FIEP 2023

SPANISH PRESIDENCY

IMPACT OF A REGIONAL CONFLICT ON PUBLIC SECURITY IN THE FIELD OF GENDARMERIE FORCES

HYBRID WARFARE

PEACE

CLIMATE CHANGE

REFUGEES

CRISIS

SECURITY

GREY ZONE

GOBIERNO DE ESPAÑA
MINISTERIO DEL INTERIOR
DIRECCIÓN GENERAL DE LA GUARDIA CIVIL

TECHNICAL SPECIFICATIONS

TITLE 2023 FIEP Publication: ***"Impact of a regional conflict on public security in the field of Gendarmerie type forces"***

COORDINATION

Brigadier-General Gregorio Pérez Turiel
Secretary of the Presidency for the FIEP23 Spanish Presidency

Lieutenant Colonel Plácido Manuel Rodriguez Moreno
2023 FIEP Human Resources Commission Chairman

Lieutenant Colonel Manuel José Silos Brianso
2023 FIEP New Technologies and Logistics Commission Chairman

Lieutenant Colonel Basilio Luis Sánchez Portillo
2023 FIEP International Affairs and Service Organization Commissions Chairman

Lieutenant Colonel José Ángel Lopez Malo
Spanish Presidency POC

Major Luis Esteban Yrazu
Spanish Presidency Secretary

Lieutenant Alejandro Espada Isaac
Spanish Presidency Secretary

Lieutenant Javier Rey Requejo
Spanish Presidency Secretary

Sergeant Diana Díaz Casas
Spanish Presidency Secretary

GC Nekane Beltrán de Heredia Álvarez
Spanish Presidency Secretary

EDITORIAL STAFF

Guardia Civil:

International Cooperation Secretary (SECI) / Peacekeeping Operations Department (OPAZ)

Prospective and Analysis Centre (CAP)

Information and Social Relations Office (ORIS)

Edita: Secretaría General Técnica del Ministerio del Interior

Catálogo general de publicaciones oficiales: https://cpage.mpr.gob.es

En esta publicación se ha utilizado papel reciclado libre de cloro de acuerdo con los criterios medioambientales de la contratación pública.

NIPO (Papel): 126-23-114-9

NIPO (En línea): 126-23-115-4

Depósito Legal: M-31217-2023

INDEX:

FIEP SUMMARY

FIEP is an Association of national Gendarmeries and Police Forces with Military Status. The goal of FIEP (which started with the military forces of France, Italy, Spain, and Portugal) is to facilitate understanding between participating Institutes with the intention to pursue and strengthen relationships and bonds, promote innovative and active ideas on the type of law enforcement cooperation, strengthen reciprocal solidarity and enhance external organizational and structural models, agree in accordance with current international agreements and national regulations.

The Association aims at promoting an innovative and active reflection on the forms of police co-operation, and to value their model of organization and structures abroad.

FIEP is organized around a Senior Council and four technical commissions. The Senior Council of Directors/ Commanding Generals is made up of members of Gendarmeries and Police Forces who are Members of the Association. During its annual meeting, it defines the general policy and program for each commitment undertaken by the Association. The technical commissions meet once a year and consists of experts of the Member forces on the chosen topic by the Presidency. Each Commission operates in coordination with the Presidency, and in accordance with the instructions provided by the Senior Council.

At the end of each year, the Secretariat of the Presidency presents the results of the work performed by the Commissions, together with the plans proposed for any particular sector, notified by the leading Institution to the Senior Council of Directors/Commanding Generals for approval. Each Commission is hosted, on a rotational basis, by a Member based on a calendar.

The Presidency of the Association is appointed annually by rotation among the Directors/Commanding Generals. Apart from representing the Association, the Chairman is the element responsible for the smooth flow and coordination of all initiatives, and therefore is called upon to oversee, control and evaluate the programs decided by the Senior Council, assisted by the secretariat of the Chairman.

