 2016 simultaneous attacks on Brussels' airport and metro by two teams of ISIL operatives. Overall, 32 people were killed and around 300 were injured.

The energy sector has witnessed sustained terrorist activity through attacks perpetrated by Al-Qaida and affiliates on oil companies' facilities and personnel in Algeria, Iraq, Kuwait, Pakistan, Saudi Arabia and Yemen.

Key water infrastructures have been the object of particular attention on the part of ISIL. Between 2013 and 2015, ISIL launched around 20 major attacks against Syrian and Iraqi targets. In addition to destroying pipes, sanitation plants and bridges, ISIL has used water infrastructures strategically, for example by closing damns and cutting off water supplies (Vishwanath 2015).

In some cases, attacks have been attempted on infrastructures 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 the suspicion of an attempt by ISIL to attack, infiltrate or sabotage the facilities to obtain nuclear/radioactive materials.

While massive attacks against CIs involving significant cascading effects/ failures have not materialized, the threat posed by this type of scenario is still very much present and calls on 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. Also, what looms on the horizon is the possibility that new generations of terrorists will become more and more familiar with ICT. Although cyber terrorist attacks have not yet materialized, increased levels of "know-how" in ICTs 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" (GGE 2015, p.6).

1.2 CIs and "soft targets"

The notion of "soft targets" is commonly associated with places where people gather in large numbers, such as museums, cinemas, religious sites, shopping malls, etc. Soft targets are contrasted with so called "hard targets", which broadly identify sites where high levels of protection are ensured, often by armed people, and/or where access by the public is restricted or subject to severe controls (e.g. military installations, embassies, airports).

As witnessed by recent attacks in the pedestrian areas of Nice and Barcelona, at the Christmas market in Berlin and other locations, the open nature and high degree of accessibility of soft targets make them especially vulnerable to terrorist attacks. At the same time, soft targets offer terrorists an ideal ground to strike with little planning effort while still causing mass casualties.

In this context, Security Council Resolution 2396 (2017) specifically recognizes the danger that foreign terrorist fighters connected to ISIL pose by planning and executing attacks on soft targets after having returned from combat zones.

Although there are clearly overlapping features between CIs and soft targets, with individual countries being responsible for defining and developing related protection strategies for both, the two concepts cannot be used interchangeably. A key element of distinction concerns the "criticality" issue. Soft targets do not necessarily appear to be critical for the provision of essential societal services. Moreover, while soft targets may involve an infrastructure (e.g. a stadium), this is not always the case (e.g. people gathering in a square for an open-air concert). Despite the conceptual differences, Section 2.3.1 considers the usefulness for countries to develop synergies between the two notions as part of their overall protection policies against terrorist acts.

1.3 Specific terrorist threats to CIs

Terrorism-related threats against CIs 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 or multiple targets). Understanding the types of threat to which CIs are subject is the first step in the process of designing adequate protection strategies, as discussed in Chapter 2.

1.3.1 Physical versus cyber threats

Physical threats targeting CIs can take a variety of forms. Their common characteristic is that they aim at destroying an infrastructure, weakening it or rendering it inoperative in full or in part by intervening on its physical structure, mechanical components, etc.

The most intuitive physical threats to CIs involve the use of explosives or incendiary devices, means of transport, rockets, MANPADS, grenades and even simple tools (e.g. matches or lighters to induce arsons), etc., to achieve the total or partial collapse or destruction of an infrastructure. Attacks may also involve intentional modification or manipulation of systems and CI processes (e.g. switching facilities on and off, opening and closing closures in piping systems, suppressing process signals, fault signals or alarms). The deployment of chemical, biological, radiological or nuclear weapons or substances represents another distinctive type of threat on CI. This can range from the spreading of infectious pathogens into food supply chains, water pipes, etc., to the use of poison gas at key traffic junctions and cross-roads. It is also pertinent to note that an attack to a critical facility containing chemical, biological, radiological or nuclear materials could also result in the release of such materials.

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

- manipulate systems or data – such as malware that exploits vulnerabilities in computer software and hardware components necessary for the operation of CIs;
- shut down crucial systems – such as DoS attacks;[2]
- limit access to crucial systems or information – such as through ransomware attacks

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

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

According to a private-sector survey of 200 industry executives working in CI 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 percent had faced a large-scale denial-of-service attack, and 85 percent had experienced network infiltrations” (McAfee 2011, p.6).

Table 1: Top 10 Threats to Industrial Control Systems

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 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 (COTS)) 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

	Source: OSCE 2013, p.34	can occur at any time – risk and potential damage can only be minimized in such cases

1.3.2 Insider versus external threats

While the protection of CIs from outside attacks benefit from a significant amount of guidance from national and international regulatory agencies, insider threats have been the object of comparatively less attention. In comparison with external actors, who can only gain access to CIs by means of violent acts or subterfuge, insider perpetrators have undisputed advantages. Insider perpetrators are often company employees or suppliers. They can either be the main conspirators or act as accomplices (e.g. informants) to outside actors. They are often in a position to observe processes undisturbed over a period of time. Their knowledge (or ease with which they can acquire knowledge) of the relevant facility can be readily exploited for criminal purposes.

With this in mind, methodologies for conducting risk assessments on specific locations should involve considering each role within the system, and insider vulnerabilities should not be considered as a separate category. Instead, threat types should be considered with an insider element included within each category. For instance, in considering a threat category such as a person-borne IED used to attack aircraft, those conducting an assessment should consider, separately, both a passenger-borne IED used to attack aircraft and a person-borne IED introduced by crew and/or employees and used to attack aircraft.

Section 2.8 provides some examples of measures to secure CIs 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.

1.3.3 Isolated versus multiple targets

Threats against CIs can be either isolated and sporadic acts, or part of a broader plan to attack infrastructures in the same sector (e.g. nuclear power plants), belonging to an identical owner/ operator, or located in the same geographical area. One may well conceive of terrorist-motivated actions targeting CIs in much the same way as occurs for industrial espionage where cyber-attacks are often launched as "campaigns", or serial attacks. For example, in 2011the so called "LURID" attack targeted, among others, the ICT systems of a number of diplomatic missions and space-related government agencies.

The identification of patterns in similar scenarios often requires strong analytical tools and the processing of information from vast and heterogeneous sources. To complicate matters further, as the OSCE highlights with reference to the energy sector, most cyber-attacks are not publicized because of the relevant operators are reluctant to make those incidents known. Still, the ability to recognize underlying dynamics and methods as early as possible is key to enable authorities to share live information. This increases the capacity to respond more effectively to current attacks and pre-empt imminent ones against likely victims (OSCE, 2013).

In some cases, what appear as an isolated attack, aimed at relatively “unimportant” targets, may in reality be part of more ambitious and incremental criminal strategies.[3]

1.4 Terrorist motivations to attack CIs

The heterogeneous nature of CIs, together with the different geographical and institutional context in which they are located and operate, make it extremely difficult to come to general conclusions as to what motivates terrorists to carry out attacks on CI as opposed to non-critical targets. And yet, analyzing terrorist motivations may provide useful leads as part of the broader threat assessments required under CIP national strategies.

Within the limited empirical research carried out in this field (Ackerman, 2007), it emerges that CIs are attractive for a variety of reasons. Firstly, they may be an appealing target because of their strategic value for societies, especially in highly industrialized countries of the Western hemisphere. Interfering in the functioning of a CI, ideally with the possibility of generating cascading effects, allows terrorists to maximize damage in just one shot and instill fear to levels that would not be attainable as easily by attacking “ordinary” targets. In this vein, Al Qaida operatives were reported to have spent a considerable amount of time surveilling the headquarters of various US-based financial firms and international organizations. Arguably, this meticulous activity followed up on Osama bin Laden's 2001 edict urging his affiliates to “concentrate on hitting the U.S. economy through all possible means”.

Other CIs may be targeted to show the impotence of the State institutions. For example, terrorist organizations may decide to attack power generating facilities, oil pipelines, etc., in order to cut off the supply of basic services and reveal the fragility of public bodies and related Governmental policies (Ackerman 2007, p.170).

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

[3] A joint DHS/FBI report issued in 2017 noted that certain US government networks in the energy, nuclear, water, aviation, and critical manufacturing sectors were at risk of targeted advanced persistent threat (APT) actions. DHS 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: DHS, Advanced Persistent Threat Activity Targeting Energy and Other Critical Infrastructure Sectors, 20 October 2017, at: www.us-cert.gov/ncas/alerts/TA17-293A. See, also: Conner Forrest, “DHS, FBI warn of cyberattacks targeting energy infrastructure, government entities”, 23 October 2017, TechRepublic, at: www.techrepublic.com/article/dhs-fbi-warn-of-cyberattacks-targeting-energy-infrastructure-government-entities).

Paradoxically, terrorists may seek control of CIs not to cause damage or intimidate, but for the very opposite reason of wanting to establish their own legitimacy/ social acceptability. As has been noted, while most operations carried out by ISIL using water-related infrastructures 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" (Vishwanath 2015).

Most likely, in several cases a combination of factors co-exists 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 target will depend on the group's operational capabilities to launch a particular attack. The protective measures in place at a certain CI will naturally influence such decision. This is not to say that terrorists 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, particularly when the target is chosen for its symbolic value.

1.5 Countering terrorist threats to CIs through a human rights-compliant approach

Terrorism poses a serious challenge to the very tenets of the rule of law, the protection of human rights and their effective implementation. In the context of their obligations under international human rights law, States have the duty to protect persons within their jurisdiction from undue interference with their human rights by third parties, including terrorist actors. This duty is particularly important considering the potential impact that attacks on CIs may have on populations, given the role such infrastructure frequently plays in maintaining or delivering vital societal functions. Damage to, 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 to a healthy environment, the right to education, as well as water, sanitation and other aspects of the right to an adequate standard of living.

States' duty to safeguard human rights implies the obligation to take necessary and adequate measures to prevent, combat and punish 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 Global Counter-Terrorism Strategy (GCTS) which emphasizes that effectively combatting terrorism and ensuring respect for human rights are not competing but complementary and mutually reinforcing goals. Indeed, the promotion and protection of human rights constitutes an independent pillar and a cross-cutting necessity to ensure successful delivery of all four components of the GCTS. Moreover, relevant provisions of Security Council resolutions require that any measures taken to prevent and combat terrorism comply with State obligations under international law, in particular international human rights law, refugee law, and international humanitarian law.

In the interest of combatting terrorist threats to CIs, State authorities may temporarily take measures that may result in the limitation of certain rights, resulting in the limitation of certain rights, provided 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, required by the exigencies of the situation, have a clear legal basis and necessary and proportionate to efficiently addressing it. States must 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 are strongly encouraged to conduct regular human rights assessments of measures taken to tackle the terrorist threat to critical infrastructure and ensure that such measures are evidence-based and therefore efficient.

2. DEVELOPING NATIONAL STRATEGIES FOR REDUCING RISKS TO CIs

Security Council Resolution 2341(2017)
Operative Paragraph 2

> *The Security Council Resolution […]*
>
> *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.*

2.1 Why a national strategy?

Most countries have been providing for safety and security measures for their CIs long before CI protection established itself as a policy field in its own right. Protective measures were mostly adopted in an incremental and piece-meal fashion in the form of regulations covering specific sectors or threats, or focusing on certain parts of the risk management processes. Sometimes State policies reached a significant level of sophistication and conformed to the highest international standards. In the nuclear energy sector, for example, following the end of the cold war, Ukraine developed a modern and efficient system for the physical protection of nuclear facilities and materials.

As a result, it may be asked why countries should design general nation-wide CIP strategies when often they have already in place detailed regulations, policies and practices covering most, if not all, critical sectors. The most compelling reason is that, in modern societies, the protection of CIs is an increasingly transversal task. The interdependence between sectors, with the potential for cascading effects in case of accidents (whether of natural origin or man-made) requires the ability to "see the big picture" as a condition to effectively coordinate prevention, response and recovery actions across sectors. Additionally, relying on purely sectoral or "vertical" approaches would appear to unduly multiply involved agencies, cause duplications of work and waste of resources. A comprehensive strategy thus aims to rationalize work-streams, produce "economies of scale" and better allocate financial and human resources around a set of pre-determined objectives.

This is not to suggest that nation-wide CIP strategies should automatically replace existing sector-specific protection measures, particularly when these measures have proven successful or conform to binding international regulatory frameworks. What is needed, however, is for countries to bring the various pieces of the mosaic under a common umbrella, and to make them part of a coherent system of governance. As CIP is linked to several fields of activity (such as energy policy, transport policy, security policy, etc.), the primary goals of a nation-wide strategy are to:

- define organizational structures;
- set measurable objectives and timeframes;
- lay the foundation for effective prevention and management of incidents through the harmonization of tasks between different policy areas.

With this in mind, CIP strategies can be tailored to suit the specific needs and approaches of individual countries. As Section 2.5 shows, countries have adopted a variety of institutional models reflecting not only their specific legal traditions, but also different cultural attitudes towards the role of the law in society, the relationship between Government, citizens and the business sector.

Countries have considerable room for manoeuvre in determining the modalities for protecting their CIs. However, they all need to have in place the conceptual building blocks (a strategy) to connect the dots and ensure smooth working relationships among all involved actors.

2.2 All-hazards versus specific-risk approaches

CIs are subject to polymorphous types of threats. These threats can be natural: on 11 March 2011, for example, an earthquake followed by a tsunami provoked a major nuclear accident in Fukushima, Japan.

Threats can have their origin in negligent human behavior: in 2006, a blackout affected ten 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 motivated by terrorism-related goals or other criminal objectives. Cyberattacks for ransom are an example of profit-making activities that may severely affect CIs by encrypting users' data and demanding payment in exchange for unlocking the data. Threats to CIs can also be linked to criminal behavior in more subtle and indirect ways. In Europe, the French Building Association ("Federation Francaise du Batiment") has repeatedly warned against criminal networks' involvement in trafficking of counterfeit and sub-standard materials used for building construction. Reportedly, many companies in the construction sector purchase non-compliant, poor quality materials affecting infrastructures' solidity and exposing them to a higher risk of collapse.

As countries are called upon to protect CIs from multiple levels of risk, a key question is: should Governments adopt one single plan covering all possible threats, or rather envisage to adopt hazard/risk-specific strategies? In principle, either approach is consistent with the international legal framework.

Among the countries that have adopted CIP strategies, the majority follows an all-hazards approach.[4] 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 make the best use of limited available resources and avoid needless duplication. The underlying rationale is that the same risk management and collaborative processes as well as crisis response mechanisms can be broadly used to respond to all types of threats indistinctively. All-hazards approaches are implemented by countries such as Canada and the UK.

Other countries adopt a mixed approach. Australia, for example, has elaborated specific guidelines on the protection of CI against terrorist attacks. 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 law 8/2011 "establishing measures for the protection on critical infrastructures". 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 Security Council resolution 2341(2017) is for the terrorist threat to be fully and urgently reflected in the preparation of Governments' strategic plans to protect CIs. With this in mind, each country is free to determine, as a matter of national policy, the best forms and modalities for protecting Cis against terrorist acts in a multi-threat type of environment.

2.3 CIP strategies vis-à-vis other national policies

Most countries, including those which have not enacted dedicated CIP strategies, address CIP-related issues in a variety of policy instruments enacted by different Governmental agencies. These documents typically include national (including cyber) security strategies and policies on counter-terrorism. While these various policies may have been adopted at different times and by multiple State agencies, it is vital that they become all parts of a coherent message and approach to CIP. This requires, in particular, that countries determine:

- the interplay between those other policies and a dedicated CIP strategy;
- the extent to which those other policies and/or the CIP strategy itself should be adjusted and streamlined in order to avoid conflict and to ensure overall policy coordination at the national level.

The following sections provide an overview of national policies that have a significant impact on CIP without being necessarily (or entirely) designed for CIP purposes.

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

2.3.1 Policies on "soft targets"

Security Council Resolution 2396(2017) stresses the need for Member 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. In the same year, the European Commission set up a plan focusing on public spaces as a key category of soft targets (European Commission 2017).

As mentioned in Section 1.2, the notion of soft targets is conceptually distinct from that of CIs. A major consequence is that countries' policies dealing with soft targets do not automatically satisfy conditions and requirements for the protection of CIs, particularly when it comes to implementing Security Council resolution 2341(2017).

This does not mean, however, that the two areas should be handled in silos. National policies and practices developed on soft targets may well be useful, and provide a source of good practices, in the CI domain, and vice versa. This is clearly the approach taken by EOS, an entity representing the European security industry and research community. In recognition of the overlapping features between policies on soft targets and CIs, EOS deals with both in the same working group.

CASE STUDY 1

Belgium's Federal Points of Interest

Belgium's law of 1 July 2011 on the protection of critical infrastructure contains the notion of Federal Points of Interest ("Points d'Intérêt Federal"). 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 General Directorate Center Crisis (DGCC)".

This law provides an example of a single normative framework taking into account both CIs and soft targets. Although the Federal Points of Interest do not meet the conditions to be regarded as CIs, they are still considered worth of particular attention and protection.

Instead of taking a compartmentalized approach, the potential for complementarities should be explored. While keeping in mind the differences in the conceptual and normative frameworks applicable to soft targets and CIs, countries are encouraged to develop synergies, taking into account that often the same public agencies have institutional and operational responsibilities in both areas simultaneously.

2.3.2 National security policies

National security is a fluid concept. Countries translates it 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 as well as 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

Poland's 2014 National Security Strategy

The document makes explicit reference to CIP under its section on "Protective Actions". While this section does not elaborate the theme in detail and does not assign specific roles and responsibilities, it has the value of unambiguously identifying CIPs as a national security priority. Other parts of the Strategy set objectives that are relevant for CIP both transversally and in specific sectors, including:

Improving and developing the national crisis management system in order to ensure its internal cohesion and integrity, as well as to allow for an undistorted cooperation within the framework of crisis management systems of international organizations of which Poland is a member;
Ensuring energy and food security;
Increasing public awareness in the domain of security and expanding citizens' competencies allowing them to appropriately respond to crisis situations.

2.3.3 Counter-terrorism policies

While most counter-terrorism strategies do not specifically mention CIs, a number of objectives and institutional arrangements set forth therein are instrumental in preserving the integrity of CIs and the vital societal functions performed by them. 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 the broad frameworks for preventing the commission of terrorist offences (e.g. by addressing preparatory acts, creating synergies between intelligence and law enforcement communities, etc.).

INTERPOL's Global Counter-Terrorism Strategy[5] incorporates the CI dimension under its "Weapons and Materials" Action Stream 4.6 by defining the Organization's mandate in terms of "enhanc[ing] the capacity of member countries to protect their critical infrastructure and vulnerable targets against both physical and cyber terrorist attacks".[6]

[5] AG-2016-RES-03

[6] The concrete implementation of Action Stream 4.6 translates into a close collaboration between INTERPOL's Counter-Terrorism Directorate, based at the General Secretariat in Lyon, France, and the Organization's Innovation Center, located in INTERPOL's Global Complex for Innovation, Singapore.

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

Sweden's Counter Terrorism Strategy

Sweden articulates its CT strategy around three pillars: prevent, preempt and protect. Under "protect", in particular, the objective is "to provide strong protection for people, information, functions and facilities – people must feel safe, secure and free within society". The strategy makes specific reference to the Swedish Civil Contingency Agency, which officially plays a coordinating role in CIP in Sweden. Sweden's CT strategy has been issued in 2014, the same year when its Action Plan for CIP was also released. The elaboration of connected policy documents at short distance from each other facilitates the adoption of uniform languages, terminologies and approaches across the various instruments.

2.3.4 Cybersecurity policies

Cybersecurity can be defined 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 organisation and user's assets" (GFCE-Meridian 2016, p.8). Cybersecurity policies have a central place in the protection of CIs as they provide the framework where countries define the objectives and means for protecting Critical Information Infrastructures (CIIs). This concept is further examined in Section 2.4.2.

A number of regional instruments explicitly associate cybersecurity concepts to CIs. For example, the African Union Convention on Cyber security (2014) demands that States Parties "undertake to develop, in collaboration with stakeholders, a national cyber security 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".[7]

Another example is the European Union's 2013 Cyber Security Strategy, under which the European Commission pledged to "continue its activities, carried out by the Joint Research Centre in close coordination with Member States authorities and critical infrastructure owners and operators, on identifying [network and information security] vulnerabilities of European critical infrastructure and encouraging the development of resilient systems" (European Commission 2013). Under the European Union's Network and Information Security Directive[8] (the "NIS Directive"), EU Member States are expected to designate Operators of Essential Services ("OES") and to introduce new security and reporting requirements for such entities.

[7] Art.24, National cyber security framework.

[8] Directive (EU) 2016/1148 concerning Measures for a High Common Level of Security of Network and Information Systems across the Union.

With this in mind, not all national cybersecurity strategies provide the same place and "weight" to CIs and there are significant differences among countries. As has been noted, "some strategies have been written from a cyber-crime perspective only or an internet-only perspective. They tend to overlook (national) disruption and crisis management for CIIs 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" (GFCE-Meridian 2016, p.8).

A useful tool offered by ITU is the National Cybersecurity Strategies (NSC) repository. This includes a vast collection of national cyber-security strategies, whether in the form of single or multiple documents or as part of broader ICT or national security strategies.[9] In view of the diversity of approaches among the various existing CIP and Cybersecurity strategies, ITU is currently leading an effort with different global actors for the creation of a common NSC reference guide. This tool aims to provide countries with a clear understanding of the purpose and content of a national cybersecurity strategy, outline existing models and resources and guide countries through their strategy development and strategy evaluation process.[10]

CASE STUDY 4

Singapore's Cyber Security Bill

The Bill formalizes the country's policy in the field and places the protection of CII firmly into cyber security concepts and protective measures. The Bill pursues four objectives:

- To provide a normative framework formalizing the obligations of CII owners to ensuring the cybersecurity of their respective CIIs;
- To entrust the Cyber Security Agency of Singapore (CSA) 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 CSA, and the protection of such information;
- To establish a light-touch licensing framework for cybersecurity service providers.

Source: Cyber security Bill, at:
www.csa.gov.sg/~/media/csa/cybersecurity_bill/draft_cybersecurity_bill_2017.pdf

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

[10] https://www.itu.int/en/ITU-D/Cybersecurity/Pages/National-Strategies.aspx

CASE STUDY 5

United States – Department of Homeland Security Initiatives

In the United States, the Department of Homeland Security (DHS) leads the federal government's efforts to secure the nation's critical infrastructure. To prevent, mitigate, and respond to threats, DHS initiatives include to:

- Develop a technology-neutral voluntary cybersecurity framework;
- Promote and incentivize the adoption of cybersecurity practices;
- Increase the volume, timeliness and quality of cyber threat information sharing;
- Incorporate strong privacy and civil liberties protections into 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 comprehensive research and development plan.

DHS encourages the adoption of the National Institute of Standards and Technology's (NIST) Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity. Revised in April, 2018, the NIST 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 regarding a detected cybersecurity incident;
Recover – develop and implement appropriate activities to maintain plans for resilience and to restore capabilities or services that were impaired due to a cybersecurity incident.

Sources:

Department of Homeland Security, Fact Sheet: EO 13636 Improving Critical Infrastructure Cybersecurity and PPD-21 Critical Infrastructure Security and Resilience, at: www.dhs.gov/sites/default/files/publications/eo-13636-ppd-21-fact-sheet-508.pdf;

Department of Homeland Security, Critical Infrastructure Cyber Community Voluntary Program, at: www.us-cert.gov/ccubedvp

NIST Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 16, 2018, at: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

2.3.5 Other national policies

When a national strategy on CIP is being designed, it is important to make a full inventory of all national policies that have a bearing on it. Some policies and regulatory frameworks may be in place dealing with infrastructures in general. For example, in 2017 Singapore adopted an Infrastructure Protection Act. The act, which is specifically devoted to the protection of infrastructures against terrorist acts, introduces a number of concepts such as that of "protected area", "protected place" and "protected infrastructure". It does not, however, make explicit reference to "critical" infrastructures in terms of assets or systems performing essential functions for the community. In similar cases, it is necessary to determine the role and place of existing normative frameworks in general CIP goals.

Some policies may not mention CIs simply because they were adopted at a time when the notion itself of CIP had not yet made its way into mainstream policy discourses, or for other reasons. If they impinge on CI-related issues in substance, they should be subject to close scrutiny for the purpose of ensuring their compatibility and complementarity with newly designed CIP national strategies.

Other relevant policies stem from countries' international obligations in various fields. For example, in order to comply with relevant international instruments,[11] countries have put in place a range of policies, laws, regulations, strategies, plans and measures to strengthen the security of CBRN materials, facilities and related information.

CASE STUDY 6
Switzerland's Federal Program on National Economic Supply (NES)

NES finds its legal basis in art. 102 of the Constitution, according to which "the Confederation shall ensure that the country is supplied with essential goods and services in the event of the threat of politico-military strife or war, or of severe shortages that the economy cannot by itself counteract. It shall take precautionary measures to address these matters."

As Switzerland's National Strategy for the Protection of Critical Infrastructure clarifies, "NES covers approximately half of the critical sectors and sub-sectors of the CIP national strategy and thus contributes decisively to achieving the objectives of this latter. […] Crucially, the NES focuses primarily on long-term national shortages, while the CIP strategy also takes into account short-term or local disturbances (e.g. regional outages or disruptions).

