PUBLIC - PRIVATE PARTNERSHIPS

A risk management approach to address security threats.

OEA Más derechos para más gente

unicri United Nations Interregional Crime and Justice Research Institute

OAS Cataloging-in-Publication Data

Public - Private Partnerships: A Risk Management Approach to Confront Security Threats [prepared by the Inter-American Committee against Terrorism of the General Secretariat of the Organization of American States (OAS/CICTE) and the United Nations Interregional Crime and Justice Research Institute (UNICRI)].

p. ; cm. (OAS. Official records; OEA/Ser.L/X.6.7)

ISBN 978-0-8270-7797-3

1. Security, International--Handbooks, manuals, etc. 2. Public-private sector cooperation--America--Handbooks, manuals, etc. 3. Public safety--Security measures--Handbooks, manuals, etc. I. Title. II. Organization of American States. Secretariat for Multidimensional Security. Interamerican Committee Against Terrorism. III. United Nations Interregional Crime and Justice Research Institute. IV. Series.

OEA/Ser.L/X.6.7

With the financial support of the Government of Canada

Canada

Review. Quick reference

The Public-Private Partnerships Manual represents a guide for the creation and strengthening of public-private partnerships in the Americas, focused on addressing and mitigating anthropogenic threats to security, such as terrorism and organized crime.

This Handbook updates and expands on the original published in 2010 by the United Nations Interregional Crime and Justice Research Institute (UNICRI). It was made possible thanks to a joint project between UNICRI and the Inter-American Committee against Terrorism of the Organization of American States (CICTE/OAS), and the financial support of Global Affairs Canada.

Its preparation is the result of the accumulated experience of the aforementioned entities and of the consultant in charge of its drafting[1] in a work that included the collaboration and validation of the focal points of the countries of the Americas, convened for this purpose.

> The objective of the Manual is to provide a working tool to promote, strengthen and support public-private partnerships in the prevention, detection, and control of anthropogenic security threats. It also seeks to motivate the actors involved to take the initiative to identify counterparts in both sectors and begin to work in the search for new and better results in terms of reducing security risks related to terrorist threats and organized crime.

Undoubtedly, public-private partnerships in the area of security have proven to be valuable tools for effectively and efficiently addressing various challenges in this area. Through two-way collaboration between the two sectors, innovative solutions have been accomplished, adding value to the projects, and increasing the positive rate of return. This updated Manual is intended to be an essential resource for all those working in the prevention and control of terrorism and organized crime as the main security threats in the region.

This Handbook is an essential document for those interested in establishing and strengthening public-private partnerships regarding security. This updated and expanded text offers a vast array of innovative tools and approaches to address the evolving security threats in the region.

[1] **Marko Magdic. International Consultant in Public Security and Organized Crime.**

It is necessary to read this manual for the following reasons:

* **Relevance and timeliness:** The text addresses current and important issues, such as terrorism and organized crime, and offers solutions based on public-private partnerships.

* **Comprehensive approach and appropriate methodologies:** The manual presents a comprehensive approach ranging from the definition of public-private partnerships to the design and management of joint projects. It also provides information on relevant aspects such as economics, gender policies and information processing.

* **Examples of success and clear objectives:** The document includes success stories of public-private partnerships in specific areas of the security environment and presents clear objectives to motivate stakeholders to identify partners and work together in pursuit of better security outcomes.

* **International collaboration and accumulated experience:** The manual is based on the experience of recognized institutions, such as UNICRI, CICTE/OAS, and expert personnel, which guarantees a well-founded approach supported by specialists in the field.

This handbook is highly recommended reading for those who would like to address the security challenges effectively and efficiently in the Americas by means of creating and strengthening public-private partnerships.

Key topics:

- *Definition and nature of public-private partnerships (PPP) for security.*
- *First steps to establish an effective public-private partnership for public security.*
- *Joint assessment of security problems and analysis of specific cases.*
- *Establishment of strategic alliances between the public and private security sectors.*
- *Design and management of joint projects with appropriate methodologies and creative thinking.*
- *Relevant aspects in the design of joint projects: the economic factor and gender policies.*
- *Information processing and challenges in data exchange between public and private entities.*
- *Building trust and overcoming challenges in public-private partnerships for security.*
- *Examples and ideas of successful cases of public-private partnerships in specific areas of security.*
- *Crisis Committee.*

Before starting

Before you begin reading the document, please answer the following questions, regardless of whether you or your entity is part of the public sector or is a member of the community or represents a non-state actor.

The answers and your score will determine if the document may actually be useful and suitable for your needs.

Question	Yes	No
Has your entity, organization or the group of affiliates, members or persons that composes it, been affected by the problems or negative externalities derived from a threat to public security?	1	0
Have you assessed the problem and identified both the factors that make it possible and those that could counteract it?	0	1
Have you done anything in this regard that has resulted in satisfactory results?	0	1
Do you consider it is possible to do more?	1	0
Does your entity or organization have specific objectives to proactively address the problems and negative externalities arising from a threat to public safety?	0	1
Are you currently implementing projects in these areas to prevent, control, early detect or respond to these threats?	0	1
Are you implementing these projects in the framework of a joint and active public-private partnership?	0	1
Do you believe that by doing the same, your results will not change, and therefore a change in the way you face some of your public security challenges is required?	1	0

If you or your entity answered all the questions and the result of adding up the answers is at least 2 points, then we recommend that you read this manual.

The initiative should be taken in identifying counterparts in both sectors, and thus, start working towards new and/or better results. How? This Manual will not solve all your questions, nor will it provide you with absolutely all the elements, but it will be a great first step.

Table of contents

Background

In 2010, the United Nations Interregional Crime and Justice Research Institute (UNICRI) published a Handbook[2] to support the establishment of public-private partnerships to protect vulnerable targets. The Manual was developed within the context of the Counter-Terrorism Implementation Task Force (CTITF).

By 2021, just over 11 years had passed since the launch of this important effort. The threats of a decade ago had experienced major changes, and so had the targets they were directed against.

Aware of this reality, UNICRI, together with the Inter-American Committee against Terrorism of the Organization of American States (CICTE/OAS), and with the financial support of the Government of Canada, decided to give new inertia to the benefits generated in the past with the aforementioned initiative, they therefore set out to promote a new Manual that, taking up the best practices of the document that preceded it, would provide new working tools that would be functional for the current security risks and for optimizing public-private partnerships to prevent, detect and respond to the various security threats.

The support and active participation of the Inter-American Committee against Terrorism of the Organization of American States made it possible to generate data collection and validation activities with individual experts and government representatives from the countries of the Americas, which explains why a significant part of the observations, comments and analyses related to the main threats, were linked to that region.

It was precisely this scenario of regional analysis and consultation that made it possible to validate and define the routes to follow in terms of the type of threats to be addressed, as well as the recommended moment of intervention for a public-private partnership.

With regard to the first point, one of the main threats to security in the Americas was determined as being related to anthropic, man-made threats that have a direct impact on public security in its various forms, although preferably regarding terrorism and organized crime (drug trafficking, arms trafficking, human trafficking and smuggling, contraband, money laundering and corruption, among others).

With regard to the second point, the regional consultations and meetings held, identified not only response to incidents and threats affecting security as a priority, but also prevention mechanisms on the one hand, and early detection mechanisms, on the other, in which the public and private sectors collaborate and work together in an alliance format. Hence the emphasis given to this manual.

[2] ***Handbook to assist the establishment of public private partnerships for the protection of vulnerable targets (UNICRI - 2010).*** **Available in English, Spanish and Portuguese.**

Initiative managers

Inter-American Committee Against Terrorism of the Organization of American States (CICTE/OAS)

> The General Secretariat of the Organization of American States (GS/OAS), through the Secretariat for Multidimensional Security (SMS), promotes and coordinates cooperation among the OAS Member States, and between them and the Inter-American System and other bodies of the International System, to assess, prevent, address and respond effectively to security threats, with the vision of being the main hemispheric reference for the development of cooperation and the strengthening of the capacities of all OAS Member States.

The Executive Secretariat of the Inter-American Committee against Terrorism (SE/CICTE) supports Member States in the design, implementation, and evaluation of national policies to prevent, combat and eliminate terrorism and strengthen their counterterrorism capacity, as well as in the design and execution of initiatives to strengthen their institutional capacities in this area. The security program for crowded spaces has more than 15 years of experience in the implementation of national strategies aimed at improving the capacity of OAS Member States, through the training of law enforcement officials, in the design and effective implementation of integrated security plans for the protection of crowded spaces and vulnerable targets, such as major events and/or tourist destinations.

United Nations Interregional Crime and Justice Research Institute

UNICRI is a United Nations agency established in 1967 to support countries in preventing crime and facilitating criminal justice. In this area, UNICRI supports intergovernmental, governmental, and non-governmental organizations in the formulation and implementation of improvement policies. UNICRI's goals are to advance understanding of crime-related problems; promote fair and efficient reforms of criminal justice systems; promote compliance with international instruments and other standards; and facilitate international police cooperation and judicial assistance.

Collaboration and appreciation

The production of this Manual was made possible thanks to the collaboration of several people and entities that deserve the gratitude of the managers of this initiative.

* To Marko Magdic, senior consultant in public security and organized crime, main drafter of this Manual.[3]

* To the working team of the Crowded Space Security Program of the Inter-American Committee Against Terrorism (CICTE) of the Organization of American States (OAS).

* To the working team of the United Nations Interregional Crime and Justice Research Institute (UNICRI).

* To the representatives of the OAS Member States who participated in the activities and validated the information that motivated this report.

[3] **Marko Magdic is a senior consultant with 20 years of experience in justice, public security, and organized crime, having participated in operational and strategic projects related to public policy and corporate and governmental risk prevention and control. He has worked in the design and execution of public-private exercises, simulations, and drills in Latin America, and has participated in the design and implementation of strategies and action plans on issues such as UN Resolution 1325, bioterrorism, cybersecurity, organized crime, nuclear and radiological security. In recent years, Magdic has focused his expertise on tourism security, organized crime, and terrorism projects, serving as a senior consultant in the Tourism Security Program of the Organization of American States. He has contributed to the preparation of the Regional Report on Tourism Safety in Mexico, Central America and the Caribbean 2016 - 2019, and collaborated in the design and optimization of national strategies and action plans for tourism safety at both the governmental and regional levels. He complements the foregoing with work on projects and initiatives in more than 30 countries in collaboration with various international organizations and governmental entities in the areas of organized crime, terrorism, and tourism security. Magdic is a member of the World Association of Prosecutors (WAP), the Global Initiative against Transnational Organized Crime (GITOC), the American Bar Association, and Lawyers Without Borders Canada, among others.**

Objective

To provide a working instrument containing tools to promote, strengthen and support public-private partnerships in the Americas aimed at preventing, detecting, and controlling anthropogenic threats to security, with a special focus on security.

Methodology and context

As can be seen from the objective of this Manual, the tool is structured around three variables that give it context and a concrete analysis framework:

* Anthropic threats, originated from intentional human activity.
* Anthropic threats to security.
* Anthropic threats to security in the Americas.

The preparation of this document took into account the inputs contained in the Manual prepared in 2010 by UNICRI, the experience of the main consultant in charge of the project, the contributions of the national contact points designated by the Member States of the Organization of American States, as well as the experience of both the OAS and UNICRI, who with various strategic partners, have developed work programs in recent years and have accumulated knowledge, with the countries of the region, in the areas of tourism security, security of major events and critical infrastructure security.

It is complemented by a series of technical meetings held to gather information and validate the focus and type of the main threats, as well as to obtain feedback. The activities conducted were as follows:

01 **Caribbean:**
Sub-regional Workshop on Security of Major Sporting Events: Premier League Cricket CPL T20. Virtual. February 23-25, 2021.

02 **South America:**
South American sub-regional workshop on Security at Major Sporting Events. Virtual. 29-31 March, 2022.

03 **Costa Rica:**
National Workshop on Major Event Security: FIFA U-20 Women's World Cup Copal. Face-to-face. July 18-21, 2022

04 **Dominican Republic:**
Regional Workshop on Tourism Security. November 15-17, 2022.

05 **Chile:**
National Workshop on Major Event Security: 2023 Pan American Games. Face-to-face. January 24-27, 2023

06 **Central America:**
Subregional workshop for Central America, the Dominican Republic and Mexico on Security at Major Sporting Events. Face-to-face. March 21-23, 2023

Current risks, threats and vulnerabilities

This chapter will address the current risks, threats and vulnerabilities facing the Americas in terms of security. The nature and impact of the most relevant threats in the region will be analyzed, as well as how the materialization probability of these threats is influenced by different vulnerability factors and the importance of addressing these challenges through public-private partnerships, generating a coordinated and comprehensive response.

Security risks are defined as the probability level that a given security threat will materialize. The degree of probability, in turn, is conditioned by the vulnerabilities present at a given time. The Americas face a variety of security threats that are varied, dynamic and relatively concentrated in some sub-regions.

These threats can be divided into two main groups:

***Results threats** (terrorism and organized crime)*

***Means threats** (corruption, money laundering and channeling of social demands through organized and non-spontaneous violence).*

The materialization probability of these threats depends on the vulnerability level to which the region is exposed. Vulnerabilities can be classified as internal (or management) and external (or environmental).

Risks

Talking about threats leads us to discuss a broader concept: Risks. Indeed, and taking into account the above-mentioned context, security risks can be conceived as the probability degree that a security threat will materialize. The greater or lesser probability level of this occurring will depend, in turn, on the vulnerabilities present at any given time.

We could also say that greater or lesser vulnerability is influenced by the way in which we organize and address these threats.

Schematic 1. Risks. Prepared by Marko Magdic

This means that we must first address the threats, and then move on to vulnerabilities.

Threats

Today, as we enter the second decade of the 21st century, the security threats facing the Americas are varied, dynamic and relatively concentrated. They are varied, as in that they are multiple. They are dynamic because they are changing and manifest themselves in constant evolution, if not in the type of threat, at least in the form and manner in which it is manifested. Finally, they have relative concentration, because although they are all-encompassing to the continent, some subregions have higher levels of intensity than others.

The information gathered in the various activities mentioned in the methodology section of this report showed that while arms trafficking was of greater concern in some Caribbean countries, extortion was a more critical phenomenon for Central American nations, while drug trafficking and contraband were recurrently mentioned by South American representatives.

The above statement is not intended to be a complete and formal assessment of what type of criminal phenomenon impacts which country or region, but rather to confirm the dynamism and concentration mentioned in previous paragraphs.

If we were to list all the threats in the region, the list would be extensive, which leads us to list those that we consider most relevant at present. The dynamism of each of them makes it necessary to constantly evaluate and monitor in order to have an updated knowledge of the way in which they operate and the geographic area in which they have the greatest presence.

Among the main threats, we consider two major groups. The first, which we could call outcome threats, and the second, means threats.

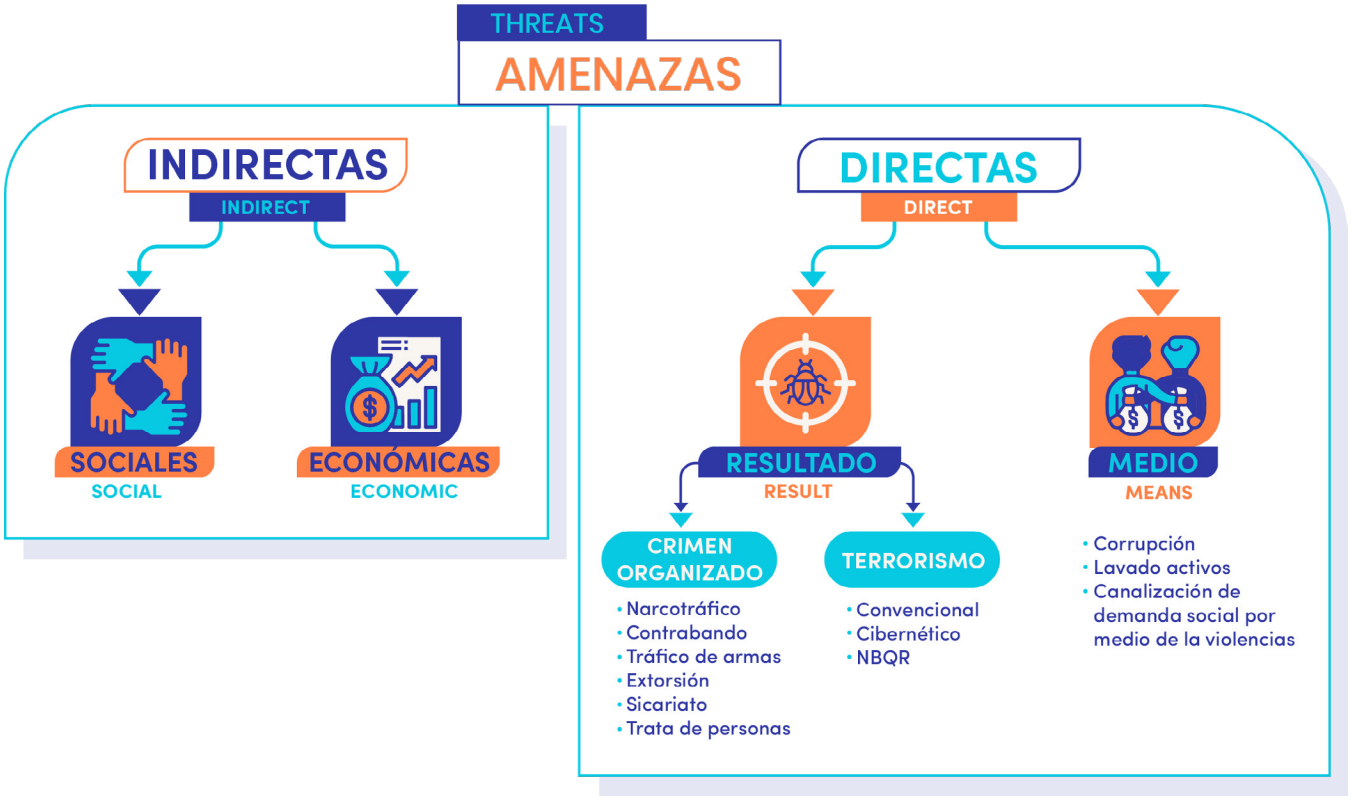
> Those of outcome are all those that, due to the way they materialize, may cause direct and immediate security damage. They are of more immediate perception. They are represented, in our view, by terrorism and organized crime. The types of terrorism we consider are conventional or classic terrorism, bioterrorism (including all those that consider the use of chemical, radiological, biological and/or nuclear elements), and cyberterrorism.

In terms of organized crime, we consider drug trafficking, contraband, arms trafficking, extortion, what is known as "sicarios" and human trafficking, as the most critical threats in the region.

They are not the entirety of them, but they are the most important ones and the ones that are generating the greatest level of damage. When terrorism and organized crime come together, the impact and challenge is even greater, as in the case of narcoterrorism, or the use of criminal activities as a means to finance terrorist activities.

The second group of threats are either a means or an effect of the first group. These are the following: corruption, money laundering and the channeling or organization of social demands through organized rather than spontaneous violence. Even when these cause damage by themselves, they would be meaningless without the first group. They are functional when both have a symbiotic and mutually beneficial relationship.

This classification is not random, because even though it goes beyond the scope of this paper, the way of approaching one and the other will not be the same.



Schematic 2. Threats. Prepared by Marko Magdic.

Vulnerabilities

The likelihood that these threats will materialize will depend on the level of vulnerability to which the continent, as well as the countries and subregions, are exposed. Several factors influence the degree of vulnerability, both internal and external. This is a distinction that will lead us more directly to public-private partnerships.

In this study, we have classified vulnerabilities into two categories. On the one hand, there are the *internal or management* ones, which refer to the way in which the State, civil society, the private sector, and the community address security threats, which are made up of variables such as strategic planning, operational response, provision and use of resources, legal framework, etc. On the other hand, we call *external or environmental* vulnerabilities those that, regardless of the direct response to threats, generate and/or represent conditions that facilitate or hinder them. These include variables associated with the level of economic development, poverty, social vulnerability, intensity of state presence, labor, and market informality, among others.

While the conditions and factors of *external or environmental vulnerability* will not be addressed by this work, the internal elements are the ones that will occupy us at this time, in order to identify how they increase or reduce the probability that a threat will materialize and generate damage to public security in our region.

In other words, they are the internal organizational and response aspects of the environment in which they take place.