The FIEP (French acronym for France-Italie-Espagne-Portugal / France-Italy-Spain-Portugal, which are the first four “historical” members) is an Association consisting of gendarmeries and police forces with military status originally from the Euro-Mediterranean area. Founded in 1994, it then comprised the French National Gendarmerie, the Italian Carabinieri Corps and the Spanish Guardia Civil. It was quickly joined by the Portuguese National Republican

Guard in 1996. Afterwards, the Turkish Gendarmerie in 1998 swelled the ranks followed by the Dutch Royal Marechaussee and the Moroccan Royal Gendarmerie both in 1999, the Romanian Gendarmerie in 2002 and the Jordanian Gendarmerie Forces in 2011. The Argentinian Gendarmeria National and the Chilean Carabinieros joined the association as Associate Members in 2005 and the Qatari Internal Security Force "Lekhwiya" in 2013. The Tunisian National Guard became a member in 2016. The Ukrainian National Guard and the Palestinian national security Forces followed in 2017, as did the Brazilian State Military Police and Military Fire Brigades. The National Gendarmerie of Djibouti joined in 2017 and finally after being observers in 2019 the National Guard of Kuwait and the National Gendarmerie of Senegal became permanent members. In 2022 the Corpo della Gendarmeria de San Marino became observer.

INTENTIONALLY LEFT BLANK

COVER LETTER

After a year of intense work from all the members of the association, I have to recognize that it has been a true honor and a deep pleasure for me to hold the Presidency. The effects, risks and threats that regional conflicts impose to our societies have been analysed in a practical, in-depth and methodical way, new forms of international police cooperation, operational procedures and techniques have been highlighted. Furthermore, various strategies from the members of the FIEP Association, shared as best practice, have enriched the knowledge and experience of our Police Forces, mainly through the exchange of information established in the different FIEP Commissions held.

However, given the complex international situation, not only from a health perspective, where the pandemic derived from COVID-19 has maintained its effects, but also as a result of the military invasion of Ukraine and the existence of other regional conflicts that devastate or have an impact on our borders, we deemed appropriate to move forward in the study and analysis of any scenario of instability and uncertainty that has a direct impact on the maintenance of public safety and security carried out by police forces with military status.

In this regard, we know that we are facing new challenges within new security scenarios. One of the most relevant is cybercrime, which increasingly affects thousands of institutions, companies and citizens. Cybercrime is a threat of priority interest and requires a strategic response, supported by new technologies.

Another risk factor, aligned with climate change policies, is environmental crime. We must be proactive, identify and anticipate the threats, as we did in the past, with the creation of environmental police forces in Spain and in Europe.

It was under this framework, aimed at sharing and promoting the best police practices for the prevention and fight against crime in order to keep citizens safe, that we proposed for the debates held during the Spanish FIEP Presidency to be focused on the central theme **"Impact of a regional conflict on public safety and security in the field of Gendarmerie forces".**

I encourage you to keep growing and improving every day, convinced that, together, we will stand not only stronger, but better.

Leonardo Marcos González

General Director of the Guardia Civil

FOREWORD

Regional conflicts threatening our borders, especially the Ukraine war, have changed the security priorities in our societies.

We have come from years in which the security challenges at the centre of the political agenda have been the economic crisis, climate change and, more recently, the COVID-19 pandemic.

In parallel, armed conflicts have materialised with direct impact on independent third nations and the involvement of other actors, including major powers and international security organisations. This is the case in the Balkans, Syria or more recently in Ukraine, which have forced states to rethink their primary responsibility: to protect citizens from violence and insecurity in the face of the emerging threats arising from these situations.

Conflicts impose a high economic and social cost on neighbouring countries in the region. The consequences spread through multiple channels, such as a decrease in transit trade through these countries and the stagnation of service exports such as tourism. The short-term economic effects are only a relatively small part of the overall impact. In addition to some unquantifiable effects, conflicts have far-reaching consequences, especially on people, such as forced migration flows or the emergence of mafias and criminal organizations that take advantage of the weakness of others.

The arrival of refugees and displaced persons impels the demand for public services, both from the point of view of security and assistance, while generating a social response to ensure that they are cared for with a minimum of guarantees and decent living and health conditions, and that security conditions and access to basic resources in our societies are not jeopardise.

Likewise, different criminal organizations can profit from this situation of insecurity and disadvantage through **illicit trafficking**, fundamentally **trafficking in human beings**, mainly targeting the **most vulnerable groups**

(women, minors, etc.), or by taking advantage of the logistical opportunities to promote **arms trafficking** in a favourable situation, such as a regional armed conflict.