[11] Such instruments include: the Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons; the Convention on the Prohibition of the Development, Production, Stockpiling and Use of Chemical Weapons and on their Destruction; the Convention on the Physical Protection of Nuclear Material; the International Convention for the Suppression of Acts of Nuclear Terrorism; the United Nations Global Counter-Terrorism Strategy and the United Nations Security Council Resolution 1540 (2004).

2.4 Which infrastructures are critical?

Resolution 2341(2017) explicitly recognizes that "each State determines what constitutes its critical infrastructure". It does not recommend, however, any particular selection method in order to single out CIs among the myriads of infrastructures located in their territories. Other international instruments do not provide any guidance either. 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 […]".[12]

Countries 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. Distinguishing between important/ relevant infrastructures and those that should acquire "critical" status is key to be able to prioritize scarce resources on the protection of vast assets, systems and processes. On the one hand, the inclusion of too many infrastructures in the "critical" category may become an unmanageable task (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 case of accident. One author has underscored a tendency by Governments to expand rather narrow down national lists of CIs. This would happen because "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 […]" (Clemente 2013, p.ix).

Despite the absence of generally applicable criteria, guidance can be found in specific sectors. For example, while ICAO's instruments do not define "critical infrastructure" as such, ICAO Aviation 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".[13]

In the maritime sector, the ISPS Code identifies the assets that Government agencies, local administrations, the shipping and port industries shall protect against security threats affecting ships or port facilities used in international trade. Accordingly, "ship security plans" are understood as those "developed to ensure the application of measures on board the ship designed to protect persons on board,

[12] Art.24, Legal Measures.

[13] Aviation Security Manual (Doc 8973 – Restricted).

cargo, cargo transport units, ship's stores or the ship from the risks of a security incident". Security plans are also expected to be prepared "to protect the port facility and ships, persons, cargo, cargo transport units and ship's stores within the port facility from the risks of a security incident."[14]

2.4.1 Determining "criticality"

The first step in the CI identification processes is normally to adopt an all-encompassing definition of what is meant by CI. This is useful to set the playground in which further policy and regulatory frameworks will be crafted. CIPRNet[15] has singled out over 100 such definitions, of which Table [number] provides a selection. Overall, whereas some countries' definitions highlight the finality or purpose of the infrastructure (i.e. criticality is linked to the performance of essential societal functions), others emphasize the effects of disruption or destruction (i.e. criticality derives from the specific consequences of service interruption).

CIs can be defined, among others, by taking into account the role they play in the promotion and protection of human rights (for example, infrastructure that is vital for the functioning of healthcare delivery systems; emergency service systems, water and wastewater systems, etc.) as well as the human rights impact that the damaging, disruption or destruction of the infrastructure would likely result in (for example, the inability to deliver adequate or even life-saving health services, environmental damage that may result in loss of life, forced displacement having negative impact on the right to health, etc.). Such an approach aligns with the spirit of existing definitions. For example, the EU defines "critical infrastructure" as an "asset, system or part thereof" which is "essential for the maintenance of vital societal 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".[16] 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).

Table 2: National definitions of CIs

Austria	Critical infrastructures are those infrastructures or parts thereof which are of crucial importance for ensuring important social functions. Their failure or destruction has severe effects on the health, security or the economic and social wellbeing of the population or the functioning of governmental institutions (Austria's Strategy for Cyber Security, 2013)

[14] www.imo.org/en/OurWork/Security/Guide_to_Maritime_Security/Pages/SOLAS-XI-2%20ISPS%20Code.aspx

[15] See, in particular, CIPedia, a Wikipedia-like online community service focusing on Critical Infrastructure Protection and Resilience - related issues, developed by the EU FP7 project CIPRNet and continued by volunteers (https://publicwiki-01.fraunhofer.de/CIPedia/index.php/Critical_Infrastructure).

[16] Council Directive 2008/114/EC, Article 2.

Canada	Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government (An Emergency Management for Canada, 2011)
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)
Germany	Critical infrastructures (CI) are 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 (National Strategy for Critical Infrastructure Protection, 2009)
Italy	System, resource, process, structure, even virtual, whose destruction, interruption or even partial or temporary unavailability has the effect of significantly weakening the efficiency and normal functioning of a country as well as the security and the economic, financial and social systems, including central and local public administration bodies (Civil Protection Agency, Glossary)
Kenya	Critical infrastructures describe assets that are essential for the functioning of a society and economy. (e.g., electrical grid, telecommunications, water supply) (Kenya's National Cyber Security Strategy)
Norway	Critical infrastructure is the construction and systems essential to maintain society's critical features which covers society's basic needs and population's sense of security (Cyber Security Strategy for Norway)
Pakistan	Critical Infrastructure includes the infrastructures so designated by any Government in Pakistan and such other assets, systems and networks, whether physical or virtual, so vital to the State or its organs including judicature that their incapacitation or destruction may have a debilitating effect on national security, economy, public health, safety or matters related thereto (Cybercrime Bill 2015)
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. Qatar Cyber Security Strategy, 2014
Saudi Arabia	Critical Infrastructure is defined as system and assets, whether physical or virtual, so vital to Saudi Arabia that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. Developing National Information Security Strategy for the Kingdom of Saudi Arabia NISS draft 7

Trinidad & Tobago	Critical infrastructure means computer systems, devices, networks, computer programs, 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 transportation, public key infrastructure or any combination of those matters (National Cyber Security Strategy, 2012)
Russian Federation	Critical infrastructure of the Russian Federation is an object the violation (or termination) of operation thereof leads to a loss of control, destruction of infrastructure, irreversible negative changes (or failure) of the economy, a subject of the Russian Federation or administrative-territorial units or a significant deterioration in health and safety of people living in these areas, for the long term (National Security of Russia - Information security (February 3, 2012, N. 803)
Spain	CIs are strategic infrastructures (facilities, networks, systems and physical and IT equipment on which operation of the essential services rests, whose operation is indispensable) and where alternative solutions are not possible so that their disruption or destruction would seriously impact essential services (Law 8/2011)
Switzerland	Critical infrastructure refers to infrastructure whose disruption, failure or destruction would have serious implications for society, the private sector and the state (National strategy for the protection of Switzerland against cyber risks, 2012)
Ukraine	(machine translation): Critical infrastructure objects - enterprises, institutions and organizations irrespective of the form of ownership, whose activities are directly related to the technological processes and / or the provision of services of great importance to the economy and industry, functioning of the society and the safety of the population, the failure or malfunctioning of which may have a negative impact on the state of national security and defense of Ukraine, the environment, to cause a property shock do and / or pose a threat to life and health (Law of Ukraine, About the basic principles of providing cyber security of Ukraine, 2163-19)
United States	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters (Patriot Act, 2001)

The second phase in CI identification is the most challenging one since this is where the "prioritization" effort takes place. In particular, this phase aims to identify sectors and sub-sectors (or services) regarded as critical. An initial approach could be to consider other countries that present similarities in societal, geographical features as well as comparable level of technical and economic development.

A number of sectors are likely to be regarded as "critical" by all countries. The energy sector is a prime example of this. Countries are dependent on the provision of electricity for the performance of almost all societal and economic functions, from telecommunication to water pumping to the supply of life-saving medical care. At the same time, it is important to note that a particular sector or sub-sector might be crucial to one nation, but not to another one. The size and specific features of a certain national economy might well determine what is critical and what is less critical. For example, some countries may be massively dependent on the tourism industry for revenue generation and eventually as a condition to maintain social cohesion and internal stability. For these countries, protecting the tourism industry as "critical" may be instrumental in ensuring the delivery of essential services to society.

Also, the fact that a certain sector is designated as critical should not automatically mean that all underlying services are critical. For example, in the energy sector a "district heating service" would most likely not be included as critical at national level, but the delivery of electrical power would. Taking these variations into account, to a great extent countries come to similar conclusions. Table 3 provides the list of 11 EU-defined sectors and 37 corresponding sub-sectors.

Table 3: Indicative list of EU-defined sectors and sub-sectors

I Energy	1 Oil and gas production, refining, treatment and storage, including pipelines 2 Electricity generation 3 Transmission of electricity, gas and oil 4 Distribution of electricity, gas and oil
II Information, Communication Technologies, ICT	5 Information system and network protection 6 Instrumentation automation and control systems (SCADAetc.) 7 Internet 8 Provision of fixed telecommunications 9 Provision of mobile telecommunications 10 Radio communication and navigation 11 Satellite communication 12 Broadcasting
III Water	13 Provision of drinking water 14 Control of water quality 15 Stemming and control of water quantity
IV Food	16 Provision of food and safeguarding food safety and security
V Health	17 Medical and hospital care 18 Medicines, serums, vaccines and pharmaceuticals 19 Bio-laboratories and bio-agents
VI Financial	20 Payment services/ payment structures (private) 21 Government financial assignment
VII Public & Legal Order and Safety	22 Maintaining public & and legal order, safety and security 23 Administration of justice and detention
VIII Civil administration	24 Government functions 25 Armed forces 26 Civil administration services 27 Emergency services

	28 Postal and courier services
IX Transport	29 Road transport 30 Rail transport 31 Air traffic 32 Inland waterways transport 33 Ocean and short-sea shipping
X Chemical and nuclear industry	34 Production and storage/processing of chemical and nuclear substances 35 Pipelines of dangerous goods (chemical substances)
XI Space Source: European Commission 2005	36 Space 37 Research

CASE STUDY 7

The **Netherlands' approach**: from critical sectors to critical processes

In 2014, the CI policy of the Netherlands underwent significant reform. This led to a 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 instead of critical sectors. Identifying critical processes allows 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. Societal developments, such as altered threats and incident evaluations, can lead to the assessment of new processes. The assessment distinguishes between two critical categories, A and B. The failure of A-critical processes have greater potential effects than the failure of B-critical processes. The distinction between A- and B-critical can be helpful in prioritizing incidents or the development of capacities that increase resilience. Prioritizing by classification of critical infrastructure in two categories, A and B, in order to be able to prioritize during incidents and custom solutions for resilience-enhancing measures.

Category A

- National transportation and distribution of electricity
- Natural gas production
- Oil supplies
- Storage, production, or processing of nuclear materials
- Drinking water supplies
- Water management

Category B

- Regional distribution of electricity and gas
- Flight and airplane management
- Maritime and inland shipping management
- Large scale storage, production, or processing of petrochemical resources
- Financial sector (banking services, electronic transfers between banks and between banks and the public)
- Communication with and between emergency services
- Police mobilization
- Government services that depend on reliable, available digital information and data systems

Each ministry is responsible for performing the assessment of the critical processes that fall under its responsibility. The coordinating 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.

Source: The Netherlands 2018

The third step links previously identified sectors and sub-sectors to a list of individual infrastructure assets, systems and processes. Numbers can greatly vary from just a few to several thousands, depending on the size of countries, level of economic development, etc. Countries have elaborated many sets of indicators to identify certain infrastructures as "critical". These indicators normally seek to "measure" the effects of infrastructures' breakdown or functional failure and include a selection/combination of the following:

- Geographical scope of the effect;
- Duration of effect;
- Severity of potential effects in terms of:
- economic consequences (impact on GDP, direct and indirect economic losses, number of personnel employed, tax revenue);
- number of victims and extent of evacuated population;
- loss of authority by the government/ disruption of public administration;
- damage to the environment.

CASE STUDY 8

Systemic versus symbolic criticality in Germany

Germany's CIP Strategy distinguishes between criticality of a systemic and symbolic nature. An infrastructure is considered of systemic criticality whenever - due to its structural, functional and technical position within the overall system of infrastructure sectors - it is highly relevant as regards interdependencies. Examples are the electricity and information and telecommunication infrastructures which, on account of the size and density of their respective networks, are of particular relevance and where a large-area and prolonged outage may lead to serious disruptions of community life and processes and of public safety and security. An 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, emotionally unsettle a nation's society and psychologically have a lasting unbalancing effect on it.

Source: Germany 2009

A variety of methodologies can be used. A consortium led by TNO, a Dutch research organization, has sought to schematically group them into three main types: i) a service-based approach (ex. Switzerland) where the Government identifies critical assets based on sector- specific criteria defining service-level thresholds/quantifiable output of the assets, e.g. number of Megawatts delivered; ii) an operator-based approach (ex. France), where the task of determining which assets or services are critical is left to individual CI operators; iii) an asset or hybrid based approach (ex. the UK), which employs elements of both the service-orientated and operator-orientated approaches (RECIPE 2011, p.23).

CASE STUDY 9
Methodologies for CI identification: the EU, France and the UK

EU

A four-step methodology to identify CI is set forth by EU Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. While technically the Directive is only concerned with the identification of European Critical Infrastructures (ECI) in the transport and energy sectors, it implicitly suggests that its methodology is applicable to the identification of national CI also in sectors other than energy and transport. Annex III outlines the relevant procedure as follows:

Step 1
Each Member State shall apply the sectoral criteria in order to make a first selection of critical infrastructures within a sector.

Step 2
Each Member State shall apply the definition of critical infrastructure pursuant to Article 2(a) to the potential ECI identified under step 1. The significance of the impact will be determined either by using national methods for identifying critical infrastructures or with reference to the cross-cutting criteria [see Step 4 below], at an appropriate national level. For infrastructure providing an essential service, the availability of alternatives, and the duration of disruption/recovery will be taken into account.

Step 3
Each Member State shall apply the transboundary element of the definition of ECI pursuant to Article 2(b) to the potential ECI that has passed the first two steps of this procedure. A potential ECI which does satisfy the definition will follow the next step of the procedure. For infrastructure providing an essential service, the availability of alternatives, and the duration of disruption/recovery will be taken into account.

Step 4
Each Member State shall apply the cross-cutting criteria to the remaining potential ECIs. The cross-cutting criteria shall take into account: the severity of impact; and, for infrastructure providing an essential service,

the availability of alternatives; and the duration of disruption/recovery. A potential ECI which does not satisfy the cross-cutting criteria will not be considered to be an ECI.
A potential ECI which has passed through this procedure shall only be communicated to the Member States which may be significantly affected by the potential ECI.

France

In France, the Government does not identify individual CI assets directly. Instead, it designates so called "vital operators" (OIV), who are in turn in charge of identifying individual assets. According to the Code of Defence, a "vital operator" (OIV) is identified by the minister in charge (the "Coordinating ministry") of a given sector of activity in consultation with other relevant ministries. The coordinating minister notifies the operator of his intention to designate it as an OIV. This step is also the occasion for an initial consultation between the Government and the operator. To be designated as OIV, operators must fulfil two conditions:

- their activity is carried out wholly or partly in a sector of activities 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 on the survival capacity of the Nation or the health or life of the population.

In general, the status as OIV can be acquired by:

- corporations;
- associations, foundation or international organizations;
- a State service, a local authority, a group of local authorities, a public establishment, an independent administrative authority.

In the case of a corporation, an OIV may be a parent company or a subsidiary. The choice ì is made after consultation with the relevant operator.

Several subsidiaries of the same group may potentially be designated. When the designation of an operator is done simultaneously by several ministers, a consultative process allows 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 OIV carries on its main activity.

As part of its normal activity, an OIV 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 OIV 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, OIV elaborate their "operator's security plans" (PSO). The risk analysis conducted during the elaboration of PSO 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" (PIV).

Source: France 2014

United Kingdom

The UK recognises nine critical sectors and twenty subordinate critical services. These services are in turn composed of assets, which need to be identified. The ministry responsible for a sector performs an initial selection of assets and operators (operators are picked on the basis of their relative market share). The Centre for Protection of National Infrastructure (CPNI) does its own assessment in parallel. Based on the combined input of operators, ministry responsible and CPNI, an asset (which can also be a process) is mapped against the consequences of a potential service failure. Six criticality levels (from CAT0 to CAT5) have been identified and are mapped against three specific cross-cutting criteria, namely: impact on life, economic impact, and impact on essential services.

At a public level, these criteria are descriptive and subjective only. At the classified level, each of eighteen possible criteria have quantitative and objective values (metrics) assigned to them. This segmentation is done in conjunction with sector-specific criteria which are unique to each of the nine critical sectors. The result is a very small set of assets at the highest criticality levels. Only assets at CAT3 and above are considered to be truly 'critical'. The combination of the CAT-level and the likelihood of attack, which is a combination of the vulnerability (e.g., ease of access to the asset) and threat (e.g., attack type and probability of the attack, or, for hazards, the likelihood of failure), identifies the asset priority. The scale of likelihood can be very dynamic and may change many times a year as far as security threats are concerned.

Source: RECIPE 2011, p.23

2.4.2 Critical Information Infrastructures (CIIs)

In modern economies, industrial production chains and the delivery of good and services by both Government and the private sector are to a great extent managed by computer-controlled systems known as Industrial Control Systems (ICS). Over the past few decades, ICS have progressively gained connectivity to the Internet and to private enterprise networks. This change has streamlined production and service delivery. Also, "networking industrial control systems on a greater scale has led to increased synergy and efficiency, and, due to utility deregulation, real time information is increasingly important for marketing purposes" (Shea 2003, p.3).

At the same time, the fact that ICS are increasingly linked to companies' computer systems via the Internet, has made them much more vulnerable to cyber-attacks. Specific security challenges are posed by legacy systems, i.e those ICS that were installed in the pre-Internet era and were not originally conceived for connectivity purposes.

Crucially, ICS are used in virtually all CI sectors as they often govern non-stop operations in power plants, dams, bridges, telecommunication towers, etc. ICS are thus key components of so called Critical Information Infrastructures (CIIs). Several national definitions exist of this concept. The OECD defines CIIs as "those interconnected information systems and networks, the disruption or destruction of which would have serious impact on the health, safety, security, or economic well-being of citizens, or on the effective functioning of government or the economy" (OECD 2008).

It is essential that CIP strategies recognize and provide protection to CIIs on an equal footing to physical infrastructures, all the more so since "we may be nearing the point where distinctions between

‘infrastructure’ and ‘information infrastructure’ are irrelevant, as the two merges into one ever-expanding circle of critical ‘stuff’. As the dependence on cyber-enabled infrastructure increases, so too does the proliferation of critical ‘nodes’ (i.e. points in a system where failure would significantly degrade the network) (Clemente 2013).
Crucially, in the identification of CIIs, cyber link needs to be taken into account. As a result, it might be necessary to include infrastructures that are not critical per se (for instance, a small power plant) to the extent that they are internally connected to critical infrastructure (for instance, a dam).

2.4.3 Interconnections and interdependencies

The delivery of essential goods and services to society is increasingly the outcome of the interplay among multiple providers. These providers cut across all CI sectors and sub-sectors, forming complex interlinkages. While the interconnectedness of assets, systems and processes is predicated on a more effective management of resources, it increases dependencies. These can 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”.[17] For example, food supply relies on transport, the banking/financial sector relies on telecommunications to authenticate transactions and telecommunications depends on the interrupted distribution of electricity. Most essential services depend on the simultaneous provision of services from multiple sectors. For instance, healthcare cannot be delivered in the absence of electricity, water and emergency services at the same time.

Dependencies can produce effects of varying intensity and be of different types. Notably, following a terrorist attack, CIs may suffer from:

- Physical dependencies: the functioning of one infrastructure depends on the supply of material outputs from another infrastructure;
- Cyber dependencies: the functioning of one infrastructure depends on information transmitted through an information infrastructure.

CASE STUDY 10

Interdependencies and France’s “vital zones”

The CIP strategy of France operationalizes the notion of dependencies by introducing the concept of “vital zone” (“zone d’importance vitale”, ZIV). A ZIV is an area in which several “vital points” (PIV) belonging to different “vital operators” (OIVs) are implanted, and for which a joint security assessment and management presents an 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

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

- security measures implemented for one PIV or on a common part affect the security of one or more other PIVs.

Three types of geographical areas exist:

- Case 1: an area consisting of neighboring PIVs. VIPs are contiguous or located at a relatively small distance from one another;
- Case 2: an area consisting of enclosed PIVs. A PIV "2" is found inside a PIV "1";
- Case 3: a zone combining the characteristics of the first two cases.

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

Source: France 2014

Crucially, dependencies increase levels of vulnerability. The threat is made more acute by the extensive reliance by Governmental agencies and the private sector on information and communication technologies, 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 cyber-attack on CIs in conjunction with a physical attack. This use of cyber-terrorism 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” (Shea 2003, p.9).

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 leading to failures in the healthcare 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 given 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 as non-static, but rather 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.

CASE STUDY 11

The Netherlands: inter-sectoral workshops and knowledge-sharing about dependencies

Under its CIP strategy, the Netherlands held a series of intersectoral workshops enabling CI sectors to gain insight into the effects of reciprocal dependencies. The involved stakeholders identified the technical and organisational 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 case of accident. The scenarios were notably used to discuss:

- Effects of CI disruptions, e.g. direct/indirect, supply chain, access/scarcity/integrity, time period of disruption, sector characteristic and human factors;
- Dependencies, redundancies and recovery;
- Measures to reduce vulnerabilities.

Source: RECIPE 2011, p.32

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.

2.5 Designing the CIP architecture

There is no single, pre-determined institutional model dictating how countries should protect their CIs. Governments are thus expected to choose the framework that best suits their characteristics in terms of faced threats, the size and structure of their economies and, more generally, their public policy culture and established institutional practices. Notably, CIP governance architectures should take into account the basic constitutional structure of the country, i.e. unitary/ centralized versus federal/ de-centralized States. This is especially important in assigning roles and responsibilities to the various levels of Government.

2.5.1 The 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 complimentary tool except in certain sectors (such as the nuclear sector) where it may take a predominant role.

At the other end of the spectrum lies the so called "mandated approach", based on the idea that cooperation is 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 standards within the set deadlines.

In practice, countries do not follow either approaches in their "pure" forms. Rather, they adopt elements of both. Their systems can only be defined as being predominantly "voluntary" or "mandated" in nature. Examples of the former are the US, the UK, Canada and Switzerland. Examples of the latter are France, Spain, Belgium and Estonia.

It may be difficult for countries to determine which model best fits their needs. Particularly when 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 US offers the example of a country that started with a pure concept of voluntary participation of CI operators in the process. While it is still based on this principle, overtime it has increasingly seen the need to strengthen its legal framework for CIP protection. A lesson here is that countries should learn from experience.

CIP institutional frameworks should, as a minimum, address the following aspects:

- Determine the Governmental agency that has the overall coordination role in the definition and implementation of the national CIP strategy;
- Assign sector-specific responsibilities, usually to individual ministries on the basis of established expertise and competence "ratione materiae" (e.g. food security to agriculture ministries, healthcare to health ministries, etc.);
- Determine the scope and modalities of the interaction between involved Governmental agencies and CI operators. Section 4.5.2 examines more closely the dynamics at stake from the point of view of public-private partnerships.

Table 4: CIP architectures in selected countries

Australia	In Australia's federal system, different governments have different direct responsibilities for CI depending upon infrastructure type or the nature of the threat. Intergovernmental work occurs on a cooperative basis. State and Territory governments are responsible for managing threats to life and property within their jurisdictions. They prepare for and respond to emergencies, and ensure law and order. They also often deliver services such as healthcare and the supply of water. All Australian state and territory governments have their own CI programs according to the operating environment and arrangements for each jurisdiction. The Strategy aims to complement these programs and support their objectives wherever possible. State and Territory governments are also key participants in the Trusted Information Sharing Network (TISN), the country's primary engagement mechanism for business-government information sharing and resilience building initiatives. The Australian Government is responsible for national defense and security, and for assisting States and Territories to respond to large scale emergencies when requested to do so. The Australian Government also has direct regulatory oversight of a number of critical infrastructure sectors, such as aviation, communications, offshore oil and gas and banking. In a number of cases, these regulatory agencies participate in the TISN (in a non-regulatory capacity) with the aim of contributing to the resilience of the relevant sector.
USA	The Secretary of Homeland Security provides strategic guidance and coordinates the overall federal effort. Sector-Specific Federal Agencies (SSAs) lead collaborative processes for CI security within each of the 16 CI sectors. Each SSA is responsible for developing and implementing a sector-specific plan (SSP) based on the unique characteristics of each sector. State, Local, Tribal, and Territorial (SLTT) 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.
United Kingdom	The Civil Contingencies Secretariat (CCS), 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 CCS are: - The 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 5 years); - The National Security Risk Assessment (identifying global risks to UK security interests, in a 5 to 20 year's timeframe). 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 their sectors and the key activities they 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.
Canada	The CIP architecture has a strong voluntary component. Responsibilities are shared by federal, provincial and territorial governments, local authorities, and critical infrastructure owners and operators. All these actors are represented in national sector networks (for each of the ten identified critical infrastructure sectors) whose goals are to: - promote timely information sharing; - identify issues of national, regional or sectoral concern; - use subject-matter expertise from critical infrastructure sectors to provide guidance on current and future challenges; and - develop tools and best practices for strengthening the resiliency of critical infrastructure 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 Defense and National Security (SDGSN) on behalf of the Prime Minister. SDGSN approves the National Security Directives (DNS) drafted by the coordinating ministries in each critical sector. Those ministries are also the points of contact of the operators. Zone and department prefects (i.e. 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: the appointment of a delegate for defense and security (privileged interlocutor with the administrative authority), the drafting of an Operator's Safety Plan (PSO), which sets out the operator's safety policy and the drafting of a Specific Protection Plans (PPP) for each of the "vital points" (PIV) identified. The task to control whether security levels at PIVs are consistent with the minimum requirements expected at the site is entrusted to CIDS and CZDS supported by the departmental prefects. Control reports aim to highlight vulnerabilities vis-à-vis identified threats and recommend measures to be taken to strengthen resilience. In extreme cases of non-compliance, the control policy may lead to referral to the judicial authority for prosecution and the application of criminal sanctions. in case of violation of the regulations.
Spain	The Secretary of State for Security, through the National Center for the Protection of CI, is the highest body of the Ministry of the Interior responsible for the CIP system. For each strategic sector, at least one entity of the General State Administration is designated with responsibilities to promote, within their 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 "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 actors within specific deadlines. In particular:

	a) National Plan for CI Protection: establishes criteria and guidelines to mobilize the operational capacities of public administrations in coordination with the operators; b) Sectoral Strategic Plans: 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. c) Operator's Security Plans: define 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 Interior; d) Specific Protection Plans: determine the concrete measures already adopted and those to be adopted by the operators to ensure the security (physical and logical) of their Cis; they must be submitted within four months of the approval of the Operator's Security Plan by the Ministry of Interior; e) Operational Support Plans: set forth the concrete measures to be implemented by the Public Administrations in support of critical operators.
Netherlands	Primary responsibility for the continuity and resilience of critical processes is borne by their actual operators. This includes gaining an insight into threats, vulnerabilities and risks, and developing and maintaining capacities that increase and safeguard the resilience of critical processes. The responsible ministry establishes general frameworks for the sectors that fall under its responsibility (in policy or in laws and regulations). The ministries, in association with the operators of critical processes, are responsible for safeguarding and inspecting capabilities related to CI. Safety and Security Regions provide support to operators of critical processes in the event of (imminent) disruption or failure if the capabilities are inadequate and public order and safety are endangered. This takes place in coordination with the operators of critical processes and ministries. The fact that there are many, diverse stakeholders necessitates coordination and management. The National Coordinator for Security and Counterterrorism (NCTV) of the Ministry of Justice and Security is responsible for overall coordination and management tasks.
Germany	The country's CIP architecture is based on the identification of 6 work packages corresponding to different phases of the risk management cycle. The public sector (under the coordination of the Federal Ministry of Interior) takes the lead on the implementation of the first 4 packages with the collaboration of the private sector/operators. Instead, 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: 1. definition of general protection targets; 2. analysis of threats, vulnerabilities, and management capabilities; 3. assessment of the threats involved; 4. 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.