Thus, and in more concrete terms as far as *internal vulnerabilities* are concerned, today we must consider as a challenge to be addressed the need to optimize and further improve the institutional capacities that allow us to work efficiently in the following areas, which we consider essential in view of the need to promote, increase, and encourage public-private partnerships:

* Economic approach to security threats
* Proactivity
* Coordinated and comprehensive response

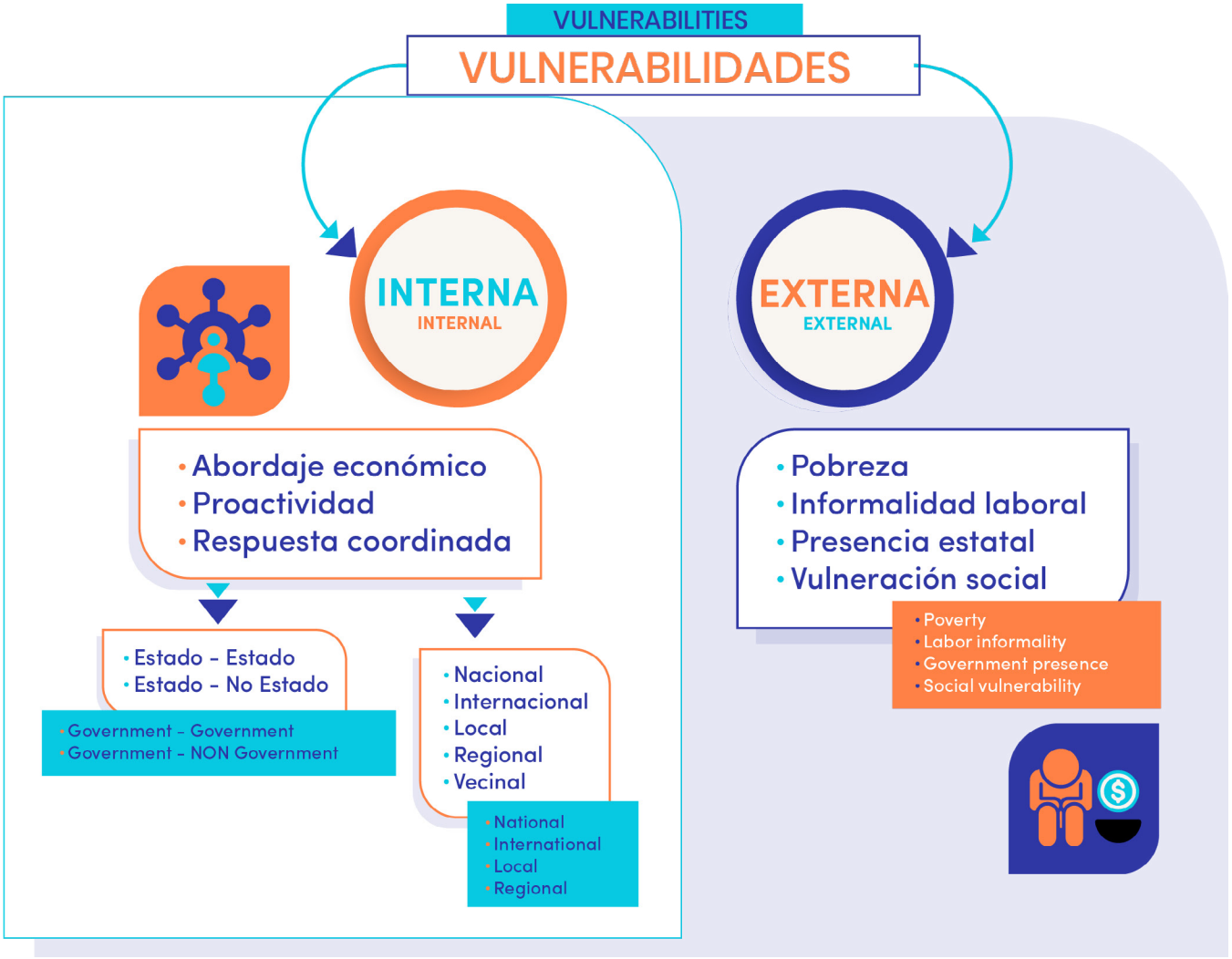
Addressing and **approaching** threats **economically** entails taking into account that, with the exception of some exceptional cases of purely ideological terrorism, the rest of the threats described are motivated and conceived in pursuit of an economic interest.[4] Whoever participates in them wishes to illicitly increase their own capital and/or that of third parties or entities. It is therefore important to address these phenomena by aiming to cause an impact on the illicit assets acquired by criminal groups.

[4] Of course, crimes, such as homicides, may have other motivations, such as personal or passion ones. However, in this section we analyze those phenomena associated with organized crime and terrorism.

Addressing threats with a **proactive approach** is important by working in public-private partnerships that not only address security problems once the events or acts have been denounced and reported, but also work on prevention and early detection.

Finally, one of the factors that has the greatest impact on the vulnerability level in relation to prevention, detection, and response capabilities in relation to security threats, is the need to increase and further strengthen a **coordinated and comprehensive response**, which applies both at the governmental level and in terms of alliances and participation between the public and private sectors.

Advancing in the creation and integral and coordinated operation between public and private entities entails the need to understand that we will be working in a way that will provide even greater success rates in relation to the desired outcomes.



Schematic 3. Vulnerabilities. Prepared by Marko Magdic

Highlights

This chapter addresses the main security risks, threats, and vulnerabilities in the Americas. The most relevant threats are divided into two groups:

Outcome threats: terrorism and organized crime.

Means threats: corruption, money laundering and non-spontaneous organized violence.

The probability of these threats happening, is influenced by vulnerabilities, classified as internal (management) and external (environment). The importance of addressing these challenges through public-private partnerships is a key strategy for generating a coordinated and comprehensive response in the region.

Public-Private partnerships

In this chapter, we will explore the concept of public-private partnerships (PPPs) in the field of security, analyzing their importance, functionality, and potential for addressing contemporary security and crime prevention challenges. Collaboration between public and private actors can result in greater effectiveness and success in combating the threats and vulnerabilities that our societies face.

PPPs are agreements established between one or more public and private sector actors, with the objective of supplying or providing services or goods in pursuit of common goals, in this case, security. These partnerships may have an economic or social focus and may be regulated by contracts, strict legal frameworks, collaboration agreements or memorandums of understanding.

Although PPPs have been widely used in sectors such as infrastructure, energy, health and education, their application in the field of security has been less prevalent. However, there are numerous opportunities and potential benefits in establishing such collaborations in the security sector, especially considering the prevalent impact that security threats have on all sectors of society.

Public-private security partnerships can address both direct threats such as terrorism, organized crime, corruption, money laundering and planned and organized social violence, as well as those of a more indirect nature, such as education and poverty. These alliances can also work to reduce the factors associated with internal and external vulnerabilities.

The differentiating factor proposed is the joint declaration of interests, which should translate into concrete actions, following previously defined objectives, in the search for measurable results that have an impact on security risk reduction.

International organizations such as the United Nations, the Organization of American States, the Inter-American Development Bank, and the World Bank have promoted and supported PPPs in the areas of citizen security, crime prevention and combating terrorism.

Public-private security partnerships represent a valuable and effective opportunity to address the security challenges our societies face. Through collaboration and resource-sharing, knowledge and experience, public and private actors can develop and implement measures to prevent, prosecute and punish crime and terrorism in all its forms and manifestations.

What are they?

Public safety is the responsibility of the States or Governments. There is no doubt about that, but it does not preclude private sector participation in this area.

The degree of involvement of the private sector can range from an eminently passive and subsidiary role to a co-participatory one. It is not the purpose of this document to analyze the exact roles and positions of each, but rather to promote the concept of coordinated work. Although it would seem that the public sector has a predominant role to play in security matters, we believe that this is not exclusive to it. It is the entire community, organized in its diverse economic, social, political, and cultural forms, that suffers the negative consequences of security threats, so that, with greater or lesser activism and participation, both public, state, and private actors have sufficient motives and justification to integrate prevention, detection, and response activities. All of them, without exception, have good reasons to increase security by addressing threats and addressing vulnerabilities. They all have much to lose as well as to gain and contribute.

Public and Private Sector

For the purposes of this Manual, we will use the concept of the private sector as a representative notion of everything that is not public, including research centers, academia, and non-governmental organizations, as well as foundations, corporations, local associations, neighborhood groups and private enterprise as such.
For the purposes of our tool, the term public sector refers to the various manifestations of state and governmental organization, considering both the federal and local spheres as well as those at the central, state, provincial, district or regional, and local levels (municipalities, city councils, counties, among others).

Having clarified the individual concepts of public and private, it makes sense to address the notion of public-private partnership.

There is no universal consensus on a definition, to such an extent that it has become problematic to comparatively evaluate different types of partnerships. Indeed, while some alliances have an eminently economic purpose, in other cases the objective pursued is social. Some are regulated by contracts or strict legal frameworks while others are regulated by collaboration agreements or memorandums of understanding.

A broad concept of public-private partnership would lead us to define it as the result of an express or tacit agreement between one or more public sector actors and one or more private sector actors to supply or provide services or goods in pursuit of common objectives, in this case, security.

Traditionally associated with this type of agreement are partnerships or collaboration agreements in the areas of infrastructure, energy supply, health, education and even waste management.

Although present and in constant development, probably one of the sectors with the greatest potential and opportunity for growth in terms of public-private collaboration is security. In spite of this, it happens that, when speaking of security, the concept is sometimes associated with investigation and/or criminal prosecution, public activities in which there is a notion of almost monopolistic participation of the State. This explains why, in the consultant's opinion, in security matters, public-private partnerships tend to be less prevalent than in other areas of communications and state interest.

There are manifestations of private or social participation in security areas that could be considered the result of tacit or express alliances between the community and the state.

These are situations in which, although public and private actors come together to a greater or lesser extent, they are far from the concept of public-private partnerships as per the terms proposed in this Manual. Indeed, and without validating or rejecting them, in some jurisdictions it is possible to visualize practices that we do not consider partnerships as such, such as:

A. the possibility for the private sector to have private security guards, sometimes armed;

B. legally authorizing the community to detain criminals in cases of flagrant crime;

C. having legislation that, with greater or lesser restrictions, enables people to acquire or carry weapons.

All the foregoing, as a whole, represent activities, as we said, in which the private sector or the community can conduct actions by means of which they could eventually have an impact, in one way or another, on security. But this is far from being a partnership as described in this Manual.

Whether they are **joint ventures** or the result of the creation of new entities specially formed for this purpose; whether we are in the presence of working networks, agreements, memorandums of understanding or collaboration agreements, we consider the distinctive factor of the public-private partnership as a **joint manifestation of interests, which translates into concrete actions, following previously defined objectives, in the search for measurable results that have an impact on the reduction of security risks, preventing, detecting early and responding to threats through collaborative work between public and private sector actors.**

Elements

- Joint expression of interests and collaborative work between public and private sector actors.
- Concrete actions
- Previously defined objectives
- Measurable results
- Security risk reduction
- Prevention, early detection of threats

This approach to the concept of public-private partnership allows us to contextualize it in two dimensions. One, as a means of addressing security threats by taking into account direct outcome or means threats (terrorism, organized crime, corruption, money laundering and planned and operated social violence), and another that addresses those of a more indirect or environmental nature, as in the case of education or poverty.

Similarly, public-private partnerships will help us to work on reducing levels related to factors associated with vulnerabilities, whether internal (coordinated response, economic approach, proactivity) or external (labor informality, poverty, state presence and social vulnerability).

Are they useful?

In addition to a set of crime prevention guidelines in which there is an express mention of this type of partnership, the United Nations, through its General Assembly, has adopted several resolutions that encourage Public-Private Partnerships that promote collaborative programs that could have an impact on security, among others.

Such is the case of the following resolutions, among others:

- Resolution A/60/288 of 2005[5]
- Resolution A/60/215 of 2005[6]
- Resolution A/58/129 of 2003[7]
- Resolution A/56/76 of 2001[8]
- Resolution A/55/215 of 2000[9]

The XII Congress on Crime Prevention and Criminal Justice in Brazil, held in April 2010, clearly stated in its Declaration[10] that it recognizes *"(...) the importance of strengthening public-private partnerships to prevent and fight against crime in all its forms and manifestations".* The above, is set forth in Resolution 65/230 of the aforementioned Congress, which was subsequently approved by the United Nations General Assembly on December 21, 2021, based on the report of the Third Committee (A/65/457).

> The document states that they are *"(...) convinced that, through the mutual and effective exchange of information, knowledge and experience, and through joint and coordinated actions, governments and businesses can develop, improve and implement measures to prevent, prosecute and punish crime, including new and evolving challenges".*

Based on the same declaration, a month later, the XIX Meeting of the United Nations Commission on Crime Prevention and Criminal Justice was held in Austria. The report of this meeting (E/2010/30 E/CN.15/2010/20)[11] reports on the intent to strengthen, public-private partnerships with international support, for the prevention and fight against crime in all its forms and manifestations, including terrorism. The document urges governments to promote and strengthen collaboration partnerships with the private sector, establish priority areas, disseminate best practices, create support networks, and raise awareness of the benefits of such partnerships in relation to crime prevention and control.

[5] https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/504/91/PDF/N0550491.pdf?OpenElement
[6] https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/500/53/PDF/N0550053.pdf?OpenElement
[7] https://documents-dds-ny.un.org/doc/UNDOC/GEN/N05/500/53/PDF/N0550053.pdf?OpenElement
[8] https://documents-dds-ny.un.org/doc/UNDOC/GEN/N01/490/05/PDF/N0149005.pdf?OpenElement
[9] https://documents-dds-ny.un.org/doc/UNDOC/GEN/N00/572/08/PDF/N0057208.pdf?OpenElement
[10] **Salvador Declaration on Comprehensive Strategies for Global Challenges: Crime Prevention and Criminal Justice Systems and Their Development in a Changing World.**
[11] https://documents-dds-ny.un.org/doc/UNDOC/GEN/V10/541/37/PDF/V1054137.pdf?OpenElement

Multilateral agencies and international entities such as the Organization of American States, the Inter-American Development Bank and the World Bank also support and promote public-private partnerships as a collaboration mechanism to address challenges related to citizen security, crime, public safety, and the fight against terrorism.

At the OAS level, the member states agreed upon promoting public-private partnerships in the fight against terrorism, as discussed at the Tenth Regular Meeting of the Inter-American Committee Against Terrorism (CICTE).

In March 2010, under the theme *"Public-private partnerships in the fight against terrorism,"* delegates from OAS Member States at the CICTE meeting discussed issues related to collaboration in the protection of basic infrastructure, security for major events and public-private partnerships in maritime security. Delegations also discussed issues such as: combating terrorism in compliance with national and international laws; strengthening existing national and international measures to identify new multilateral cooperation strategies to strengthen the fight against terrorism; adopting cooperative programs to exchange information and best practices to prevent and combat such threats; and strengthening ties with the private sector and civil society to develop preventive and protective capacity-building programs, among others.

The relevance of the statements and recommendations is enormous. This provides guidelines and directives to the various governments to implement programs with public-private components. This is no coincidence, as the impact of the threats is tremendous. When security risks become evident through threats materialization, everyone is affected: the State, the community, the civil society and the organizations and companies. Specific events could affect a specific sector or interest group, but when these threats permeate and take shape in a given territory, community or system, the impact and damage are all-encompassing.

If we assume the above to be true, in the understanding that both the public and private sectors experience and suffer the negative effects, we can only maintain that, to a greater or lesser extent and intensity, an integral or at least collaborative approach between both sectors will be highly beneficial and even necessary. Higher security levels have a positive impact on both sides.

The importance of the State in public-private partnerships lies in the fact that projects can be focused on geographic areas, develop thematic areas, or have an impact on target populations that are not necessarily a priority for private or non-State groups. The speed, flexibility, and adaptability of the private sector to work on the interests of the partnerships, represents a much-needed injection of dynamism in a context of developing innovative and impactful solutions to security problems.

Nevertheless, when it comes to building a dam or a highway, the importance of a public-private partnership is undeniable, which is not always the case in security matters. However, it is equally beneficial, which is precisely what justifies this Manual.

Public-private partnerships are important for the public sector for many reasons, including the following:

- They contribute to secure the commitment of the private sector to become part of the threat prevention and emergency response planning global community process.
- Cooperation and joint use of resources for multiple vulnerable "soft" targets can significantly increase security and create a single, much "harder" target.
- They provide better understanding of the needs of the private sector and its capacity and resource availability.
- In terms of prevention, they actively encourage communication with the private sector before an incident happens.
- They provide an opportunity to discuss and plan joint response and recovery strategies.
- They provide better conditions and more early detection tools for the threats that have materialized, facilitating a faster response, and hindering the spread of the damage.

On the other hand, these partnerships are important for the private sector for many reasons, including the following:

- They provide the private sector with a communication channel with the public sector and develop an understanding of the support that can be received from the public sector.
- They provide an opportunity to explain and describe to the public sector why business continuity is important for private entities and for the community.
- They provide incentives for the business community to invest in preventive measures to reduce threats and risks, as well as providing support to the academia in the formulation of policies and development of research activities in this subject.
- They provide the opportunity to receive information, additional support, and advice on crime prevention.
- They generate better conditions for the early detection of security threats, allowing both the private sector and the State to intervene more quickly and reduce the damage of a given incident.

- They could help to reduce liability and expenses derived from insurance costs associated to damages that could be suffered by an activity, people, or infrastructure as a consequence of security incidents (crime, terrorist attack, etc.).

- They generate the opportunity to discuss and develop continuity and recovery business plans.

- They develop a better understanding of public sector capacity and resources.

- They encourage and promote that private interests and needs are considered when setting public sector security priorities and objectives.

Highlights:

This chapter explores the concept of public-private partnerships (PPPs) in the field of security and their potential to address contemporary security and crime prevention challenges. PPPs are agreements between public and private actors with common objectives, and although they have been used in sectors such as infrastructure, energy, health and education, their application in security has been less prevalent.

The main aspects to highlight are:

1. Security PPPs can address direct and indirect threats, as well as reduce internal and external vulnerabilities.

2. Collaboration and knowledge, resource and experience sharing between public and private actors can improve effectiveness and success in combating threats and vulnerabilities.

3. International organizations promote and support citizen security, crime prevention and counter terrorism PPPs.

Public-private security partnerships represent a valuable opportunity to address the security challenges of our societies more effectively.

Starting collaborative work: the first steps

In this chapter, we will address the beginning of collaborative work between the public and private sectors in the area of public security, focusing on the first steps to establish effective collaboration. Partnership on these issues is not usually spontaneous, so it is crucial that one of the parties takes the initiative to identify and address specific problems, such as the increase in homicides, the decrease in the number of complaints, terrorist attacks, among others.

To build the first bridges of collaboration between the two sectors, activities such as open fairs, seminars or workshops, sectoral meetings and targeted meetings are recommended. These instances make it possible to identify stakeholders, learn about new technologies or ideas, and compartmentalize topics of interest, thus facilitating interaction and information exchange.

State entities, neighborhood councils, research centers, private companies and civil society organizations should incorporate this type of work in their annual planning. Joint problems require joint solutions, and being proactive is key in this process.

This chapter seeks to motivate readers to take the initiative to identify counterparts in both sectors and start working towards new and better results in reducing security risks related to terrorist threats and organized crime.

The beginning or formation of any public-private security partnership should be approached as a project.

As in any partnership, one of the parties will always have a greater share of the initiative, which will probably end up being seconded by the other. The spontaneous and automatic associativity in the issues that bring us together is rare.

In other words, projects and first meetings will not happen on their own. It will always be necessary for one or the other to take that first step. The foregoing assumes that at least one of the parties has visualized a problem, such as an increase in homicides, a decrease in money laundering reports, an intensification of terrorist attacks, an increase in violence associated with extortion of private companies, a greater number of stolen vehicles related to serious crimes of social impact, etc. This first acknowledgement or acceptance that the issue affects both the public and private sectors, should motivate the implementation of activities aimed at generating the first bridges of collaboration between the two sectors in relation to a specific problem to be addressed. For this purpose, it is advisable to generate:

- Open Fairs[12]
- Seminars or workshops
- Sector meetings
- Targeted and limited meetings with counterparts

It is quite likely that the identification of counterparts and the initial stages of establishing a public-private partnership will take place in the same order, starting with open fairs and ending with targeted meetings. Thus, it is possible that through either a private or public initiative, a fair is organized that, while addressing security as a general theme, also addresses a specific issue such as for example, vehicle theft, drug trafficking, smuggling or the terrorist threat. In this type of event, we will see the existing offering and initiatives operating in the field, and we will also be able to easily identify those actors who are highly interested in showing their work. This type of initiative is extremely useful to learn about new players, technologies, or ideas.

Seminars and workshops are usually held at these types of fairs but could also well be part of a subsequent event. The idea is to provide structure and higher levels of methodology to the topics covered. In this type of activities, we will be able to better compartmentalize the issues of interest.

[12] **These are events of a cultural, economic, social or industrial nature, established on a temporary basis, which take place in a specific physical venue and address a common issue, in this case, security. Not only do they allow communication and information exchange among private actors involved in the issue, but also between them and the public sector. They are also excellent places to learn about the latest trends, needs, challenges and opportunities. They bring a group of relevant public and private security stakeholders together in one place, substantially improving mutual knowledge and encouraging collaboration.**

Thus, prevention initiatives could be addressed separately from those related to detection or control. Similarly, it is possible to focus on a particular topic and break it down. While a counter-terrorism fair brings together the most interested actors in the field to interact and exchange information more spontaneously in one place, by organizing seminars and workshops, the organizer can methodically direct this interaction, promoting agreements, statements, or concrete results.