The potential demographic shock derived from these migratory flows unequivocally increases waste, water and air pollution, and is a challenge for authorities, including Police Forces. Even environmental protection is questioned, not only by the human effect of overusing natural resources, but also by the impact of the devastation caused by conflict or the outbreak of tensions.

Consequently, this Presidency has addressed **active environmental protection** as a specific dimension to be taken into account within the cross-cutting approach to the central theme of the proposed dialogs.

Many other political, social and security dimensions related to the impact of a regional conflict are critical, and they have been seen to under a holistic approach of the Presidency.

Gendarmerie Forces are supposed to be particularly qualified to adapt to this complex milieu, even with a possible responsiveness or resilience in the so-called "grey area". They can be decisive actors in these circumstances thanks to their military nature and experience in crisis situations and to other specific capabilities worth mentioning, such as **cyber-threat detection** and reaction proficiencies, prevention and investigation of environmental crimes, the investigation of war crimes, recently implemented, or even by **mitigating disinformation campaigns** aimed at destabilizing our societies, in order to profit from and fulfil FIEP Association's objectives.

Regarding FIEP Association's members, and as a result of the Russian invasion of Ukraine and the recent events occurred in the West Africa region, close to the borders of our common security space, Russia has prompted the

biggest boost in Europe's defence since the end of the Cold War. Furthermore, the instability and the critical scenario in Mali and Niger have a direct impact on their neighbourhood.

Almost every state in Europe has announced an increase in defence expenditure and the EU finalised its Strategic Compass, its first Common Security and Defence Policy strategy, with a much greater sense of urgency and purpose, thus providing a framework for aligning the efforts of EU member states and ensuring the incorporation of the EU's indispensable objectives. The Strategic Compass is a vital opportunity for the State Security Forces to demonstrate their adaptability and added value to Public Safety.

Important conclusions have been put in common, drawing therefrom, together with the latest policing techniques and procedures, and with the efforts to mitigate disinformation campaigns aimed at destabilizing societies, in order to profit from and fulfil FIEP Association’s objectives.

To that extent, the publication of this Book of the Presidency, as a result of the common and hard efforts carried out throughout this last year, performs the highest level of ambition in exchanging best practices and bringing together knowledge between the FIEP members, achieving the main scope of the Association.

WORK PROGRAMME OF THE SPANISH PRESIDENCY OF THE FIEP ASSOCIATION

The main objectives achieved under the Spanish Presidency have been:

1. Keeping and strengthening the values provided by the cross-cutting nature of FIEP, especially in periods of uncertainty and instability;

2. Providing continuity and profit from lessons learnt and shared knowledge from the Portuguese Presidency;

3. Commitment in achieving and performing tasks set forth in the "Common Declaration", ratified in 2022, especially by means of:

   a. Sharing knowledge regarding tools and experience that allows to effectively anticipate, prevent and respond to potentially emerging threats, especially those arising from regional conflicts, taking into account the intentional use of disinformation and under the **cross-cutting approach of impact on the environment;**

   b. Promoting the **exchange and joint training programmes** that will enable to better meet the needs described above;

   c. Ensuring and enhancing a wider visibility of the FIEP Association by virtue of the agreements reached.

4. Taking advantage of the capabilities that most of the forces of the Association offer as regards the **prevention and eradication** of:

   a. **cyber-threats**,

   b. **illicit trafficking** derived from a regional conflict, with special emphasis on trafficking in human beings and firearms

   c. the fight against **environmental crime**;

   d. **disinformation campaigns**.

In order to fulfil these objectives, the Presidency, with the outstanding support, management skills and commitment of four host nations (France, Djibouti, Qatar and Senegal), has been able to organize the four commissions defined in the Statutes of the Association, according to this Work Programme and the proposed topics.

HUMAN RESOURCES COMMISSION

SUB-THEME: Impact of regional conflicts on recruitment, education and training processes.

In the context of regional conflicts at European borders it was necessary to explore different people management strategies. Talent and team management from this perspective is one of the key tasks for police forces.

To hunt the most appropriate talent, professional skills and personal values to meet the needs of police forces. It is important that all the members of the Institution align with its objectives and feel that they act as its representatives.

In a conflict situation, stress and concern levels rise, in addition to a possible deployment and support in peacekeeping missions in the conflict region. In these circumstances, personnel selection must focus on more vocational profiles capable of sacrificing themselves for the sake of common good and public service.