	5. Implementation of goal attainment measures primarily by means of: i) association-specific solutions and internal regulations; ii) self-commitment agreements by business and industry; iii) development of protection concepts by companies. 6. 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. These security partnership platforms may be organized as: - Round Tables on CIP (Federal level); - Round Tables on CIP (Länder); - Round Tables on CIP (local government level); - Joint round tables Federation/Länder or Länder/local authorities.

2.5.2 Public-private partnerships for CIP

In most countries, the vast majority of CI assets are privately owned. Additionally, private operators are at the fore-front of investments and efforts to develop new production and protection technologies. These circumstances, combined with the fact that the main responsibility for protecting CI assets/systems lies with their owners/operators, highlight the importance of establishing effective public-private partnership (PPPs) in order to achieve adequate levels of resilience.

In dealing with PPPs, drafters of CIP strategies should aim at creating the conditions for their effectiveness by: i) appreciating success and constraint factors; ii) defining their scope; iii) defining their forms; iv) anticipating problems and challenges.

i) Appreciate success and constraint factors of PPPs

The Meridian Process, an open forum for the exchange of ideas on CIP and collaboration among senior government policymakers, has identified the following factors as underpinning effective PPPs GFCE-Meridian 2016, p.55):

Trust: as PPP often concern touchy subjects (commercially, in terms of reputation, security wise, shifting responsibilities), it is essential to create an atmosphere of trust in which all organizations show awareness of each other's need for discretion and consistently act accordingly. Clear membership guidelines of operating rules may support the building of trust;

Value: participation in a PPP must produce benefits otherwise the enthusiasm to participate will quickly fade;

Respect: all organizations have to recognize and respect the added value the other organizations bring to the collaboration. This can be reached by 'selling' your own added value (in your partner's terminology) while actively looking for the added value of your partners;

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 each other's possibilities and restrictions: this prevents conflict through misjudgment of the cause of a negative response and allows for an optimum return on the efforts of the alliance. This implies that both organizations should know each other's business. A good way to attain this is to have worked together for a long period of time, preferably years;

Realistic expectations: all organizations have to take into consideration affordability of resources, development budget, etc., to be able to form realistic expectations of the PPP.

ii) Define the scope of PPPs

PPPs should not focus on one particular stage of the CIP cycle, but encompass all of them, from measure design and implementation to the risk and crisis management phases. 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, etc.

Information-sharing is a crucial (albeit not the exclusive) dimension of PPPs and raises specific challenges such as in the field of data protection. Issues related to information-sharing are examined in Chapter 4.

iii) Determine the forms of PPPs:

The most appropriate form of a given partnership 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 governmental agencies aim to exercise. From a different angle, it has been argued that "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 (Kolesnikova 2017, p.13.15).

CASE STUDY 12
Public Private Partnerships for Critical Infrastructures Resilience in Finland

The National Emergency Supply Agency (NESA), created in 1993, is tasked with planning, developing and maintaining the security of supply in Finland. While its historic role of maintaining reserve stockpiles to protect the livelihoods of the population as well as the functioning of the economy remains part of its strategic tasks, NESA is more and more active in mainstreaming business continuity and resilience in various sectors of the economy through public-private partnerships. NESA has established a network of thematic clusters where key stakeholders of critical sectors develop partnerships in order to assess vulnerability and performance and plan for resilience. NESA also proposes dedicated tools, such as information systems, storage and transport facilities to support business continuity on these domains. NESA also finances specific activities related to business continuity and critical infrastructure protection. The agency prepares annual reports that evaluate the performance of companies in the critical sectors including ranking and specific recommendations. Among its results, NESA boasts increased public-private partnerships with companies in critical sectors (now more than 1000) which all yielded a business continuity plan specific to their activities and sector.

Source: OECD Toolkit for Risk Governance, at: www.oecd.org/governance/toolkit-on-risk-governance/home/

iv) Anticipate challenges of PPPs

PPPs that are not accurately thought through are exposed to the risk of becoming "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 endeavors, it is necessary for countries to bear in mind the most recurrent reasons for failure. Shortfalls can be rooted in expectation gaps between the private and the public sector, unsustainable funding models, unclear divisions of labor, etc. Arguably, "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" (Kolesnikova 2017, p.13-15).

Other challenges may be associated with lack of motivation for business to invest financial resources on the protection of their own CIs. Section 2.10.1 discusses the need for CIP strategies to identify the appropriate types of incentives in this regard.

The OSCE has elaborated basic 8-step guidance on how countries should maximize the benefits that can be obtained by PPPs 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 (OSCE 2013, p.69):

- Step 1: Analyze 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. And provide mechanisms for voluntary efforts, including the development and exchange of best practices, consultation, and dialogue to ensure ongoing and effective partnering;
- Step 5: Set up an institutional structure that fosters cross-organizational co-operation and information exchange; clarify the roles and contributions of each partner (e.g., government agencies, owners and operators of critical infrastructure, product suppliers, associations); identify single points of contact for each partner; establish guidelines for co-operation;
- Step 6: Start small by focusing on one or two critical infrastructure sectors; grow steadily while building on the readiness of all stakeholders to co-operate 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.

CASE STUDY 13

UP Kritis: Germany's platform for CIP public/private partnership

Institutionalized in 2007 and adjusted in 2013, UP KRITIS is Germany's public/private platform for CIP for sectoral and cross-sectoral cooperation. Mutual trust underpins its work. Participants exchange know how and experiences and learn from each other with respect 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 pro-active engagement, the goal being to ensure the system remains manageable while reaching out to as many companies as possible from all CI sectors. In particular, an organisation 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 a participant of

UP KRITIS. Participants appoint representatives for their organisation, who are granted access to the products of the UP KRITIS, including confidential information. If an organisation wishes to collaborate more actively, it can become a "partner" and apply for the integration of their 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 UP KRITIS's strategic key activities, deciding on the establishment or dissolution of working groups, planning future joint action, etc. The Plenum consists of representatives of the CI operators, their professional and sectoral associations as well as representatives from the public sector. The Council strengthens the 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 the private sector. The council consists of high-ranking decision-makers of the CI operators and of the public sector.

Source: UP KRITIS 2014

2.5.3 The role of civil society and the public

The public at large has an important role to play in both preventing attacks against CIs and in reducing damage once an attack has occurred (crisis management). Some countries explicitly and actively envisage individuals' roles into CIP strategies. For example, France's Plan Vigipirate[18] instructs citizens how to behave in case of attacks in specific contexts which are relevant for the protection of CI, such as in metros, trains, airplanes and ships, or in case 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" (Lindberg & Sundelius 2013, p.1304).

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 programs and awareness-raising campaigns. Communication strategies should be different depending on 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 messages in loud-speakers reminding users of public transport about reporting duties, etc. Following waves of terrorist attacks in the transportation system 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.

[18] http://www.gouvernement.fr/vigipirate

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

CASE STUDY 14

France' s Peoples' Alert and information System (SAIP)

Developed by the Directorate General for Civil Security and Crisis Management (DGSCGC) of the Ministry of the Interior, in collaboration with the Government's Information Service (GIS), SAIP allows citizens to be alerted, via notification on smartphone, in case of suspicion of an attack or exceptional event likely to result from an attack.

Safety instructions sent through SAIP direct users to take specific actions such as find shelter in a building or evacuate a danger zone, avoid calling (except medical emergency), do not pick up children at school, etc. The decision as to whether to send a message and related content is reserved to an authority in charge of the general protection of the population, public order and civil defense. Locally, this competence is held by the mayor and the prefect of the department. This application complements the existing system for alerting and informing the population (SAIP) and is part of a global approach to raise the population's awareness of the risks involved.

Source: www.gouvernement.fr/risques/l-application-d-alerte-mobile-saip

2.6 Building CIP strategies around risk and crisis management concepts

An effective national strategy should place risk management and crisis management processes at the heart of CIP efforts. Whatever institutional model is chosen, stakeholders involved in CIP (whether private-sector CI owners/ operators or public authorities) need to be familiar with these concepts and consistently apply them within their respective sector and fields of competence.

2.6.1 Risk management

The United Nations Office for Disaster Risk Reduction (UNISDR) 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" (UNISDR 2009).

In the context of risk management processes as applied to CIP, it is important to have a clear understanding of key concepts that are often (and mistakenly) used interchangeably, notably:

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

There is no unique or universal standard for running risk management. Use of different "terms of reference" by the various stakeholders in charge of this task may lead to incompatible results. At the country-level, employment of different method 15ologies may make it more difficult, if not impossible, to compare findings within and across sectors, thus potentially affecting the reliability of the exercise as a whole. It is therefore important for countries to support the establishment of risk management processes covering, as a minimum, the following elements:

- Establishing the context – scope and parameters for the risk assessment;
- Risk Assessment (Identify, Analyze, Evaluate) – transforming the risk data into decision-making information;
- Risk Mitigation- translation of risk information into decisions and mitigation actions;
- Throughout the entire process:
- Communication and consultation- identifying the communication methods used among all stakeholders involved throughout the process; and
- Monitor and Review – conducting the regular checking or oversight to improve risk management, detect changes to the context of existing risks, and to identify new risks.

In order to ensure the identification of appropriate preventive security measures, the risk management system should detail the mechanisms for obtaining valid threat information and conducting risk assessments, taking into account international, national and regional situations and environments. Security measures and procedures should be flexible and commensurate with the risk assessment which may fluctuate given various changing factors. This system should be implemented in a timely and efficient manner to ensure the resultant risk assessment is always up-to-date, accurate and complete.

At the international level, ISO has established a universally recognized paradigm in the field by issuing ISO Standard 31000. This refers to a family of standards that ISO defines as a "set of components that provide the foundations and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organization." [19] Crucially, ISO 31000 are not specific to any industry or sector.

[19] ISO 31000:2009(en), at: www.iso.org/obp/ui/#iso:std:iso:31000:ed-1:v1:en
Adopting the same risk management approach as ISO 31000, ISO 27000 series provides the reference standard in the field of information security systems. ISO 27000 thus offers a useful guiding framework for the protection of Critical Informational Infrastructures CIIs.

CASE STUDY 15
ICAO's aviation security risk assessment methodology

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

- identification and analysis of plausible threat scenarios and their likelihoods, and consequences;
- assessment of current mitigations and remaining vulnerabilities;
- residual risk assessment taking into account the likelihood, consequences, and vulnerabilities of a specific threat scenario; and
- recommendations for further risk-based work and possible mitigation.

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

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, and/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 it is normally assumed are being effectively applied, where that is clearly not the case, the risk will be higher) or other relevant national and/or local programs and regulations, in reducing the likelihood of the attack being successful and/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; and

Possible additional mitigation: identified measures that Member States or ICAO could implement to further mitigate residual risks where necessary.

It is important that the risk assessment identifies the plausible scenarios carefully and in sufficient detail, being 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, as well as 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 (e.g. whether person- or vehicle-borne) and by whom (e.g. 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. However, this does not cover the full list of possible scenarios and states or other entities conducting risk assessments are encouraged to develop their own versions reflecting local circumstances as appropriate.

Some countries, notably the US and Canada, have set up public programs to specifically encourage CI operators to adopt a common assessment framework. These programs are also designed to provide technical assistance in carrying out the assessments following a "soft approach" based on incentives and voluntary-based plans.

CASE STUDY 16

Canada's Regional Resilience Assessment Program (RRAP)

RRAP is a comprehensive risk assessment program for owners and operators of Canadian Critical Infrastructure (CI). This program features site assessments to help organizations measure and improve their resilience to all hazards in Canada, such as cyber threats, accidental or intentional man-made events, and natural catastrophes. These site assessments are voluntary, non-regulatory, free-of-charge and confidential.

- To enhance critical infrastructure resilience, the RRAP uses three main tools:
- Critical Infrastructure Resilience Tool (CIRT): an on-site, survey-based tool that measures the resilience and protective measures of a facility;
- Critical Infrastructure Multimedia Tool (CIMT): a multiplatform software tool that generates an interactive visual guide of a critical infrastructure facility, featuring spherical photography;
- Canadian Cyber Resilience Review (CCRR): an on-site, survey-based tool that measures the cybersecurity posture of an organization.

The program may include workshops, meetings, geospatial products and subject matter expert interviews. The results from the RRAP's assessments are intended to help owners and operators to identify dependencies and vulnerabilities within their organization. The site assessments also identify a series of optional cost-effective measures to help owners and operators mitigate risks and improve their ability to respond to and recover from disruptions. Specifically, the RRAP provide for:

- Better risk management – Increases an organization's understanding of its vulnerabilities, based on the use of trusted assessment tools.
- Strengthened government relationships – Enhances relationships with multiple government departments, including first responders.
- Improved cyber security awareness – Better understand how well an organization is prepared for cyber-attacks and other cyber threats.

Other key considerations for critical infrastructure owners and operators:

- Minimal investment of time and resources – RRAP service is quick and is offered at no cost.
- Security – Public Safety Canada will protect the confidentiality of documents and information provided in confidence by owners and operators of critical infrastructure to the Department

Source: Public Safety Canada, at: www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/crtcl-nfrstrtr-rrap-en.aspx.

2.6.2 Crisis management

Crisis management identifies the processes that need to be activated when threats do materialize. Crisis management steps include:

- identifying a crisis;
- planning appropriate responses to the crisis;
- confronting and resolving the crisis.

When dealing with the terminology related to crisis management, countries sometimes refer to "contingency plans" and "emergency plans" as synonymous. 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 to normal service as quickly as possible.

A single entity, designated by the State, should be assigned primary responsibility and authority to determine the course of action to be taken when crisis occurs. This entity should coordinate all actions with all entities involved and affected. As part of the crisis management plan, an effective emergency response plan should be developed, including assuring the interoperability of communication systems and adequate response times, as well as evacuation plans to limit the impact. Emergency team response should be planned, tested and evaluated in advance to mitigate the effects of an attack.

2.7 Mapping threats, consequences and vulnerabilities

In articulating their CIP strategies around a risk management approach, countries should consider a number of guiding principles. These principles are fleshed out below.

2.7.1 A multi-level exercise

The determination of the nature and levels of threats to CIs and related vulnerabilities is necessarily the joint and harmonized product of assessments carried out at different levels. Like the lenses of a zoom that can capture the broad picture and move on to capture the smallest detail on the ground, a CIP strategy should be in a position to integrate multiple-level threat, consequence and vulnerability assessments. Schematically, these levels are: i) the national level; ii) the sector level; iii) the infrastructure/ company level.

i) National-level assessments

The objective of a national risk assessment is to reach an overview of the threat that a country's CIs face as a whole, its vulnerabilities, and the consequences of a successful attack. An important contribution of nation-wide assessments is that they highlight how multiple sectors interact with each other. In the development of this type of documents, the intelligence-based findings that supported the drafting of national security and counter terrorism strategies may offer relevant guidance and insights.

CASE STUDY 17
Sweden's National Risk Assessment

According to domestic law, all Governmental entities are under the obligation to elaborate and submit a risk and vulnerability analysis to the national Civil Contingencies Agency (MSB). Based on such reports, since 2011 MSB has been producing National Risk Assessments. These documents (the latest of which was issued in 2016) aim to provide strategic groundwork for the direction and further development of civil contingencies.

The 2016 Assessment identifies five development areas that MSB finds particularly important to address in order to strengthen disaster preparedness (and thus directly relevant for CIP):

- Efforts in the areas of disaster preparedness and civil defence needs to become a higher priority by the responsible stakeholders in Sweden;
- Knowledge and awareness regarding roles and responsibilities related to disaster preparedness need to be raised, especially when it comes to responsibilities for geographical areas;
- The risk and vulnerability analyses carried out at local, regional and national level require improvements in order to be used as a planning basis for disaster preparedness and civil defence;

- Scenarios provided by MSB could be a supportive tool for the planning and development of disaster preparedness;
- More explicit demands for protective measures need to be established for critical infrastructures.

MSB stresses the need to further develop capabilities in the following areas:

- The capability to respond to interruptions in the supply of electricity;
- The capability to prevent and respond to interruptions in the supply of drinking water;
- The area of information and cybersecurity;
- The capability to prevent and respond to interruptions in the supply of medicines;
- The capability to prevent and respond to radiological and nuclear events.

Source: Sweden 2016

ii) Sector-level assessments

It is critical to develop risk profiles for specific CI sectors. These profiles crucially include an assessment of existing mitigation practices, consequences and vulnerabilities. Depending on the sector under consideration, risk assessments may be undertaken for specific sub-sectors and subsequently be fed back into broader sector risk profiles. For example, Australia's Critical Infrastructure Resilience Strategy breaks down the transport sector into the following sub-sectors: 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.

iii) Infrastructure-level assessments

CI operators are often those that know best how their infrastructures function in terms of systems and processes. Consequently, they have specific insight into their intrinsic vulnerabilities. Additionally, companies often run risk management cycles independently of the institutional role 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 limit 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 can be of direct benefit to companies' infrastructures and increase their resilience. Countries 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.

2.7.2 A 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 Governmental agencies, emergency services and private-sector entities. While normally Governmental agencies take the lead in elaborating national and sector-specific threat assessments and CI operators take the lead for CI-specific plans, the input and involvement of all stakeholders is in all cases 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 to achieve acceptance. This is a key pre-requisite considering that multiple actors have responsibilities for implementing CIP strategies.

The inclusiveness of the process also allows for consideration of risks from multiple angles. Joint understanding is gained on the interplay between different infrastructures and sectors. Ensuring the broad participatory nature of the process and its overall coherence, however, comes with challenges. A general one is that different stakeholders perceive risks in different manners. As has been observed, "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" (NIPP 2013, p15).

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" (NIPP 2013, p.15).

2.7.3 Mapping terrorist threats against CIs

In comparison with threat assessments against other hazards, the identification and evaluation of terrorist threats on CIs raises specific issues. Part of the 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 behavior to changes in the security landscape" (CTED 2017). From this perspective, the terrorist threat should be regarded as a dynamic one, adjusting for example to changes in resources available to a terrorist group and to changes in the security features of a potential target.

In terms of sources from which to draw elements for terrorism-related threat assessments, CIP strategies should recognize the mainstream role of the intelligence community. Intelligence agencies are in charge of protecting national security. In the execution of their missions, they often handle confidential information as means to protect sources and methods, in order not to alert targets of ongoing surveillance activities, etc. Consequently, CIP strategies need to have mechanisms in place to deal with information whose circulation is restricted. As Section 4.2 shows, a major challenge is to ensure that as much information as possible is shared among all stakeholders while protecting its confidential nature. This can be both sensitive business information held by companies or classified information held by State agencies.

CASE STUDY 18

Australia's intelligence-led approach to the protection of CIs against terrorist attacks

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/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.

In particular, ASIO's 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/ 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 will contact State and Territory police and other relevant organisations, including owners/ 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 one CI facility.

Source: Australia-New Zealand 2015

CIP strategies should also recognize that terrorism related threat assessments against CIs are predicated on the ability to handle multiple sets of indicators as well as to contextualize available information. Changes in geopolitical realities, economic situations, power dynamics between criminal organizations, etc., should all be weighted in and encourage the repetition of the exercise at regular intervals of time.

One useful indicator is provided by evidence of previous attacks or threats against CIs, especially when these have taken place repeatedly over time or have consistently targeted certain sectors or CI in specific regions. Assessments could also benefit from data available from other countries, particularly when analogies can be drawn. By way of example, if a terrorist group has already attacked nuclear facilities in Country X and Country Y is allied with Country X, one could infer a higher level of threat to nuclear facilities in Country Y.

CASE STUDY 19

Germany's analysis of cyber-security threats

As part of its cybersecurity analyzes, the German Federal Office for Information Security (BSI) has drawn up a list of the most critical threats currently facing Industrial Control Systems (ICS). Threats are ranked by considering factors such as perpetrator groups, the distribution and ease of exploiting vulnerabilities, and the possible technical and economic consequences of an attack. To gain the information, databases of actual occurrences are analyzed.

Source: OSCE 2013, p.35.

Radars should also be able 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 a CI is structured, or attempts to carry out close surveillance activities of certain places. At the same time, inferences are often impossible to make based on single and sporadic acts. Here again, 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 indicators and sources, they should be constructed in such a way as to empower (or mandate, depending on chosen CIP governance models) relevant authorities to shape risk assessment processes to the specifically fluid and volatile nature of the terrorist threat.

2.8 Minimizing the vulnerability of CIs to terrorist attacks

The previous sections have highlighted the importance of a comprehensive risk management process and carrying out risk assessment at different levels as a condition to minimize the vulnerability of CIs to terrorist attacks. Risk management should eventually translate into concrete preventive plans and measures. This section considers the place of preventive measures in the context of CIP strategies from the physical, personnel and cyber protection angles.

In considering such measures, countries are always encouraged to explore the extent of their potential impact on the exercise of human rights (e.g. impact on the freedom of movement created by site security restrictions, interferences in private privacy caused by video surveillance technologies, etc.). In all such cases, the goal of protecting CIs 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 so doing, only measures that are deemed necessary to achieve CIP should be retained. Planned measure should also be evaluated in terms of their proportionality to the sought objectives.

2.8.1 Prevention

Preventing terrorist attacks on CIs is part of the nation-wide 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, the law enforcement community at large, etc. The extent to which criminal laws take a preventive approach as well as the ability of investigative agencies to be proactive (as opposed to simply react to the commission of terrorist acts) play a fundamental role in preventive efforts. CIP strategies should build upon existing frameworks by concentrating on those policies and measures that are directly relevant to step up the prevention of terrorist attacks which specifically target CIs. They can, in particular:

- Identify the main roles and responsibilities in the prevention field, including at the level of CI operators (i.e. the overall role of top-level managers, of security officers and, more generally, establish the concept that the implementation of preventive measures is a task for the entire company and requires support from all levels);
- Outline the working playground and methodologies for developing manuals and practical guidelines for use by CI operators in the field of prevention;
- Directly identify methods and approaches that should be broadly applied or considered by stakeholders. For instance, countries increasingly promote "security-by-design" as a tool for achieving preventive objectives. Another example is the requirement for CI owners/operators to maintain effective security arrangements to maximize the likelihood that terrorist preparatory activity, such as *site reconnaissance*, is identified quickly. As part of its CIP strategy, for example, the Government of Australia requires that any such suspicious activity should be reported to the police and has established a dedicated National Security Hotline;
- Encourage or mandate (depending on the chosen governance model) the adoption of specific sets of preventive measures by CI operators, either cross-sectoral or in specific sectors.

CASE STUDY 20
Security by design

An increasing number of countries incorporate security-by-design concepts into their strategies to increase the resilience of CI against terrorist attacks and other hazards. Security-by-design aims to achieve prevention from a durable and long-term perspective. According to the UK's Centre for the Protection of National

Infrastructure, "considering the physical security requirements at the outset, as part of the building or facility design, will often result in more effective and lower cost security. For new builds, high level security requirements should be incorporated into the original brief. Physical security requirements should also be considered during the construction phase of new builds or the modification of existing facilities, as these are likely to be subject to different risks and issues. Consideration should be given to:

- Identification and assessment of existing and new security risks
- Identification of security requirements for both the construction works and any changes to the security of the facility itself (this will depend on whether the construction works are adjacent to or within the facility)
- Determination of the transition of the security measures from 'construction phase' into normal operations.