Sectoral meetings, on the other hand, usually bring together a smaller number of public and private entities on a particular issue. Let's say, for example, actors from both sectors in charge of and/or interested in biosecurity and bioterrorism, or IT, cyberterrorism, and cybersecurity. In the same vein, if the meeting is intended to address the problem of drug trafficking at the border, it is possible that the public sector will include representatives of the most important law enforcement agencies involved in border control, as well as authorities from the municipalities, states or provinces located in those areas. On the private sector side, chambers of commerce, transportation companies, logistics operators and technology providers should be involved.

The progress of these activities will probably lead to more focused work at the level of specific counterparts or more bilateral-type work, which will allow to better understand and comprehend the expectations, needs and possible tensions between the different stakeholders, in a safe space of greater trust.

The COVID-19 pandemic, which struck the world at the beginning of the second decade of the 21st century, demonstrated that this type of initiative can not only be supported physically and in person, but also virtually, which evidently reduces costs and time and encourages a greater number of events. Whether they are held consecutively, simultaneously or in another order, what is important is that the actors interested in addressing a security problem take the initiative and develop activities focused on the exchange of opinions, learning and bridging gaps, a recommendation that applies to both sectors. Proactivity is a key word.

In the case of state-owned entities, this process should be part of their work methodology. We consider that, when addressing the main threats mentioned in this Manual, it should be done so through a public-private partnership line of work, one for each of them, which can be done at the national, state, provincial, cantonal, regional, municipal or district level, depending on the degree and extent of the negative impact caused by the threats mentioned.

Neighborhood councils or territorial or functional community associations, research centers, chambers of commerce, private companies, and civil society organizations whose objective is to deal proactively with these threats, or which have been affected by them, should also incorporate these collaborations into their annual planning. **Joint problems require joint solutions.**

One way to establish or measure the need to implement proactive programs to address security threats is by answering the questions listed at the beginning of this Handbook.

If you are reading this section, it is probably because you scored at least two points in the survey at the beginning of the Manual. It is time, then, to be proactive and take the initiative to identify partners in both the public and private sectors to commence working towards new and/or better results when reducing security risks related to terrorist threats and organized crime.

Highlights

This chapter focuses on the first steps to establish effective public security public-private partnerships. The main items to highlight are:

1. The importance of taking the initiative to identify and address specific security issues.

2. Activities such as open fairs, seminars, workshops, and meetings to facilitate interaction and information exchange between the two sectors.

3. The need for state entities, neighborhood councils, research centers, private companies, and civil society organizations to incorporate collaborative work in their annual planning.

The goal is to encourage readers to identify partners in both sectors and work together to find effective solutions to address terrorist threats and organized crime.

Assessment of the problem

This chapter addresses the assessment of the security problem, emphasizing the importance of collaboration between the public and private sectors to develop a comprehensive and efficient analysis of the threats and challenges to be faced. It explores several key factors that should be considered in the assessment process and highlights concrete examples that illustrate the relevance of incorporating both sectors in the identification, prevention, and control of security issues.

The chapter discusses the need to produce joint assessments including both public and private sectors in order to obtain a broader and more accurate view of security problems. There are 13 essential factors to consider in an assessment, including the threat, the problem, the modus operandi, among others. Specific cases, such as terrorist financing and vehicle theft, are discussed to illustrate how collaboration between the two sectors can provide valuable information and improve understanding of these phenomena.

Collaborative and joint work between public and private entities can identify new variables, provide tools for a better understanding of the problem and, ultimately, help design more effective and innovative strategies. It addresses the importance of continually updating assessments and adapting policies and programs based on the results obtained.

The chapter highlights the value of public-private collaboration in the assessment of security problems, aiming to improve prevention, early detection, control, and response to the threats we face.

Assessment of security-related problems and threats has always been made and will continue into the future. Both the public and private sectors have participated in these processes. However, it is more likely to find assessments constructed from the perspective one of the two sides (public or private), rather than jointly. It is recommended, of course, that assessments are done through the collaborative participation of both sectors from the outset.

A good security assessment should cover at least the following 13 factors:

* **The threat.** What threat do I want to address?
* **The problem.** What specific problem is generating this threat?
* **The modus operandi.** How is the threat committed or manifested?
* **Place, time.** Where does it happen, at what time?
* **Motive.** What is the interest sought to make the threat real?
* **Target profile.** Against whom or against what is the threat verified?
* **Main Actors involved.** Could/should the stakeholders intervene directly to prevent, detect, control, and respond to the threat?
* **Actors involved by extension.** Who has something to say or contribute in terms of knowledge, skills or experience in prevention, early detection, control and/or response to the particular threat we are addressing?
* **Historical strengths.** What best practices and success stories can we identify?
* **Historical weaknesses.** What malpractices and difficulties have we experienced to date?
* **Opportunities.** What current conditions should we take advantage of, be they institutional, legal, media, financial or operational, among others?

* **Challenges.** What challenges or threats are we facing, or could we face when addressing the problem, given the current scenario or during an imminent and upcoming scenario?

* **Cumulative measurements.** How have we scored the various indicators associated with the threat and the specific problem we are addressing so far, and what successes, on the one hand, and problems, on the other, have we had with this type of scoring?

* **Future indicators.** What new indicators would we have, or could we take into account to evaluate the analyzed problem in a better or different way and that would allow us to provide an added value, a new perspective or understanding for it?

In the past, when the first steps were taken to address terrorist threats, the state approach was almost exclusive. Private sector participation was minimal or practically non-existent.

In recent decades, and as a result of an analysis of the terrorist phenomenon by government agencies, academia, research centers and private enterprise, it has become possible to establish that identifying organizations' lines of financing has two advantages: it becomes easier to reach the organization itself, and the flow of assets can be interrupted, hindering its operation and power.

The highest percentage of the financing comes through the private sector, whether through money movements and transfers, the shipment of arms by sea, or the operation of companies that act as fronts to launder assets linked to terrorism. In all these cases:

does it make sense to include banks, logistics companies, shipping companies, gambling casinos or money transfer companies?

Could it be beneficial, beyond regulating them, to develop lines of work that make them collaborating partners in public-private initiatives?

The answer is yes.

It becomes important to work with the regulatory bodies in this industry, such as the Financial Analysis or Financial Intelligence Units, as well as the work being done by the FATF, the Financial Action Task Force. What is proposed here is to go a step further and incorporate the relevant private entities involved in terrorist financing to learn, first hand, and based on their experiences and capabilities, the ways in which terrorist groups could take advantage of their vulnerabilities to transfer money or goods. Banks and logistics companies need to operate without setbacks. If they get feedback from the State regarding the issues in which they can jointly participate, there will be a greater willingness to share data.

On the other hand, if we analyze, for example, the security problem associated with vehicle theft, a classic diagnosis would allow us to know not only the number of vehicles stolen, the way in which they are stolen and even the times and places. We could also evaluate the legislation that punishes theft, the type of vehicle stolen, and identify strengths and weaknesses related to the system of reporting and searching for cars that have been stolen from their owners.

A collaborative participation with the private sector could yield diverse and complementary data, which would help to better understand some new variables, making it possible to consider alternative and/or new courses of action.

Thus, it may be interesting to learn the percentage and even the type and profile of stolen vehicles that had insurance and the impact that this could have on this crime. Likewise, to learn the time it took to find the vehicles when they were recovered, how far away or in where they were found, the type of damage suffered by the recovered vehicle in order to be able to deduce the use given to it during the time of the theft.

In turn, auctioneers or managers of auction houses or auction agencies could indicate the type, quantity and percentage of vehicles that are sold through this system as scrap or waste. A cross-check of data between insurance companies and auction houses could indicate the percentage and type of vehicles that, despite being sold as scrap or junk and having been fully compensated for total loss to their owners, their registration has not been cancelled, an aspect that has a direct impact on the cloning or twinning of stolen vehicles.

Private participation could go further with many other variables not traditionally considered, that would not only allow us to have a different image and view of the problem but would also provide us with tools and elements for a better understanding, which would ultimately help us to propose better and new strategies for solution or, at least, containment.

It therefore makes sense to include the highway administrators in the analysis and solution of a problem such as this, in order to find out the amount, type and schedules of stolen vehicles driven on their roads. The same applies to municipalities, counties, or territories where the authorities have license plate reader systems. Of course, the foregoing involves a first level of collaboration, which requires cross-referencing police databases that contain the license plates of stolen vehicles with those private or even public databases that incorporate the registration of vehicle circulation based on their identification numbers.

Let us imagine, in addition, bringing in companies that manage parking lots, whether they are parking spaces or parking lots destined exclusively for this purpose or for shopping centers that, for the purpose of a more efficient fee collection, also register the license plates of their users or customers.

Would it be interesting to learn the percentage of stolen vehicles that entered your facilities, the time they remained there, and even if they are still there?

Would that help in understanding the problem? Yes, of course. This aspect will be addressed in the upcoming section addressing the formulation, design of ideas and solutions within the framework of public-private partnerships.

In addition, in those cities or towns in which public employees or private companies register and charge for parking vehicles on the streets or public roads, it is quite likely that, among other variables, they will take note of the license plates of those vehicles. This is data that, when cross-referenced with the stolen vehicle databases, could yield interesting results. We could learn, in real time, the location of a vehicle that was registered as stolen.

Collaboration may be extended to other public bodies not traditionally considered in these matters, such as customs, border control authorities, insurance company regulators, agencies in charge of issuing vehicle license plates or patents, agencies in charge of regulating or supervising agencies or auction houses where wrecked vehicles are sold, among others.

Indeed, we must bear in mind that, depending on the country and specific context, a percentage of stolen vehicles cross national borders through unauthorized locations, therefore a cross-check of data and joint work with border authorities could yield interesting insights into the number, type, times, days, and places through which, even in presence of border control agencies, stolen vehicles left or entered our countries. Such data could be relevant, because in the event that the number of cross-referenced hits is considerable, we could realize that the strategy of investing resources in control and detection of vehicles circulating through informal, illegal and unauthorized crossings, could not actually be as profitable as starting to detect and control those places where there is a presence of authorities given the conditions of formal, authorized crossings.

Would it be useful to learn about existing private or even public-private initiatives regarding physical marking of vehicle parts and pieces, as well as the operation, coverage, and capabilities of GPS, whether applied voluntarily by vehicle users or in response to obligations, whether legal or contractual with insurance companies?

Will the information provided by the counterparts regarding this type of issue have any relevance, if what we are doing is diagnosing a problem from a different and, why not, more efficient point of view?

The better the assessment, the greater the likelihood of understanding the essence of the problem and the better the prospects for designing successful prevention, early detection, control, and response solutions.

When a problem, in this case a security threat, has not been successfully addressed, at least not in the desired terms, and the numbers, the cases, the associated violence and the associated negative effects continue to rise, one would think that intensifying the existing response, increasing resources, and injecting means, to a greater or lesser extent, should generate certain levels of positive impact.

The question is whether this will solve the problem, at least at such a level that the desired impact is generated. If at the beginning of a program or project, ten units of resources generate impact on one crime, and 20 units generate impact on two crimes, there will come a time when sustained increases in the injection of assets, personnel, time and money will not generate the same level of impact, so that, for example, a thousand units of resources instead of generating impact on one hundred crimes will generate impact on ninety, which will begin to make the return or profitability sought, increasingly inefficient.

Thus, continuous intensification policies or programs must necessarily be complemented by other systems, solutions, and actions. Hence the importance of conducting assessments, continually adjusting them, and doing this work from both the public and private perspectives, making use not only of the experience of both sectors, but also of the information, capabilities, ideas, and resources that they can provide, doing so within the framework of a predefined work program that includes representatives from both sectors.

In short, whether there is a prior assessment conducted by any of the parties, or the process is done starting from scratch, it is advisable that from the beginning, the current knowledge of the problem must be implemented or updated, as appropriate, with an active and collaborative intervention of both the public and private sectors, taking into account, at least, the 13 elements provided in this section. To this end, we suggest to incorporate not only the primary actors, but also the so-called "extension" actors, which are the public and private entities that have something to say or contribute in terms of knowledge, capabilities or experience in terms of prevention, early detection, control and/or response to the particular threat we are dealing with.

The most relevant:

This chapter highlights the importance of collaboration between the public and private sectors in assessing security issues. The main items to highlight are:

1. The need for joint assessments to obtain a broad and accurate view of security problems.

2. Consideration of 13 essential factors in the assessment process, such as threat, problem and modus operandi.

3. Discussion of specific cases, such as terrorist financing and vehicle theft, to illustrate the value of collaboration between the two sectors.

4. The importance of continually updating assessments and adapting policies and programs based on the results obtained.

The objective of the chapter is to highlight the value of public-private collaboration in the assessment of security problems, thus improving prevention, early detection, control and response to threats.

The scope of the strategic alliance

This chapter addresses the scope of the strategic alliance between the public and private sectors in the field of security, exploring the opportunities and benefits that arise from this collaboration. The aim is to promote the integration of both sectors, taking advantage of their strengths to improve efficiency and effectiveness in the fight against security threats.

The bidding of funds for security projects is an example of how the synergy between the two sectors generates mutual benefits, allowing the public sector to take advantage of the private sector's management, resources, and investment capacity. These forms of public-private partnerships have proven to be successful and are expected to continue in the future.

However, the proposal of this chapter goes beyond simple collaboration or mutual assistance between the two sectors. The aim is to establish a strategic alliance in which both actively participate from the beginning of a project, contributing with resources, information, intelligence, experience, means and measurement systems.

This more intense and associative collaboration would allow public and private sector actors to work together in the formulation, implementation, evaluation, and adjustment of security initiatives. In this way, we seek to enhance the capacity to prevent, early detect, control, and respond to public security threats, generating a significant impact on the protection and well-being of the community.

This chapter advocates for a strategic alliance between the public and private sectors in security matters, where collaboration and co-participation go beyond the mere delegated execution of one in relation to the other. The aim is to achieve a joint and integrated approach that will make it possible to deal more successfully with the challenges and threats to public security in the 21st century.

The bidding of funds for security projects generates synergies between the public and private sectors. There is no doubt about that. The outsourcing of some security services from the public to the private sector allows them to take advantage of the benefits of their management, resources, and investment capacity.

Like these, many other initiatives in which the interests of both sectors converge can be considered types of public-private partnerships. It is good that they are, and it is desirable that they continue operating this way. Anything that nurtures legitimate joint interests and generates benefits for a safer community must be recommended.

But the participation, or rather the public-private collaboration that we propose through this Manual is more intense and follows an even more associative logic. The idea is to work in a strategic alliance in which both sectors participate actively and contribute not only resources but also, above all, information, intelligence, experience, means, management, and measurement systems.

Therefore, without undermining the relevance and importance of other forms of joint collaboration, we propose to encourage and work not only on delegated execution of tasks supporting one another, or the assistance or aid that may exist between the parties, but rather, and above all, that both the public and private sectors participate simultaneously from the beginning of a project, making joint assessments and acting together in the formulation, execution, evaluation and adjustment of initiatives that seek to prevent, early detect, control and respond to threats to public safety.

The most relevant:

This chapter focuses on the importance of establishing strategic alliances between the public and private sectors focused on security. The main aspects to be highlighted are:

1. Promoting the integration of both sectors to improve efficiency and effectiveness in the fight against security threats.

2. Synergy between both sectors through the bidding of funds for security projects, generating mutual benefits.

3. The search for a strategic alliance in which both sectors actively participate from the beginning of a project, contributing resources, information, intelligence, and experience.

4. Intense and associative collaboration to work together in the formulation, execution, evaluation, and adjustment of security initiatives.

The purpose of the chapter is to advocate for a joint and integrated approach between the public and private sectors, making it possible to face the challenges and threats better and more successfully to public security in the 21st century.

The joint project. Methodologies and creative thinking

This chapter focuses on a collaborative and associative approach for the creation of joint projects, focusing on the importance of methodology and creative thinking in the formulation and management of security projects involving the public and private sectors. We emphasize the need for cooperation and partnership throughout and from the beginning of the project, in order to maximize the effectiveness and impact in the prevention, early detection, control and response to security threats.

Firstly, various methodologies and standards applicable to project formulation and management are analyzed, such as ISO 9001, ISO 10006, ISO 21500, the Logical Framework and the PMBOK (Project Management Fundamentals Guide). These methodologies and standards provide guidelines and best practices for project design, development, implementation, and evaluation according to the needs and characteristics of each specific partnership and project.

The importance of using creative methods to design solutions and courses of action is discussed below. We also emphasize the value of innovation and originality in the search for solutions to security challenges, through the application of critical and creative thinking techniques. Among the examples mentioned, is the broken windows theory, which has proven effective in crime reduction, prevention, and control.

The main objective of this chapter is to highlight the relevance of following a specific methodology that facilitates discussion and encourages the creative process in the development of public and private projects, avoiding improvisation and encouraging the generation of innovative and effective ideas.

The aim is to encourage collaboration and co-participation in the formulation and management of security projects, using appropriate methodologies and promoting creative thinking to achieve a significant impact on the reduction of risks and threats to public safety.

Having clarified the collaborative aspect, we recommend understanding and approaching the partnership in a way that the generation of the project should always be joint, associative, and co-participative from the beginning.

Having accepted the foregoing, it becomes interesting to learn how to continue.

Whether the assessment has been made jointly, but prior to, or isolated from the project, or whether this assessment is part of the project as an initial stage, what is important is that the specific project will be formulated based on this assessment.

The stages that will follow comprise designing the solution, executing an action plan, controlling, measuring, and reporting, and finally evaluating eventual adjustments.

It is a unique process, which is built through the integration of a series of coordinated and controlled activities, with a start date and end date, and which are executed to achieve a predefined objective, taking into account variables such as leadership, coordination, time, available resources and assets, and costs, among others.

Methodologies

From the design stage alone, all available alternatives and methodologies for project formulation and management should be considered, the choice of which will depend on each particular partnership and project. It is beyond the scope of this Manual to analyze all the alternatives in detail. However, it may be useful to at least mention or list them.

Thus, among other possibilities we find ISO standards,[13] and models or methodologies such as the PMBOK or the Logical Framework, among many others. Of course, there are other functional standards and methodologies for project management, design, and development. Herein, we would like to provide the user with some of them so that they can be taken into account.

[13] ISO norms are internationally validated standards that establish common or homogeneous guidelines in relation to issues related to management, efficiency and safety of products and services as well as processes. The fact that two or more entities follow the same ISO standard makes it possible to ensure common and comparable standards, facilitating measurement, evaluation, and control.
More information can be found at www.iso.org, the official website of the *International Organization for Standardization* (ISO), an independent, intergovernmental international organization based in Switzerland.

ISO 9001[14] provides guidelines for the design and development of products and services by establishing elements for implementing a quality management system, which provides guidance on how to develop a formal system that can help improve performance and form the basis for sustainable development. It is a standard that employs a process-based approach incorporating the PDCA cycle - Plan, Do, Check, Act.

In turn, the **ISO 10006** Standard[15] applied to project management contains indicators that, if followed correctly, ensure high levels of quality. It seeks to generate a universal language and treatment for project management, ensuring a general harmonization of the different elements, as well as a correct conception and development.

Finally, **ISO 21500**[16] is composed of guidelines on Project Management. The purpose of this guide is to provide elements for efficient project management. It provides orientation regarding the concepts and processes related to the management and direction of any type of project.

There is a number of other ISO standards that could be applicable, such as those related to cybersecurity, occupational safety, environment, operational risk and compliance, among others. However, those related to the management, direction and design of projects, products and services seem to be the most relevant.

As far as the **logical framework methodology**[17] is concerned, we can point out that it is a project management tool used in project design and planning, as well as in execution and evaluation.

Finally, among other alternatives, it is worth mentioning the **PMBOK** instrument[18], which establishes a set of good practices related to leadership, administration, and management through the implementation of tools, systems and techniques that identify a considerable number of processes distributed in a smaller number of macro-processes.

Whichever methodology is followed, we should bear in mind that all of them consider a stage in which, based on an assessment of the problem, they work on the design of solutions and lines of action.

[14] www.iso.org
[15] www.iso.org
[16] www.iso.org
[17] **More information can be found in the United Nations Economic Commission for Latin America and the Caribbean (ECLAC) manual titled Logical Framework Methodology for Project and Program Planning, Monitoring and Evaluation. According to the Manual itself, the Logical Framework is a tool to facilitate the process of project conceptualization, design, implementation and evaluation. Its emphasis is on an objective-based approach, beneficiary group targeting and facilitating participation and communication among stakeholders.**
https://repositorio.cepal.org/bitstream/handle/11362/5607/S057518_es.pdf
[18] **More information on the PMBOK® tool can be found in the Program Management Institute's Guide to the Fundamentals of Project Management (PMBOK® Guide). *(Program Management Institute)***
https://www.pmi.org/pmbok-guide-standards/foundational/pmbok?sc_camp=D750AAC10C2F4378CE6D51F8D987F49D

Creative Methods

There is a wide range of systems and methodologies that facilitate the creative process, which we consider essential for the design of novel, original, different, efficient, and result-oriented solutions within the framework of the public-private partnership, in order to generate a direct impact on the substantial reduction of security risks through prevention, early detection, control and response activities.