The Human Resources Commission aimed to analyse and promote human resources management in terms of attracting interest, recruitment and training, with a view to generating the necessary capabilities and to finding and creating the best professional profiles in the event of an international conflict.

Contributing experts from every FIEP member were invited:

- To present possible training exchange programmes, either of general nature or aimed at qualification and specialization;
- To discuss the need for joint training or at least with common core elements, in order to achieve harmonization in the instruction and training of FIEP police forces;
- To maintain a permanent and smooth communication channel for the exchange of information in this area;

-To make available for Partners the international training offers of interest in relation to the central theme and sub-theme of the Commission.

NEW TECHNOLOGIES AND LOGISTICS COMMISSION

SUB-THEME: Adaptation of military status police forces to cyber-threats arising from regional conflicts.

One of the phenomena observed in recent conflicts is that they have generated complexity, chaotic dynamics and disruptive mutations linked to numerous (hybrid) threats and security challenges.

Cyber-threats are very real and security agencies cannot escape their responsibility to protect citizens in this dimension as well.

When facing disturbing scenarios, only a coordinated and sensible response will be possible, but with the right level of ambition for the current and potential capabilities offered by FIEP Members as regards cyber-threats.

The New Technologies Commission aimed to analyse cyber-threats to Public Order and how to deal with them, both from the point of view of the influence of the Gendarmerie Forces in the new legislation necessary to face these threats, and from the operational and organizational perspectives.

Contributing experts were invited to:

- Explain cyber-training best practices.
- Discuss and develop a joint digital proximity model
- Share strategies and procedures to mitigate cyber-threats derived from regional conflicts and in the field of public safety and security, especially the effects caused in our societies by transnational criminal organizations that profit from and take advantage of the windows of opportunity generated by the conflict.

INTERNATIONAL AFFAIRS COMMISSION

SUB-THEME: How to minimise the impact of regional conflicts on international relations. Approach: protection against disinformation.

The world is extremely complex and necessarily relies on a geopolitical status quo to try and solve the Public Order problems faced by Law Enforcement and Security Forces on a daily basis.

As the geopolitical situation evolves, no single approach to international politics can account for everything that is happening at any given time, can predict exactly what will happen in the coming weeks and months, or can offer a precise plan of action that guarantees success, especially when a regional conflict occurs nearby geographic space.

Taking advantage of regional conflicts, hackers and organizations have stolen and leaked emails, passwords and other details about institutions and individuals on both sides of the conflict and their allies. They also distort websites and conduct information operations aimed at undermining public opinion regarding the conflict among their opponents.

Disinformation campaigns promote political objectives of state actors involved in the conflict and seek to destabilize governments that support

different actors. Fake news undermining democratic institutions and rules does not necessarily have to do only with the notion of truth. The impact of misinformation must be interpreted in the context of the social relationships among those people who read, respond to and share news in a conflict situation.

The police forces with military status members to FIEP are well aware of the destabilization stemming from intentional disinformation. Therefore, efforts have focused on understanding how international police relations have developed so far, analysing how they are currently proceeding and how future relations will evolve in the light of existing regional conflicts, and how to achieve institutional resilience against disinformation and its effects.

The International Affairs Commission sought conflicts, and how the Gendarmerie Forces could make the necessary adjustments to minimise impact on Public Order, either in their own national areas of responsibility or as instruments within the Foreign Action of their respective governments, always under an approach of resilience against disinformation.

Contributing experts were invited to:

- Analyse and expose the achievements made within their Institutions after almost thirty (30) years of institutional relations through the FIEP Association.
- Review the organizational, operation and institutional relations models in the FIEP Association.
- Find possible solutions that contribute to the achievement of FIEP's objectives, taking into account the impact of regional conflicts, by sharing strategies and procedures to mitigate the effects of disinformation.

SERVICE ORGANIZATION COMMISSION

SUB-THEME: Capabilities of military-status police forces against threats arising from regional conflicts. Approach: Environmental protection and migration flow control.

The multiple problems associated with conflicts in neighbouring countries and regions require integrated and coordinated responses, capable of adapting to and facing the current challenges.

In this context, it is essential to plan services adapted and focused on emerging problems: border control, refugees reception and management, increase both in ordinary and specialised crime, or even the necessary training in the prevention of environmental crimes and protection against climate change.