The security-by-design concept can be applied not only to physical assets, but also to CII. Singapore's 2016 Cyber Security Strategy specifically sets the objective of pre-empting cyber vulnerabilities "by going upstream and promoting Security-by-Design practices. Cybersecurity will no longer be an afterthought but will be consciously implemented throughout the lifecycle of technology systems. Accordingly, the Government has committed to take the following steps:

- Progressively institutionalize Security-by-Design into the governance framework for CII protection;
- Promote the practice of penetration testing to discover vulnerabilities early for remediation at the design stage;
- Build a strong community of practice in product and system testing based on established international standards, such as the Common Criteria product assurance certification;
- Continue to refine methodologies and develop new security validation tools to improve the efficacy of Security-by-Design.

2.8.2 Processes, physical security (including technology), personnel security and cyber protection measures

CIP strategies and related implementing actions should be predicated on the idea that effective protection measures at the CI-level requires the integration of physical, personnel and cyber-security elements. Table [number] references a selection of practically oriented tools elaborated by a number of Governments with the objective of providing guidance to CI operators. While these tools have a national focus, most guidance contained therein is applicable across borders and may be a source of inspiration to authorities and CI operators from other countries.

i) Processes

CIP strategies should reflect the regulatory requirements for preventive security measures in relation to CIs and should focus on establishing performance targets to be achieved, with preventive measures, rather than describing specific procedures or measures. A comprehensive organization and legal structure, with clearly defined responsibilities and methods of implementation, should be established. Strategies should include the policy underpinning regulations, practices and procedures applying to “normal” operating conditions, and additional measures required in the event of an increase in the threat level.

ii) Physical security measures (including technology)

This is effectively achieved through the implementation of the so called “defense-in-depth” concept whereby protection requires the multi-layering of different measures. The underlying principle is that the security of an infrastructure is not significantly impaired by the loss of any single layer.

In order to detect any unauthorized access and allow for the apprehension of any intruders before they can reach essential facilities, a multi-layered approach may include the following:

- delineation of CI area perimeters and protection by physical barriers;
- patrols and sufficient surveillance;
- access control with additional 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 methods and/or techniques (e.g. explosive detection dogs, manual searches, hand-held metal detectors, explosives trace detection and mobile screening units.

Physical security measures should be supported by properly trained personnel, sound and comprehensive contingency planning, and concise, well written security plans and orders.

CASE STUDY 21
The UK National Centre on the Protection of National Infrastructure

The Centre lists the following as examples of physical security measures:

- Measures to assist in the detection of threat weapons, including for example explosives, knives, firearms, chemical/ biological/radiological material, etc.;
- Measures to assist in the detection, tracking and monitoring of intruders and other threats, such as unmanned aerial vehicles;
- Access control and locking systems;
- Physical and active barriers to deny or delay the progress of adversaries;
- Measures to protect people or assets from the effect of blast or ballistic attack;
- Measures to protect against or limit the spread of chemical, biological or radiological material;
- Measures to protect sensitive (e.g. classified) material or assets.

Source: National Centre on the Protection of National Infrastructure, at: www.cpni.gov.uk

iii) Personnel security:

Personnel security refers to the policies and procedures needed to reduce the risk associated with insider threats (e.g. a company's employees) exploiting their legitimate access to an infrastructure's premises, systems or processes in order to carry out unauthorized/ malicious acts. Effective personnel security involves a variety of measures ranging from background checks, selection procedures, security awareness training promoting vigilance and a general culture of security, training of staff, perimeter security and access controls systems, surveillance, and quality control.

Table 5: Practical tools for CI operators

Title/ Topic and Country	Description
Protection of Critical Infrastructures – Baseline Protection Concept, Recommendation for Companies Germany, Federal Ministry of the Interior	This tool has been elaborated by the Federal Ministry of the Interior, 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. https://www.preventionweb.net/files/9266_2967ProtectionofCriticalInfrastruct.pdf
Personnel & People Security Physical Security United Kingdom, Centre on the Protection of National Infrastructure (CPNI)	CPNI's advice, toolkits and guides deal with the following topics and sub-topics: Personnel & People Security (Reducing Insider Risk; Optimising People in Security; Disrupting Hostile Reconnaissance) Physical Security (Threat Specific Mitigation Search & Screening; Physical Defences; Access Control and Locks; Intruder Detection & Monitoring; Active Access Delay; Building Structures; Windows & Facades; Doors; Building Services & Spaces; Control Rooms; Sensitive Information & Assets) https://www.cpni.gov.uk/advice
Cyber strategy IT infrastructure End user device Operational technology	Available guidance is organized by topic under the following categories and sub-categories:

United Kingdom, National Cyber Security Centre (NCSC) www.ncsc.gov.uk/guidance	Cyber strategy (Flexible working - Incident management - Operational security - Personnel security -Physical security - Risk management - Skills and training - Sociotechnical security) IT infrastructure (Cryptography - Data in transit - Design and configuration - Destruction and disposal -Malware protection - Monitoring -Network security - Secure storage - End user technology – BYOD) End user device (Identity and passwords - Secure communications - Digital services - Citizen services - Cloud security - SaaS offerings - Transaction monitoring) Operational technology (Cyber threats - Cyber-attacks - Vulnerabilities)
Critical Infrastructure Protection and Resilience Toolkit USA, Department of Homeland Security	The toolkit is intended to be a starting point for small and medium sized businesses to integrate infrastructure protection and resilience into preparedness, risk management, business continuity, emergency management, security, and other related disciplines. For more information: IP_Education@hq.dhs.gov.

iv) Cyber security

Cyber security measures represent the third group of measures for the development of which CIP strategies need to set an adequate framework. This encompasses a set of measures designed to protect CIs against cyber-attacks. Not only technological in nature, they help to preserve integrity, resilience and normal functioning of CIs. They may, for example, include security procedures, policies, organizational measures, awareness and training, specific development guidelines and processes or regular security assessments.

CASE STUDY 22

Sweden's Guide to increased security in industrial information and control systems

Sweden's Civil Contingency Agency, has elaborated 17 basic recommendations on the basis of internationally recognized guidance, practices and working methods. Some recommendations are technical in nature and others focus on methodology.

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, standardisation bodies and other networks for security in industrial information and control systems.

The full text of the Guide (https://www.msb.se/RibData/Filer/pdf/27473.pdf) provides explanations about each recommendation, the text of sub-recommendations and examples of risks and problems that might encountered.

Source: Sweden 2014

2.9 Respond to and recover from a terrorist attack against CIs

Section 2.6 has introduced the concept of "crisis management" in relation to CIs. In the counter-terrorism context, "response" refers 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 place of the incident suggest that in some cases recovery may be understood as a process requiring integrated and sustained collaboration among governmental agencies, the private sector and civil society organizations.

CIP strategies need to consider how existing crisis management structures should be integrated within their remit and what changes to the general system(s) in place, if any, should be made to better fit crisis specifically affecting CIs. Clear human-rights compatible legal and operational frameworks must be established, noting that crisis management is important not only in case of particularly disruptive terrorist attacks, but also minor incidents to avoid or reduce the impact of crisis escalation.

The identification of an appropriate crisis management framework requires consideration of two basic issues. The first one is whether emergency management will follow an all-hazard or hazard-specific approach. New Zealand offers an example of the latter (see case study below). 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. However, choosing a hazard-specific approach may 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.

The second issue to address is whether the scope of CI crisis management structures and procedures should be sector-specific or cross-sectoral. 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. Instead, the cross-sectoral approach often sees general legislation adopted.

CI sector-specific normative frameworks are often found in the telecommunication sector. In the Netherlands, for example, the National Continuity Forum Telecommunications (NCO-T) aims to ensure that an operator be able to run critical telecommunications services during a situation of Exceptional Circumstances. Participants of NCO-T are the designated operators and the Directorate-General Energy, Telecommunications and Markets of the Ministry of Economic Affairs. In France, the PIRANET plan is triggered by the Prime Minister in the specific event of a major ICT crisis.

Other CI sectors may establish equivalent arrangements based on legal frameworks adopted by sector-specific regulators. Following the 9/11 attacks, for example, "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" (Sinai 2016).

An example of cross-sectoral normative frameworks is Estonia's Crisis Act, whose chapter IV 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 as well as CI operators to guarantee the continued delivery of 41 critical services.

CASE STUDY 23

New Zealand's crisis management governance structure

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 they need to be managed.

Risk Characteristics

- Unusual features of scale, nature, intensity, or possible consequences;
- Challenges for sovereignty, or nation-wide law and order;
- Multiple or interrelated problems, which when taken together, constitute a national or systemic risk;
- A high degree of uncertainty or complexity such that only 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 over who has the lead in managing a risk, or there are conflicting views on solutions;
- The initial response is inappropriate or insufficient from a national perspective;
- There are cross-agency implications;
- There is an opportunity for 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

They 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 actions on behalf of their organisation. The exact composition of Watch Groups depends on the nature of the event and includes agencies with a role to play in responding to the issue at hand. Sometimes this might include agencies which do not usually think of themselves as "national security" agencies and do not have a lot of experience in operating within the National Security System structures.

Officials Committee for Domestic and External Security Coordination (ODESC)

Provides strategic direction, supports the lead agency and links to the political level including advising the Cabinet National Security Committee.

Working or Specialist Groups
They form 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: Government Legal Network, Economic Advisory Group, Science Network and Intelligence Community).

National Crisis Management Centre
Provides a secure, centralized facility for various coordinating tasks such as directing response operations, planning and support; Information gathering, management and sharing; 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 challenge 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 provide a fresh perspective on the approach being used to manage the threat.

Source: Department of the Prime Minister and Cabinet, New Zealand, at: www.dpmc.govt.nz/our-programmes/national-security-and-intelligence/national-security

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. The basic prerequisites for achieving fluid and rapid decision-making are examined in Chapter 5 (Ensuring coordination among domestic agencies). The same chapter also discusses joint public-private exercises as key tools in crisis management.

Another consideration is that in the event of an attack to a chemical, biological, radiological or nuclear facility, a specialized response would be required to protect the public and first responders from contamination and mitigate potential release of dangerous materials. A specialized response would entail specific emergency and contingency planning as well as specialized equipment for detection, personal protection and decontamination.

2.10 Ensuring strategies' relevance and sustainability

CIP strategies should lay the ground for their practical implementation by: i) ensuring the financial viability of the overall CIP effort; ii) setting up reviewing and monitoring mechanisms as a part of risk management processes for existing lists of CI and the strategies themselves.

2.10.1 Financial sustainability

While CI operators have primary responsibility for ensuring the resilience of their critical assets and processes, the enhancement of physical and IT protection measures often requires committing significant amounts of resources. Achieving CI resilience can be a costly endeavor. In such context, CIP strategies must ensure that investments towards an optimal level of CI are financially sustainable. In practice, countries need to find a balance in terms of cost-sharing arrangements between CI owners/ operators, Government agencies and insurance providers.

An important tool to encourage business engagement appears to be the creation of incentives. These range from regulation to subsidies, tax relief efforts and loans. Incentives appear all the more important in periods of economic crisis, when operators may naturally lean towards spending resources on short-term growth objectives rather than long-term protection goals.

CASE STUDY 24
Incentives and funding mechanisms for CI resilience in Sweden, Japan and the US

Sweden:
Sweden's 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.

Source: Action Plan for the Protection of Vital Societal Functions & Critical Infrastructure, 2014, at: www.msb.se/RibData/Filer/pdf/27412.pdf

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

Source: Arie H.2017

USA:
Through the NIPP Security and Resilience Challenge, the Department of Homeland Security - in partnership with the National Institute of Hometown Security (NIHS) - funds innovative ideas that can provide technologies and tools to the critical infrastructure community. Projects funded under the NIPP Challenge are meant to not only have tangible, near-term results so they can be quickly developed and implemented, but also 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 NIHS independent panel according to a range of criteria which also take into account their viability and expected impact.

Source: Department of Homeland Security, at: www.dhs.gov/nipp-challenge

The financial sustainability of CIP strategies is also predicated on designing effective insurance mechanisms, particularly in case of "recovery" action necessary for the reconstruction of seriously damaged assets and to restore interrupted services. The discussion about insurance schemes for CI only started after the events of 9/11. Before then, the terrorism risk was commonly included in standard insurance policies without payment of any higher premiums. Following 9/11 and other hugely destructive terrorist attacks such as those occurring in Madrid on March 11, 2004, perceptions changed radically due to the unprecedented compensation amounts 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" (Michel-Kerjan 2018, p.12). 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" (Michel-Kerjan 2018, p.12).

CASE STUDY 25
Insurance schemes for CI resilience against terrorist acts in France, Spain, US, and the UK

France:

Active since 2002, Insurance and Reinsurance Management of the Risks of Attacks and Terrorist Acts (« Gestion de l'Assurance et de la Reassurance des Risques d'Attentats et Actes de Terrorisme », GAREAT) is a non-profit making structure composed of insurance companies. GAREAT manages the reinsurance of the risks of "attacks" and acts of terrorism that cause damage in France (regardless, however, 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's 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 program through the Caisse Centrale de Réassurance.

Source: GAREAT, www.gareat.com

Spain:

The Consortio de Compensacion de Seguros compensates damage to people and property caused by "extraordinary risks". In order to be entitled to compensation by the Consortio, an insurance policy in certain specific branches must have been subscribed to. Special cover by the Consortio is automatic when damage is the result of an act of terrorism. The Consortio is a public organisation attached to the Ministry of Economy, Industry and Competitiveness.

Source: Ministry of Economy, Industry and Competitiveness, at: www.consorseguros.es/web/inicio

USA:

In the US, the system revolves around a risk-sharing arrangement between the federal government, the insured and the insurer. Based on the Terrorism Risk Insurance Act of 2002 (TRIA), insurers are obliged to offer terrorism insurance to their clients (although they are free to set the price of coverage). In turn, clients are not under an obligation to take out coverage. Crucially, under TRIA 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.

Unted Kingdom:

In the UK, the system is a public/private partnership called Pool Re. Most insurers providing commercial property and consequential loss insurance in the UK are members of Pool Re and have agreed to offer terrorism cover to their clients. Any policyholder which has taken such a cover and sustains losses as a result of damage from an act of terrorism is 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 they pay under the terrorism cover they provide. Insurers pay premium to Pool Re for this purpose. The Government commits to support Pool Re if ever it has insufficient funds to pay a legitimate claim.

Source: Pool Re, www.poolre.co.uk/

2.10.2 Reviewing and monitoring mechanisms

Economies are dynamic. Infrastructures that used to deliver critical services to societies and the economy may be closed for whatever reason or set to perform functions that are no longer considered critical. For example, coal-extracting mines may give way to different types of energy-producing sources. Also, more simply, certain assets may no longer perform the functions they were destined to as they become obsolete, or for other economic reasons they were dismissed.

Moreover, the nature and intensity of threats to CIs can change. The outcome of even accurate risk assessments conducted at a certain point in time may no longer match realities on the ground. Some terrorist groups may simply pose less of a threat over certain geographical areas while continuing to exert pressure elsewhere. For example, at the end of 2017 ISIL had lost control of approximately 95% of the territory it used to control in 2014. CIs located in those territories are probably no longer subject to the same type and intensity of threat coming from ISIL, although the danger may well come from new groups/ actors. In other cases, the threat might not have changed as much as the vulnerability of a certain infrastructure due, for example, to aging or lack of maintenance.

With all this in mind, CIP strategies need to provide for mechanisms aimed to, at regular intervals of time:

- Update what are often vast “lists” of national CIs;
- Re-assess risks;
- Revise the strategic document(s) underpinning CIP to improve risk management, detect changes to the context of existing risks, and to identify new risks.

In performing the three above-mentioned functions, governmental agencies should naturally engage CI operators following the same logic of public/private partnership underlined in the previous sections.

CASE STUDY 26

Spain’s update of its CI “catalogue”

According to Royal Decree 704/2011 containing regulations for the protection of critical infrastructures, “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 Center for the Protection of Infrastructures and Cybersecurity (CNPIC), which shall validate them prior to their inclusion into the Catalogue. In any case, the update of available information should take place on an annual basis” (Art.5(5)

3. ESTABLISHING CRIMINAL RESPONSIBILITY

Security Council Resolution 2341(2017)
Operative Paragraph 3

> *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.*

3.1 Purposes of criminalizing attacks against CIs

The requirement to criminalize acts directed at CIs is instrumental in achieving three inter-connected objectives:

- To provide adequate levels of deterrence through the application of serious penalties to perpetrators of terrorist acts against CIs;
- To disrupt criminal /terrorist plans directed at CI through the use of criminal law as a preventive tool. The preventative focus of Resolution 2341(2017) emerges clearly from the requirement that countries should criminalize, among others, "the planning of, training for, and financing of and logistical support" for terrorist attacks;
- To set the legal bases and pre-conditions for smooth international cooperation in the criminal justice field on CI-related matters.

Section 3.2 discusses the extent to which the universal legal framework against terrorism address criminal conduct against CIs. Sections 3.3, 3.4 and 3.5 provide an overview of how countries' criminal statutes deal with issues of liability relating to CIs and how the establishment of criminal offences is linked to international cooperation in criminal matters. Moreover, these sections consider the main criminal law options from a legislative drafting perspective, taking into account international standards and requirements, including from a human rights perspective.

3.2 Criminalizing acts against CIs: Security Council resolutions and international conventions

A unique feature of Resolution 2341(2017) lies in its being the first Security Council instrument specifically calling upon states to criminalize acts against CIs. That said, resolution 2341(2017) builds upon a number of previously adopted resolutions setting forth general requirements to establish the criminal responsibility of perpetrators of terrorist acts. The landmark instrument in this field (to which res.2341(2017) explicitly refers) is resolution 1373(2001). Adopted shortly after the events of 9/11, this instrument provides for, among others, 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. Lacking agreement of the scope of application of a comprehensive convention covering all aspects and manifestations of international terrorism, these instruments were adopted in a time span of over fifty years following a sectoral approach. The incremental and pragmatic approach followed by the international community has resulted in the adoption of conventions and protocols focusing on areas such as maritime and aviation security, nuclear and terrorist financing, etc.

Similarly, to Security Council resolutions, these conventions and protocols do no mention the word "critical infrastructure". In part, this can be explained by the fact that most of these instruments were adopted at a time when the notion itself of "critical infrastructure" had not yet established itself into the counter-terrorism global policy discourse. However, as illustrated in table [number], most of them contain offence-creating provisions directly targeting malicious acts aimed at destroying or interfering with the functioning of CIs. Such offences are often described in detail, having been the object of careful drafting exercises as part of time-consuming technical and diplomatic negotiations.

To the extent that countries are parties to such instruments, they have an obligation to domesticate their provisions by, among others, establishing conduct set forth therein as criminal offences in national legislation. Countries that are not parties to some of the counter-terrorism conventions and protocols are encouraged to ratify or accede to them as called upon to do so by, inter alia, Resolution 1373(2001).

Table 6: CI-related offences in the universal counter-terrorism instruments

CI sector	Convention(s)/ Protocol(s)	Main offences * * *(For the full range of criminalization requirements and exact wording used by the conventions, refer to treaties' official texts)*
Aviation	1963 Convention on Offences and Certain Other	Requires the following contracting States to establish jurisdiction to punish offences committed on board aircraft:

	Acts Committed on Board Aircraft (and its supplementary Protocol of 2014)	- The State of registration of the aircraft; - the State of landing, when the aircraft on board which the offence is committed lands in its territory with the alleged offender still on board; - the 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.
	1970 Convention for the Suppression of Unlawful Seizure of Aircraft (and its supplementary Protocol of 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
	1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation and 1988 Protocol for the Suppression of Unlawful Acts of Violence at Airports Serving International Civil Aviation as supplemented by 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 known to be false, thereby endangering the safety of an aircraft in flight; - Using against or on board an aircraft in service any BCN 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 disrupts the services of the airport, if such an act endangers or is likely to endanger safety at that airport
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 BCN 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 causes damage to it which is 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	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. 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 BCN 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 Amendments to the Convention on the Physical Protection of Nuclear Material	Using or damaging a nuclear facility, interfering with its operation, or commits 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

Government	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 of her person or liberty

Cross-cutting	1997 International Convention for the	Delivering, placing, discharging or detonating an explosive or other lethal device into or against a place of public use, a State

	Suppression of Terrorist Bombings	or government facility, a public transportation 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 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

Beside the universal counter-terrorism legal framework, a number of counter-terrorism regional instruments establish CI-related criminalization requirements, particularly in the field of critical information infrastructure (CII). The ground-breaking convention in the field is the 2001 Council of Europe on Cybercrime, which for the first time introduced at the international level descriptions of 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 EU has adopted a directive aimed to, among others, harmonize the criminal law of the Member States in the area of attacks against information systems. Another recent example is the 2014 African Union convention on cyber-security and data protection (see case study below).

CASE STUDY 27
EU and African Union legal frameworks on the criminalization of attacks against information systems

2013 EU DIRECTIVE on attacks against information systems

A key objective of this instrument 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 botnets, i.e. the act of establishing remote control over a significant number of computers by infecting them with malicious software through targeted cyber-attacks. 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 cyber-attack.

Crucially, the Directive identifies three "aggravating" circumstances in which the offences in question need to be punished by a maximum term of imprisonment of at least five years. In particular:

- 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 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).

Among the provisions dealing with criminalization requirements, those more directly related to the CIIs protection are set forth in art.29 (Offences specific to Information and Communication Technologies) under the two sub-heading of "attacks on computer systems" and "computerized data breaches".

In addition to establishing offences dealing with direct attacks on computer systems, the African Union Convention takes a marked preventative approach to the commission of the cyber-related offences. Under article 29(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".

3.3 Drafting criminal legislation on CIP

National authorities are under the obligation to incorporate into national legislation the elements of the offences set forth in counter-terrorism conventions to which they are parties. In addition, they need to determine the extent to which they wish to criminalize CI-related offences beyond treaty requirements, which, as seen in the previous section, only cover certain aspects of the topic. In planning the introduction of comprehensive CI-related criminal legislation, national authorities should bear in mind that there is no international definition of "critical infrastructure". In general terms, a number of drafting options can be envisaged:

i) Criminalize conduct related to specific types of infrastructure (sector-specific approach);
ii) Criminalize conduct against CIs generally (cross-sectoral approach);
iii) Rely on non-CI specific criminal legislation (indirect 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. Whatever 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.

i) Sector-specific approach

CI-related offences can target specific critical sectors such as the nuclear, transport sector, etc. 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 counter terrorism conventions 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 "common law" countries, for instance: Fiji's Civil Aviation (Security Act), 1994, Sri Lanka's Suppression of Terrorist Bombings Act, 1999, and UK's Internationally Protected Persons Act, 1978. Often, when a sector-specific approach is chosen, related offences are part of broader normative frameworks also aimed to regulate in detail sector operations, licensing requirements and procedures, etc. An example is Japan's 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 specificities of certain types of infrastructure and sectors. It also allows for 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/ assets, thus leaving the others unattended.

ii) Cross-sectoral approach

Several countries criminalize attacks against CIs directly as terrorist offences. While normally the scope of CI-related terrorist offences is not restricted to any specific sectors, a number of countries provide non-exhaustive examples of the types of covered infrastructure. For example, Kenya's 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 […]".

In the EU Framework decision on combating terrorism,[20] attacks against CIs feature prominently among the material elements of terrorist offences in the form of, 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

[20] EU framework Decision of 13 June 2002 on Combating Terrorism (2002/475/JHA), art.1.

or result in major economic loss", or "seizure of aircraft, ships or other means of public or goods transport", or "interfering with or disrupting the supply of water, power or any other fundamental natural resource the effect of which is to endanger human life".

On the other hand, the expression "critical infrastructure", which features in most national policy documents and strategies, does not appear as such in national counter-terrorism statutes. More commonly, references are to notions of "public infrastructure", or "essential services, facilities or systems", often when their destruction or interference in their functioning leads to major economic loss, danger for human life, etc.

It is worth noting that a number of laws criminalizing attacks against CIs as terrorist acts are careful to provide exemptions for action taken in the context of the legitimate exercise of certain civil, political or social rights. For example, Canada's 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 [the definition of "terrorist activity"].[21]

The advantage of a cross-sectoral approach is that it provides a framework to ensure coverage of all CIs sectors, including those that may potentially be added as critical ones in the future. If other domestic criminal laws exist dealing with specific sectors, these laws would normally apply as "lex specialis". One possible disadvantage is lack of precision in that the legislator may establish one range of sanctions which is indistinctively applicable across sectors. In these cases, judges may have a bigger room for manoeuvre in adapting sanction levels to the circumstances of the case than would be the case under a narrow sector-specific approach.

CASE STUDY 28

South Africa's Protection of Constitutional Democracy against Terrorist and related Activities Act 33 of 2004

South Africa's definition of terrorism/ terrorist act contains particularly extensive and detailed reference to CIs. Accordingly, "terrorist activity", means, among others:

"(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;

[21] Criminal code, 83.01(1).

> (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 destabilisation 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-
> threaten the unity and territorial integrity of the Republic;
> 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
> 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 organisation or body or intergovernmental organisation 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 organisation 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 […]

iii) Indirect approach

This approach consists of criminalizing acts against CIs by using "standard" criminal offences such as damage to property, arson, trespassing (e.g. unauthorized access to property), etc.