As with project management methods, it is beyond the scope of this Manual to discuss in detail the various creative thinking methodologies and techniques. However, their impact can be of such importance that it is worthwhile, at the very least, to be aware of their existence, usefulness, and denomination.

Today, few would dispute the beneficial effects generated by the set of solutions achieved with the broken windows theory as a crime reduction, prevention, and control mechanism, but prior to 1982, the year of its first theoretical formulation, no one knew about it.[19] It is precisely the new measures that fulfill certain quotas of innovation and originality that will generate an environment with greater probabilities of change in the results intended.

Mentioning or using this broken windows theory for the processes of analysis or discussion that happen during the early stages of public-private project formulation may be either by chance or as a consequence of a work methodology that, when applied, promotes or generates the conditions for participants to formulate this type of input or contribution.

The purpose of this section is to emphasize the importance of following a specific methodology to facilitate the process of discussion and problem and idea gathering, rather than leaving it to the mere spontaneity or random work of the members of the discussion group.

It is about seeking different results, forcing oneself to deliberate consciously and under a determined methodological guideline, so that, through specific techniques of critical and creative thinking, the blockages that hinder the creativity of ideas can be eliminated, favoring understanding and progress while achieving creative results.

[19] Criminology theory according to which the visible signs of crime are antisocial behavior and civil disturbances, among others, which create an urban environment that fosters crime and unrest, including serious crimes. According to this theoretical construct, state methods, in general, and police methods, in particular, that focus on targeting petty crimes, such as vandalism, loitering, public drinking, jaywalking, and evasion help create an atmosphere of order and legality.
Wilson, George L. Kelling, James Q. (March 1, 1982). «Broken Windows». *The Atlantic* (in English).

It is not a matter of recommending specific methods, but rather suggesting a methodology to be followed, one that facilitates discussion and avoids improvisation.[20]

The most relevant:

The chapter emphasizes the importance of a collaborative and associative approach in the generation of joint public-private security projects. The key points to highlight are:

1. The need for cooperation and partnership from the outset of the project to maximize effectiveness and an impact on security.

2. Analysis of various methodologies and standards applicable to project formulation and management, such as ISO 9001, ISO 10006, ISO 21500, the Logical Framework and the PMBOK.

3. The importance of using creative, innovative, and original methods in the design of solutions and courses of action, applying critical and creative thinking techniques.

4. The encouragement of collaboration and co-participation in security projects, using appropriate methodologies and fostering creative thinking to achieve a significant impact on risk reduction and public security threats.

The main objective of the chapter is to promote a specific methodology that facilitates discussion and a creative process in the course of public and private projects, avoiding improvisation and encouraging the generation of innovative and effective ideas.

[20] Among the various existing methodologies that can be applied are Mind Maps; Attribute Lists; Brainstorming; CRE-IN Method; Random Words; TRIZ - Theory to Solve; Inventive Problems; Checklist; DO IT - Define, Open, Identify and Transform; Conceptual Identification; Elimination of mental blocks; Inversion; The 6 Hats - conciliation, neutral, emotion, negative, positive and divergent; 635 Method; SCAMPER - substitute, combine, adapt, modify, put to other uses, eliminate or reorder; 4x4x4; PNI - positive, negative and interesting; Mind map; Analogies; Synectics;

Beginning the partnership. First steps

This chapter discusses the start and development of a successful public-private partnership, highlighting the importance of establishing a common methodology, shared concepts, and values, as well as the prerequisites necessary to carry out the project.

The methodology agreed between the partners is the first level to consider, followed by common concepts and shared values. Once consensus is reached at these levels, the prerequisites for the project are then to be discussed.

This section addresses the so-called "Common Concepts", emphasizing the need to generate consensus and clarity on key issues, such as identification of stakeholders, definition of objectives and sites, development of a common lexicon, predefined structures for cooperation, information processing, exercises and tests, definition of roles and tasks, and efficiency in the use of resources.

In addition, we analyze a key component in public-private partnerships, related to the values that must be recognized and shared by all partners in a project. These include equality, mutual benefit, dynamism, long-term commitment, shared responsibility, flexibility, and trust.

Finally, the prerequisites are addressed as a necessary condition for the success of the partnership, including the business case, information exchange, trust between partners, political will, coordination, application of expertise, accountability, must be discretionary and compliant with the legal framework.

This chapter provides detailed guidance on how to establish a successful public-private partnership, addressing key aspects such as methodology, common concepts, shared values, and prerequisites. By following these guidelines, the partners involved will be able to develop effective and sustainable collaborative projects, maximizing the use of resources and optimizing results.

This section discusses in more depth the process of how to start a public-private partnership.

This process can be divided into three different levels. The first level, that of methodology, already mentioned, should be the first to be considered by all potential partners. Once all the parties have agreed on the methodology, it is advisable to address issues related to *common concepts* (first level) and *shared values* (second level), which will be explained as follows. Upon mutual agreement, they should then discuss the level of *prerequisites* (third level) for the project.

Common concepts

When considering the development of a public-private partnership project to protect vulnerable targets or counteract security threats, it is very necessary to generate consensus and have clarity and agreement on a series of key issues, applying the preselected work methodology.

* **Identification of the interested parties:** Contact potential stakeholders and ask them if they are willing to join the project. It will also be necessary to define who will act as facilitator/ coordinator of the public-private partnership project. We should be open to the idea that no matter how closely the project is linked to the concept of security, this does not necessarily mean that a state agency must be the coordinator. It is relevant to take this into account.

* **Identify objects:** It must be clear which sites, objects and places fall within the scope of the project. This is obviously a sensitive issue and should therefore perhaps be classified as a reserved subject matter by all parties involved in relation to third parties external to the project.

* **Common lexicon:** Based on the background and experience of the stakeholders, it is desirable to develop a common lexicon, which can be understood by all partners. In government systems, for example, it is not unusual to use different terms for the same thing, or a similar term for different things.

* **Objective at which it aims:** Project partners should carefully and realistically define the objective(s) of the public-private partnership project. In short, what we hope to achieve.

* **Process-based:** Arrangements for cooperation and coordination within the framework of the public-private partnerships should preferably be based on predefined and pre-agreed structures. Hence the importance of the preceding chapter, which deals with the methodological aspect.

* **Information processing:** Arrangements and time frame(s) should be defined for the exchange of information between partners. The treatment of this concept has a separate section in this Manual due to its relevance.

* **Exercises and testing:** Agreeing upon a schedule for conducting and testing both theoretical and practical exercises is highly recommended.

* **Definition of roles and identification of tasks:** The specific roles and tasks to be performed by each individual and each organization should be very clearly defined, as well as any limitations that may be foreseen in this regard.

* **Efficiency:** The aim must be to optimize the use of resources, maximize efficiency and avoid duplication of efforts.

Shared values

In a successful public-private partnership project, all partners must agree in advance to identify shared values and their significance. Depending on their culture, capacity and prevailing obstacles, these values may change. A list of some of them is herein provided, for illustrative purposes in relation to this subject.

* **Equality:** Partners in a joint project between public and private entities must have the same status. A mutually beneficial approach: All partners should have the opportunity to "earn something" from their participation in the project, including a range of business benefits, for example. Identifying and disclosing the objectives of each stakeholder in terms of understanding what they want to gain will be relevant to the success of a partnership, especially if it is expected to last.

* **Dynamism:** All public-private partnership projects should seek a dynamic approach from both public and private partners, and all partners should agree to work, think, and exchange information in a dynamic way.

* **Long-term commitment:** A public-private partnership project is very likely to involve a long-term commitment. Over time, trust and relationships will grow if consortium membership remains as consistent as possible.

* **Shared responsibility:** Since a collaborative project must be based on mutual trust and accountability, all partners involved are responsible for maximizing their contribution and increasing the effectiveness and efficiency of the project.

* **Flexibility:** All partners have to be flexible due to the fact that both circumstances and terrorism and criminality are constantly changing. Partners should be willing to redefine their positions, if appropriate, and to discuss changes in a productive manner when circumstances change.

* **Trust building:** Within the framework of a public-private project, partners must trust each other, particularly given the critical level of effective information exchange between members.

Prerequisites

Once the partners have agreed on shared values, it is advisable to consider meeting the following necessary prerequisites:

* **Business case:** The project details of the specific one that addresses a public-private partnership should ideally be structured and explained in the format of a business case.

* **Information Exchange:** All partners, both private and public, should be willing to exchange, without breaking the law, operational and/or threat-based information on security and risk levels.

- **Trust:** All partners should trust each other. If private sector partners present, are in the same industry, clear measures should be taken in advance to avoid a conflict of interest or unfair competition. Given that trust is not a neutral element that exists, but rather a value that is achieved or attained, it will be important for the project to have elements that will not only generate trust, but also those that will prevent trust from being lost once achieved.

- **Political will:** Political will and support will always be necessary to ensure that government or state partners make all their resources available to the project and operate as efficiently as possible.

- **Coordination:** Establishing and defining efficient coordination mechanisms is essential. Efficiency cannot rest on the spontaneous initiative of one or more members, it must be regulated and defined jointly by all stakeholders.

- **Application of expert knowledge:** Develop expertise, share experience, support new participants, and promote the concept of collaboration, integration, association, and public-private partnership.

- **Responsibility:** A public-private partnership always generates rights and obligations for the parties, which should be recognized both generically and specifically in a written document or agreement. While memoranda of understanding or framework agreements represent expressions of general collaborative interest, subject-specific action protocols or procedures take this commitment to a more concrete level, as is the case with procedures for information exchange, social networks management, administrative aspects, operation, relations with external third parties, etc.

- **Discretionary Partnership:** Although any partnership entails obligations for the parties, the formation of a public-private partnership implies must be voluntary and should not be a consequence of an obligation imposed on one of the members. In the obligations there are restrictions to which the members are subject that are based on their willingness to accept them.

- **Legal context:** The project and all those involved in it, must at all times act in accordance with local, national and international laws.

The most relevant:

This chapter focuses on initiating and developing a successful public-private partnership and highlights the key aspects to achieve it. The main items to be highlighted are:

1. The importance of establishing a common methodology, shared concepts, and values among project partners.

2. The need to generate consensus and clarity on key issues, such as identification of stakeholders, objectives, common lexicon, cooperation structures, roles, and efficiency in the use of resources.

3. Shared core values, such as equality, mutual benefit, dynamism, long-term commitment, shared responsibility, flexibility, and trust.

4. The prerequisites necessary for the success of the partnership, including the business case, information exchange, trust, political will, coordination, expertise, accountability, and it must be discretionary and comply with the legal framework.

By following these guidelines, public-private partnerships will be able to develop effective and sustainable collaborative projects, maximizing the use of resources and optimizing results.

Main focus for the design of public-private solutions

This chapter will analyze the main focus for the design of public-private solutions in the context of security and threat prevention. Through several subchapters, we examine the critical factors that impact the design of a solution and specific courses of action in the framework of a Public-Private Partnership (PPP). Topics covered include the identification of threat profiles, target analysis and potential victims, understanding the motivations behind threats and the study of behavioral patterns in the execution of criminal or terrorist actions.

The chapter addresses the following key issues in the design of public-private solutions to address security threats:

01 ***Identification of the threat profile:*** *Determine who is committing the criminal or terrorist act and direct specific actions to counteract their activities.*

02 ***Analysis of targets and potential victims:*** *Establish against whom, against what or in relation to what the threat is made, including people, critical facilities or services that could be affected.*

03 ***Understanding the motivations behind threats:*** *Analyze the economic, ideological, or personal reasons and objectives that drive perpetrators to commit criminal or terrorist acts.*

04 ***Study of behavioral patterns:*** *Identify where and when threats are committed, as well as patterns of behavior in the execution of criminal or terrorist actions.*

05 ***Design of joint and collaborative solutions:*** *Address threats through public-private partnerships that combine technology, resources, information, and capabilities of both sectors.*

Successful implementation of public-private security solutions depends on effective collaboration between public and private actors and a comprehensive and programmed approach to the execution of the lines of action proposed in this chapter.

In the section of this Manual entitled "Problem Assessment", a total of 13 key factors were mentioned that should be taken into account at this stage of public-private partnership formulation.

Of these elements, a minimum of five are equally important for the following stages that have a direct impact on the design of a solution, as well as concrete courses of action.

Who perpetrates it?

Profile of the target whose action we seek to counteract. The actions to be developed must be oriented to specific profiles in order to generate the desired effect.

Obviously, not everyone can be fit into a single profile, but the work should be focused on a specific group of people, whose characteristics are probably associated with those of some of the other variables.

Thus, if the program claims to be related to threats to a crowded or massive event, it is important to analyze and determine the profile of the persons and/or organizations that have or could have interests and/or operational capacity to make the threat real through one or more terrorist attacks. Defining this profile will be useful for aligning the other actions and elements, as they should all be conditioned and associated with this particular profile.

Against whom, against what and/or in relation to what is the threat being made?

What is the audience, people, critical facilities, or services that could be affected by the threat you want to address? Determining that profile is just as important as determining who would or could target that audience, people, facilities, or services.

If we are in the presence of a crowded event, such as a sporting event or a concert, the direct victims of a terrorist attack, for example, would be the attending audience. Then, within this category, it is important to go further, since those who intend, could or would like to execute an attack could have different final objectives:

A to attack a specific group of people attending the activity;

B to destroy a sports facility or specific infrastructure, regardless of the type or profile of the potential victims;

C to interrupt a service or event;

D a combination of the above, among others.

Thus, it is necessary to profile the victims or affected population when the threat is directed against specific individuals or groups, an exercise that will not be the same if it is established that the criminal or terrorist action is directed against a facility. The variety is extensive, as it could be threats that, when they materialize, generate damage and harm to people in a more indirect or diffuse way, as in the case of drug trafficking or contraband, situations in which the affected groups could be residents living in neighborhoods or sectors taken over by drug trafficking groups or those who cannot compete with illicitly imported products.

Defining the potential target of attack, people or facilities that could be affected will make it possible to generate preventive mechanisms and to better protect them, but it will also be essential to define concrete lines of action.

If the threat is against a certain group of people, working with them on the threat will be key, as well as learning their routines and main vulnerabilities.

In the case of car theft, such an analysis would allow us to generate differentiated lines of action when the thefts are committed against parked vehicles, cases in which everything indicates that the characteristics of the owner or the person do not have a significant impact, as does indeed the type of vehicle. But when it comes to armed robbery of vehicles, it is quite likely that the type of vehicle is complemented by the profile of the person behind the wheel (elderly or with babies, whose response capacity is limited, for example).

This simple illustrative example makes us realize that the strategies for one type of theft or another, based only on the profile of the object or person involved, must be different. Does the private sector have anything to contribute to this? Of course, it does. Often, the mere requirement of a GPS system to acquire insurance can not only generate relevant data for the integrated project but also, produce an impact on the critical variables that we want to counter. Similarly, a public-private partnership around importing all new vehicles equipped with anti-theft systems is also useful. Marking vehicle parts and components could help a lot, an area in which the private sector has a lot to say, but which would be meaningless if the authority does not then incorporate this variable into its search operations. Again, collaborative integration is essential.

In the case of a threat against critical facilities or essential services committed using cybernetic means, whether for terrorist purposes or not, the lines of prevention, early detection and mitigation of damage will not be the same if the target is an airport or the state entity in charge of issuing identity documents, not because one or the other is less important, but because the architecture of their information systems is different.

When faced with a stadium, sports facility or event center, the layout of the emergency exits alone, a physical element that is difficult to change on short notice, could determine how plans are developed to mitigate terrorist attacks. The type of event, whether sporting, social or political, will also influence the way in which specific lines of action are decided upon.

What is the reason to perpetrate such attacks or crimes?

The motive, interest or reason behind an attack or crime provides a lot of information about important variables such as the profile of the person or organization that perpetrates or could perpetrate it, the profile of the person or group of people who are victims, as well as the modus operandi.

It is essential to consider the motivations of the threat we want to address to ensure an effective design. With the exception of a few organized threats of an ideological or personal nature, the vast majority have an economic objective or motivation. Whether it is terrorist attacks, drug trafficking, exploitation of human trafficking victims, contract killings, extortion, or arms smuggling, those behind the acts that affect security seek to generate economic gains.

Thus, a good assessment will allow us to understand that while some vehicles are stolen to be dismantled and sold for parts and components, others will be smuggled to other countries and exchanged for drugs or money, while there will be those that are stolen and abandoned after a few days, during which they were used to perpetrate other crimes. As can be seen, the motivations are diverse. Thus, we also find cases of vehicles that will not be exchanged for drugs, nor dismantled for parts, nor used to commit other crimes, but rather to adulterate their legal identity through cloning, in order to allow their fraudulent sale in the formal market.

Does the private sector have a say in this? They are the ones who buy and sell vehicle parts and components, in a market that will be affected by the introduction of stolen products. Thus, their contribution, in terms of knowledge about how the purchase and sale of these goods works, is extremely relevant and could give rise to specific and practical ideas about how to identify stolen products and what measures to adopt to prevent these crimes, such as the application of markings that facilitate identification by police agencies and inspection and control entities.

Will the contribution of auctioneers or auction houses be relevant, knowing that they often sell at public auctions destroyed vehicles that will never be repaired, and the sole purpose of buying them being is to use their identity in order to facilitate cloning into other stolen vehicles? Will it be beneficial to share databases of buyers or brokers in order to identify patterns compatible with the threat we intend to address? Any concrete line of work to be executed to this end will be more successful if we involve the proper representatives of the private sector.

The benefits will be enhanced when these same activities, and within the framework of the same project, are complemented and integrated with control actions by the authority in charge of tax control, which could be integrated into a strategy traditionally linked only to the police and which, in this case, could favor actions of greater impact.

Just as in the case of vehicle theft, when dealing with crowded spaces security, understanding the reasons and motivations will be relevant not only to assess the problem but also to design solutions. The theft of a tourist's camera is not the same as a terrorist attack on a hotel. The cloning of a tourist card will not be the same as the kidnapping of a tourist. The motivations in each case are different and, consequently, the way of dealing with the threat will vary according to these motivations.

It happens that probably the first and last contact of a tourist in a country will be with the state, specifically, the migration checkpoint at the border, but other than that, it will be the private sector that will have much more information: places visited, type of visit, incidents that occurred, size of family group, value of the tourist package, means of transportation used, among many other elements. Therefore, initiatives such as those of Mexico, through CAPTAs, or Ecuador, through PIATs, are interesting to analyze.[21]

Again, inclusion of the private sector in identifying problems and designing solutions is essential.

Where and when is it perpetrated?

Threats occur in specific geographical areas and, as a general rule, at specific times (days, hours, months). Some are continuous and permanent, as in the case of organized crime, while others are more occasional but have a greater impact, such as terrorist attacks and activities. Identifying these variables is essential in the design of security-related public-private lines of action, both because programmatic actions should be directed to these physical and temporal spaces, and also because circumscribing these concepts will provide better impact measurements.

[21] See notes 39 and 40 of the Manual, which explain these initiatives in greater detail.

Returning to our example of vehicle theft, knowing the place and time of day and night when the highest number of car thefts from parked cars take place, will allow us to design and implement more efficient prevention and control techniques when using decoy cars. Indeed, the use of vehicles equipped with remote monitoring (cameras, GPS, microphones) and control systems (lights, horns, door locking, engine start-stop) represents a very good working tool to counter this threat, but also a very expensive one. The purpose of a decoy car is to be stolen, not so much to stop people from getting into the car as soon as they get into it, but to find out the fate of the car and thus affect the entire value chain.

It is not only important that the decoy vehicle is stolen, but also that it is stolen as soon as possible. Having a decoy vehicle parked for weeks or months is not very profitable. In order to increase the probability of theft, we must use as a decoy the type, color and year of the most stolen vehicle and place it in the area or location with the highest theft rate. Will the parking lots of shopping malls with high incidence of robberies have something to say? Does it make sense to think of an alliance for these purposes? As long as we dismantle criminal organizations, will certain privately managed public spaces benefit?

It is not just a matter of placing the vehicle in a shopping mall parking lot. Collaborative work goes much further. From the use of cameras, early warnings, and even preventive advertising, these are private interventions that have a direct impact on public policy. If they are to function efficiently, they must be part of a joint collaborative program and integrated into a larger, planned, and measured solution.

A significant percentage of vehicles are parked in public spaces or spaces franchised out. The possibilities of control and supervision in all of them are limited to the police resources available for this task. If we assume that early detection of each of these cars, motorcycles or trucks is useful, in terms of identifying those parked units that have been previously stolen, then it will be essential to incorporate the private entities that have an impact on these public or franchised-out spaces into the design of the solution.

Let's look at an example. Let us imagine that, in certain geographical areas, countries or locales, the vehicles that park on the street, instead of paying for the parking meter with text messages or coins, an officer or employee is in charge of arrival and departure control. This person is an employee of a private company that has a concession for those parking spaces. Nowadays, a significant percentage of such employees are equipped with devices that, after entering the license plate, begin to count the elapsed time, to collect parking rates the moment the driver leaves. The vast majority of these devices have internet connection and GPS to facilitate reporting and to keep real-time control of the parking collection operation. In this context, how useful would it be for this database to be interconnected with the stolen vehicles database held by the authorities, so that every time a parking attendant enters the license plate of a stolen vehicle, this information is automatically reported to the authorities, even providing a geo-referenced location of that vehicle? A similar approach could be taken with highways and all other private entities that, having the possibility and capability to register vehicle data, do not have access to databases of stolen vehicles.