One advantage is that countries can rely on a basic range of well-established offences pending the adoption of more targeted legal frameworks, or in order to fill gaps left by new CI-specific legislation. Another potential advantage is that judges in many countries are often more familiar and comfortable with the application of these "classical" offences than new CI-related regimes. Drawbacks to this approach include lack of differentiation between critical and non-critical assets. Also, the prohibition to apply criminal laws by analogy raises at least serious doubts as to the possibility to apply to the cyber domain offences that were conceived for the physical world only (e.g. using traditional trespassing offences to deal with unauthorized access to computer systems).[22]

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

3.4 The reach of CI-related criminal laws

When drafting CI-related criminal offences, important considerations should be given to their scope of application. National authorities should ensure that their criminal laws duly address the following scenarios:

- An attack against an infrastructure located in the territory of the State produces substantial effects in another State. A similar scenario would mostly occur in case of acts involving CIIs. For example, an industrial control system (ICS) located in Country A governs gas delivery in Country B. Following the manipulation of the ICS, disruptions are felt in Country B, but not in Country A;

- Following an attack against a CI located in Country A, the alleged perpetrator finds refuge in Country B. All the universal counter-terrorism treaties oblige countries to establish their extra-territorial 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).

Some counter-terrorism conventions set forth specific jurisdictional criteria. For example, in the case of an offence involving aircrafts under the 1970 Convention for the Suppression of Unlawful Seizure of Aircraft or the 1971 Convention for the Suppression of Unlawful Acts against the Safety of Civil Aviation, national courts shall establish jurisdiction over offences onboard 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.

In other cases, the counter-terrorism conventions provide for optional grounds for jurisdiction, e.g. in case of offences committed abroad against a national (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 offences.

3.5 International cooperation in criminal matters

As mentioned in Section 3.1, the need for States to criminalize conduct set forth in the universal legal framework against terrorism is also instrumental in facilitating international cooperation in criminal matters. To the extent that the relevant (CI-related) offences have been introduced in the criminal legislation of States parties, significant legal obstacles to smooth cooperation can be removed. For example, the classical requirement that extradition (and, to a lesser extent, mutual legal assistance) can only be granted when the offence in question is criminalized in both the requested and the requesting member states, would be automatically fulfilled if both States faithfully transpose treaty language into their respective criminal statutes.

At the same time, the ability of individual countries to effectively 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. Crucially, countries intent on maximizing the protection of their CIs from the criminal justice angle should bear in mind the role of the universal counter terrorism instruments in providing legal bases for extradition and mutual legal assistance, either in complement of or in the absence of bilateral or regional arrangements to this effect.

From a law enforcement perspective, INTERPOL's Strategic Framework 2017-2020 sets the first strategic goal for the Organization to "serve as the worldwide information hub for law enforcement cooperation" by managing secure communication channels that connect National Central Bureaus in all INTERPOL's 192 member countries, along with other authorized law enforcement agencies and partners, and which give access to a range of criminal databases.

The INTERPOL I-24/7 network underpins all INTERPOL operational activity in support of international cooperation in criminal matters amongst its member countries. From routine checks at border crossings to targeted operations against different crime areas, and from the deployment of specialized response teams to the search for international fugitives, I-24/7 is the foundation of information exchange between the world's police.

In relation to counter-terrorism and CI, the INTERPOL Global Counter Strategy stresses the crucial importance of international cooperation amongst law enforcement authorities across the world. It defines INTERPOL's counter-terrorism mandate as assisting and creating opportunities for law enforcement in its member countries in preventing and disrupting terrorist activities through the identification of members of terrorist networks and their affiliates, by tackling the main factors enabling their activities: travel and mobility, online presence, weapons and materials, and finances.

Whatever cooperation channel is used, there is a need for countries 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.

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 sub-regional organizations and entities to identify and share good practices and measures to manage the risk of terrorist attacks on critical infrastructure*

4.1 Information-sharing in the context of CIP strategies

If a governance architecture for CIP is the backbone of any related strategy, information-sharing is its life-blood. Proper information-sharing is instrumental in achieving CIP at all levels and in all phases. It is a key factor on which public-private partnerships are built (see Section 4.5.2). Domestic agency coordination is predicated on information-sharing (see Chapter 7). Finally, the extent and quality of international cooperation on CIs is shaped by the ability and willingness of States' to exchange information across borders (see Chapter 8).

4.2 The dimensions of information-sharing for CIP

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

- what information should be exchanged and why;
- how information for any given task will be shared;
- among whom information will be shared.

Information can be exchanged at the strategic, technical or tactical level. 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 crisis when the recipient is expected to take immediate action. Whenever this latter type of information is concerned, the platforms for information-sharing (and attached security features) will be structured very differently from those that seek to convey best practices, or strategic advice, etc.

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

- Between public entities and CI operators (both within a given sector and across sectors);
- Between CI operators (both within a given sector and across sectors);
  Between public entities.

4.2.1 Public entities - CI operators

The process of privatization of several CI sectors and sub-sectors 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 in a vital task to be performed under such partnerships.

The exchange of information between Governmental agencies and CI operators should flow from both directions and cover, notably:

Threats: for example, law enforcement bodies and intelligence services should convey information about new types of threats to CI operators. This information will ensure that CI operators conduct risk assessment and take the necessary mitigation measures. On the other hand, CI operators should communicate the result of risk assessment and mitigation measures put in place to relevant State entities to ensure a better modulation of mitigation plans. In this context, INTERPOL's "Purple and Orange Notices" are of particular relevance to disseminating urgent information amongst the global law enforcement community, and the public. While the Purple Notices help to seek or provide information on modus operandi, objects, devices and concealment methods used by criminals, Orange Notices are used to warn of an event, a person, an object or a process representing a serious and imminent threat to public safety;

Suspicious activities: CI operators may be encouraged to report so called "weak signals", i.e. unusual situations which are not per se sufficient to trigger the alarm, but reveal an impending threat when examined in the context of similar events or when a mere suspicion is corroborated by information stemming from other sources;

Incident data: lessons learnt from past incidents (including what was done and not done to address them) may offer important insights into ways of preventing the same situation from occurring again; this, in turn, provides a basis for more effective risk management and recovery action.

Table [number] summarizes the main types of CI-related information that the public sector could exchange with the private sector (and vice versa) to address cyber terrorist threats.

Table 7: Types of public/private information sharing on cyber-terrorism threats

Public sector[23] information	Private sector information
• Insights about cyber capabilities of key terrorist organizations	• Information about major asset categories in the energy sector (e.g., gas, oil, electricity, 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 analyzes of cybercriminal underground websites	• Insights on recovery needs to deal with different forms of attacks
Source: OSCE 2013, p.74	• Insights from attack patterns in other critical infrastructure sectors that could serve as early warning indicators for the energy sector

Private-public information-sharing is often seen as a tool to break the wall between two separate worlds and help create a genuine sense of community around CI issues. Reaching this goal is all the more important considering mutual suspicion attitudes and the reciprocal tendency by the private and the public sectors not to exchange information, particularly sensitive one. An interesting type of challenge in this area can be found in the energy sector. According to the OSCE, "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" (OSCE 2013, p.58).

In the context of cyber threats, valuable information sharing can include information regarding:

[23] Reference to "public sector" in the Table is understood to cover "Governmental agencies".

- Vulnerabilities (e.g. a flaw in software that can be exploited);
- Cybersecurity incidents (e.g. a successful attack on company systems);
- Defensive measures (e.g. patch information).

Information-sharing in this context has significant benefits of increased security and improved cyber defense. It can be helpful to consider steps to encourage cyber information sharing and mitigate these risks. For example, as one initial step to address the legal risk of cyber information sharing, the United States introduced the Cybersecurity Information Sharing Act[24] that provides, in some circumstances, safe harbors from civil liability for certain information-sharing activities "conducted in accordance" with CISA's provisions.

CASE STUDY 29

Incentives for the private sector to share information in Japan's cybersecurity strategy

Japan's cybersecurity strategy seeks to overcome business' hesitation 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: Japan 2015, p.27

4.2.2 CI operators – CI operators

The delivery of most critical services is the outcome of complex supply chains requiring the input of different companies operating in multiple infrastructure sectors and industry segments. Supply chain dependencies show the importance of having proper private-private channels for information flows across sectors. Information exchanges in this area may be of a technical or organizational nature.

The need to have in place adequate information-sharing arrangements also concerns CI operators producing or delivering the same type of goods or services within the same industry sector. This seems to be especially relevant for the purpose of exchanging good practices, information about risk assessment methodologies, protective measures employed, lessons learnt following incidents, etc. Well-experienced companies with long-standing practices in CI protection my usefully transmit their knowledge to

[24] Consolidated Appropriations Act of 2016, P.L. 114-113, Division N (Cybersecurity Act of 2015), Title I (Cybersecurity Information Sharing Act of 2015), 129 Stat. 2936, 6 U.S.C. §§ 1501-1510.

companies that are less familiar with applicable regulatory frameworks and CI compliance strategies. At the same time, one has to be cognizant of the intrinsic difficulty of ensuring smooth information flows between companies that are often competitors. For this reason, they may be wary of cooperating with each other, especially in the exchange of sensitive information, for fear of losing market shares.

4.2.3 Public entities – Public entities

The establishment of information-sharing mechanisms among public agencies is vital to the extent that public institutions are mandated to coordinate and implement CIP-related action both horizontally and vertically. An example of "horizontal" information-sharing is when multiple ministries are responsible for specific sectors and must come together to address cross-sectoral issues. Another one stems from the need for intelligence agencies to feed information to relevant authorities in charge of CIP for the purpose of elaborating national risk assessments. Examples of vertical-type arrangements are those necessary to support the division of labor between municipal, regional and national authorities, particularly (but not exclusively) in federal states.

Public-public information sharing is one dimension of the broader inter-agency coordination effort which is examined further in Chapter 5.

CASE STUDY 30

Securing the flow of information: UK's satellite-based communication system (HITS)

Technology can significantly support agencies in keeping critical information flowing at times of emergency. In the UK, this objective is pursued by HITS. Developed by the UK Government, 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 UK, 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 co-ordination during any kind of disruptive event.

Source: UK Cabinet Office, at: https://www.gov.uk/guidance/resilient-communications

4.3 Pre-requisites for effective information-sharing

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

- The ability of leading agencies to create 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 impinge on each other. While levels of trust will decrease 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 to a certain information-sharing arrangement can be a time-consuming effort and requires the active commitment of all stakeholders. However, once trust has been established, flows of information stand to gain significantly both in qualitative and quantitative terms.

Based on a survey of CIP methodologies predominantly focusing on European countries, RECIPE has compiled a list of "main success factors" in information-sharing. In particular, "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. 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" (RECIPE 2011, p.52).

4.3.2 Protecting sensitive information

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 need to respect applicable instruments dealing with the rights to privacy and data protection. Under the EU 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".[25]

A definition of "sensitive CIP related information" is provided by the EU Council Directive 2008/114/EC as follows: "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".[26]

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 the Member States or to the Commission is not used for any purpose other than the protection of critical infrastructures. [This] also apply to non-written information exchanged during meetings at which sensitive subjects are discussed".[27]

CASE STUDY 31
Protection of sensitive aviation security information

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 thereto (so called "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 may also need to be applied when identifying, classifying, receiving, retaining, disclosing, disseminating or disposing of sensitive aviation security information.

Sensitive aviation security information should be securely stored when not in use to prevent unauthorized access. For example, the use of security cabinets, locked rooms or safes may be considered a way of affording greater protection if considered necessary. Electronic copies of sensitive aviation security information documents should be equivalently protected. States and relevant entities should adopt measures to ensure that authorized persons with access to sensitive aviation security information do not disclose such information to any unauthorized persons. For example, consideration should be given to having authorized persons sign a "non-disclosure agreement" before being allowed access to such information.

[25] Art.8.

[26] Article 2(d).

[27] Article 9.

Whenever information needs to be exchanged between 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. States receiving sensitive aviation security information should apply the required protective measures to ensure that unauthorized use or disclosure is prevented.

Source: ICAO Security Manual, Doc 8973-Restricted

Concerning private-sector CI operators, they 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 them (e.g. it will not provide competitors with a competitive advantage, or will not be used against them by public agencies for purposes other than CI protection).

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 way to enable early and effective dissemination of critical information to all responders in charge of reducing impact.

The protection of CI-related information may begin with the enactment of legislation on the basis of the principle that the inappropriate release of sensitive data may pose national security or public safety risks. In Canada, the 2007 Emergency Management Act includes an amendment to the 1985 Access to Information Act to ensure the protection of sensitive information provided by critical infrastructure sectors.

CASE STUDY 32

National approaches to the protection of sensitive CI-related information: Australia and France

Australia:

Established by the Australian Government in 2003, the Trusted Information Sharing Network (TISN) is the country's primary engagement mechanism for business-government information sharing and resilience building initiatives. TISN 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 of TISN include banking and finance, communications, energy, food and grocery, health, transport and water services. In addition, there are specialist forums (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 TISN is provided by the Critical Infrastructure Advisory Council (CIAC). CIAC consists of the Chairs of each of the TISN Groups, senior

Australian Government representatives from relevant agencies, and senior State and Territory government representatives.

Source: Trusted Information Sharing Network, at: https://tisn.gov.au/

France:

The directives and plans adopted under the national system for the Security of Vital Activities (SAIV) are classified at the Confidential Defense level. Whether it is the issuer or the recipient, the CI operator ensures the destruction of classified documents which he no longer needs, especially when:

- a classified document is revised or repealed;
- a "vital point" (VIP) is canceled;
- a "vital zone" (ZIV) is canceled;
- an operator loses its status as "vital operator" (OIV).

An OIV may not wish to reveal some very sensitive information related to risk and crisis management. In that case, he must invoke specific procedures or provisions by referring to its internal documents which provide for them. The competent administrative authorities overseeing the operator's security plans may discuss the issue with the operator if necessary for the performance of their role. Such authorities may take cognizance of the information that the operator wishes to withhold, without necessarily disposing of it.

Source: France 2014

Operationally, a number of methods and solutions are available to protect the circulation of sensitive information. Typically, these are centered around: i) security and vetting procedures; ii) color-coding systems; iii) electronic tools. All three often complement each other.

i) Security clearances and vetting

Governments may provide security clearances for key stakeholders who need to access sensitive CI-related information. According to EU 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".[28]

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 agree, or in the form of background screening, interviews with the public bodies in charge of the information-sharing platform, etc.

In some cases, there may be resistance to involve members of the law enforcement community for fear that revealing certain types of information would trigger action of their part that would prejudice the

[28] Art.9.

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.

ii) Color-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 (TLP) applies this concept in that the originator of the information labels it with one of four colors:

- *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.

The advantage of TLP lies in its user-friendliness and in setting clear boundaries between the responsibilities of the issuer and the recipient.

iii) Electronic tools

In order to secure information sharing, some platforms use electronic tools, such as extranet, to exchange documents. An extranet is a telecommunication 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 to be allowed to view the network information.

CASE STUDY 33

Canada's Critical Infrastructure Information Gateway (CI Gateway)

One of the objectives under the National Strategy and Action Plan for Critical Infrastructure (the Strategy) is the timely advancement of information sharing and protection among CI partners. To achieve this objective, 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 recognizes that several information sharing arrangements were developed under the original Action Plan and seeks to build 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 2014-2014 action plan, key objectives in this area include:

Expanding stakeholder membership and participation on the Canadian Critical Infrastructure Gateway and leverage the CI Gateway's capabilities to improve information sharing and collaboration on specific projects: Public Safety Canada is committed to build 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 Canada's security and intelligence community is sensitive and can only be shared with individuals with an appropriate security clearance. Public Safety Canada is committed to work with lead federal departments and agencies to increase the number of security cleared stakeholders in the private sector.

Sources: Critical Infrastructure Information Gateway, at: https://cigateway.ps.gc.ca/_layouts/pscbranding/trms-eng.pdf; Action Plan for Critical Infrastructure 2014-2017, at: www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/pln-crtcl-nfrstrctr-2014-17-eng.pdf

5. ENSURING COORDINATION AMONG DOMESTIC AGENCIES

Security Council Resolution 2341(2017)
Operative Paragraph 6

> *The Security Council […]:*
>
> *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 The need for a multi-agency approach to CIP

Different public agencies (legislative bodies, regulators, etc.) set a plethora of norms, rules and standards on safety and security issues in different CI sectors. 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. Effective crisis management and response measures require the ability of several public entities (at the local, municipal, regional and national level) to play their part in a smooth and quick manner. Also, in many cases a number of entities may be involved in a given security function. 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 thus a key prerequisite to implement adequate levels of CIP. Related strategies need to "connect the dots" among a variety of domestic agencies with responsibilities for CIP-relevant action. Coordination should be achieved with stakeholders such as ministries (e.g. Communications, Economic Affairs, Security, Cabinet Office, Justice, Interior and Defense), regional bodies and regulators collaborating at the strategic, tactical and operational levels. Achieving this overarching objective, however, is not always at hand. Use of different terminology and jargon by the various entities involved in prevention/ protection/ response action as well as lack of unified procedures and communication channels have the potential to severely affect the quality of the overall CIP effort. It has been observed, also, that "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 co-operation when engaging with the private sector." (OSCE 2013, p.68)

CASE STUDY 34

Canada's Federal-Provincial-Territorial Critical Infrastructure Working Group

Beside the sectoral networks and the cross-sectoral forum, Canada's National Strategy and Action Plan have created a Federal-Provincial-Territorial Critical Infrastructure Working Group. 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 clearinghouse for governments on critical infrastructure related issues to the Federal-Provincial-Territorial Senior Officials Responsible for Emergency Management;
- Facilitate federal/provincial/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. Decision 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/territorial representative determined by group consensus.

The next section considers the main conceptual and institutional building blocks for achieving agency coordination in crisis scenarios. The ensuing sections provide an overview of the main challenges of inter-agency coordination in general and key tools for overcoming them, notably joint exercises/training and interoperability solutions.

5.2 Agency coordination in crisis situations

An important aspect of inter-agency coordination is the ability of all stakeholders to promptly and effectively act in crisis situations. The concept of crisis management has been introduced in Section 2.6.2. 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:

- Clear attribution of roles and responsibilities, a corollary being that decisions should be taken at the lowest appropriate level, with co-ordination being 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 co-operation, learning each other's slang" (RECIPE 2011, p.82);

- Full understanding of the consequences of CI disruption, including its cascading effects. It has been noted, in this regard, 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 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" (RECIPE 2011, p.81);
- 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 as well as 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 (see Section 4.3 on issues of data security and protection in the context of information exchange).

CASE STUDY 35
Crisis management following the 2005 London bombing

On 7th July 2005, as a result of four bombs being detonated on London's transport system, fifty-two members of the public were killed. The circumstances of the accident made the coordination of the emergency response particularly difficult. 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, according to the Coronel, "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 endeavored 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".

Notably, the report observed that while training (either in the form of tabletop' or 'real-life' exercises) was already been extensively provides 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 TfL [Transport for London] and the emergency services; the 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; and emergency care of the type provided by the London Air Ambulance and Medical Emergency Response Incident Teams.

In her 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: Coroner's Inquests into the London Bombings of 7 July 2005, 6 May 2011, at: http://image.guardian.co.uk/sys-files/Guardian/documents/2011/05/06/rule43-report.pdf

5.3 Joint exercises/ trainings

In the context of CIP, inter-agency exercises/ trainings are universally recognized as essential tool to pursue at least following goals:

- Achieve common understandings 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 that the operational reliability and compatibility of all communication equipment designated for use during an incident.

CASE STUDY 36
Cyber Europe

Managed by ENISA, Cyber Europe is a series of cyber incident and crisis management exercises for both the public and private sectors from the EU and EFTA Member States. The exercises are simulations of large-scale cybersecurity incidents escalating to become cyber fully-fledged crises. They offer IT security, business continuity and crisis management teams opportunities to analyze 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 2016 edition involved more than 1000 participants. The next one is scheduled for 2018.

Source: European Union Agency for Network and Information Security (ENISA), at: www.enisa.europa.eu/topics/cyber-exercises/cyber-europe-programme

Inter-agency can take place on a compulsory or voluntary basis depending on the circumstances. Countries implement different forms of exercises depending on the objectives sought, the number of entities and participants to involve, resource availability, etc.

CASE STUDY 37
Training, exercises and drills under the ISPC Code

The International Ship and Port Facility Security Code (ISPS Code) provides for mandatory training and exercises as part of the measures needed to step up stakeholders' understanding of their respective security-related duties and responsibilities (Sections 13 and 18 of the Code).

Drills, in particular, shall be envisaged at appropriate intervals. On 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.) On 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).

In all cases, training exercises and drills shall take into account the guidance provided in part B of the ISPS Code itself.

Ukraine's Institute for Strategic Studies has compiled an inventory of the most common types of exercises and their main uses (Ukraine 2017, p.110). Among them, the following can be mentioned:

- *Seminars*: To provide general guidance on existing strategies, plans, policies, procedures, protocols, resources and concepts;

- *Table-top exercises (TTXs)*: To generate discussion of a hypothetical, simulated emergency. TTXs are useful to facilitate conceptual understanding, identifying strengths and areas for improvement and achieve 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.

It is important to note that some of the exercises mentioned below, particularly those involving high number of participants and based on complex live simulations, require careful planning and often months, if not years, of preparation.

CASE STUDY 38

Ukraine's "Coherent resilience 2017"

«Coherent Resilience 2017» was a NATO-sponsored table-top exercise designed to further the resilience of Ukraine's critical energy infrastructure. The exercise aimed to:

- check existing procedures on prevention, protection and response on energy-sector related incidents;
- facilitate inter-departmental cooperation in enhancing the resilience of the National Power System, including international efforts to meet emerging security challenges.
- «Coherent Resilience 2017» involved twenty Governmental entities, including more than one hundred people in exercise planning and execution, across four work-streams: cyber/terrorism, crisis management, strategic communications and international organization response. Participants included, among others, personnel of government agencies and ministries in the field of energy, emergency services and national security in addition to military personnel, national police and other institutions and agencies responsible for protection and building resilience in the critical electricity supply sector.

The various scenarios were designed to encourage participants to:

- analyze vulnerabilities of critical energy infrastructure based on identified risks and threats;
- determine the consequences of failure, attack and/or damage to critical energy infrastructure and impacts on other related dimensions of society;
- determine cooperation and coordination between institutions, agencies and organizations establishing emergency services and assess their plans;

- exercise crisis management processes, including military and civil emergency planning as a response to conditions provoked by hybrid means in pre-conflict, conflict and post-conflict situations.

Source: Ukraine 2017

5.4 Promoting interoperable processes and solutions

A key concept for inter-agency coordination is “interoperability”. This can be either operational/ functional or technical. Canada’s Chemical, Biological, Radiological, Nuclear and Explosives Resilience Strategy defines both as follows:

“(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.” (Canada 2005).

In the context of inter-agency coordination, the possibility to rely on interoperable processes appears especially important 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 come down, 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” (Federal Signal 2013).

The use of interoperable systems is key not only to allow police and other responders (police, fire and rescue, ambulance services, etc.) to communicate with each other to coordinate action, but also to enable them to streamline resources in budgeting and planning for disaster relief and recovery efforts.

5.5 Overcoming cultural barriers

While the adoption of interoperable solutions and streamlined/ uniform processes can go a long way towards breaking silos and promote 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 extent to which cultural gaps among CI- actors may stand in the way towards achieving optimal levels of collaboration has been examined with particular attention in Sweden in the framework of this country's "whole-of-society" approach to CI resilience and, more in general, societal security. Accordingly, a study devoted to disaster resilience has isolated a number of professional relationships involved in CI protection and analyzed the specific cultural challenges attached to each of them. The study stressed, 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. 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 & Sundelius 2013, p.1301).

While certain behavioral gaps may be found along the civilian-military divide, the study observes 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 behaviors can be highly sensitive among proud professionals" (Lindberg & Sundelius 2013, p.1300-1301).

Other countries' experiences and perceptions may vary significantly depending on the specific institutional, social and economic structures in which their various professions operate. Without necessarily aiming to "uniformize" deeply rooted behaviors, each country may wish to develop awareness of these issues and find ways (e.g. by openly and regularly discussing these in joint trainings) to ensure that these do not eventually jeopardize ongoing time and resource consuming efforts to achieve CI resilience.

6. ENHANCING INTERNATIONAL COOPERATION TO PROTECT CIs

Security Council Resolution 2341(2017)
Operative Paragraphs 8 and 9

> *The Security Council […]*
>
> *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;*
> *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 The dimensions of international cooperation on CIP

One of the most prominent manifestations of globalization is the internationalization of supply chains, whether for the delivery of critical or non-critical products and services. Consequently, CI interdependencies and interconnectedness run across borders. Risks to countries' CI can originate in neighboring ones (especially in the case of shared physical infrastructure) or very distant ones (notably in case of cyber-attacks). In the event of an ICT crisis, it is even possible that an emergency unfolding in one country could only be addressed in another country which, in turn, is not directly affected.

Potential scenarios illustrating the need to place international cooperation firmly within countries' CIP strategies include the following:

- Two or more countries share the same infrastructure (cross-border CI);
- A CI located in one country depends, wholly or partly, on products, services, technologies, etc., delivered by another country;
- The disruption or anomalies in the functioning of a CI located in one country produce effects in other countries.

Current levels of international cooperation on CIP vary substantially on the basis on country needs and perceptions. It can be more or less broad in scope depending on the specific type of arrangements in place, countries' proximity and levels of economic integration.

In considering plans for new or reinforced cross-border partnerships on CIP, countries should be looking at a number of areas. As illustrated by the case studies in the following sections, international cooperation efforts usually focus on information sharing, crisis management and joint exercises. Somehow forgotten areas are international law enforcement and judicial cooperation in criminal matters. These latter forms of international cooperation may not be serving the purposes of CIP exclusively, but remain essential ingredients in State responses to terrorist attacks against CIs. To the extent that Security Council Resolution 2341(2017) requires the establishment of criminal responsibility, the application of effective penalties is inseparable from the need for countries to rely on effective channels for international cooperation in the criminal justice field.

In this context, a global platform for law enforcement communication is provided by INTERPOL's I-24/7. The system connects law enforcement officers in all 192 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 INTERPOL's range of criminal databases. Authorized users can search and cross-check data in a matter of seconds, with direct access to databases on suspected criminals or wanted persons, stolen and lost travel documents, stolen motor vehicles, fingerprints, DNA profiles, stolen administrative documents and stolen works of art. With I-24/7 installed at all National Central Bureaus, INTERPOL is now focusing on extending access to INTERPOL services beyond the NCB and out to frontline officers such as immigration and customs officials.

CASE STUDY 39

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.

ICAO's 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, as well as e-mail and aeronautical fixed service (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, i.e. 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. Additionally, the parameters of special security measures, responsibility for additional costs and the time frame to initiate action should be negotiated with the concerned aircraft operator and/or airports.

Urgent communications may be facilitated through use of the ICAO Aviation Security Point of Contact (PoC) Network, established for the communication of imminent threats to civil air transport operations, pursuant to the views expressed by the G8 Roma-Lyon Anti-Crime and Counter-Terrorism Group. Pursuant to Assembly Resolution A39-18: Consolidated statement of continuing ICAO policies related to aviation security, States who have not done so are urged to participate in the ICAO PoC Network. The objective of the ICAO PoC Network is to provide details of international aviation security contacts within each State, who 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/or 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, Security Manual, Doc 8973-Restricted

6.2 Major cross-border initiatives

Over the past few years, increased awareness that CI interdependencies do not stop at State borders have facilitate the conclusion of a number of international agreements and partnerships. Due to the economic weight of the countries involved and the presence of highly complex infrastructure networks linking them, this section examines the EU framework and the US-Canada cooperation arrangements in the field.

6.2.1 European Union

Efforts to ensure that the EU's 27 member states design an overall strategy dealing with CIP started in 2005. Upon request by the European Council, the Commission adopted a Green Paper containing a number of policy options on the establishment of a CIP program. The feedback received highlighted the added value of a Community framework in this area. In April 2007, the Council stated that it was the ultimate responsibility of the Member States to manage arrangements for CIP within their national borders. At the same time, it welcome efforts by the Commission to develop a European procedure for the identification and designation of European critical infrastructures (ECIs). The current EU approach is now enshrined in a 2008 directive which defines ECIs as "critical infrastructure located in Member

States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure" (art.2.b).

Crucially, the Directive concentrates on the energy and transport sectors. Moreover, it is aimed to complement, as opposed to replace, existing sectoral measures at Community level and in the Member States. Where Community mechanisms are already in place, they should continue to be used and will contribute to the overall implementation of this Directive.

The designation process for ECIs follows a number of steps, which involve the duty of member states to:

- Inform other member states about potential ECIs located in its territory and affecting them, and engage them in bilateral or multilateral discussions;
- Designate such infrastructure as ECIs following agreement with the involved member states;
- Inform the Commission on an annual basis of the number of designated ECIs per sector and of the number of Member States dependent on each designated ECI;
- Inform the concerned owner/operator that its infrastructure has been designated as an ECI;
- Ensure that designated ECIs possess an Operator Security Plan (OSP) and that this plan is regularly reviewed;
- Ensure that each ECI designates a Security Liaison Officer to act as a focal point between the ECI and the relevant member state authority;
- Conduct a threat assessment in relation to ECI subsectors within one year following the designation of critical infrastructure on its territory as an ECI within those subsectors;
- Report every two years to the Commission generic data on a summary basis on the types of risks, threats and vulnerabilities encountered per ECI sector in which an ECI has been designated;
- Appoint a "European critical infrastructure protection contact point" (ECIP) to coordinate European critical infrastructure protection issues domestically, with other Member States and with the Commission.

In 2013, an evaluation of the status of implementation of the 2008 Directive revealed a mixed situation. While having an EU-wide framework on CIP was clearly accepted as a priority, a number of challenges were highlighted. In particular, it was pointed out that "less than 20 European critical infrastructures have been designated and consequently very few new Operator Security Plans have been produced. Some clear critical infrastructures of European dimension, such as main energy transmission networks, are not included. Despite having helped foster European cooperation in the CIP process, the Directive has 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)" (European Commission 2013 bis).

Accordingly, in 2013 the European Commission proposed to re-orient CIP action in a new, more practical direction that would basically switch from a sector-specific to a systemic approach. The new approach starts with a pilot project aimed to evaluate risks, vulnerabilities and CIP measures implemented by four ECIs, namely: 1) the EU's electricity transmission grid; 2) the EU's gas transmission network; 3) EUROCONTROL; 4) GALILEO (the European programme for global satellite navigation).

The European Commission envisages the pilot phase to provide "the necessary indicators to allow for the shaping of an EU approach towards CIP. It would be based on the results achieved and the gaps identified through working with the Four and seek to provide useful tools for improving protection and resilience, including through providing for strengthened risk mitigation, preparedness and response measures [...] The following step could be to implement this approach in regions where Member States are interested in cooperating with each other. Examples could potentially include a resilience concept for the overall critical transport infrastructure around the Baltic Sea, and a programme for supply chain criticalities in the Danube region" (European Commission 2013 bis).

CASE STUDY 40
AIRPOL and RAILPOL

Cross-border collaboration on the protection of CIs within European countries is not limited to the framework set by the 2008 Directive. It also takes place in fora that, albeit not specifically devoted to CI protection, are very much instrumental towards this goal. The transport sector, through the activities implemented by AIRPOL and RAILPOL, offers two relevant examples.

Created in 2011, 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 types of deliverables:

- The 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;
- The coordination of high impact Cross Border Actions;
- The establishment of an advisory role as a representative body of experts

RAILPOL is an international network of the organizations responsible for policing the railways in EU 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 EU Member States.

6.2.2 Canada – US cooperation

Not only is the Canadian-US border the longest in the world, but in Canada over 90% of the population lives within 160 km of that border. Add to this the fact that several refineries, nuclear power plants, big manufacturing facilities and other CIs are located close to the border. A major consequence is the presence of a high number of dependencies and cross-border infrastructures the protection of which crucially depends on bilateral cooperation initiatives.

The main tool for cross-border cooperation on CIP is the 2010 Canada-US Action Plan. 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-U.S. Action Plan is structured around three objectives: i) Partnering for Critical Infrastructure Resiliency; ii) Information-sharing; iii) Risk management.

i) 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 (EMCG), established under the 2008 Canada-US Agreement on Emergency Management Cooperation 2008 to provide central oversight in support of joint emergency management. One of the working groups established under the EMCG deals specifically with CI and has been identified to "provide direction and continuity to support the Canada-U.S. Action Plan's".

Under this objective, the Action Plan also envisages to "provide mechanisms and opportunities for the US Sector and Government Coordinating Councils and the Canadian sector networks to work together to improve sector-specific cross-border collaboration". Moreover, the Action Plan has created a virtual Canada-US Critical Infrastructure Risk Analysis Cell (VRAC) to "develop and produce collaborative analytic products with cross-border applicability".

ii) Information-sharing

Under this objective, the two countries have notably 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 analytic products;
- Ensure effective information sharing during and following an incident affecting critical infrastructure.

iii) Risk management

Under the Action Plan, CI risk management commits the two countries to "work together to assess risks and develop 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".

6.2.3 INTERPOL

In March 2016, INTERPOL produced and circulated to all its member countries an Intelligence Note entitled *"Unmanned Aircraft Systems pose an increasing threat to critical infrastructure and other sensitive sites"*. The Note concluded, "as UASs become more popular, cheaper, and easier to acquire and use, it is only a matter of time before these devices are used more widely for nefarious purposes (…). Law enforcement entities around the world are not equipped to deal with the UAS threat". Indeed, reports suggest that ISIS used drones as a dispersal device of explosive materials and for surveillance purposes in Syria and Iraq. The Note also recommended that "law enforcement entities should consider using UASs, if they are not already, as a force multiplier to not only combat UASs used for nefarious purposes but also to aid in investigations, especially bomb incidents, CBRNE/HAZMAT management, crowd control, emergency and disaster response, and other day to day police activities".

In a parallel, yet relevant, development, INTERPOL ensures the Chairmanship of the United Nations Counter-Terrorism Implementation task Force's (UN-CTITF) Working Group on "Critical Infrastructure Protection, Vulnerable Targets, Internet and Tourism Security". Within this framework, several international entities and member countries highlighted the rising threat of drones use by terrorists and criminals without having the proper legal framework or operational capabilities to counter it.

In response, in October 2017 INTERPOL's Innovation Center (IC) and Counter-Terrorism Directorate (CTD) hosted the "1st Drone Investigational and Forensics Framework Working Group Meeting", which gathered 42 participants from 20 countries. Participants were essentially from law-enforcement, with 16% of attendants coming from the private sector and academia. The Working Group served as a forum to exchange of information on current issues and emergent trends related to drones use, such as threat of drones in prisons environment, terrorist use of drones, countermeasures against drones, forensics toolset approach, drones forensics, etc.

INTERPOL indeed enjoys a unique position to provide a global and neutral law enforcement platform bringing together experts governments, industry, academia and private sector to help member countries addressing this emergent threat. In addition, this initiative will represent INTERPOL's flagship initiative and contribution to the international community within the framework of the Organization's responsibility of Chair of the UN-CTITF WG on Critical Infrastructure Protection.

The Programme is intended to be launched and based in INTERPOL's IGCI, Singapore, and implemented in close collaboration with the Organization's IC, yet under the mandate of the Organization's CTD and its CBRNE and Vulnerable Targets Sub-Directorate. This will also crown the ad-hoc endeavors that have so far been deployed by INTERPOL's IC and answers to the mission and mandate prerogative of the CTD to address critical infrastructure protection (Reference to the INTERPOL Global Counter-Terrorism Strategy, Action Stream 4.6 "Enhance the capacity of member countries to protect their critical infrastructure and vulnerable targets against both physical and cyber terrorist attacks".

6.2.4 Other initiatives

The past few years have seen a growing number of initiatives addressing the cross-border dimension of CIP at both the sub-regional and cross-regional levels.

The Nordic Emergency Management Cooperation is worth mentioning as an example of sub-regional initiatives. A "reinforced version" of this operational platform was agreed upon in 2009 linking Denmark, Sweden, Iceland, Norway and Finland. The initiative is structured around a series of working groups with annually 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. Specific areas of cooperation include: rescue service; exercises and education; CBRN preparedness; crisis portals; recruitment of volunteers; research and development; tactical fire prevention; strategic air transportation to disasters; strategic air transport; host nation support.

From a cross-regional perspective, the issue of CI protection has been the object of yearly expert meetings between the EU and the US and the EU and Canada. As highlighted in the 2013 Commission paper, "these meetings addressed mainly the need to strengthen cooperation by sharing knowledge, best practices and information on CIP, including the development of a global infrastructure security toolkit. […] In future meetings, we will focus on selected topics considered of growing importance for CIP in terms of the international dimension, namely: foreign interdependencies; interconnectedness of critical infrastructure; the possibility of global cascading effects; and the interdependence of physical and cyber infrastructure" (European Commission 2013 bis, p.6).

6.3 Cross-border technical and financial assistance

Not only is CIP a resource-consuming effort in its various phases and dimensions, but it also requires high levels of expertise in several domains. While CIP is indeed a priority shared by all countries, the necessary resources and multidisciplinary skills are not readily available in all of them. With this in mind, the drafters of Security Council Resolution 2341(2017) explicitly "urge […] 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".

Along these lines, in the civil aviation field 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".[29]

A specific legal framework for cross-border technical and financial assistance is provided by the EU vis-à-vis non-EU countries in the crisis management area.[30] Specific objectives are:

- in a situation of crisis or emerging crisis, to contribute swiftly to stability by providing an effective response designed to help preserve, establish or re-establish the conditions essential to the proper implementation of the Union's external policies and actions […];
- to contribute to the prevention of conflicts and to ensuring capacity and preparedness to address pre- and post-crisis situations and build peace;
- to address specific global and trans-regional threats to peace, international security and stability.

Crucially, the above-mentioned technical and financial assistance may specifically cover "support for measures necessary to start the rehabilitation and reconstruction of key infrastructure, housing, public buildings and economic assets, and essential productive capacity, as well as other measures for the re-starting of economic activity, the generation of employment and the establishment of the minimum conditions necessary for sustainable social development".

Beyond the type of crisis management assistance envisaged by the above-mentioned normative instrument, countries may also envisage to assist countries in their planning stage for enhancing CI resilience. This could notably take the form of knowledge/ "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, in the field of CIIs 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

[29] Security Manual (Doc 8973-Restricted).

[30] Regulation (EU) No 230/2014 establishing an instrument contributing to stability and peace, at: http://ec.europa.eu/dgs/fpi/documents/140311_icsp_reg_230_2014_en.pdf

[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" (GFCE-Meridian 2016, p.53).

7. SECTOR-SPECIFIC INTERNATIONAL INITIATIVES

This Chapter provides an overview of key initiatives carried out by UN-system agencies in a selected number of CI sectors. Neither the list of sectors or the described initiatives aim to be comprehensive. The purpose is rather 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, 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".[31] 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 [have] evolved, IMO's focus on reactive efforts to counter terrorism [has] 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 [is] a main obstacle, as those agencies often competed for scarce resources.

IMO's Global Maritime Security programme, in particular, is in charge of designing and executing technical cooperation projects primarily focusing on assisting States in the implementation, verification, compliance with, and enforcement of the various IMO legal and operational frameworks. One key framework in the field is the ISPS Code. The Code is divided into two sections, Part A and Part B. Part A is mandatory and outlines detailed maritime and port security-related requirements that parties to the International Convention for the Safety of Life at Sea (SOLAS), port authorities and shipping companies must adhere to. Part B provides a series of non-binding guidelines on how to meet the requirements and obligations set out in Part A. The main objectives of the ISPS Code include:[32]

- establishing an international framework that fosters cooperation between Contracting Governments, Government agencies, local administrations and the shipping and port industries,

[31] Intervention by the Representative of IMO, Security Council Calls on Member States to Address Threats against Critical Infrastructure, Unanimously Adopting Resolution 2341 (2017), at: https://www.un.org/press/en/2017/sc12714.doc.htm

[32] Source: IMO, Maritime Security and Piracy, at: www.imo.org/en/OurWork/Security/Pages/MaritimeSecurity.aspx

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;

- determining the respective roles and responsibilities of all parties concerned with safeguarding maritime security in ports and on board ships, at the national, regional and international levels;
- ensuring that there is early and efficient collation and exchange of maritime security-related information, at national, regional and international levels;
- providing a methodology for ship and port security assessments, which facilitates the development of ship, company and port facility security plans and procedures, which must be utilized to respond to ships' or ports' varying security levels;
- ensuring 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.

In addition to the ISPS Code, the IMO's Maritime Security programme relies on a number of other maritime security instruments that in 2012 have been collected in a "Guide to Maritime Security and the ISPS Code". The Guide aims to provide stakeholders with a comprehensive source of guidance.

7.2 Aviation sector

The International Civil Aviation Organization (ICAO) is a UN specialized agency, established by States in 1944 to manage the administration and governance of the Convention on International Civil Aviation (Chicago Convention).[33]

ICAO works with the Convention's 192 Member States and industry groups to reach consensus on international civil aviation Standards and Recommended Practices (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 aviation's global 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 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

[33] Doc 7300/9

and reports on numerous air transport sector performance metrics; and audits States' civil aviation oversight capabilities in the areas of safety and security.

With regard to the Aviation security and Facilitation Strategic objective, it is essentially carried out through the following domains:

- policy initiatives;
- audits focused on the capability of Member States to oversee their aviation security activities;
- capacity building assistance and training to improve State's related capabilities;
- development and implementation of the ICAO Traveller Identification Programme (TRIP) Strategy;
- management of the ICAO Public Key Directory (PKD).

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, and its Supplementary Protocol of 2014;
- 1970 Convention for the Suppression of Unlawful Seizure of Aircraft, and its Supplementary Protocol of 2010;
- 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, and its Supplementary Protocol of 2010;
- 1991 Convention on the Marking of Plastic Explosives for the Purpose of Detection;
- 2010 Convention on the Suppression of Unlawful Acts Relating to International Civil Aviation;
- 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 (GASeP). Approved in 2017 by ICAO Council, GASeP 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 developed by ICAO is its *Aviation Security Manual*[34] (, which is designed to assist the States in the implementation of Standards and Recommended Practices included in Annex 17[35]- *Security* - to the Convention on International Civil Aviation (Chicago Convention). Published in 2017, the latest version of the Manual features new and updated guidance material. Of particular interest for CIP are guidance materials related to security of landside areas of airports, staff screening and vehicle screening, and cyber threats to critical aviation systems.

Another relevant tool is the Aviation Security Global Risk Context Statement. Published annually, this "living document" provides States with the most pertinent information on the threat-and-risk environment. It contains analysis of global threats to civil aviation, information on recent developments in terrorist tactics, technical analysis on specific aviation security threats Its latest version highlights that a number of terrorist groups continue to explore innovative methods to conceal improvised explosive devices and circumvent existing security measures.

Acknowledging the urgency and importance of protecting civil aviation's critical infrastructure, information, and communication technology systems and data against cyber threats, the 39th Session of the ICAO Assembly called for a coordinated approach to achieve an acceptable and commensurate cyber resilience capability on a global scale. To that end, Resolution A39-19 on "Addressing cybersecurity in civil aviation"[36] sets out the actions to be undertaken by States and other stakeholders to counter cyber threats to civil aviation through a cross cutting, horizontal and collaborative approach.

The ICAO TRIP Strategy was endorsed, in 2013, by the 38th Session of the ICAO Assembly. It emphasizes a holistic approach to identification management in order to maximize both aviation security and facilitation, and is expected to increase the capacity of States to uniquely identify individuals by providing authorities with effective identification tools and guidance. It provides the framework for achieving significant enhancements in aviation security and facilitation by bringing together the elements of identification management and building on ICAO leadership in matters related to MRTDs. The five interlinked elements of the ICAO TRIP Strategy, are Evidence of Identity, MRTDs, Document Issuance and Control, Inspection Systems and Tools, and Interoperable Applications. The technical specifications that enable global interoperability of travel documents are found in Doc 9303, *Machine Readable Travel Documents* (MRTDs).

[34] Doc 8973. 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 through at: https://drm.icao.int/ website.

[35] Annex 17 – *Security* - includes, notably, the Standards and Recommended Practices for international aviation security and is constantly being reviewed and amended in light of new threats and technological developments that have a bearing on the effectiveness of measures designed to prevent acts of unlawful interference.

[36] Res A39-19, October 2016, at: www.icao.int/Meetings/a39/Documents/Resolutions/a39_res_prov_en.pdf

Travel critical infrastructure would include the cyber and physical infrastructure that supports the issuance of travel documents and the border controls systems that integrate inspection systems and tools and interoperable applications that are used for processing travelers at borders. The national identity security infrastructure plays a crucial upstream role in the travel critical infrastructure.

Numerous TRIP guidance materials developed with the support of the technical experts of the Technical Advisory Group are available at: www.icao.int/Security/FAL/TRIP/Pages/Publications.aspx.

With a view to encouraging participation in the ICAO Public Key Directory (PKD), Amendment 26 to Annex 9 – *Facilitation* - introduced a new Recommended Practice (RP), RP 3.35.5 that is targeting those ICAO Member States utilizing Automated Border Control (ABC) systems. This RP encourages the use of the information available through the ICAO PKD as a means to validate ePassports by comparing the facial recognition to the ePassport holder's photograph.

7.3 Information technology sector

The protection of CIIs against cyber-security risks is a priority goal of the International Telecommunication Union (ITU). The Buenos Aires Action Plan, adopted at the 2017 World Telecommunication Development Conference, included as Objective 2 "Foster[ing] the development of Infrastructure and services, including building confidence and security in the use of telecommunications/ICTs".[37]

ITU's work directly relates to enhancing CII (and subsequently CI) resiliency against cyber-attacks, regardless of the origin of those attacks. ITU's activities revolves around three major blocks: i) standard setting; ii) awareness raising; iii) capacity building. For each of these blocks, the following paragraphs highlight key ongoing initiatives.

i) Standard setting

Standardization work is carried out by a number of technical Study Groups (SGs) in which representatives of the ITU membership develop Recommendations (standards) in the various fields of international telecommunications. Study Group 17 (SG17), 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[38] (ITU-T Recommendations and Supplements) have been adopted so far.

[37] The Conference's Final Report is available at: www.itu.int/en/ITU-D/Conferences/WTDC/WTDC17/Documents/WTDC17_final_report_en.pdf

[38] ITU-T Recommendations developed by ITU-T Study Group 17 are publically available at: http://www.itu.int/ITU-T/recommendations/index_sg.aspx?sg=17

Ongoing work areas for SG17 include, among others, cybersecurity, security management, security architectures and frameworks, identity management, application security, and security aspects of cloud computing, IoT, Intelligent Transport System, big data, distributed ledger technology etc. 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.

ii) Awareness-raising

A ground-breaking tool developed by ITU is the Global Cybersecurity Index (GCI). Conceived primarily as an awareness-raising tool, GCI 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 GCI score. The third iteration of the GCI is currently being prepared.[39]

iii) Capacity-Building

In this field, ITU supports Member States in establishing National Computer Incident Response Teams (CIRTs). These are viewed as national focal points for coordinating timely and effective response to cyber-attacks. ITU is committed to assist countries all along the process of setting up CIRTs, from assessing their readiness to helping with the planning and implementation phases, based on the principle of continued collaboration. ITU further organizes regular regional cyber-exercises (Cyber-Drills) to enhance collaboration among national CIRTs within the same region.

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".[40]

In particular, paragraph 7 of the Resolution emphasizes the importance of Member States taking appropriate measures to prevent […] looting or acquiring small arms and light weapons from national

[39] Previous versions can be consulted at: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/GCI.aspx

[40] 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/export controls, and stockpile management – and to engage in cooperation and assistance (www.un.org/disarmament/convarms/salw/programme-of-action/).

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 infrastructures, ensuring the physical security and management of stockpiles of conventional weapons is critical in a double sense. First, it reduces the risk that that such weapons may be used against CIs such as transport systems, Government premises and any other installation deemed critical by individual countries. Secondly, those very stockpiles may be considered as critical infrastructure in themselves as being instrumental in upholding countries' defense policies.

A variety of international and regional instruments form part of the international legal regime on conventional weapons. While these instruments provide a solid legal and operational framework for 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)[41] 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 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);

[41] The Protocol supplements the United Nations Convention against Transnational Organized Crime

- International Instrument to Enable States to Identify and Trace, in a Timely and Reliable Manner, Illicit Small Arms and Light Weapons (2005);

Africa

Treaties

- Protocol on the Control of Firearms, Ammunition and Other Related Materials in The Southern African Development Community (SADC)(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);
- Convention on Small Arms and Light Weapons, Their Ammunition and Other Related Materials (ECOWAS) (2006);
- The Central African Convention for the Control of Small Arms and Light Weapons, their Ammunition, 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 - Politically Binding (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 (CIFTA) (1997)

Other instruments

- Andean Plan to Prevent, Combat and Eradicate Illicit Trade in Small Arms and Light Weapons in All Its Aspects - Politically Binding (2003);
- CICAD Model Regulations - Model Regulations for the Control of the International Movement of Firearms, Their Parts and Components and Ammunition; Model Regulations for the Control of Brokers of Firearms, Their Parts and Components and Ammunition;
- Code of Conduct of Central American States on the Transfer of Arms, Ammunition, Explosives and Other Related Material (2006).

Asia-Pacific

Instruments

- Nadi Framework (Legal Framework for a Common Approach to Weapons Control);
- Plan of Action to Combat Transnational Crime (ASEAN) (1999)

Europe

Organization for Security and Cooperation in Europe

- Plan of Action on Small Arms and Light Weapons (OSCE Document FSC. DEC/2/10);
- Handbook of Best Practices on Conventional Ammunition, Handbook of Best Practices on Conventional Ammunition (2008);
- Principles on the Control of Brokering in Small Arms and Light Weapons, Forum for Security Cooperation, Decision No. 8/04, (2004);
- Standard Elements of End-User Certificates and Verification Procedures for Small Arms and Light Weapons Exports, Forum for Security Cooperation, decision No. 5/04, (2004);
- Handbook of Best Practices on Small Arms and Light Weapons, (2003);
- Principles Governing Conventional Arms Transfers Programme for Immediate Action Series No. 3 (DOC.FSC/3/96), (1993);
- Organization for Security and Co-operation in Europe (OSCE) Document on Small Arms and Light Weapons (2000 reissued in 2012);
- 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;
- EU Council Common Position on Brokering 2003/468/CFSP;
- Common position 2008/944/CFSP;
- European Parliament and Council Regulation 258/2012 implementing article 10 of the 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, and establishing export authorization, and import and transit measures for firearms, their parts and components and ammunition (Official Journal of the European Union, L 94, 2012);
- EU Code of Conduct on Arms Exports (1998);
- EU Strategy to combat illicit accumulation and trafficking of SALW and their Ammunition (2005).