What is relevant is not to see this as a bilateral agreement between police and parking company or shopping mall, but as a public-private collaboration within the framework of a specific line of action that is an integral part of a much broader joint project.

On the other hand, in the cybernetic arena, it is also possible to identify the virtual places where threats could be realized or were realized in the past. This will help to generate better prevention mechanisms and reinforce systemic security.

It is a fact that a cyber attack, whether criminal or terrorist, can impact almost any type of open or semi-open virtual infrastructure, however a potential targets risk map could be produced in conjunction with the private sector. There is no doubt that a country's passport database or identity records could become targets of interest. The foregoing includes many government or police databases, including computer operation systems, such as in the case of fugitive registration, convictions, customs, or tax records.

It happens that attacking private targets can cause equal or greater damage to a country. Just imagine banking databases, or airline transportation databases, or those of any private company that operates facilities that provide public utility services such as a power company, cellular telephone company or airport. An outage of any of these operations of the private sector would inevitably be of great cost to a country, its inhabitants, and its security. Even so, expecting the State, on its own, to address this threat is not advisable. Once the vulnerable targets towards which a threat is directed or could be directed have been identified, if they are operated directly or indirectly by a non-public entity, be it a private company or a community association, their inclusion becomes critical, both in the assessment of the problem, and in the design and implementation of lines of work.

Behavioral patterns and joint solutions design.

A public-private partnership, in the terms proposed in this Handbook, represents an alternative way to address security threats, one that is different to the way they have traditionally been addressed.

In fact, the essence of this lies in the concept outlined above. The aim is to provide tools to design solutions that help achieve different results or further enhance the impact generated. For such public or private sector wanting to hinder certain terrorist or organized crime threats, obviously, doing the same thing will not produce greater effects, at least not at the desired levels. It is therefore advisable to change the way we work. One of these ways is precisely through a public-private partnership and collaboration aimed at reducing the risks presented by security threats. The contribution of the private sector through technology, resources, information, and capabilities will generate more advantageous conditions to prevent and/or detect a terrorist threat or one coming from organized crime.

On the contrary, while the State and the private sector face the challenge of incorporating changes in the way they work, a relevant percentage of terrorist, anti-social, anti-systemic and criminal groups will probably not, and will keep the way they operate the same, materializing their threats under similar behavioral patterns.

Unlike us and given that many of their objectives have been met, they do not have, to a large extent, any major incentive to change.

In other words, while the way we work should change to seek different results, those behind the main security threats tend to maintain the way they operate in order to maintain the same results they are already having.

The realization of this fact represents an opportunity to generate successful impact programs through joint initiatives between the public and private sectors, finding indicators in behavioral patterns that will facilitate the measurement, quantification, and identification of our threats.

Any solution design should consider this variable, to which both public and private entities have much to contribute.

For this purpose, the use of Fusion Centers or data analysis software will prove very useful. Both aspects, discussed later in this Manual, involve the participation of public and private actors.

Success will depend not only on the supply of experiences, ideas, and resources from each of the parties, but also on the execution of this line of action in a joint, programmed, and integrated manner, under the terms set forth in this Manual.

The most relevant:

This chapter analyzes the key aspects for the design of public-private solutions in the context of security and threat prevention. The main items to be highlighted are:

1. Identification of the threat profile: Determine who the perpetrators are and target specific actions to counter their activities.

2. Analysis of targets and potential victims: Establish who or what could be affected by the threat, including people, critical facilities, or services.

3. Understanding the motivations behind threats: Analyze the economic, ideological, or personal reasons that drive perpetrators to commit criminal or terrorist acts.

4. Study of behavioral patterns: Identify where and when threats and patterns are committed in the execution of criminal or terrorist actions.

5. Design of joint and collaborative solutions: Address threats through public-private partnerships that combine technology, resources, information, and capabilities of both sectors.

Successful implementation of public-private security solutions for depends on effective collaboration between public and private actors and a comprehensive and programmed approach to the execution of proposed actions.

Information processing

This chapter addresses the issue of information exchange between public and private entities in the context of partnerships to improve security. Generation, use and exchange of information are critical to the success of these partnerships, but they can also be sources of challenges and tensions. This chapter discusses the challenges related to data and information sharing, collaboration between entities and the dissemination of sensitive information. The chapter begins by addressing challenges and information sharing resistance between law enforcement agencies and public and private entities. We emphasize the importance of establishing clear guidelines and protocols, to ensure secure retention and proper exchange of sensitive data.

We discuss data and information exchange in detail, highlighting the need to identify the expected benefits and costs associated with information sharing. We suggest that all collaboration and information exchanges do not necessarily mean providing all the information, but rather identifying specific and concrete data, as well as analysis and evaluation.

Solutions are being explored to overcome the natural resistance to information sharing, such as the Fusion Centers in the USA, which allow data to be shared between public and private actors in a structured and collaborative way. Examples of similar initiatives in Europe are also mentioned.

Finally, the dissemination of sensitive information is addressed, highlighting the importance of adopting protocols to regulate this challenge. We propose dissemination level classification based on associated risks, including Red, Amber, Green and White, each with different levels of restriction.

This chapter highlights the importance of information exchange and collaboration between public and private entities in security partnerships. Challenges are examined and solutions are proposed to address data sharing resistance, with the goal of improving the effectiveness and success of these partnerships.

One of the critical aspects for the success of a public-private security partnership is the generation, use and exchange of information. Indeed, one of the main assets of security agencies and related public entities is usually the access, management, analysis, and disclosure of information.

So much so, that often the friction or collaboration problems between various agencies that are all part of the same government or state entity, are often the result of reluctance to share their own data among themselves, even though they are all part of the state.

In the private sector, the situation is not very different. Even when there are initiatives and activities for information exchange among the different actors, when the data is sensitive, reticence emerges as a defense mechanism in a highly competitive market.

More commonly than one might think, the value attributed to the information that a given entity possesses is so high that it sometimes prefers to continue working in isolation than to obtain complementary benefits from collaborative work. Many entities, both public and private, will be willing to sacrifice positive externalities associated with shared use in order not to share data considered key within their respective organization.

It is advisable to have clear guidelines as to what type of information public authorities can share with the private sector, in accordance with data protection regulations. Similarly, minimum standards should be established for the secure retention of such information, ensuring that all stakeholders know how to handle background information properly.

Protocols for information sharing between private and public entities can help establish the principles for data sharing arrangements within the partnership, clearly defining what type of information will be subject to joint work, by whom, with whom, for what purpose and with what safeguards. Shared understanding of the limits of such a protocol is essential.

Data and information exchange

Although this does not occur at all levels, nor with all agencies, information sharing is a key factor in public-private partnerships that needs to be managed efficiently.

Private entities often find it easier to identify areas of common interest with other strategic partners in the same sector and find it easier to make trade-offs by sharing key information, on the understanding that this could provide them with quantifiable benefits within the framework of a given project. Sometimes, this greater flexibility is generated in a less restrictive environment than that which regulates the public sector, in terms of information exchange, but also as a consequence of a more pragmatic, results-oriented vision, which is more typical of the private world.

The main challenge for the members of a partnership will be to achieve high levels of willingness, collaboration, and willingness in security projects in which the expected benefit will not be achieved in the short term and in which the financial returns, although existing, will be more diffuse and difficult to measure.

If the aforementioned challenges arise in relation to data and background information exchange in security projects, when these occur only in one of the sectors, whether public or private, the challenge and scenario becomes even more complex when the need to transfer and work on joint information must happen between both groups.

1. The *first step* is to **understand this natural reluctance** to share with third parties an asset that the various players in an alliance might consider essential, both because of the cost involved in generating it and because of the added value it represents to their own entity.

2. The *second step* consists of **identifying the benefits** expected or sought by each participating entity and showing them how the information concessions made will generate lower costs that will be offset by the benefits the project is expected to generate. This is essential, since regulatory enforcement for information exchange is not always successful and, moreover, escapes from an association concept to become more of an imposition.

   So much so that, on occasion, when the provision of data and information is the result of an obligation or imposition, it ends up as just that: flat provision of data, losing the intelligence and analysis that the issuer of the information could provide in relation to it.

   Therefore, when talking about information exchange, it is important to consider not only a neutral background in terms of quantity or type of data, but also evaluations, analysis and intelligence, elements that add quality and value to the information and, ultimately, to the project.

3. *Thirdly*, once the individual costs, limitations and resistance have been identified, as well as the benefits and expectations for each of the members, it becomes necessary to **show** each of them that, in terms of cost-benefit, there will be **greater profit** in a collaborative scenario than in an individual one.

Collaborating and exchanging information does not necessarily mean handing over everything. It involves identifying both specific and concrete data needed for the specific project as well as the analysis and evaluation of the project.

Collaboration entails regulating how this information will be treated, the way it will be processed and the mechanisms for its dissemination.

Each of these aspects must finally be incorporated into a specific protocol or agreement that is integrated into the general collaboration framework.

It could happen, for example, that the success of a line of work in a public-private project determines that certain private actors who are natural competitors in the market must provide cross-referenced information. This collaboration could, in certain cases and depending on the type of project, actors and data involved, be conditioned to the shared data being used for the integral analysis of information, but that the storage of all the information be done by a third party member of the project, with the commitment to show only the results of the analysis, but not to share the databases provided among all the members of the project.

Let us assume that the highways are required to send data of all the license plates circulating, so that these data can be crossed-referenced with stolen vehicles records, thus enabling a series of prevention and control actions to be triggered.

It is likely that, if the project were to consider the creation of a large database of all traffic on all highways, this could generate some resistance among highways, who compete for the traffic market. The solution is to identify this natural and sometimes even healthy mistrust, and to find a way to manage the information as a whole while safeguarding compartmentalization, which would be achieved - *in* this *specific* case - by means of three steps:

A. the identification of the challenge, needs, expectations, fears, resistances and benefits;

B. holding a protocol or agreement that makes all the factors at stake compatible, delivering individual bases to a single physical actor or, to a computer system, which will process the information by accessing individual repositories without creating a database, and without sharing the source data with the other actors but only the results of the analysis; and

C. the implementation of a control and monitoring system to ensure that the previous point is respected on an ongoing basis, as an essential requirement to ensure that the trust put into play is not broken.

In security, information is - as we have stated - an essential asset. The more information available, the better the analysis and the more successful the resulting lines of work. Expecting entities to give up their natural reluctance to share their data from one day to the next is difficult and sometimes, in some cases, may even be utopian. Fortunately, nowadays computer systems allow massive analysis, data mining and cross-checking of information without the need to create an integrated database, just by consulting individual sources of information one by one.

In this way, a security project that integrates private and public actors could successfully overcome this natural barrier linked to mutual trust and its impact on the exchange and use of proprietary information for collective benefit.

Fusion Centers have become an interesting alternative for sharing data between public and private actors. These are working methodologies focused on collecting, processing, analyzing, and disseminating a large amount of data in order to prevent and/or detect terrorist or organized crime activities at an early stage. A fusion center is comprised by structured and organized mechanisms and methods of inter-institutional data exchange, operating under a collaborative logic.

These centers are instances where representatives of the main agencies involved in the investigation and prevention of terrorism and organized crime collaborate through predefined protocols to exchange of information in order to achieve a clearer and more complete picture of a given threat. Even though the main fusion centers are made up of government agencies, several initiatives have begun to incorporate the private sector, therefore it is essential that they receive benefits from this participation through feedback, otherwise they will feel that they are only giving and receiving nothing in return.

Regardless of the model to be followed to implement a fusion center, the comparative advantage they provide is to quickly make available the existing information among many agencies and entities without the need for the requesting authority to directly access the database of the one that is being required to provide the information. This solves one of the main security challenges: the natural resistance to allow unlimited access to proprietary databases.

This trend began to spread more widely in the United States after the September 11 attacks. The United States realized that the intelligence and investigation agencies possessed a lot more information than previously thought, which was not used in the best way because it was disaggregated and disseminated among a multiplicity of entities.

Aware that the unification of databases is a task with little chance of success, they sought to create methods that would facilitate the exchange or joint processing of information.

According to the U.S. Department of Homeland Security, there are currently 78 fusion centers in the United States.[22] There are so many that there is even a National Network of Fusion Centers. Although their proliferation had terrorist threats as one of their main targets, today their use is extended to all criminality, including successful cases of countering human trafficking.[23,24]

Similar initiatives exist in Europe, although with a major focus on terrorist threats, highlighting experiences in Belgium, Germany, Italy, the Netherlands, Spain, and the United Kingdom.[25]

[22] https://www.dhs.gov/fusion-center-locations-and-contact-information
[23] https://www.dhs.gov/2015-fusion-center-success-stories
[24] https://wvva.com/2020/01/31/w-va-fusion-center-helps-combat-human-trafficking/
[25] https://icct.nl/app/uploads/2019/02/ICCT-VanderVeer-Bos-VanderHeide-Fusion-Centres-in-Six-European-Countries.pdf

Dissemination of sensitive information

The use of data considered sensitive or strategic in terms of joint processing is one thing, but the way such data is disseminated is another. With regard to this second aspect, it is necessary to adopt protocols that regulate this challenge in advance in a clear and precise manner, so that stakeholders can weigh the costs and benefits, and - in the event of moving forward - have predefined guidelines that can be monitored.

Dissemination can happen within the framework of isolated initiatives or as part of a more comprehensive project. The first case would be, for example, the dissemination done by the alert systems for terrorism prevention of various countries to both public and private organizations regarding the status and level of alert in terrorism prevention. Something similar happens in tourism security, when a relevant number of governments decide to inform their citizens of the threat levels to which they could be exposed if they visit a certain destination.

On the other hand, private sector companies may be in the position to report to certain public entities risk indicators or sensitive variables calculated and stored by private entities, but which taken as a whole give the public entity an added value and a vision with more perspective on the problem to be addressed.

The dissemination of data in both one-directional and cross-directional formats acquires added value if this shared information is analyzed and processed by some, or by the entirety of the members of a public-private partnership, whether results are to be disseminated internally (among the members) or externally (media, press, other organizations, etc.).

Hence, such dissemination - internal or external - must be subject to specific regulations. Protocols addressing this should consider dissemination levels around the associated risks. Let's take a look at a proposal.

* **Red:** Non-disclosed and restricted information, only for representatives present at the meeting or project.

Exchange: This information is exclusively exchanged with certain preselected persons or persons identified by the information sender. If the data flow is done electronically or in writing, it will be necessary to take specific measures to secure the information, possibly including an assurance that the person and entity to whom it is addressed is the sole recipient and is properly identified.

Risks to be mitigated: This type of information, classified as red, is such that if it were to reach unauthorized persons:

* *could endanger lives.*
* *could seriously harm a company, institution, or government agency in a number of ways.*
* *could seriously damage relationships with other companies, governments, organizations, or partners.*

* **Amber:** Limited disclosure restricted to information sharing group members and those in their organizations that "need to know" in order to take action.

Exchange: Information is only exchanged with a select group of individuals, from a limited number of entities. They are allowed to share this information within their own organization on a "need to know" basis.

Risks to be mitigated: If this type of information were to be passed on to unauthorized persons:

* *could still harm a company, institution, or government agency, but with fewer consequences than "red" information.*
* *may affect relationships with other companies, governments, organizations, or partners.*

* **Green:** This information can be shared with a wider group of individuals or entities, both within and outside the public-private partnership, while its publication may not be advisable in print or on social media.

Exchange: This information is only exchanged with a specific group of people or entities. Data may, however, be shared with other organizations, information platforms or individuals employed in security-related positions. This information should not be publicly exchanged or posted on public websites.

Risks to be mitigated: This is information that if passed on to unauthorized persons could:

* *result in disadvantages, significant to a lesser extent, for the company, institution, or government agency.*
* *damage relations with other companies, institutions, or government agencies.*
* *lead to the publication of the information by the media.*

* **White:** Unrestricted dissemination.

Exchange: Public information that may be disseminated without restriction.

Risks to be mitigated: Minimal or null. The information is not sensitive and can be made public. Information may, if appropriate or desirable, be disseminated through open sources such as social networks.

The most relevant:

This chapter addresses the exchange of information between public and private entities in partnerships to improve security. The main items to highlight are:

1. Challenges and information exchange resistance: Establish clear guidelines and protocols to ensure the secure retention and proper exchange of sensitive data.

2. Benefits and costs of data exchange: Identify specific and concrete data to share, as well as analysis and evaluation, without giving away all the information.

3. Solutions to overcome information exchange resistance: Implement Fusion Centers and other initiatives that allow structured and collaborative data sharing between public and private actors.

4. Dissemination of sensitive information: Adopt protocols and dissemination levels classifications based on the associated risks to regulate sensitive data handling.

The chapter highlights the importance of information sharing and collaboration in security partnerships, examines the challenges and proposes solutions to improve the effectiveness and success of these partnerships.

Building trust

In this chapter we explore the difficulties and challenges facing public-private partnerships in the field of security and violence or terrorism prevention. The importance of trust and cooperation between the public and private sectors is critical to effectively address these complex and multifaceted problems. Firstly, we discuss the need to offer alternatives that do not entail the transfer of financial resources, as well as the need to reduce bureaucratic options to facilitate collaboration. In addition, we emphasize the importance of agreeing upon common objectives, which can serve as a basis for cooperation and joint work.

A commitment statement can be useful to formalize the collaboration, establishing responsibilities, activities, and goals to be achieved by both parties. We also suggest considering the intervention of neutral actors, such as civil society organizations, to facilitate partnership building with the private sector.

Communication is a key aspect of trust building. On the one hand, it is important to disseminate both successes and failures jointly, avoiding attributing responsibility to a single actor. On the other hand, care must be taken when sharing know-how or specific knowledge acquired during the project, as it could benefit undesired actors. To address these issues, we recommend communication aspects to be regulated through jointly agreed communication protocols and policies.

Finally, we address the need to establish special norms and regulations to facilitate security public-private partnerships, providing an appropriate legal and administrative framework. This may include agreements and conventions between states, especially when facing international threats such as terrorism or transnational organized crime.

This chapter highlights the importance of building trust and developing effective strategies to overcome the challenges facing security public-private partnerships. Successful collaboration between the two sectors is crucial to address and prevent situations of violence and terrorism that affect the security of the population.

Institutional or corporate mistrust is perhaps one of the main challenges in building a successful public-private partnership. How and what type of information to exchange and disseminate is one of the most critical aspects to consider. Hence, a special section has been dedicated to it. But there is more. This chapter will address some of them.

Offer alternatives that do not entail transfer of resources.

We must dismiss the perception that the biggest strength of the private sector is its capacity to finance programs. That's one possibility, but there are other interesting and creative ways to enter into alliances. Therefore, it is important to create alternatives that do not require the transfer of financial resources to make the execution of joint projects feasible.

Generate less bureaucratic alternatives

Companies tend to avoid entering into partnerships with the public sector due to the high degree of bureaucracy and excessive procedures. Even though these procedures sometimes exist to guarantee public interest, it is advisable to think about how to reduce the levels of bureaucracy and make them simpler in order to attract the interest of companies and to facilitate partnerships.

Agree upon common objectives

One way to establish the partnership is for the public and private sectors to agree upon common objectives. Thus, if a common objective is to reduce the involvement of teenagers and young people in situations of violence and promote their full development, it becomes possible to establish a partnership that integrates a project already developed by a given company that takes in young people who are former offenders to work as employees, under a program developed by the public sector that offers social, legal and psychological support to young people in conflict with the law and their families. These are two programs that have already been implemented, whose common objective is the full development of young people, in order to reduce the chances of them coming into conflict with the law. The company does not need to invest additional resources beyond what it already invests, nor does the public sector. Once the first part has been resolved, which is identifying programs with common objectives, then the second part must be tackled, which consists of integrating work strategies and monitoring them to ensure that they meet the agreed common objective.

Sign a commitment declaration

A statement of commitment can serve to formalize the working model proposed in the previous segment, or to plan a new project, assigning new responsibilities to both parties. It is important that the statement establishes general responsibilities, activities, and goals to be achieved by the parties.

Then, the specific regulation of rights and obligations, administrative and operational procedures will be established through specific work protocols.

Consider the involvement of more neutral actors.

Formalizing the partnership through a civil society organization is an interesting alternative for the private sector to participate in violence or terrorism prevention initiatives. The public sector can seek out local civil society organizations and outline joint proposals, with the involvement of the private sector. In general, NGOs already have partners in the private sector and joint work with them can make it easier to build alliances.

Dissemination of successes and failures

Many partnerships between public and private partners fail when the success of the projects is publicized by one of the actors to the detriment of others. It is natural to want to show good results and receive recognition from the community or a certain sector. Mistakenly forgetting or motivationally displacing some of the project's stakeholders is extremely harmful.

Similarly, a failure, problem or difficulty experienced in a public-private action project or program to address security threats should not be blamed on only one of the actors.

If the project is the result of joint work, a collaborative initiative, and a multi-entity alliance, both successes and failures must be celebrated on the one hand, and assumed on the other, by all the actors involved in the project, without exception.

Take care of the *know how*

Disseminating results within the group of the public-private alliance or project is fundamental. Doing so towards the community and the media is very relevant. Although it is not exactly the same information that is communicated in both cases, these are activities that must be taken care of.

The success of the strategy will be the result of a well-prepared recipe. As an example, we can show the cooked cake, and even explain its components in broad strokes. What is not recommended is to share the secret ingredient with third parties.

Many security project participants will be eager to show results. However, telling the distinctive details that made the difference of a successful project and sharing the *know-how* may generate more costs than expected.

Sharing the recipe generates, of course, an immediate benefit, as the community and the media will marvel at this new ingredient or formula. While this effect will be seen in the short term, what will happen in the long term is that the entities and individuals that are the target of the threat, be they terrorist groups or criminal organizations, will have access to the same information, and will also understand the innovative or distinctive methodologies used, from which they will probably take note, learn, generate countermeasures and modify their actions. If the work plan for our project was prepared based on an assessment and the identification of specific parameters, modus operandi and behavioral patterns, any change in any of these variables will not only detract from the positive impact of the work but will also take time to detect and adapt public-private intervention.

Therefore, disseminating and communicating is necessary. Showing results, even more. Explaining the benefits of working together is essential. But making *know-how* available to everyone in its most detailed expression is not advisable. Such satisfaction should be reserved for internal review meetings.

Regulating communication

To ensure greater success, reduce the risk of internal conflicts and generate greater trust among all members of a partnership, it is essential to have a protocol for dissemination and relations with the community and the media.

We recommend that a communications policy be jointly designed and agreed upon and that protocols be drafted to be implemented in the field, including aspects such as spokespersonship, communications approach, frequency of contacts with the media and the community, crisis management, among others.

Special regulations

In addition to working to reduce the natural barriers that could entail an eventual and considerable degree of bureaucracy, sometimes the regulatory framework, be it legal, administrative, or even constitutional, could represent an important challenge that affects the motivations -especially- of the private sector. It is advisable not only to generate a specific regulatory framework to promote anti-corruption or transparency activities, but also to generate concrete conditions that encourage the private sector to enter into a partnership with the State.

When it comes to public tenders for the construction of large public works such as highways, dams or airports, many states sign the respective contracts with the private sector within the framework of a complete set of specific regulations that govern this type of joint activities. In security matters, this approach is not as common. The larger the project, and the higher the investment or involvement of the private sector, the more necessary it will be to have legal frameworks that ensure stability, long-term results projection, and trust.

If the threat is of an international nature, as is the case with terrorism or some transnational organized crime phenomena, extending the regulatory framework to agreements or conventions between States will be convenient.

The most relevant:

This chapter addresses the challenges and difficulties in public-private partnerships in the field of security and violence or terrorism prevention. The key aspects to highlight are:

1. Offer non-financial and less bureaucratic alternatives to facilitate collaboration.

2. Establish common objectives as a basis for cooperation and joint work.

3. Use statements of commitment and the intervention of neutral actors to formalize and strengthen partnerships.

4. Foster communication and trust through joint sharing of successes and failures, and the establishment of agreed communication protocols and policies.

5. Create special regulations to facilitate security partnerships, including agreements and conventions between States.

This chapter highlights the importance of building trust and developing effective strategies to overcome challenges in public-private security partnerships, with successful collaboration between the two sectors being fundamental to address and prevent situations of violence and terrorism.

Relevant aspects in the design of joint projects

This chapter addresses relevant aspects in the design of joint security projects, focusing on two fundamentals: the economic factor and gender policies. The objective is to provide a comprehensive view of how these elements can be incorporated into the creation and execution of efficient and effective public-private partnerships.

Firstly, the chapter examines supply and demand from an economic perspective, arguing that a comprehensive approach to combating threats such as organized crime, terrorism and corruption must address both supply of illicit goods and services and demand considering its determinants. The importance of destabilizing the economic structures that sustain these threats, affecting their assets and undermining their financial capacity, is emphasized. Second, the chapter addresses the incorporation of gender policies in the design and development of joint projects. We highlight the importance of integrating gender perspective from the beginning of a project, both in terms of internal organization and target audience. We include practical recommendations to promote gender equality and inclusion in the organizational structure, recruitment and personnel management processes, trainings, internal protocols, intersectional approach, imaging, and language.

The chapter provides a solid framework for the creation and execution of efficient and effective joint security projects, highlighting the importance of considering both the economic factor and gender policies in their design and development. By addressing these aspects in a comprehensive manner, public-private partnerships can strengthen their approach and improve their medium- and long-term results in the fight against today's threats.

Supply and demand. The economic factor.

Security projects, whether autonomous from the public or private sectors, and those resulting from a joint alliance, usually approach the threat from the perspective of who or what generates it. If we analyze it from an economic point of view, and understanding that, in general, there is a financial motivation behind it, the threat is usually addressed from the supply side.

The focus is usually on the drug trafficker, the hitman, the money launderer, the human trafficker, the terrorist, the arms dealer, or the smuggler. Sometimes they are also oriented, in a complementary manner, to the object or subject of the crime, it being drugs, stolen vehicles, illegal weapons, victims of trafficking.

This approach does not always extend to all the factors, actors and elements that shape and condition demand. The drug user; the "client" who wants the victims of human trafficking; the buyer of pirated or contraband goods; the purchaser of weapons; the one who finances terrorist activities.

If we understand criminal groups, organized crime, terrorism and other threats as entities whose purposes have an economic nature, as if it were a company, then an efficient public-private action plan must address both factors related to the supply and the object of the illicit goods, products or services it transacts, as well as the demand for such goods products or services and those persons or groups that condition it.

The more threats materialize, the greater the financial revenue of criminal groups. The more terrorist attacks are committed, the more funding will they receive. As the money grows, the entities and groups behind the threats become stronger and stronger, which in turn will allow them to materialize new and greater threats, with increasingly significant quotas of impunity.

This is why a public-private security alliance should consider an analysis and confrontation of the financial and economic foundations of the groups or entities responsible for these threats, regardless of their size.

The most efficient way to combat them, be it organized crime, terrorism, corruption, money laundering or the channeling of social demands through organized violence, is through the destabilization of the economic structures that support them.

Asset impairment is essential, and any project designed with this component will show positive effects in the medium and long term.

Gender policies

Gender approach must be incorporated not only from the point of view of the organization and project management in relation to its members, but also towards the target audience to whom it is directed and for whose benefit the activity is deployed.

* Context and importance

The Major Events Security Planning Guide and Manual, by UNICRI and CICTE/OAS, 2011[26] recommends integrating gender perspective from the very beginning of a public-private project, in its design stage, which should be complemented during the development of the project, as well as during evaluation and reporting.

> *"Gender equality, inclusion and diversity are achieved through carefully designed HR strategies and practices and with resources based on the principles of equality and non-discrimination to which States have committed themselves in international human rights treaties. Starting with upper leadership, managing the institution in a way that reflects the principles of equality and non-discrimination, including the promotion of diversity, and ensuring that they are taken seriously, sets the tone and shows what is and is not permissible. Gender equality leadership does not only move downwards through the hierarchy, but ideally includes openness among senior management to the input, suggestions, and concerns of more junior staff. Accountability, disciplinary, grievance and oversight mechanisms relating to the security and justice sector also play a key role in supporting inclusiveness, non-discrimination, and gender equality.".*[27]

As indicated in the European Union's Institutional Transformation Manual[28], which provides tools for gender mainstreaming, it is the **responsibility** of the entire organizational hierarchy of an entity and a project to incorporate gender equality and human rights into the cultural fabric of the participating entities. Gender equality must be a guiding principle in all areas of the public-private partnership and in each of its members, including aspects that interact with race, ethnicity, class, religion, rank, and other factors. These principles should be clearly communicated with all staff members and, where possible, incorporated into official mission and vision statements, applied at the organizational structure level, as well as in institutional documents. It also means working on the elimination of sexist, exclusionary and discriminatory language.

[26] See the Major Events Security Planning Guide and Manual, by UNICRI and CICTE OAS. Document updated in 2021 by consultants Brian London, Superintendent (R) and Brendan Heffernan Chief Superintendent (R), both of the Royal Canadian Mounted Police.
[27] DCAF, OSCE/ODIHR, UN Women (2019) Security Sector Governance, Security Sector Reform and Gender."
[28] https://eige.europa.eu/gender-mainstreaming/toolkits/gender-institutional-transformation

It is not only a matter of complying with legal requirements, but also of promoting the effective inclusion of the gender perspective by integrating it into all processes and practices of a public-private partnership.

Gender-balanced recruitment and personnel management processes will ensure and strengthen women's participation in leadership and decision-making roles. Gender equality in a public-private partnership involves recognizing and involving the entire lesbian, gay, bisexual, transgender, intersex, and other communities, both in personnel processes and in the development of work plans.

* **Elements to consider**

In the more concrete definition of how to incorporate gender policies, we recommend taking into account the following elements:

External policies. Policies should be incorporated in relation to the target community, beneficiary or affected community, and type of threat the project intends to counter.

Internal policies. Similarly, these policies should be considered in terms of how the project and its team are internally organized and with an effect on them.

Training. Gender equality training both for the staff and the team coordinating and executing the project, should be done at the beginning of the project and on an ongoing basis.

Protocols. For the purposes of the internal work of both coordinating and operating personnel, it is important to have protocols for prevention, detection, and response to situations of possible harassment, bullying, discrimination and practices that violate gender equality.

Intersectionality. A number of factors such as education, income level, religion, race, disability, among others, impact people differently, and they must be taken into account. The elements that affect equality do not behave in the same way, so that a given situation may have a different impact on two different people.

[29] **Thus, by way of example, a white, university-educated woman living in a developed country, although she may experience inequality quotas, the level of impact will not be the same as that of an indigenous woman of limited resources and with a low educational and economic level. This fact coupled with the concept of intersectionality should motivate us to identify differences and develop specific strategies tailored for each of the groups.**

Imaging. One of the fastest and most efficient ways to generate impact and to promote messages associated with the importance of gender and equality policies is through images, their use is highly recommended.

Language. Both internally and externally, the project must use inclusive language that generates a culture and normalizes equality and gender perspective among the beneficiaries of the public-private initiative, as well as among the teams working on the project.

The most relevant:

This chapter focuses on two key aspects for the design of joint security projects within public-private partnerships: the economic factor and gender policies. The main issues to highlight are:

1. Addressing both supply and demand to counter threats, destabilizing the economic structures that sustain them and affecting their assets and financial capability.

2. Integrate gender policies from the beginning of a project, considering the internal organization and the target audience, promoting gender equality and inclusion in all aspects of the project.

The chapter provides a solid framework for creating and implementing efficient and effective joint security projects, stressing the importance of considering both the economic factor and gender policies in design and development. By addressing these aspects in a comprehensive manner, public-private partnerships can improve their medium- and long-term performance countering today's threats.

Examples and ideas

This chapter will address the importance of public-private security partnerships, analyzing various success stories in which two-way collaboration between the two sectors has had a positive impact on the prevention, detection, mitigation, and response to different threats. Concrete examples of partnerships will be presented in areas such as human trafficking, drugs, victims of criminal violence, theft, stolen vehicles, labor reinsertion, critical infrastructure, biosecurity, technological development, and tourism, among others.

Public-private security partnerships have proven to be valuable tools for effectively and efficiently addressing various security challenges. Through two-way collaboration between the two sectors, innovative solutions have been accomplished, adding value to the projects, and increasing the positive rate of return.

Some outstanding examples include the training of transportation personnel for the early detection of human trafficking, cooperation between electricity companies and authorities to address security problems in impoverished areas, financial support for victims of criminal violence, the marking of stolen products, collaboration in the surveillance of public spaces, the recovery of stolen vehicles, the promotion of local security councils, the reinsertion of people with criminal records into the labor market, the development of critical infrastructure, biosecurity and tourism.

This section presents a series of cases in which public-private partnerships have been successful in addressing different security challenges. These examples serve as a reference for future collaborations between both sectors, always seeking to enhance prevention, detection, mitigation and response to the threats facing our societies.

Throughout this Manual, several examples of public-private security partnerships have been introduced. Except in exceptional cases, we have tried to exclude those projects in which, although both sectors have been involved, the relationship between them is rather unidirectional, as is the case when private entities finance specific security projects -such as community panic buttons or a mobile emergency application- or when the public sector deploys an offer through a public bid for security funds or one where the whole community may apply.

There are several examples of success that deserve to be mentioned and in which bi- or multidirectional collaboration proved to be an innovative factor that in addition to adding value to the respective projects, increased the positive rate of return. Rather than a detailed study of each of the cases, the aim is to show the varied extent to which a public-private partnership can be used to address security threats, whether from the standpoint of prevention, early detection, mitigation, or response.

* Human trafficking and public transport

Training and education program for flight attendants, flight personnel and commercial airline operators to detect early indicators of human trafficking, which are reported to the authorities prior to the landing of a flight, facilitating the control and detection of suspects, as well as the rescue of the victims. Reporting is not random and follows a previously agreed plan between the public sector agencies for prevention and investigation on the one side, and the transport companies on the other.

Among the indicators applied, we can mention the presence of teenagers or young women traveling accompanied by adults who are not their direct relatives, who sit in an airplane as far away as possible from an aisle, limiting contact with airline personnel as much as possible, to the point of not leaving them alone at any time, not even to go to the bathroom and not allowing them to talk to the crew, not even to choose their meal preferences. None of this alone indicates that we are in the presence of human trafficking, but rather, these are indicators that, analyzed with others, raise the level of risk, and help the airline crew identify potential cases.

Similar initiatives can be deployed in airport terminals through civil society organizations dedicated to combating human trafficking, whose work teams are made up of rescued victims or survivors and who are better able to detect potential cases in such locations. While the public sector manages to address a crime in a much more efficient manner, the private entity conducts its detection activities in a safer, more controlled theater and place of operations with a greater flow of potential cases.

An interesting example of this type of partnership or initiative is the Blue Lightning Initiative (BLI), an element of the United Nations Blue Campaign against human trafficking developed by the United States Department of Homeland Security, with the participation of the United States Department of Transportation and Customs and Border Protection.

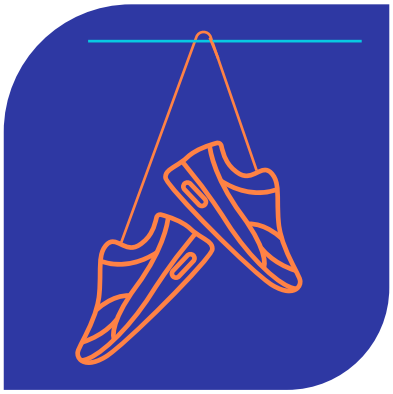
BLI trains aviation personnel to identify potential traffickers and victims of human trafficking, and to report their suspicions to law enforcement agencies. Through the end of 2022, more than 200,000 aviation industry personnel have been trained through BLI, and practical advice continues being given to law enforcement.[30,31]

The international community has consistently supported these initiatives, validating the public-private partnership as an efficient mechanism to address the security threats posed by human trafficking.[32]

* Drugs and electricity

Vastly impoverished sectors in some cities have shoes hung by their laces on their power lines, as symbols of territorial control, drug sales or illicit activities. While these shoes generate physical environments that increase the sense of power of certain criminal groups, they foster a sense of insecurity among the population and represent a security problem for the communities residing in those sectors.

What seems to be an exclusive problem for the authorities and the community, becomes a headache for the electric companies that must perform maintenance in high-risk areas. The result, often enough, is that the police do not remove the shoes because it is not their job and because they do not know how to climb the poles and wires without risk, while the electric companies do not do so for fear of reprisals or being attacked by the groups or entities responsible for hanging those shoes.



In this context, a public-private partnership allows the formation of mixed or joint crews of police officers and electric company officials. The protection provided by the former to the latter makes their work possible, which in turn increases the sense of security, improving the environment for a given community and eliminating signs of criminal co-optation.

[30] **For more information see** https://www.dhs.gov/news/2023/01/25/dhs-and-dot-host-joint-intersections-human-trafficking-and-international-aviation
[31] **For other cases of interest, see:**
-https://www.nytimes.com/2017/02/07/us/flight-attendants-human-trafficking.html
-https://www.aa.com/i18n/customer-service/about-us/combating-human-trafficking.jsp
[32] **See** https://www.unodc.org/unodc/en/frontpage/2021/April/unodc-engages-public-private-partnerships-in-the-fight-against-human-trafficking.html

* Victims and the financial industry

Many victims of crime violence live in contexts or areas where it is highly probable that they will again suffer the same crimes and harm. The circle of poverty or the social conditions of certain places prevent them from leaving, which may motivate a public-private alliance for support and assistance through giving loans or financial instruments that -without the endorsement of the state- would hardly be granted by a bank to people whose risk classification is high. It is not only a matter of facilitating the opening of checking accounts or getting loans, which in some cases already means a lot, but also of accompanying these people and assisting them in terms of training or business entrepreneurship coaching, self-help programs.

A public-private partnership goes far beyond bidding for services and handing over money or signing as a state guarantor for a private obligation. Success necessarily involves designing a joint program that identifies needs and benefits for all stakeholders, defines roles, assigns responsibilities, agrees on a common communication policy, and contains significant amounts of mutual feedback.

A successful example of such an initiative is Canada's *Project Recover*. It is based on the premise that financial fraud and identity theft are an important component in the exploitation of a survivor of human trafficking.

This project is led by a corporation under Canada's Not-for-Profit Corporations Act and represents a voluntary initiative by financial services industry executives, providing support to survivors and advocating on their behalf with creditors. Support for victims and survivors is free of charge.[33] The role of the State not only endorses the project, but also provides training. Something similar is happening in the United States with the Anti-Trafficking Intelligence Initiative (ATII), which counters human trafficking globally by promoting corporate social responsibility through increased awareness, facilitating intelligence integration and technological advancement, and fostering strategic data collaboration.[34]

[33] See https://projectrecover.ca/
[34] See https://followmoneyfightslavery.org/

* Theft and markings

A high percentage of theft crimes are committed so that the perpetrators can sell the stolen goods. Practically every country on the planet has informal markets that offer a space for commercial transactions of products that mix licit and stolen goods. One of the great challenges for the authorities when inspecting or controlling these markets is to associate a product with a specific victim and crime, as a means of seizing the goods, arresting the seller or retailer of stolen goods, and returning the goods to the victim.

We may suspect that certain products are stolen, but there is little progress to be made other than tax offenses for non-payment of taxes, or administrative offenses for selling objects without permission from the authorities.

People continue to buy these products knowingly or at least knowing that there is a high probability that they have been stolen, especially because of their low price. In order to efficiently counter theft or property crime, it is necessary to complement existing actions against the supply side of the market (who steals and sells) working also on the demand side (who buys).

In this context, a public-private partnership can make an important difference in achieving even better results, through various lines of action: a) ongoing work and loyalty building of sellers who want to adhere to the law; advertising campaigns to avoid buying stolen products; inter-agency control through agencies complementary to the police, such as tax collection services or customs; integrating private initiatives for marking products whose databases are in private hands and allow easy identification of the owner of a good, among others.

But even if we had an efficient and comprehensive system for marking products to facilitate their identification and connection with their respective owner, this contribution from the private sector will be of no use if the authorities do not work on actively searching for these markings, contacting the victims, and providing feedback to the industry with information and results. Isolated initiatives from each sector will never achieve the same success rates that would be achieved through the integration of a joint project.

* Public spaces and surveillance

When a crime is committed, or when a large number of crimes affect an area, it becomes a serious security problem and the time the police takes to react is essential. A robbery or street assault that is not solved within hours has an extremely low probability of not being solved weeks later. The large number of filed cases not only generates a sense of impunity, but directly facilitates it.

The above scenario is even more critical in the area of tourism security. Criminal groups know that the speed at which criminal justice systems address theft in public spaces works in their favor. If the chosen victim is a tourist, the probability of conducting successful investigations is even lower, especially when the tourist is a foreigner. Indeed, when a tourist suffers a robbery - let's say of his cell phone or camera - they experience language barriers and lack of knowledge of the operation of the local justice system, meanwhile, their active participation in the process is hindered, either because they have to travel back to their country that same day or will do so in the next few days.

Among the various measures that could be mentioned to address such challenge are audiovisual records, which usually have a more immediate effect and impact, making it possible to find the person(s) who approached the tourist, which could lead to recovering their belongings.

Thus, being able to register cameras in range of the incident within moments after a crime has been committed has a much greater and better result than doing so weeks or months later. Incidentally, a significant number of these cameras are operated by the private sector. Often enough, the authority does not know who owns cameras, nor where they are located, what area they cover, what is their recording system and its duration, and what resolution capacity they have, among other features. This survey work is usually conducted in the case of serious high-impact crimes, such as homicide or rape, but not for the theft of cell phones and money from tourists.

Thus, when a crime of this nature occurs, a pilgrimage generally begins in search of cameras or recordings in the possession of the residents and neighbors of the sector, wasting valuable reaction time. If we wanted to follow up and view the recordings of the path the offender took to get to and/or leave the scene, it would be even more difficult. As a result, in a significant percentage of cases we work with the audiovisual records of public sector cameras (traffic, security units, etc.), thus wasting a vast network of private surveillance.