7.5 Chemical, Biological, Radiological and Nuclear (CBRN) sectors

The prospect of non-State actors, including terrorist groups and their supporters, gaining access to and using weapons and materials of mass destruction is a serious threat to international peace and security. Recognizing the prevalence of this concern, the UN Secretary-General has placed prevention at the very core of his peace and security agenda. In its resolution (A/Res/70/291) completing the Fifth Review of the UN Global Counter-Terrorism Strategy (A/Res/60/288), the UN General Assembly also called upon all Member States to "prevent terrorists from acquiring weapons of mass destruction (WMD) and their means of delivery… and (encouraged) cooperation among and between Member States and relevant regional and international organizations for strengthening national capacities in this regard." The UN Security Council too has made similar pronouncements, including resolution 2325 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).

i) UNOCT

In June 2017, General Assembly resolution (A/Res/71/291) established the UN Office of Counter-Terrorism (UNOCT) subsuming the UN Counter-Terrorism Implementation Task Force Office (CTITF) and UN Counter-Terrorism Centre (UNCCT). Since 2006, the CTITF Working Group on Preventing and Responding to WMD Terrorist Attacks facilitated an interactive exchange of knowledge, sharing of information on existing activities and emergency plans of the UN entities and international organizations in the prevention and response to an attack using WMD or related materials. Since 2013, UNCCT has been supporting the Working Group project on "Ensuring Effective Inter-Agency Interoperability and Coordinated Communication in Case of Chemical and/or Biological Attacks". The project assesses how the UN system and international organizations would collectively respond to a terrorist attack where chemical and biological weapons or materials are used, and the level of planned coordination among the different entities to facilitate rapid provision of assistance to the affected State/s.

In 2018, UNCCT began to expand its WMD/CBRN counter-terrorism activities in line with four strategic objectives: 1) Advance the understanding of the threat of WMD/CBRN terrorism; 2) Broaden capacity-building activities to support prevention, preparedness and response in Member States in line with the UN Global Counter-Terrorism Strategy, including in the areas of border and custom control, strategic trade control, illicit trafficking, and the security of critical infrastructure; 3) Develop partnerships to contribute to the ongoing capacity-building efforts of the international community; 4) Improve visibility and support mobilization of additional resources.

ii) UNICRI

Within the framework of the European Union Chemical, Biological, Radiological and Nuclear Risk Mitigation Centers of Excellence (EU CBRN CoE) initiative, UNICRI supported several UN Member

States in producing National CBRN Action Plans (NAPs) which highlighted key risks and national capacity-building priorities. The NAPs covered various aspects of preventing and combating both intentional and unintentional CBRN risks, including the safety and security of critical infrastructure.

In addition, UNICRI managed the implementation of a multi-regional project within the framework of the EU CBRN CoE (Project 19) entitled 'Development of procedures and guidelines to create and improve secure information management system and data exchange mechanisms for CBRN materials under regulatory control'. This project, which was implemented from 2013-2015, aimed at reinforcing national capabilities for secure information management and data exchange in relation to CBRN materials and facilities, establishing an expert team consisting of leading specialists from both the public and private sectors.

iii) INTERPOL

In 2010, INTERPOL's 80th General Assembly took a historic decision[42] to launch a comprehensive CBRNE terrorism prevention and response capacity in support of the Organization's 192 member countries. In 2016, the INTERPOL Global Counter-Terrorism Strategy cemented the Organization's mission in the CBRNE field in its "Weapons and Materials" action stream by *assisting 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" in regards 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 countermeasures programs;
- *Action 4.5*: Design 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 the global scale.

In implementing the aforementioned actions – and owing to INTERPOL's Constitution[43] – the Organization exclusively focuses on addressing non-state actors CBRNE threats. Accordingly, INTERPOL refrains from addressing matters related to state-sponsored proliferation of Weapons of Mass Destruction (WMD), which are thoroughly addressed by other international legal and institutional mechanisms. Nevertheless, the spectrum of non-state actors encompasses not only terrorist groups, lone

[42] AS-2011-RES-10

[43] Art 3 of INTERPOL's Constitution enshrines the guiding principle of neutrality by explicitly forbidding INTERPOL from engaging in matters of a political, military, religious, or racial character

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 INTERPOL's purview.

With the global realization of the crucial role of law enforcement in the prevention of and response to non-state actor based CBRNE threats, INTERPOL has progressively become one of the key international organizations contributing to the global efforts against CBRNE terrorism. Furthermore, the Organization has integrated all major multinational frameworks and established close ties with all relevant international partners, in a concrete interpretation of the inter-agency approach on the global scale.

UNSCR 1540's explicit mention of non-state actors made the resolution a natural point of reference for INTERPOL's CBRNE-related activities. Since the early days of INTERPOL's CBRNE capacity, the Organization 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 UNSCR 1540 "Assistant Provider Agency" and the majority of its activities within the CBRNE field supports – either directly or indirectly – the Resolution's implementation.

INTERPOL has been maintaining a close working relationship with the United Nations Office for Disarmament Affairs (UNODA), especially in contributing to the capacity building activities of the roster of experts belonging to the "The Secretary-General's Mechanism for Investigation of Alleged Use of Chemical, Bacteriological (Biological) or Toxin Weapons" (UNSGM).

At INTERPOL, specialized teams focus on the prevention of three types of terrorism:

- Radiological and nuclear terrorism
- Bioterrorism
- Chemical and explosives terrorism

INTERPOL's activities range from data analysis, training workshops and table-top exercises, to international conferences and on-the-ground operations. INTERPOL's methodology for countering the threat of CBRNE consists of three main pillars:

i. Information sharing and intelligence analysis: As well as conducting threat assessments and analysis, we publish a regular analytical report: the INTERPOL CBRNE Monthly Digest. Shared with our member countries and other subscribers, it summarizes open source reporting on all aspects of CBRNE crime and terrorism and provides an analytical perspective on particular issues;

ii. 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.

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, we run a number of initiatives, projects and operations to support the international law enforcement community in tackling the trafficking of CBRNE materials.

7.5.1 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 has compiled a best practices manual which collects and elaborates information received from sixteen Member States (OPCW 2016).

OPCW's approach is notably to tackle security issues (understood as measures addressing the "deliberate" releases of toxic chemicals) hand-in-hand with safety issues (i.e. measures to confront "non-deliberate releases"). OPCW's overarching objectives in this area are to ensure countries' coverage of the following safety and security dimensions:

- *Prevention*: refers to the understanding of 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*: refer 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.

From 2009 to 2016, the capacity-building programs on integrated chemical risk management carried out by OBCW's Technical Secretariat have reached over 1400 participants from more than 130 Member States. Activities are based on standards set by international regulation (mainly the Chemical Weapons Convention) and national level regulations. Among existing international instruments and initiatives, OPCW has highlighted the following as incorporating useful elements on chemical safety and security issues:

- *UN Security Council Resolution 1540*, which obliges 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*, dealing 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*, seeking 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*, supporting the labelling and handling of hazardous chemicals, in particular internationally-traded one. It contains standards and guidance useful to support supply chain security practices;
- *Seveso Directive* (I, II, and III), EU instruments aimed to improve the safety of sites containing large quantities of dangerous substances;
- *Globalized Harmonized System of Classification and Labeling of Chemicals (GHS*), a UN-managed standard established to replace the plethora of hazardous material classification and labelling schemes previously used by countries around the world. While voluntary in nature, several country regulations have made it a binding one domestically;
- *Responsible Care*, a global chemical industry initiative aimed, among other, to enhance security of products and processes and "provide help and advice to foster the responsible management of chemicals by all those who manage and use them along the product chain";[44]
- *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.[45] 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

[44] http://www.cefic.org/Responsible-Care

[45] Expert Workshop on International Chemical Security Coordination, 7 December 2017, at: https://www.opcw.org/fileadmin/OPCW/Protection-Against-CW/OPCW_Chemical_Security_Workshop_-_Informal_Summary_-_October_2017_-_for_release.pdf

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".

7.5.2 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 the International Atomic Energy Agency (IAEA). Its initiatives in this field are pursued under the nuclear security program, 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 their associated facilities. Legal bases underpinning the program are 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 1373,1540 and 2325;
- International Convention for the Suppression of Acts of Nuclear Terrorism.

IAEA Nuclear Security Series of publications complement the above by providing best practices, technical guides, training manuals, etc., for the benefit of Member States.

Among such publications is the Implementing Guide on "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 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 13 September 2017, the IAEA's Board of Governors approved the Organization's Nuclear Security Plan for the period 2018-2021 (IAEA 2017). The stated objectives of the Plan are to:

- contribute to global efforts to achieve effective nuclear security, by establishing comprehensive nuclear security guidance and, upon request, promoting its use through peer reviews and advisory services and capacity building, including education and training;
- assist in adherence to, and implementation of, relevant international legal instruments, and in strengthening the international cooperation and coordination of assistance;

- play the central role and enhance international cooperation in nuclear security, in response to the priorities of Member States expressed through the decisions and resolutions of the Agency's Policy Making Organs.

Activities envisaged under this Plan focus on assisting countries, upon request, in establishing effective and

sustainable national nuclear security regimes as well as promoting compliance with relevant international instruments. The Plan identifies, in particular, a set of priority areas and sub-areas for intervention through technical assistance and capacity building activities under the following headings:

Information management

- Assessing nuclear security needs, and priorities
- Information sharing
- Information and computer security, and information technology services

Nuclear Security of Materials and Associated Facilities

- Nuclear security approaches for the whole nuclear fuel cycle
- Enhancing nuclear materials security using accounting and control
- Upgrading security of radioactive material and associated facilities
- Nuclear security in the transport of nuclear and other radioactive material

Nuclear Security of Materials out of Regulatory Control

- Institutional infrastructure for material out of regulatory control
- Nuclear security detection and response architecture
- Radiological crime scene management and nuclear forensic science

Programme Development and International Cooperation

- International cooperation on nuclear security networks and partnerships
- Education and training programmes for human resource development
- Coordinating nuclear security guidance and advice services

REFERENCES

Ackerman 2007, Assessing terrorist motivations for attacking critical infrastructures, Centre for Nonproliferation Studies, Monterey Institute of International Studies, at: https://e-reports-ext.llnl.gov/pdf/341566.pdf

Arie H.2017, Japan's Approach to Tackling Cybersecurity Challenges, at: www.japanindustrynews.com/2017/01/japans-approach-tackling-cybersecurity-challenges/

Australia-New Zealand 2015, National Guidelines for Protecting Critical Infrastructure from Terrorism, Australia-New Zealand Counter-Terrorism Committee, at: www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf

Canada 2005, Chemical, Biological, Radiological and Nuclear and Explosives Resilience Strategy and Action Plan for Canada, at: www.publicsafety.gc.ca/cnt/mrgnc-mngmnt/mrgnc-prprdnss/chmcl-blgcl-rdlgcl-en.aspx

Clemente 2013, Cyber Security and Global Interdependence: What Is Critical?, Chatham House, February 2013, at: www.chathamhouse.org/sites/files/chathamhouse/public/Research/International%20Security/0213pr_cyber.pdf

Coroner's Inquests into the London Bombings of 7 July 2005, 6 May 2011, at: http://image.guardian.co.uk/sys-files/Guardian/documents/2011/05/06/rule43-report.pdf

CTED 2017, Physical Protection of Critical Infrastructure against Terrorist Attacks, Trends Report, Counter Terrorism Executive Directorate, at: www.un.org/sc/ctc/wp-content/uploads/2017/03/CTED-Trends-Report-8-March-2017-Final.pdf

European Commission 2005, Green Paper on a European Programme for Critical Infrastructure Protection, COM(2005) 576 final

European Commission 2013, Cyber Security Strategy of the European Union, JOIN(2013) 1 final, at: https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

European Commission 2013 bis, Working Document on a New Approach to the European Programme for Critical Infrastructure Protection - Making European Critical Infrastructures More Secure, SWD(2013) 318 final, at:

https://ec.europa.eu/energy/sites/ener/files/documents/20130828_epcip_commission_staff_working_document.pdf

European Commission 2017, Action Plan to Support the Protection of Public Spaces, 18.10.2017 COM(2017) 612 final, at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/european-agenda-security/20171018_action_plan_to_improve_the_protection_of_public_spaces_en.pdf

Federal Signal 2013, The basis of interoperability for emergency communications, Thought Paper, at: www.fedsig.com/sites/default/files/news/pdf/The%20bais%20of%20Interoperability%20for%20Emergency%20Communications.pdf

France 2014, General Inter-Ministerial Instruction on the Security of Vital Activities (available only in French), General Secretariat on Defence and National Security (N°6600/SGDSN/PSE/PSN), at: http://circulaire.legifrance.gouv.fr/pdf/2014/01/cir_37828.pdf

Germany 2009, National Strategy for Critical Infrastructure Protection, Federal Ministry of the Interior, at: http://ccpic.mai.gov.ro/docs/Germania_cip_stategy.pdf

GGE 2015, Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, General Assembly (Doc.A/70/174), at: https://ccdcoe.org/sites/default/files/documents/UN-150722-GGEReport2015.pdf

GFCE-Meridian 2016, Good Practice Guide on Critical Information Infrastructure Protection for Governmental Policy-Makers, at: www.meridianprocess.org/siteassets/meridian/gfce-meridian-gpg-to-ciip.pdf

Japan 2015, Cyber Security Strategy, at: www.nisc.go.jp/eng/pdf/cs-strategy-en.pdf

IAEA 2013, Establishing the Nuclear Security Infrastructure for a Nuclear Power Programme - Implementing Guide, at:
www-pub.iaea.org/books/iaeabooks/10436/Establishing-the-Nuclear-Security-Infrastructure-for-a-Nuclear-Power-Programme

IAEA 2017, Nuclear Security Plan 2018-2021, doc. GC(61)/24, at: www.iaea.org/About/Policy/GC/GC61/GC61Documents/English/gc61-24_en.pdf

Kolesnikova 2017, Challenges for PPP in time of new types of security threats, World Security Report, at: www.worldsecurity-index.com/

Lindberg & Sundelius 2013, Whole-Of-Society Disaster Resilience: The Swedish Way, in "The McGraw-Hill Homeland Security Handbook" (2nd Edition) / [ed] David Kamien, New York: McGraw-Hill, at: www.msb.se/Upload/Nyheter_press/McGraw-Hill%20Homeland%20Security%20Handbook,%20Helena%20Lindberg%20and%20Bengt%20Sundelius.pdf

McAfee 2011, In the Dark: Critical Industries Confront Cyberattacks, McAfee's Second Annual Report on Critical Infrastructure, at: www.mcafee.com/in/about/news/2011/q2/20110419-01.aspx

Michel-Kerjan 2018, Financial Protection of Critical Infrastructure: Uncertainty, Insurability and Terrorism Risk, Institut Veolia Environnement, at: file:///Users/SM/Downloads/Financial_Protection_of_Critical_Infrastructure_Un.pdf

NIPC 2002, Terrorist Interest in Water Supply and SCADA Systems, Information Bulletin 02-001, January 30.

NIPP 2013, Partnering for Critical Infrastructure Security and Resilience, Department of Homeland Security, 2013, p.15, at: https://www.dhs.gov/publication/nipp-2013-partnering-critical-infrastructure-security-and-resilience

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

OSCE 2013, Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection from Terrorist Attacks Focusing on Threats Emanating from Cyberspace, 2013, at: www.osce.org/atu/103500?download=true

OPCW 2016, Needs and Best Practices on Chemical Safety and Security Management, at: www.opcw.org/fileadmin/OPCW/ICA/ICB/OPCW_Report_on_Needs_and_Best_Practices_on_Chemical_Safety_and_Security_ManagementV3-2_1.2.pdf

RECIPE 2011, Good Practices Manual for CIP Policies for Policy Makers in Europe, at: file:///Users/SM/Downloads/RECIPE_manual%20(1).pdf

Shea 2003, Critical Infrastructure: Control Systems and the Terrorist Threat, Congressional Research Service, at: https://fas.org/irp/crs/RL31534.pdf

Sinai 2016, New Trends in Terrorism's Targeting of the Business Sector, The Mackenzie Institute, , at: http://mackenzieinstitute.com/new-trends-in-terrorisms-targeting-of-the-business-sector/#reference-27

Sweden 2014, Guide to Increased Security in Industrial Information and Control Systems, Civil Contingencies Agency, at: https://www.msb.se/RibData/Filer/pdf/27473.pdf

Sweden 2016, National Risk and Capability Assessment, Civil Contingency Agency, at: www.msb.se/Upload/Forebyggande/Krisberedskap/National%20risk%20and%20capability%20assessment%202016%20-%20Summary%20English.pdf

The Netherlands 2018, Resilient Critical Infrastructure, National Coordinator for Security and Counterterrorism, Ministry of Justice and Security, at: https://english.nctv.nl/binaries/Factsheet%20Critical%20Infrastructure%20ENG%202018_tcm32-240750.pdf

Ukraine 2017, Developing the Critical Infrastructure Protection System in Ukraine, National Institute for Strategic Studies at: http://en.niss.gov.ua/content/articles/files/niss_EnglCollection_druk-24cce.pdf

UNISDR 2009, Terminology on Disaster Risk Reduction, at: www.unisdr.org/we/inform/publications/7817

UP KRITIS 2014, Public-Private Partnership for Critical Infrastructure Protection – Basis and Goals, www.upkritis.de

Vishwanath 2015, The Water Wars Waged by the Islamic State, Stratfor, at: www.stratfor.com/weekly/water-wars-waged-islamic-state

ANNEX I - SELECTED GOVERNMENTAL RESOURCES ON CIP[46]

Country	Title	Type	Description	Year	Web address
Australia	Critical Infrastructures Resilience: Plan	Strategy/Policy document	Aims to support the continued operation of CI in the face of all hazards. The key outcomes that the Strategy seeks to achieve are: 1. A strong and effective business-government partnership; 2. Enhanced risk management of the operating environment; 3. Effective understanding and management of strategic issues; and 4. A 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.	2015	https://www.tisn.gov.au/Documents/CriticalInfrastructureResilienceStrategyPlan.PDF
Australia	National Guidelines for Protecting Critical Infrastructure from Terrorism	Strategy/ policy document	Complement the CI Resilience Strategy by providing a framework for a national approach on the CI protection from terrorism.	2015	https://www.nationalsecurity.gov.au/Media-and-publications/Publications/Documents/national-guidelines-protection-critical-infrastructure-from-terrorism.pdf
Australia	Australia's Cyber Security Strategy	Strategy/ policy document	This Cyber Security Strategy sets out the Australian Government's philosophy and program for meeting the dual challenges of the digital age—advancing and protecting Australia's interests online. This strategy establishes five themes of action for Australia's cyber security over the next four years to 2020: a national cyber partnership, strong cyber defences, global responsibility and influence, growth and innovation, a cyber smart nation.	2016	https://cybersecuritystrategy.pmc.gov.au/index.html
Belgium	Law of 1 July 2011 on the security and protection of critical infrastructures	Normative instrument	Together with Royal Decree of 2 December 2011 on critical infrastructure in the air transport sub-sector, this law constitutes the transposition of Council Directive 2008/114 / EC of 8 December 2008	2011	https://centredecrise.be/sites/default/files/loi_du_1er_juillet_2011_sur_les_ic_0.pdf
Canada	Emergency Management	Strategy/Policy document	Establishes a common approach for the various federal, provincial and territorial	2011	www.publicsafety.gc.ca/

[46] The documents displayed in this Annex do not form any comprehensive list of existing Governmental resources on CIP. Materials have been selected on the basis of relevance, open and full web-based access, geographical representation and the availability of translations into the English language.

	Framework for Canada		(FPT) emergency management initiatives. The Framework aims to enable consolidation of FPT collaborative work and ensure more coherent, complementary actions among the different FPT governmental initiatives. 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.		cnt/rsrcs/pblctns/mrgnc-mngmnt-frmwrk/mrgnc-mngmnt-frmwrk-eng.pdf
Canada	Cyber Security Strategy	Strategy/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.	2010	www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cbr-scrt-strtgy/cbr-scrt-strtgy-eng.pdf
Canada	National Strategy for Critical Infrastructure	Strategy/Policy document	Based on the principles of the Emergency Management Framework, the Strategy proposes that federal, provincial and territorial governments and 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.	2009	www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx
Canada	Action Plan for Critical Infrastructure (2014-2017)	Strategy/Policy document	Builds upon the original 2010 Action Plan, by further setting out action items for each of the objectives set forth in the National Strategy for Critical Infrastructure.	2014	www.publicsafety.gc.ca/cnt/rsrcs/pblctns/pln-crtcl-nfrstrctr-2014-17/pln-crtcl-nfrstrctr-2014-17-eng.pdf
Canada	Cyber Incident Response Centre (CCORC)	Coordination Centre	CCIRC is the national coordination centre responsible for reducing the cyber risks faced by Canada’s key systems and services. CCIRC works within Public Safety Canada in partnership with provinces, territories, municipalities, private sector organizations and international counterparts. It		www.publicsafety.gc.ca/cnt/ntnl-scrt/cbr-scrt/ccirc-ccric-en.aspx

			coordinates the national response to any serious cyber security incident.		
Canada / US	Agreement on Emergency management cooperation	International agreement	Sets out principles for mutual bilateral cooperation during an emergency. It establishes the Canada – US Consultative Group	2008	www.treaty-accord.gc.ca/text-texte.aspx?id=105173
Canada / US	Framework for the movement of goods and people across the border during and following an emergency	Strategy/Policy document	Sets out principles for communication and border management in the event of an incident (including explicitly terrorist acts) that contribute to significant borer disruption.		www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cnd-ntd-stts-frmwrk-en.aspx
Canada/ US	Action Plan for Critical Infrastructure	Strategy/Policy document	Aims to more effectively address a range of cross-border critical infrastructure issues and work together to share information/ best practices, identify interdependencies, and conduct joint exercises.	2010	www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cnd-ntdstts-ctnpln/index-en.aspx

Canada / US	Agreement on Emergency management cooperation	International agreement	Sets out principles for mutual bilateral cooperation during an emergency. It establishes the Canada – US Consultative Group	2008	www.treaty-accord.gc.ca/text-texte.aspx?id=105173
Canada / US	Framework for the movement of goods and people across the border during and following an emergency	Strategy/Policy document	Sets out principles for communication and border management in the event of an incident (including explicitly terrorist acts) that contribute to significant borer disruption.		www.publicsafety.gc.ca/cnt/ntnl-scrt/crtcl-nfrstrctr/cnd-ntd-stts-frmwrk-en.aspx
Canada/ US	Action Plan for Critical Infrastructure	Strategy/Policy document	Aims to more effectively address a range of cross-border critical infrastructure issues and work together to share information/ best practices, identify interdependencies, and conduct joint exercises.	2010	www.publicsafety.gc.ca/cnt/rsrcs/pblctns/cnd-ntdstts-ctnpln/index-en.aspx

China	Critical Information Infrastructure Security and Protection Regulations (Draft)	Normative instrument	First draft of national law aimed at defining China's policies on the protection of CIIs.	2017	https://chinacopyrightandmedia.wordpress.com/2017/07/10/critical-information-infrastructure-security-protection-regulations/ (Unofficial English

					translation)
France	Decree n° 2007-585 of 23 April 2007 on Certain Regulatory Provisions of the First Part of the Code of Defense (in French)	Normative instrument	Amends the Code of Defense 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 to 1332-42).	2007	https://www.legifrance.gouv.fr/affichTexte.do;jsessionid=B3D2B93BA4D5B3162AC56B149F71F4EC.tplgfr30s_3?cidTexte=JORFTEXT000000615627&dateTexte=20070424
France	White Paper on Defence and National Security	Strategy/Policy document	Sets forth the basic tenants for the protection of CI in the broader framework of France' s approach to national security	2013	http://www.livreblancdefenseetsecurite.gouv.fr/pdf/the_white_paper_defence_2013.pdf
France	Inter-ministerial Instruction on the security of activities of vital importance (n°6600/SGDSN/PSE/PSN du 7 janvier 2014)	Normative instrument	Adopted by the General Secretariat for Defence and National Security, the Instruction contains provisions for the implementation of France's institutional architecture on the protection on CI.	2014	http://circulaire.legifrance.gouv.fr/pdf/2014/01/cir_37828.pdf
France	National Digital Security Strategy	Strategy/Policy document	Sets out the strategic objectives and institutional approach to ensure the resilience of France against cyber-related threats, including threats against CII.	2015	https://www.ssi.gouv.fr/uploads/2015/10/strategie_nationale_securite_numerique_en.pdf
France	Plan Vigipirate	Strategy/Policy document	Envisages 300 measures covering 13 main areas of action such as transport, health and networks. These may be activated according to the evolution of the threat and vulnerabilities. On the basis of the assessment of the terrorist threat made by intelligence services, the General Secretariat for Defense and National Security issues guidelines determining the measures to be implemented by the actors concerned with vigilance, prevention and protection from threats of terrorist action. CI operators have to translate the measures of the VIGIPIRATE plan into their own security plans.	2015	http://www.gouvernement.fr/sites/default/files/risques/pdf/brochure_vigipirate_gp-bd_0.pdf
Germany	National Strategy for Critical Infrastructure Protection	Strategy/Policy document	Summarizes the Federal Administration's aims and objectives and its political-strategic approach. The Strategy is also the starting point for consolidating the results achieved so far and for further developing them in view of novel challenges.	2009	https://www.kritis.bund.de/SharedDocs/Downloads/BBK/EN/CIP-Strategy.pdf?__blob=publicationFile