As a consequence, and even if the State had obtained limited results, these could have been better if the authority had a more efficient way of accessing the cameras in real time or, at least, in a more immediate fashion, specifically for cameras the hands of the private sector. The private sector continues to be victimized, lacking a significant number of solved crimes.

A public-private partnership could allow for an initial census, periodically updated, of all the existing cameras in a given sector which, through a coordination protocol and within the framework of a joint project, could be integrated into the security surveillance network. Either by being technologically incorporated into the public control system -allowing online access- or because previously established agreements allow not only to know their location and coverage but also facilitate viewing and delivery in times very close to the occurrence of the crime, without waiting for official and formal orders or instructions that often take hours, days, or weeks.

The authority will have access to more information and tools to solve more crimes, identify the criminals and return stolen goods to the victims. The private sector will enjoy a safer environment that will result in a positive impact on commercial activities, generating a better image of a certain sector or area, which will attract more public and tourists, whichever the case may be.

* Stolen vehicles and private sector

Coordination between the public sector (law enforcement agencies) and highways, shopping malls and parking meter collectors, which facilitates the early identification and location of stolen vehicles, represents a public-private partnership that will generate higher success rates not only in terms of early detection and response, but also prevention, as mentioned earlier in this Manual.

Similarly, the collaborative work between the authorities and the auction houses will facilitate the detection of persons linked to the cloning and twinning of stolen vehicle identities, generating important prevention quotas.

Likewise, the widespread use of decoy cars or vehicles, as mentioned in the Manual, is no longer a tool for control and detection, but rather an element that seeks to achieve a preventive and deterrent effect, generating benefits both for the public sector in the control of this threat, but also for the private sector and the community, who will perceive a substantial reduction in the threat.

Indeed, a good public campaign focused on the impact of decoy cars can be complemented by private sector campaigns, especially in shopping malls, which have the possibility of delivering the message to their users indicating that one of the vehicles in their parking lots could be a decoy, in order to discourage these spaces from being victims of theft. This type of private advertising or publicity will have no effect if the authority does not use this means as a criminal investigation system. Again, isolated actions will never produce the same impact and effect as those conducted jointly, especially in the framework of a public-private partnership in which both actors integrate their needs, efforts, and resources in a joint project.[35]

[35] **Successful decoy car initiatives have been deployed by British Columbia, Canada, through programs focused on such issue. More information can be found at the following links:**
-https://news.gov.bc.ca/factsheets/opinion-editorial-after-10-years-auto-thieves-still-hooked-on-bait-cars
-https://www2.gov.bc.ca/gov/content/justice/criminal-justice/policing-in-bc/road-safety-auto-crime/bait-cars
-https://www.baitcar.com/

* **Local security councils (communes, cantons, counties, municipalities)**

Local security councils are instances of public-private collaboration at the local level that integrate all the actors involved in the security problems of a given territory and in which not only the authorities are usually and should be represented, but also the community, the most affected actors and all those who could contribute to a solution to the threats that affect them.

It is beneficial to encourage and support local leadership not only at the level of municipalities, city councils or mayor's offices, but also neighborhood councils, civil society organizations, and other related entities, since all of them have a greater relationship, impact and knowledge of the local territory, problems, and resources. Working at the local level not only contributes to a better understanding of the problem, but also to a higher level of commitment and more participatory involvement.

Who better than the neighbors of a neighborhood or sector know what is going on in it. Without tools or an alliance, this interest, information, and capacity fade away.

Thus, the recommended best practice is for local, federal, and national governments to promote the implementation and operation of security councils at the most basic territorial level, incorporating private, community, business, and civil society actors, both because of their intimate knowledge of local problems and because of the direct impact that various measures will generate in their territory, which should ensure high levels of commitment and participation.

* **Reinsertion into the job market**

Whether they are people recently released from prison or demobilized paramilitaries, their reintegration is key to prevent them from committing or reoffending in criminal activities or terrorist acts. The main interest in preventing this from happening lies with the State, and there are many programs and examples worldwide. However, the state's labor supply may not be large enough to meet the existing hiring needs. In turn, the length of time that a job hiring process in the public sector could take, its formality and rigorousness in terms of compliance with requirements, could go against the interest and desire to generate employment as quickly as possible once the person is released from a prison or demobilized.

Every day spent on the street without work and support, the risk of recidivism increases substantially.

Hence, the private sector could represent a tremendous opportunity, both in terms of diversity, size of job supply, flexibility, and contracting speed. Of course, the private companies have well-founded fears that the new workers will commit misconducts or irregularities if hired. They are also concerned about the fact that they could not always access the applicant's criminal or terrorist history. In turn, contracting generates risks to the operation of the business itself and to its employees, therefore the private party will want to be compensated.

A public-private partnership can efficiently address each of these aspects, which should be regulated in advance so that both parties have clear rules. The state should be aware, with a higher level of certainty, about the type of labor supply, the speed and, above all, capacity, and amount of available hiring. This will allow them to structure their reinsertion and crime prevention plans in the best possible way. But if they want to work with the private sector, be it private enterprise, civil society, or community organizations, they will need to address each of their fears and concerns. You must learn how to captivate. Find - as stated at the beginning of this Manual - the business case that will be of interest to the potential recruiter.

Thus, the public sector should ensure the provision of detailed information on the applicant's past, generate reports on the danger index and -why not- provide direct subsidies for each worker hired or indirect subsidies associated to tax payments, among other benefits.

Periodic meetings between the job performance departments of the companies, on the one hand, and the social reinsertion departments of the State units, on the other, should always be considered in order to generate feedback on the benefits, progress, setbacks and challenges of the initiative, as well as on the level of fulfillment of the expectations of both actors involved. Considering the opinion and consultation of the reintegrated persons themselves could be relevant.

* Projects in areas with scarce state presence

There are many places worldwide where a stronger territorial presence of terrorist groups has led to a historically scarce state presence. Sometimes this condition is due to geographical difficulties, being precisely those what terrorist groups exploit to their advantage; other times it is the local population's distrust of the State; and sometimes it is due to the risk it represents for a public official to operate in a territory where a terrorist organization is active.[36]

[36] FARC in Colombia and Sendero Luminoso in Peru are some examples of these types of organizations and the impact they have had at the territorial level.

In all these places, and despite a scarce state presence, there are consolidated community organizations, private companies that develop commercial or industrial activities of various types, and civil society organizations.

An interesting strategy to generate territorial and human intervention on the part of the State in this type of areas can be done through public-private partnerships where the State can extend support, assistance and development programs through local actors more closely linked to the private sector, who in addition to knowing the area, have an interest in achieving better services for the community.

* Critical infrastructure and terrorism

In most countries, infrastructure considered critical by the State receives special attention in terms of security, protection, analysis, and resources, subjecting them not only to intensified prevention mechanisms, but also equipping them with capabilities for early threat detection and prompt response.

Traditionally, the State has owned or has had control over an important part of a country's critical infrastructure. But in recent decades this has been changing to the point that today, a large number of ports, water systems, airports, hospitals, essential factories, electricity transmission systems and sewage systems are in private hands or, at least, being state-owned, but operated by private organizations. These are facilities whose destruction or impairment could have a debilitating impact on security, national economy and public safety or health stability.

However, there is a type of infrastructure that, without being critical as per the terms defined above, has been increasingly targeted by terrorist attacks. Incorporating these new potential targets is highly desirable.

> Indeed, it has become evident that the latest terrorist attacks in Spain, Paris, the United States, the United Kingdom, Indonesia, Turkey, and Somalia, to mention just a few, were not against military or government facilities, but were directed against the civilian population, in areas operated or with a large private presence or intervention, such as offices, shopping malls, theaters and hotels.

The objective of terrorist groups is no longer only to weaken a State by attacking its operational resources or its critical infrastructure, but also to cause panic in the population, seeking to instill fear and insecurity. This should motivate considering shopping centers, stadiums, and hotels, among others, as critical infrastructure for a State, both from a regulatory and operational point of view.

Therefore, in order to prevent the risk of terrorist attacks on critical infrastructure, a first approach is to broaden the concept of critical infrastructure at the legislative level, so that those facilities, services and areas relevant to the country's progress, but also for safe and peaceful coexistence, can be considered and incorporated into critical infrastructure plans.

It is not about imposing, by legal or administrative means, obligations on the private sector that would lead them to spend more money on security, cameras, guards, or metal detectors. This course of action is not ruled out, but it does not reflect the public-private partnership that this Manual promotes.

The private sector's interest in preventing terrorist attacks against the facilities they operate is evident. The damage is not only produced by the attack itself, resulting in deaths and physical destruction. A negative effect happens in the medium term, when the population, naturally fearful, stop going to the places that were the target of attacks for a while. Recovery becomes even slower. Preventing attacks or detecting them early is not only of interest in relation to the attack itself, but also to the medium-term effects it produces.

For this reason, private entities interested in business continuity must develop plans together with the State, as the governing body and manager of security and protection, in the context of a public-private alliance as the criteria for joint action.

While the private sector will have many more tools to apply detection activities, through video surveillance, physical controls or checks on people and vehicles, it will be the State who is in a better position to provide information about imminent threats, and risk profiles on which detection should operate.

* Ports, airports, organized crime, and terrorism

The air and maritime industry[37] move people and cargo, which may be associated not only with terrorist movement or activities, but also with criminal operations such as arms and drug trafficking, human trafficking, and contraband, among others. The latter could also be a source of financing for terrorist activities.

It is a fact that it is not possible to inspect every single passenger and all cargo. Risk profiling becomes necessary. In fact, physical inspection of container cargo does not exceed 4% of all movements worldwide. Notwithstanding the existence of technological solutions and the development of new ones, the control of cargo and passengers inevitably generates delays that, if excessive, seriously affect world trade.

[37] For the purposes of this Manual, maritime transport activities also include river and lake transport activities.

A conflict then arises. Both the public and private sectors wish to counter the threats described above in terms of deterring these organizations from using maritime or air transport or hindering them, so they do it in much smaller quantities.

While the State wants to directly combat these threats because of the risk to population and security, the private sector does not want the supply chain or logistical processes to be disrupted by discoveries of terrorist or criminal activity.

Once again, and in much the same way as in the case of critical infrastructure -in fact, ports and airports are critical infrastructure in many countries- it is necessary to identify needs and objectives in each of the sectors and seek a common understanding, so that the resources of each can be used to benefit a common interest, avoiding the costs and challenges that currently prevent this type of partnerships from being massively adopted.

As it is not possible to inspect all cargo, information and risk profiling is essential. If logistics operators upload and enter the information correctly, it will result in more and better data for analysis. Having this information allows government agencies to develop better intelligence that will result in better risk profiles and, ultimately, controls with a more efficient hit rate.

Constant feedback between both sectors and the implementation of monitoring and evaluation activities are essential so that the information provided by the private sector to the State, or the alerts provided, are seen as a mutual benefit and not as a service provided by one sector to the other.

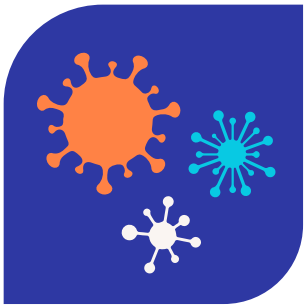
* **Biosecurity and terrorism**

The coronavirus pandemic experienced by the entire world demonstrated that a public health emergency could not be efficiently addressed by the State alone, nonetheless, required a significant private contribution and intervention, not from spontaneous collaboration, but from a public-private alliance which, in this case, occurred at local, national, and international levels.

While the State contributed resources and lines of financing, as well as all the know-how and information accumulated in the development of vaccines, complemented with strict restrictions to reduce contagion, the private sector contributed with research and technological development capacity, as well as vaccine production.

In terms of distribution, both worked hand in hand, in an unprecedented effort.

Although all indications are that the latest pandemic was a natural occurrence, it may well have been created, spread, and propagated intentionally in the form of a bioterrorist attack that could have been complemented by various viruses and bacterial agents.



Although with increased development as a consequence of the coronavirus pandemic, there is - in comparison to other specialties - a need for more expertise in microbiological and immunological sciences. This is a scenario in which a public-private partnership should be considered, this time not only with laboratories, but also with universities and training centers in order to generate more specialists in the field.

Developing vaccines is a long and expensive process. The State undoubtedly needs to advance along these lines, but with the understanding that there is greater capacity in the private sector, which, of course, sometimes faces bureaucracy, as well as legal, regulatory, and financing limitations. In the case of bioterrorism, the State will have more information on the main and most relevant threats, which will allow the laboratories to focus their work.

A partnership between the two sectors could effectively address these challenges as well as the need to generate a long-term commitment because investment - no matter who makes it - takes a long time to show results.

An aspect that has traditionally been a barrier to public-private collaboration for development of bio-threat solutions is intellectual property, which should be regulated as clearly as possible at the start of the project. Without securing intellectual property rights entirely or partially, it will be difficult for the private sector to see this alliance as a business case.

A partnership such as the one described above makes it possible to share both the financial risks and the benefits. Incidentally, it will help centralize dispersed knowledge and diverse technology. Initiatives such as these, in the context of bioterrorist threats, should be consider not only the development of medical solutions, but also joint work for the early detection of entities or groups that could possess knowledge and capabilities to develop biological weapons; early detection in cases of infection and spread; containment tasks and finally vaccination, if necessary.

As of today, probably the pathogens with the highest level of risk and that pose the greatest threat are the Ebola and smallpox viruses and the anthrax bacteria.

* Technological developments to prevent and counter terrorism

One of the lessons learned after the terrorist attacks in the United States in September 2011 is the need to develop security cooperation programs, not only among public or state actors, but also between them and the private sector.

This coordination, ideally in a public-private partnership format, allows for better preparedness, but also for response to biological and chemical attacks, conventional terrorists, and cyber-attacks.

The private sector has an important and varied technological capacity, resources, and information, which the State should never miss out on, given the usefulness of synergies between the two. In fact, the private sector has been leading in the development of vaccines and equipment to detect threat materials or particles (metals, explosives, radioactive elements, pathogens, etc.), information systems and cyber protection programs, which have supported countries in having higher and better levels of protection and security. Without going any further, the vast majority of passport and identity document control systems at border controls are currently automated through the use of scanners developed by the private sector for this sole purpose, therefore private companies have designed products to provide solutions to public needs. However, scanning passports in isolation does not generate the same benefit as having the same data, but analyzed cross-referenced with government databases, or processed with risk profiling and analysis software developed by private industries.

Just as the use of artificial intelligence to build predictive security models ideally requires information from state actors who should provide important background information regarding what is to be predicted, under what terms and in what formats, there are other developments from the private world, whose added value will only be attainable through joint work with the state sector, in terms of needs and feedback.

An example of this can be the data analysis programs or software that analyze massive amounts of data and define behavioral patterns, designed to be used by the private sector, but that with the correct inputs and feedback from the State, allowed for the design and operation of modules focused on public sector needs and the investigation and prevention of crime and terrorism.

Indeed, in a globalized world that provides the investigator or threat preventionist with countless data, processing such data properly and on time represents an enormous challenge. Analyzing years of bank or immigration records, product exports or thousands of phone calls is an extremely difficult task. The daily challenge for criminal and counter-terrorism analysts is to discover and uncover networks, patterns, and trends in the current and growing volumes of complex structured and unstructured data, for which there is currently a diverse technological offering of programs (software) used for data analysis from different perspectives and that are used not only in the private world, but also in the public world.[38]

It is a fact, however, that technology developers and industry leaders are often in competition with each other. Spontaneous collaboration is possible, but not easy to achieve. Hence, it is the State that should generate the legal, financial, and planning conditions that would allow for real and natural competitors to come together to work jointly, both to identify technological obstacles associated with security threats and to develop plans to collectively overcome these obstacles.

However, it is possible to appreciate interesting cases of public-private collaboration where the initiative came from the private sector and was welcomed by the State, further enhancing the benefits of working together. An interesting example in this area is the BENS Program in the United States, which was able to combine efforts, knowledge, experience, capabilities, and resources from both sectors, in this case, under the initiative of the private sector, but always with the aim of improving prevention, detection and response capabilities to security threats, some of which, are linked to terrorist activities.

[38] On the one hand, there are programs such as *I2, Visallo, Neo4J, DataWalk* or *Cellebrite* that in general terms analyze data and establish relationships and patterns when the data come from static databases such as file repositories.
Thus, when an investigator is confronted with a list of 1500 telephone calls between several investigation subjects, these programs will draw a picture in a matter of minutes through which it will be easy to see who talks to whom, how often and at what times, for example. Arriving at that same information without a program like the ones described above could take days or weeks for even the best of investigators or preventionists.
On the other hand, there are programs such as *Maltego, Social Links, Lampyre* or *Geph* that -with some differences- perform a similar job of pattern matching and detection, however these programs are fed with information from open sources available on the Internet. Thus, when we want to analyze, for example, social profiles or service offerings on the web, it will be easier to do so with software with the capability to search for data in an open source that can be accessed via the Internet. The other programs need to be fed with information that would be very difficult to transport from the web.
It will be easier for the first group to analyze banking transactions or migratory movements when the programs are fed by static databases contained in file repositories. The second group is more efficient if you want to establish links between people based on information contained in *Instagram, Facebook, Linkedin, Twitter, Snapchat* and even the *Dark Web.*

* **Terrorism prevention. State and community.**

Working with the community to prevent violence associated not only with organized crime, but also with terrorism, is more cost-effective than managing response once the attack has taken place or the crime has been committed.

The community has a lot to contribute in terms of information and social support. One of the main challenges is the need to develop greater lines of trust with government agencies. It is advisable to work with society as a whole to establish and expand local prevention frameworks. Through technical, financial, and educational assistance, it is possible to successfully support local efforts that prevent people from becoming radicalized to violence. This type of initiative has a high impact on the community in general, but especially on the protection of schools and universities, as well as on high attendance events. A good example of this type of initiative is CP3[40] in the United States.

[39] **CPR - U.S. Department of Homeland Security's Center for Prevention Programs and Partnerships *(Center for Prevention Programs and Partnerships)*. This program, promoted by the public sector, seeks to create the conditions for communities to be united to help put an end to violence and terrorism. They work with the whole of community to build local prevention frameworks. The initiative works to design and implement programs to build trust, partnerships, and collaboration at all levels of government, the private sector, non-governmental organizations, and the country's diverse communities. Among other lines of work, CP3 works with the community supported by methodological resources and guides that provide an overview of public, private and community threat assessment and management teams working on terrorism and violence.**
For more information see https://www.dhs.gov/CP3

* Tourism and security

The creation of public-private partnerships in the area of tourism security is crucial when it comes to generating safer spaces for tourists, generating not only programs for threat prevention and early detection, but also rapid responses to reduce the impact of a given incident.

A tourist is exposed to threats from organized crime and in addition, to terrorist attacks. While the State wishes to promote an area, a place or the entire country as a safe destination, the private sector wishes to avoid a drop in bookings and travel as a result of incidents affecting the safety of visitors.

It is not just a matter of working together to prevent these threats from materializing, because to reduce the risk to zero would mean closing a country to tourism. In addition to prevention activities, it is advisable to develop lines of work in the area of tourist assistance. Several countries have advanced along these lines, such as Mexico, through CAPTAs[41] or Ecuador through PIATs.[42]

[41] An interesting example is represented by Mexico's Tourist Assistance and Protection Centers - CAPTA, led by the tourism authorities of the states and municipalities, with representation from the three levels of government. In these activities, consular entities from countries with high affluence of tourism, international organizations such as the Red Cross, through its Mexican branch, and the private sector, through tourism service providers and operators, actively participate. The main function of the CAPTAs is to assist and orient domestic and foreign tourists, both to receive information and support, as well as to channel and follow up on complaints, reports, and risk situations. A more detailed explanation can be found at http://scm.oas.org/pdfs/2019/CICTE01300D.pdf

[42] Ecuador's Comprehensive Tourism Assistance Plan (PIAT) is a tool that Ecuador uses to guarantee the mobility and safe travel of tourists visiting the country. Its objective is to implement strategies and protocols with a comprehensive approach that strengthen the active participation of the public sector, the private sector and the communities in risk assessment, damage prevention and emergency and crisis management, taking into account the needs of the destination. A more detailed explanation can be found at https://amevirtual.gob.ec/wp-content/uploads/2017/05/PLAN-INTEGRAL-DE-ASISTENCIA-TURISTICA-PIAT.pdf

The most relevant:

This chapter highlights the importance and success of public-private security partnerships, presenting concrete cases in various areas. The main issues to highlight are:

1. Bidirectional collaboration between the public and private sectors generates innovative and effective solutions for prevention, detection, mitigation, and response to threats.

2. Notable examples include training for early detection of human trafficking, cooperation in impoverished areas, financial support for victims of criminal violence, recovery of stolen vehicles, job market reinsertion, and development in areas such as critical infrastructure, biosecurity, and tourism.

The cases presented in this chapter demonstrate the success of public-private partnerships in addressing security challenges and serve as a reference for future collaborations, always seeking to improve prevention, detection, mitigation, and response to the threats our societies face.

Security crisis committees and public-private partnerships

In this chapter, we will address a crucial issue for the security and wellbeing of society: Security Crisis Committees and Public-Private Partnerships. These committees are public-private collaboration entities created to address critical situations that put the safety of the population at risk. Their role is ongoing and permanent, and their effectiveness lies in the joint and integrated management of the public and private sectors.

The chapter is structured in three temporal sections: before, during and after a crisis. Each section presents a series of actions and measures that allow for better preparedness and response to critical situations. Some of the key actions include risk analysis, the development of generic response plans, communication, and the structuring of a Crisis Committee. In addition, we address aspects related to infrastructure, the appointment of committee members, training, and drills.

During a crisis, the activation and operation of the committee is essential, in addition to effective and coordinated decision making to reduce negative effects. Finally, we emphasize the importance of recovery and assessment after a crisis, to learn from the experience and improve in the future.

The chapter concludes by stressing the importance of appointing a team to implement the recommendations and ensure their execution in both pre-crisis actions and post-crisis assessments. The creation and management of a public safety crisis management mechanism with public-private representation will generate greater benefits and contribute to the protection of the community and economic activities.

Crisis committees are instances of public-private collaboration designed as a mechanism to face a certain serious and decisive situation that endangers the development of an issue, or a process connected, in this case, to security.

Contrary to what many might think, the committee is not created to die with a crisis. These are ongoing entities that operate continuously and permanently over time and which, in the event of a crisis, experience intense and highly demanding activity.

Virtually all security crises impact both the public and private sectors. Joint issues must be addressed jointly in order to execute joint actions.

Knowing how to efficiently manage a joint committee with public and private actors will impact the success of the committee's work, which will result not only in risk reduction, but also reduction of the impacts of the threats towards the public security of a community. The operation and management of a crisis committee necessarily requires a committee to have been formed and prior to being in the midst of a crisis.

The various activities where a community participates, including tourism, commerce, transportation, sports, housing and even health, are not immune to being affected by serious public security situations, which jeopardize their advance and operation, harming not only future growth but also their current development. The business continuity management system regulated by ISO 22301[43] defines a crisis as a situation with a high level of uncertainty that affects the basic activities and/or credibility of an organization, requiring urgent measures.

Outside the ISO standard, we could confirm that the various activities or sectors mentioned face a security crisis when they are exposed to rapidly escalating negative events, when communication control is lost and/or when a seriously damaging image is being projected.

> As far as security is concerned, critical damage is caused by complex, catastrophic, large-scale, or high-impact events that affect the community, the economic activity, and the sector where such activity takes place.
>
> Good preparation - prior to crisis situations - makes it possible to face crises in a better way, helps reduce damaging impact and accelerates recovery. Thus, this section of the Handbook is intended to be a guide that provides the essential concepts and tools that should be taken into account when dealing with a security crisis in its three temporal dimensions: before, during and after.

[43] **International standardization norm that aims to provide guidelines and procedures to implement, maintain and improve a management system to protect against an interruption of service, production, or operation, as well as to reduce the probability of its occurrence, prepare for the event when it happens and recover from interruptions when they occur. See more details of this standard in the publication of the International Organization for Standardization (ISO)** https://www.iso.org/files/live/sites/isoorg/files/store/en/PUB100442.pdf

We will provide a wider approach with the purpose of providing a crisis management tool that can be applied jointly and comprehensively by the public and private sectors, not only in public security crises, but in any serious situation. All in all, its application is absolute and far-reaching when applied on public security problems, especially when they reach critical dimensions or levels.

Prior to a crisis (A)

* Risk analysis

Security crises, as well as crises connected to other activities or sectors, occur when the risks to which a certain sector, community or activity is exposed are realized, therefore the best way to prevent and/or manage these risks is to identify them beforehand.

Identifying and assessing risks arising from threats involves an exercise whereby four factors are determined and weighted, which are analyzed based on the main tourism assets -both tangible and non-tangible- such as image, country, communication, tourists, sector operators, etc. These variables can be combined with the 13 elements that, according to this Manual, are recommended to be taken into account when developing an assessment of the threats.

Factors to consider are:

- ***The nature of the threat.*** Establish the types of threats, which can be classified into two categories:
  - *real vs. perceived threats, which can sometimes be just as damaging as the former; and*
  - *threats of a physical-natural origin (earthquakes, tsunamis, floods, floods, volcanoes, etc.) vs. those of a human-social-economic nature (terrorism, epidemics, political or social conflict, war, criminal activity, cyber-attack, market collapse, serious alteration of exchange rates, errors in the operation of systems or equipment, among others).*

- ***The magnitude or level of the threat.*** Threats must be categorized by identifying and assigning impact levels based on the tangible or intangible asset being evaluated.

- ***Vulnerability to threat.*** After analyzing the external factor (threat), it is necessary to establish and evaluate the internal factors, which are, internal threats and vulnerabilities. The aim is to determine the aspects of organization, equipment, human and financial resources, construction, and coordination that make a given infrastructure, sector, organization or activity more or less vulnerable to the threats previously identified.

- ***Consequences and damage, in the event that the threat becomes real.*** This stage seeks to define the impact caused when the threat materializes and can be categorized and evaluated according to four factors:

    - *Public health. Effect on human lives and well-being of the population (deaths, illness, injuries, etc.).*

    - *Economy. Direct or indirect economic loss (reconstruction cost; response cost; recovery cost; cost or impact on other infrastructure or services; long-term damage due to environmental contamination; etc.).*

    - *Psychology and image. Effect on public morale and trust in the national economy and public or private institutions. The way a crisis is managed will impact positively or negatively on this aspect, which encompasses the changes in perception that arise after a larger-scale incident that affects the public's sense of security and well-being, which could even manifest itself in disruptive behavior.*

    - *Governance and institutional framework. Effect that comes from the capability of the State, government and/or private sector to maintain order, ensure continuity of operations and basic services, ensure health, and maintain public security and stability actions, as needed.*

* Generic response plans

Based on the main risks and threats detected, it becomes possible and advisable to build and develop standard work and response plans to better address possible future scenarios. Training will then be provided subsequently on these plans, drills and simulations will be conducted.

This section of the Manual compiles all the indications and references regarding the importance of a joint approach by both the public and private sectors since security crises affect the entire community and institutions transversally.

* Activation

Regardless of the fact that a Crisis Committee may be convened as per the indication of its director or coordinator, it may also be formed as a consequence of the occurrence of certain events previously determined during the risk survey. These are the so-called alerts or indicators, such as a riot in a prison, an unusual increase in contract killings or homicides, a terrorist attack or the appearance of criminal groups that act with extreme violence, firepower or impunity protected by high levels of corruption, among other examples.

It is important to bear in mind that at the time the hypotheses for activating the Committee are brought to bear, these could have occurred or be presently occurring (earthquake, terrorist attack, etc.) or be a threat (airport strike or road stoppage, epidemic in neighboring countries, storm that has not yet made landfall, complex criminal phenomena in neighboring countries with a high probability of beginning to occur at the place the plan is being produced, etc.).

* Registry

Prepare a registry containing clear identifications of the main entities linked to the affected sector or activity, including both the public and private sectors, indicating their competencies and roles, formal points of contact, emergency liaisons, and response and support capacity in crisis situations.

The objective is to understand what resources and capabilities are available for both, devising response plans and managing the crisis itself. Information should be collected and updated periodically, including the main *stakeholders* related to security issues.

* Communication

Efficient crisis management requires efficient communications management.

- **Messages**

> One element that contributes to the achievement of this objective is preparing standard messages beforehand, aimed at the community and stakeholders, depending on the type of information that needs to be provided. This action reduces the risks associated to improvisation and better prepares the messages the Crisis Committee communicates.

Each crisis is different and virtually no two are alike. It is impossible to cover all scenarios, so one way to address this challenge is to develop generic communication messages designed according to the type of risk, and which will be adapted on a case-by-case basis.

It is not the same to provide information about tourists victims of an earthquake as it is to provide information about a terrorist attack, nor is it the same to face a natural crisis -generally of a temporary impact limited to seconds, minutes or days- as it is to face a crisis linked to social, human or economic causes, which in some cases may last for months, such as using social demands and promoting them to cause planned violence. The challenges are clearly different. While short-term crises -with a defined beginning and end- can be managed with fewer, better prepared, and anticipated communications, long-term scenarios such as structural public security problems, economic crises, pandemics or social conflicts require a more refined, flexible and adaptable management, adaptable to the way the situation evolves through time.

Therefore, the best way to respond to the different scenarios is with short, reiterated, specific messages containing timely, objective, transparent, truthful, and accurate information.

These messages must:

* *describe the events (place, date, impact, damage, causes),*
* *indicate the measures taken and those to be implemented in the future,*
* *show solidarity with victims or those affected by the crisis,*
* *mention when the next press release will be issued,*
* *mention in which places, media and formats updated information can be found.*

- **Guidelines**

It is important to design predefined guidelines to help in the training of the groups involved in communication management, and to train the operators in this department on the best way to communicate in a crisis. It is about training on what to say, how to say it, when to say it and what **not to** say in a crisis.

Crisis communication rules have certain differentiating characteristics compared to other scenarios that are always important to consider. The communications equipment must be ready.

* Structuring a Committee

A crisis committee must have at its disposal a group of people in charge of coordinating, executing and/or supervising a series of tasks. Not all these people should always have a seat at the Committee's table. Some of them will participate in the group work sessions when the topics they are responsible for are discussed (legal, for example) and others, due to the nature of their work, will always be present (as is the case of the coordinator or the person in charge of communications).

All of them must be on call for the Committee, in the same building or area where it operates and must be ready to be summoned as needed. Of course, experience indicates that, in the first sessions, when the impact of a crisis is still being measured and the first responses are being coordinated, the presence of everyone is what is desirable.

* Members

- **Address**
  - Directs the Committee.
  - Declares or validate the crisis.
  - Assigns tasks and delegates responsibilities.
  - Determines who will participate in each of the sessions.
  - Approves and validates the communication plan, messages, and lines of action.
  - Acts as spokesperson if circumstances demand it.
  - Maintains close contact and coordination with other sectoral crisis committees (if more than one).

- **Operation and Internal Control**
  - Ensures that things happen (agreements, instructions).
  - Supervises execution of delegated and/or assigned tasks.
  - Follows-up and evaluates the Committee's internal work.

- **Study and Evaluation**
  - Collects permanent information about the crisis, its impact and its development.
  - Generates periodic reports for the Committee for proper decision making.
  - Uses information provided by the media, surveys, social networks, public and private stakeholders, as well as field visits.
  - Coordinates with the person in charge of the Committee's communications to monitor both national and international media.

- **Communication**
  - Acts as spokesperson (unless this responsibility falls on the Committee Director).
  - Develops communication strategy and proposes it to the Director or Coordinator: what is going to be said, when, to whom, through what media.
  - Prepares and maintains up-to-date information at hand for use at press conferences, in fact sheets and in both external and internal (employee) statements.
  - Maintains relationships with the media.
  - Collects and updates media list and points of contact.
  - Coordinates with evaluation and research for both national and international media monitoring.

- **Technology and Communications**
  - Ensures and oversees the optimal and continuous functioning and operation of computer and communications systems.

- **Finance**
  - Identifies available resources, both internal and external (financial, equipment, human, etc.).
  - Manages the availability, allocation, and management of resources.
  - Controls the use of resources.

- **External response**

  - Coordinates and supervises operational response (when applicable), this is work that can be done autonomously by the organization that comprises the Committee or with the support and assistance of other entities (health, security, transportation, etc.).

  - Coordinates work with the liaison officer, when appropriate.

- **Legal**

  - Analyzes scenarios and legal implications of the crisis.

  - Provides technical-legal information for better decision making by the Committee.

- **Registration**

  - Keeps a detailed record of all the Committee's actions (decisions and agreements adopted, instructions issued, presentation of reports and research, communication pieces, follow-up on the execution of tasks, among others).

- **Liaisons**

  - Maintains relationships with other liaisons or with entities or persons external to the Committee.[44]

  - Coordinates his work with the operations manager, when appropriate.

  - The number of liaisons will depend on the type of crisis, its size, the extent and complexity of the entities or individuals involved, them being either counterparties or affected.

    - *Public.* Maintains a coordinated relationship with government stakeholders, embassies, consulates, and international organizations.

    - *Private.* Maintains relationships with private stakeholders and NGOs.

[44] The liaison(s) connect(s) with any other entity external to the Committee, with the exception of the media. For media coordination, we recommend to have a person specially designated for this purpose, who will have it as his or her sole function.

- *People.* Maintains relations with victims and affected persons (assistance to affected entities, victims, and their families).
- *Internal.* Maintains relationships with internal structures (work departments and personnel).

- **External advisors by specialty**
  - Depending on the type of crisis, its magnitude, duration, specificity and complexity, external advisors may be called in on a permanent or sporadic basis to provide support in specific areas such as public security, health, civil protection, public image, and media, etc.

- ***Stakeholders* and other external entities**
  - In order to facilitate the coordination of specific aspects, or to obtain more detailed information, it is advisable to consider convening certain public or private, national or international stakeholders in certain sessions.

* Infrastructure

The Committee should operate in a physical space that provides ideal working conditions. To this end, at the pre-crisis stage, the venue where the Committee will be able to operate must be considered, as well as the minimum necessary resources it must have.

Along with defining the location and resources, it is important to ensure their availability at the time the Committee is convened. Among the elements to consider we suggest:

- **Physical space**
  - A main crisis room for group work that has the capacity to gather the extended Committee (20 people minimum).
  - Two group work rooms for meetings to address specific issues both among Committee members and between them and external entities.
  - Press room or a venue for issuing statements to the press.
  - A room for individual work that allows Committee members who do not participate in a Committee session to work optimally in an area close to where the Committee operates.

- **Parking**
  - Ease of access and secure parking available for use by Committee members.

- **Financial Resources**
  - Availability of funds for food and minor miscellaneous expenses to ensure and facilitate the Committee's operation.

- **Equipment**
  - Communication equipment (radio, cellular phones, satellite phone, IP phone or communication, among others).
  - Work equipment and supplies (notebooks, printers, sheets, pencils, blackboard, markers, projector, projection screen, among others).
  - Emergency lighting equipment and power generators.
  - Adequate furniture for work (tables, chairs, etc.).

- **Communication**
  - Operations communication lines (telephone, internet, etc.).

- **Basic utilities**
  - Optimal operation of water, electricity, heating, among others.

- **Security**
  - Security personnel to control access to the site where the Committee operates and to provide protection if necessary.

* Appointment of Committee members

It is necessary to appoint specific individuals to each of the positions identified for the Committee, even if the Committee is not convened. These people must be trained as a matter of priority (see next item).

Each time one of these persons is replaced, a new individual must be appointed to replace them, so that at all times there is an updated register and list of the persons who comprise the Committee, even if they never become part of it, operationally.

* Training, simulations, and drills.

It is important to design and have a training plan for all the actors involved in a potential crisis, both in relation to those who would comprise the Committee and those who could be affected by the harmful effects of the situation. The content of such training should prepare the recipients in the knowledge contained in this Guide and all other elements that could complement it (e.g., how to handle a communications crisis).

The training plan should be executed periodically at least once a year, although it is recommended that it be executed every six months. Given the personnel turnover that may exist among the Committee's members, it necessary to ensure that training is provided both as a group and individually to each of the individuals appointed for the functions related to the Committee's operation.

In addition to training, it is advisable to conduct periodic simulations and drills. Simulations are table-top exercises that construct fictitious scenarios and assess knowledge and response capabilities taking into account only theoretical variables. Drills, on the other hand, go a step further and add an operational variable. In fact, in conjunction with tabletop exercises, the participants in a drill go to the field and empirically validate some of the most critical variables. The participants in the activity know that they are part of a hypothetical situation and are asked to operationally demonstrate their capabilities.

It is by means of a drill that we can determine that an ambulance, which theoretically would take 15 minutes to arrive at a place, actually does so in 25 minutes when the transfer takes place on a Monday from 8 to 9 am. Similarly, when considering the theoretical use of *hazmat* suits for chemical, radiological, or biological protection, or explosion-proof suits, only a practical exercise will show that in environmental conditions of 30°C a person cannot wear the suit for more than 20 minutes, and that the process of putting on and taking off takes another 20 minutes.

A final tool for training and coaching are the so-called *reserved drills* or tests. These are drills in which only a very small group of people know that it is an exercise. Although they represent the best way to learn, as they test actual response capabilities without the operators' knowledge that it is part of an education and training activity, the challenges to successfully manage this initiative without causing public alarm are enormous. This type of training is recommended only for those entities or groups that have already successfully conducted several prior simulations and drills.

During a crisis (B)

* Committee Activation

The committee is convened:

- **By declaration.**
  - At the discretion of the Director or Coordinator.

- **Automatically.**
  - Due to the occurrence of certain events that have been previously determined during the risk assessment (see section A3).

As mentioned in section A3, it is important to consider that the events that trigger the activation of the Committee could be only threats that have not yet materialized or events that have already occurred or are occurring at the time (earthquake, terrorist attack, etc.).

* Operation of the Committee

The operation of the Committee, the issues to be discussed, the approach to be taken, the frequency of the extended and sectoral meetings, as well as the intensity and frequency of communications will depend on the way each of the crises develops.

Thus, in situations such as earthquakes, tsunamis, consummated terrorist attacks, where the major emergency has already occurred, it is likely that the initial meetings will happen in a very intense frequency, to then give way to weekly meetings for follow-up purposes. On the contrary, scenarios of long or indeterminate duration such as economic crises, social upheaval, structural public safety problems or an epidemic are quite likely to spread their action over a longer period of time.

In both cases, the first action to be taken by the Committee is: a) to broadly summon all of its members; b) to appoint a spokesperson; and, c) to carry out an initial assessment both internally and through liaisons in order to determine the impact and type of crisis it is facing, the extent of the damage caused and the number of people affected, among other variables.

Based on this first assessment, which will be adjusted in the light of subsequent assessments, the Committee will make all decisions within its power to reduce the effects of the crisis in terms of both its duration and the level of damage caused. To this end, the committee: a) will deploy coordinated actions through each of its areas (finance, operations, legal, communications, etc.); b) will define and begin to implement a communications policy; c) will further define and specify the communications messages previously developed; d) will establish the entities with which the liaisons will interact (government, private, embassies, etc.), as well as the objectives and goals of these external coordination efforts; e) will define the initial schedule of meetings and their duration; f) will assess the availability of resources to deal with the crisis; g) will define the initial schedule of meetings and their duration; h) will assess the availability of resources to deal with the crisis; i) will define the initial schedule of meetings and their duration; j) will assess resources available to deal with the crisis.), as well as the objectives and goals of these external coordination efforts; e) will define the initial schedule of meetings as well as their duration; f) will assess the availability of resources to address the crisis; g) will define the members that should participate in the respective sessions, ensuring the integration of both the public sector and representatives of the private sector in relation to the particular crisis being addressed; among others.

After the crisis (C)

The crisis does not end with the crisis. Once the most serious events have begun to give way to calm, it is important to work in two areas:

* Recovery

- Work in coordination with other stakeholders to design, implement and support recovery plans, at the operational, financial and media levels. Always based on truth, transparency, and honesty, it is very important to recover the image and perception of security.

- Recovery has a triple dimension: a) guaranteeing free, quiet, clean, and safe access and movement of people and organizations; b) reestablishing and optimizing the operational capabilities of the affected public and private sectors; c) restoring social peace and public-private institutional trust.

* Evaluation

- **It is important to measure two aspects:**
    - The crisis itself. Why did it happen? Could it have been avoided or better anticipated? What was the impact? How can we learn to better face the next one, etc.?
    - Crisis management. How was the crisis handled? How did the Committee operate? What were the best successes and the worst mistakes? Were we prepared? If the events were repeated, what would we have done differently, etc.?

Implementation (D)

It is important to designate a person or a team to be in charge of the implementation of these recommendations related to the creation and management of a public security crisis management mechanism. A public-private partnership or representation will generate greater benefits. They are responsible for ensuring that each of the pre-crisis actions (section A) and post-crisis evaluations (section C of this chapter) are conducted.

The most relevant:

This chapter analyzes the importance of Security Crisis Committees and Public-Private Partnerships to face critical situations for the security of the population. The main items to highlight are:

1. The structure of the chapter covers three temporal stages: before, during and after a crisis, with key actions and measures to take at each stage.

2. Pre-crisis actions include risk analysis, development of response plans, communication, and formation of the Crisis Committee.

3. During a crisis, the activation and operation of the committee and effective and coordinated decision making is crucial.

4. After a crisis, recovery and evaluation are essential to learn from the experience and improve in the future.

5. The designation of a team in charge of implementing the recommendations ensures the effective execution of actions and evaluations.

The creation and management of a public security crisis management mechanism with public-private representation is essential to protect the community and economic activity.

PUBLIC - PRIVATE PARTNERSHIPS

A risk management approach to address security threats.

OEA Más derechos para más gente

unicri United Nations Interregional Crime and Justice Research Institute