Germany	Protection of Critical Infrastructures – Baseline Protection Concept – Recommendations for Companies	Guidelines/ Practical manual	Elaborated by the Federal Ministry of the Interior, the Federal Office for Civil Protection and Disaster Response and the Federal Criminal Police Office, with expertise from the business community, the document provides companies in Germany with recommendations from the point of view of internal security.	2006	https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/Baseline%20Protection%20Concept.pdf?__blob=publicationFile
Germany	Cyber Security Strategy for Germany	Strategy/Policy document	Provides the axes of the national policy on cyber security.	2011	https://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_engl_download.pdf?__blob=publicationFile
	National Plan for Information Infrastructure Protection	Strategy/Policy document	Aims at the full protection of CII in Germany by posing three strategic objectives: prevention, preparedness, sustainability	2005	http://www.qcert.org/sites/default/files/public/documents/GER-PL-National%20Plan%20For%20Information%20Infrastructure%20Protection-Eng-2005.pdf
Germany	CIP Implementation Plan of the National Plan for Information Infrastructures Protection	Strategy/Policy document	The Implementation Plan is an IT security guideline for CI operators. It aims to assist political decision-making and national and international cooperation. It is recommended to companies as a guideline for implementing an adequate IT security level.		https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/CIP%20Implementation%20Plan.pdf?__blob=publicationFile
Germany	UP Kritis - Public-Private Partnership for Critical Infrastructure Protection	Strategy/Policy document	Overview of the achievements and a new vision for Germany’s public-private partnership programme on CIP.	2014	https://www.kritis.bund.de/SharedDocs/Downloads/Kritis/EN/UP%20KRITIS.pdf?__blob=publicationFile
Japan	The Basic Policy of Critical Information Infrastructure Protection	Strategy/Policy document	Established to serve as the basis for the policy related to information security measures for Japan's CI.	2015	https://www.sbs.ox.ac.uk/cybersecurity-capacity/system/files/actionplan_ci_engv3_r1.pdf

Japan	Cyber Security Strategy	Fact sheet	Sets out national priorities and goals on cyber security and devotes a section to CIIP	2015	https://www.nisc.go.jp/eng/pdf/cs-strategy-en-pamphlet.pdf
Japan	National Security Strategy	Strategy/Policy document	Establishes the country's fundamental approaches to national security and its objectives. While it does not directly refer to CI, it foresees the strengthening of measures that have a direct impact on CI, such as enhancing maritime and cyber security, intelligence capabilities, etc.	2013	http://www.mofa.go.jp/fp/nsp/page1we_000081.html
Japan	Basic Cyber Security Act	Normative act	The first cybersecurity-specific law enacted among the G7 nations. It prescribes, in addition to the cybersecurity duties of the state and the local authorities, the cybersecurity duties of CI operators, universities and other educational or research institutions in the economic field. It envisages that, in the future, duties for these business operators may be prescribed in further detail by more specific laws.	2014	http://www.japaneselawtranslation.go.jp/law/detail_main?re=02&vm=02&id=2760
Malaysia	CNII Portal	Coordination centre	Online portal in which the critical infrastructure operators work together by sharing information on security issues. It provides information about the National Cyber Security Policy, which seeks to address the risks to the Critical National Information Infrastructure (CNII) in ten critical sectors.		https://cnii.cybersecurity.my/main/index.html
Netherlands	Resilient Critical Infrastructures	Information brochure / Factsheet	Prepared by the National Coordinator for Security and Counter Terrorism, the factsheet illustrates the shift, occurred in 2014, in the approach followed by the Government in its CIP policy.	2018	https://english.nctv.nl/binaries/Factsheet%20Critical%20Infrastructure%20ENG%202018_tcm32-240750.pdf
New Zealand	National Security System Handbook	Strategy/ Policy document	Sets out New Zealand's arrangements with respect 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.	2016	www.dpmc.govt.nz/sites/default/files/2017-03/dpmc-nss-handbook-aug-2016.pdf
New Zealand	Cyber Security Strategy	Strategy/ Policy document	Sets out national priorities and goals on cyber security and devotes a section to CIIP.	2015	www.dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-strategy-december-2015.pdf

New Zealand	National Cyber Security Centre (NCSC)	Coordination centre	Established in 2011, it focuses on providing specialist security advice and support to New Zealand’s most significant organizations and information systems. This includes government departments, key economic generators, niche exporters, research institutions and operators of critical national infrastructure. NCSC assists these entities to protect their networks from the types of threats which are typically beyond the capability of commercially available tools, and from threats which could potentially impact on the effective functioning of government administration or key economic sectors.	2011	https://www.ncsc.govt.nz/
New Zealand	Cyber Security Strategy: Action Plan Annual Report	Policy document/ report	Supports the Cyber Security Strategy by seting out concrete steps to protect the country’s information technology systems.	2015	www.dpmc.govt.nz/sites/default/files/2017-03/nz-cyber-security-action-plan-december-2015.pdf
New Zealand	Cyber Security Strategy: Action Plan Annual Report	Policy document/ report	It is the first Annual Report on the implementation of the objectives set forth in the 2015 Cyber Security Strategy and Action Plan.	2016	www.dpmc.govt.nz/sites/default/files/2017-06/nzcss-action-plan-annual-report-2016.pdf
Poland	National Critical Infrastructure Protection Program	Strategy/Policy document	Sets out the basic concepts of CIP in Poland and the division of labor among stakeholders on the basis of the legal principles and definitions contained in the 2007 Act on Crisis Management.	2015	http://rcb.gov.pl/wp-content/uploads/NPOIK-2015_eng-1.pdf
Poland	National Security Strategy	Strategy / Policy document	Identifies national interests and strategic objectives in the domain of security. Under its section on “protective actions”, the national security strategy explicitly mentions CIP.	2014	https://www.bbn.gov.pl/ftp/dok/NSS_RP.pdf
Russian Federation	Law on security of critical information infrastructure	Normative instrument	Sets out the basic foundations and principles for ensuring security of Russia’s CIs, including the foundations for the functioning of the state system for detecting, preventing and liquidating the consequences of cyberattacks against Russian Federation information resources. This is a unified system, distributed across the country and endowed with the capability and resources needed to detect, prevent and liquidate the consequences of cyberattacks and respond to cyber incidents. The Federal Law sets out the mechanism for preventing cyber incidents at important components of CIIs. It defines the powers of state bodies for ensuring the security of CII and the rights and obligations of the various actors in this area.	2017	http://en.kremlin.ru/acts/news/55146

Senegal	National Cyber Security Strategy	Strategy / Policy document	includes the following elements: -an assessment of the strategic context of cybersecurity in Senegal, including current and future threats; -Government's vision for cybersecurity and strategic objectives to reach; -General principles, roles and responsibilities that may strengthen the said strategy; -Ghe logical framework for its implementation. Strategic Objective 2 deals specifically with "Strengthen[ing] Infrastructure Protection Critical Information Systems (CII) and the information systems of the State of Senegal".	2017	www.numerique.gouv.sn/sites/default/files/SNC2022-vf.pdf
Singapore	National Security Strategy	Strategy/ Policy document	Explains Singapore's security priorities and the strategy adopted to counter terrorism. It establishes the national security architecture, which organizes the various agencies around the three essential security pillars of policy, operations and capability development and the coordination role of a National Security Coordination Secretariat.	2004	https://www.nscs.gov.sg/public/download.ashx?id=1031
Singapore	Cyber Security Strategy	Strategy/ Policy document	Sets out Singapore's vision, goals and priorities for cybersecurity, including on strengthening the resilience of CII.	2016	https://www.csa.gov.sg/~/media/csa/documents/publications/singaporecybersecuritystrategy.pdf
Singapore	Cyber Security Agency	Coordinating center	Oversees the country's cybersecurity strategy. It is part of the Prime Minister's Office and is managed by the Ministry of Communications and Information. Among its goals is protecting critical sectors such as energy, water, and banking.		https://www.csa.gov.sg/
Singapore	Infrastructure Protection Bill	Normative instrument	Introduced as part of the Ministry of Home Affairs' counter-terrorism strategy to protect buildings which house essential services, or with high human traffic. It seeks to ensure that there are adequate building security measures in place as a means to help deter and deny attackers, as well as minimize casualties and damage in an attack.	2017	file:///Users/SM/Downloads/Infrastructure%20Protection%20Bill.pdf
Singapore	Cyber Security Bill	Legislative instrument	The Bill pursues four objectives: - To provide a framework for the regulation of Critical Information Infrastructure (CII). This formalises the duties of CII owners in ensuring the cybersecurity of their respective CIIs. - To provide the Cyber Security Agency (CSA) with powers to manage and respond to cybersecurity threats and incidents.	2017	https://www.csa.gov.sg/~/media/csa/cybersecurity_bill/draft_cybersecurity_bill_2017.ashx?la=en

			- To establish a framework for the sharing of cybersecurity information with and by CSA, and the protection of such information. - To establish a light-touch licensing framework for cybersecurity service providers.		
Spain	Law 8/2011 establishing measures for the protection on CIs (in Spanish)	Normative instrument	Seeks to coordinate the actions of all public bodies and promote collaboration and involvement of CI owners and operators. The law transposes into national legislation the measures included in EC Directive 2008/114 / EC, in particular the identification and classification of European critical infrastructures.	2011	http://www.cnpic.es/Biblioteca/Legislacion/Generico/Ley_8-2011_PIC.pdf
Spain	Normative instrument	Royal Decree 704/2011 approving Regulations for the protection of critical infrastructures (in Spanish)	Implements the framework provisions contained in Law 8/2011.	2011	http://www.cnpic.es/Biblioteca/Legislacion/Generico/REAL_DECRETO_704-2011_BOE-A-2011-8849.pdf
Spain	Coordinating centre	National Centre on the Protection of Critical Infrastructures and Cyber Security	Ministerial body in charge of promoting, coordinating and supervising all the activities entrusted by the Ministry of the Interior's y in relation to CIP in the national territory.	2007	http://www.cnpic.es/index.html
Spain	Strategy/Policy document	National Security Strategy (in Spanish)	Threats to CI are fully integrated into the document as threats to national security.	2017	http://www.cnpic.es/Biblioteca/Eventos/Estrategia_Seguriad_Nacional_2017.pdf
Spain	Strategy/Policy document	National Cyber Security Strategy (in Spanish)	Sets out the objectives and approaches of Spain's strategy, among which those relevant for the protection of CI.	2013	https://www.ccn-cert.cni.es/publico/dmpublidocuments/EstrategiaNacionalCiberseguridad.pdf
Sweden	Action Plan for the Protection of Vital Societal Functions and Critical Infrastructures	Strategy/Policy document	Prepared by Sweden's Civil Contingency Agency, the Action Plan creates conditions allowing all Vital Societal Functions and Critical Infrastructures to have implemented systematic safety work into their operations locally, regionally and nationally by 2020.	2014	https://www.msb.se/RibData/Filer/pdf/27412.pdf
Sweden	Guide to increased security in industrial	Strategy/Policy document	Prepared by Sweden's Civil Contingency Agency, the guide provides 17 basic recommendations for increasing security and, through its widespread	2014	https://www.msb.se/RibData/Filer/pdf/27473.pdf

	information and control systems		distribution, has achieved its status as a Swedish industry standard. The recommendations are based on internationally recognized standards, practices and working methods.		
Sweden	National Risk and Capability Assessment	Strategy/Policy document	Submitted by the Civil Contingency Agency to the Government on a yearly basis, the Assessment provides a strategic groundwork for the direction and further development of civil contingencies.	2016	https://www.msb.se/en/Prevention/National-risk-and-capability-assessment/
Switzerland	National Strategy for CIP 2018-2022	Strategy/Policy document	Adopted by the Federal Office on the Protection of the Population, it updates the original strategy issued in 2012 by setting forth higher objectives for its stakeholders. The revised strategy is supposed to translate accomplished work into an institutionalized process, to fix it in legislation and to supplement it on an ad hoc basis.	2017	https://www.babs.admin.ch/fr/aufgabenbabs/ski.html
Switzerland	National Strategy on Protection against Cyber Risks	Strategy/Policy document	Through this strategy, the Federal Council, in close collaboration with the business community and the CI operators, seeks to reduce cyber risks to which all these actors are exposed daily. The strategy includes 16 measures to be implemented until 2017. A new strategy will enter into force in 2018.	2012	https://www.isb.admin.ch/isb/fr/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html
United Kingdom	National Security Strategy	Strategy/Policy document	Lays out the pillars and objectives of the country's vision to protect national security. It devotes a section to Cis.	2015	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf
United Kingdom	Centre for the Protection of National Infrastructures	Coordinating centre	Provides protective security advice to businesses and organizations across the national infrastructure. Advice aims to reduce the vulnerability of the CIs to terrorism and other threats.	2007	https://www.cpni.gov.uk/
United Kingdom	National Cyber Security Centre	Coordinating centre	Provides advice and support for the public and private sector in how to avoid computer security threats.	2016	https://www.ncsc.gov.uk/
United Kingdom	Sector Security and Resilience Plan 2017	Strategy/Policy document	Sets out the resilience of the UK's most important infrastructure to the relevant risks identified in the National Risk Assessment. Produced annually, plans are placed before ministers to alert them to any perceived vulnerabilities, with a programme of measures to improve resilience where necessary.	2017	https://www.gov.uk/government/collections/sector-resilience-plans

			Individual plans are classified, but the Cabinet Office summarizes each version into one overall sector resilience plan for critical infrastructure.		
United Kingdom	National Risk Register of Civil Emergencies	Policy document (public version)	Provides an overview of the key risks that have the potential to cause significant disruption in the UK. Explains the types of emergencies that might occur, what the Government and partners are doing to mitigate them, and how you as individuals, families or small businesses can help to protect yourself. A number of sections directly address the protection of CI against malicious/terrorist acts.	2017	https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/644968/UK_National_Risk_Register_2017.pdf
Ukraine	Green Paper on Critical Infrastructure Protection in Ukraine	Strategy/Policy document	Formulates strategic public policy objectives in the area of critical infrastructure protection in Ukraine.	2015	http://en.niss.gov.ua/content/articles/files/niss_EnglCollection_druk-24cce.pdf
Ukraine	Decision of the National Security and Defense Council on improvement of measures to ensure the protection of critical infrastructure objects (put into effect by Presidential decree of 16 January 2016 No 8/2017)	Normative instrument	Sets a timetable for the gradual establishment of a comprehensive national CIP policy and legal framework	2016	http://en.niss.gov.ua/content/articles/files/niss_EnglCollection_druk-24cce.pdf
USA	Strategic National Risk Assessment	Strategy/Policy document	Conducted by the Secretary of Homeland Security, it seeks to identify the types of incidents that pose the greatest threat to the Nation's homeland security. Critical assets, systems, and networks face many of the categorized threats, including terrorists and other actors seeking to cause harm and disrupt essential services.	2011	https://www.dhs.gov/xlibrary/assets/rma-strategic-national-risk-assessment-ppd8.pdf
USA	National Infrastructures Protection Plan (NIPP)	Strategy/Policy document	Outlines how government and private sector participants in the CI community work together to manage risks and achieve security and resilience outcomes.	2013	https://www.dhs.gov/sites/default/files/publications/national-infrastructure-protection-plan-2013-508.pdf
USA	Presidential Policy Directive 21 (PPD-21): Critical Infrastructure	Normative instrument	Directs 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	2013	https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/

	Security and Resilience		-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 plan		presidential-policy-directive-critical-infrastructure-security-and-resil
USA	Executive Order (EO) 13636: Improving Critical Infrastructure Cybersecurity	Normative instrument	Directs the Executive Branch to: -Develop a technology-neutral voluntary cybersecurity framework -Promote and incentivize the adoption of cybersecurity practices -Increase the volume, timeliness and quality of cyber threat information sharing -Incorporate strong privacy and civil liberties protections into every initiative to secure our critical infrastructure -Explore the use of existing regulation to promote cyber security	2013	https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
USA	NIPP Security and Resilience Challenge	Funding mechanism	Provides an opportunity for the CI community to help develop technology, tools, processes, and methods that address immediate needs and strengthen the long-term security and resilience of critical infrastructure. It helps identify and fund innovative ideas that can provide technologies and tools to the CI community that are ready or nearly ready to use.	2017	https://www.dhs.gov/sites/default/files/publications/nipp-challenge-overview-fact-sheet-2017-508.pdf

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 governmental 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 Executive Directorate (CTED) 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 – THE COUNTER-TERRORISM IMPLEMENTATION TASK FORCE (CTITF)

The United Nations Secretariat, agencies, funds and programmes, and affiliated organizations contribute to the implementation of the United Nations Global Counter-Terrorism Strategy both through their individual mandates and through their membership in the Counter-Terrorism Implementation Task Force.

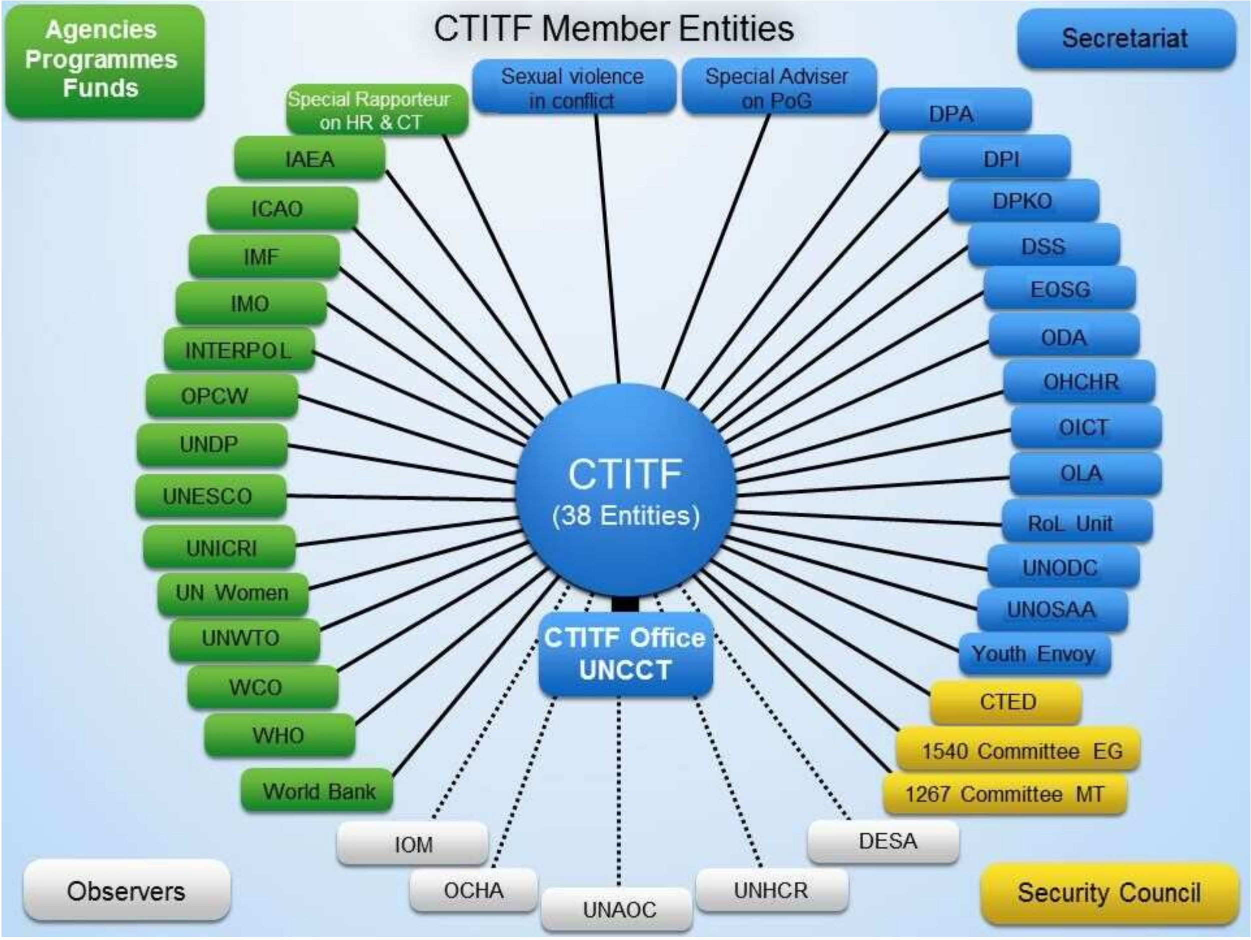
The Task Force consists of 38 international entities and INTERPOL which by virtue of their work have a stake in multilateral counter-terrorism efforts. Each entity makes contributions consistent with its own mandate. The members of the Task Force are:

1. Al Qaida/Taliban Monitoring Team
2. Counter-terrorism Committee Executive Directorate (CTED)
3. Department of Peacekeeping Operations (DPKO)
4. Department of Political Affairs (DPA)
5. Department of Public Information (DPI)
6. Department of Safety and Security (DSS)
7. Group of Experts of 1540 Committee
8. International Atomic Energy Agency (IAEA)
9. International Civil Aviation Organization (ICAO)
10. International Maritime Organization (IMO)
11. International Monetary Fund (IMF)
12. International Criminal Police Organization (INTERPOL)
13. Office for Disarmament Affairs (ODA)
14. Office of the High Commissioner for Human Rights (OHCHR)
15. Office of Legal Affairs (OLA)
16. Office of the Secretary-General (OSG)
17. Office of The Special Adviser on The Prevention of Genocide
18. Office of the Special Representative of the Secretary-General on Children and Armed Conflict (CAC)
19. Office of the Secretary-General's Envoy on Youth
20. Organization for the Prohibition of Chemical Weapons (OPCW)
21. Special Rapporteur on the promotion and protection of human rights while countering terrorism
22. United Nations Development Programme (UNDP)
23. United Nations Educational, Scientific and Cultural Organization (UNESCO)
24. United Nations Interregional Crime and Justice Research Institute (UNICRI)
25. United Nations Office on Drugs and Crime (UNODC)
26. United Nations Office of the Special Adviser on Africa (OSAA)
27. United Nations Rule of Law Unit
28. UN Women
29. United Nations World Tourism Organization (UNWTO)
30. World Customs Organization (WCO)

31. World Bank
32. World Health Organization (WHO)

Observers

33. International Organization for Migration (IOM)
34. Office of the Coordinator for Humanitarian Affairs (OCHA)
35. United Nations Department for Economic and Social Affairs (DESA)
36. United Nations High Commissioner for Refugees (UNHCR)
37. United Nations Alliance of Civilizations (UNAOC)



Within the Task Force, a Working Group has been established on Protection of Critical Infrastructure including Vulnerable Targets, Internet and Tourism Security.

Mandate:

The mandate of the Working Group is drawn from the United Nations Global Counter-Terrorism Strategy (A/RES60/288):

- *"To work with the United Nations with due regard to confidentiality, respecting human rights and in compliance with other obligations under international law, to explore ways and means to: (a) Coordinate efforts at the international and regional levels to counter terrorism in all its forms and manifestations on the Internet" (Section II, paragraph 12);*

- *"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." (Section II, paragraph 18);*

- *"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."* (Section III, paragraph 13)

Considering that the Global Counter-Terrorism Strategy reaffirms "that the promotion and protection of human rights for all and the rule of law" as "essential to all components of the Strategy", the Working Group integrates a human rights perspective into its work.

Objectives:

The objectives of the CTITF Working Group on the Protection of Critical Infrastructure including Vulnerable Targets, Internet and Tourism Security are:

- to establish appropriate mechanisms to facilitate the development and sharing of best practices on the protection of vulnerable sites, public spaces or critical infrastructure that carry importance for their respective States and regions, or are of international importance;
- to strengthen the capacity of both public and private sectors and to increase the development of public and private partnerships on protection of critical infrastructure, including Internet, cyber and tourism security, in order to prevent and react in an efficient manner to potential risks and threats to related facilities, including by promoting awareness and understanding of the necessary balance between economic and security issues.
- to improve responsiveness and resilience by promoting methods of planning, prevention, crisis management and recovery;

- to promote the exchange of information and best practices and establish a network of experts;
- to support States in the implementation of the provisions of the UN Global Counter-Terrorism Strategy that are relevant to the Working Group's focus areas (as listed under 'Mandate' below).

Participating entities:

- International Criminal Police Organization (INTERPOL) (Chair)
- CTITF Office (Co Chair)
- Counter-Terrorism Committee Executive Directorate (CTED)
- Al-Qaida / Taliban Monitoring Team
- Department of Public Information (DPI)
- Office of the High Commissioner on Human Rights (OHCHR)
- Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism
- United Nations Educational, Scientific and Cultural Organization (UNESCO)
- UN Office on Drugs and Crime / Terrorism Prevention Branch (UNODC/TPB)
- Department of Safety and Security (DSS)
- United Nations Interregional Crime and Justice Research Institute (UNICRI)
- Department of Political Affairs (DPA)
- Department of Peacekeeping Operations (DPKO)
- International Civil Aviation Organization (ICAO)
- International Maritime Organization (IMO)
- United Nations Development Programme (UNDP)
- World Customs Organization (WCO)
- World Tourism Organization (UNWTO)
- Office for the Coordination of Humanitarian Affairs (OCHA)