Thus, the Gendarmerie Forces must develop and adapt their organizational structure to render these services, creating dedicated bodies and/or departments. To that end, it would be of great interest to analyse the threats and think about how to address them.

The Service Organization Commission aimed to promote mutual knowledge of the structures that each Force has in place to deal with threats arising from regional conflicts, and to share good practices, so that possible models to be followed can be subsequently analysed and discussed. In particular, the exchange of information on environmental protection police capabilities has been promoted, as well as on migration flow control and on the emergence of illicit trafficking, especially with regard to trafficking in arms and human beings, mainly targeting the most disadvantaged groups.

Contributing experts were invited to:

- Analyse the direct consequences cause by regional conflicts with impact on national public security on the environment;
- Discuss the need for common training or qualification to effectively tackle the risks arising from regional conflicts that have a direct

impact on the environment, as well as the control, management and protection of migration flows;

- Maintain a permanent and smooth communication channel for the exchange of information in this area;
- Make available for Partners the international training offers of interest in relation to the central theme and sub-theme of the Commission.

HUMAN RESOURCES COMMISSION

Paris, 16th November 2022

Lieutenant Colonel Plácido Manuel RODRÍGUEZ MORENO

Captain Roberto FERNÁNDEZ ORTEGA

1. INTRODUCTION

The Human Resources Commission of this Association pursued harmonization in the training of partner bodies, and to this end, and in close coordination with national academies, facilitated the exchange of experiences and practices and the comparison of curricula, where the promotion of joint training in subjects such as languages and human rights were encouraged.

The aim of the Human Resources Commission was to analyze and promote personnel management related to recruitment, training and development focused on generating the necessary skills, to share training exchange programmes of a general nature or aimed at training and specialization, to achieve harmonization in instruction and training, with the maintenance of a fluid and lasting channel of communication for the exchange of information in this field, in order to make available to the Associates an international training offer that is considered to be of greater interest.

In accordance with the central theme chosen for the Spanish Presidency of the FIEP, which is "the impact of a regional conflict on public security in the area of the Gendarmerie Forces", the FIEP Human Resources Commission has sought to carry out an analysis and study of human resources management related to:

- Recruitment.
- Enlistment.
- Training.
- Selection of the best professional profiles in the event of a possible regional conflict between several States.

In this regard, the Spanish Presidency of the FIEP has sought to highlight the experience of joint training between Gendarmerie Forces, taking as a reference the collaboration in recent years between the French National Gendarmerie and the Guardia Civil.

Given all this, the Guardia Civil decided to carry out a comparative study of the different access and training systems of the twenty (20) Institutions that make up the FIEP, compiling the curricula (PLEST) of of each of the Law Enforcement Institutions.

To this end, the expert appointed by the Guardia Civil for the FIEP HR Commission drew up some tables in which certain data on the access and training systems of the different FIEP Forces were inserted. As support, the information corresponding to the Guardia Civil access and training systems was provided and submitted to the FIEP members before the HR Commission meeting took place in Paris in November 2022.

1.2. Conclusions and commitments adopted by the experts participating in the HR Commission in Paris.

Following the interventions of the experts attending the Human Resources Commission at the meeting held in Paris (November 2022), the Spanish Presidency of FIEP highlights the following commonly agreed conclusions:

- Members will share information and experience to understand the different selection and training processes and structures, as well as the institutional positions of each FIEP members.
- The experts will analyze the skills and needs for selection and training, taking into account the impacts of a regional conflict on public security in the area of Gendarmerie Forces and Police Forces with military status
- Experts will develop best practices on how to adapt selection and training to the new skills and curricula required.

The conclusions of the experts' meeting are set out in point 9 of the minutes of the HR Commission, and were approved and signed by the POCs attending the meeting.

2. COMPARATIVE STUDY OF INFORMATION ON RECRUITMENT, SELECTION AND TRAINING IN THE FIEP INSTITUTIONS ANALYSED

In accordance with the above, and within the framework of the FIEP HR Commission, the Spanish Presidency of the FIEP has carried out a comparative study which has reflected:

1. The different systems of access to the institutions that make up FIEP.
2. The different training systems within each of the FIEP institutions, compiling each and every one of the different curricula (PLEST), established for the training of the future members of the different Gendarmerie Forces of FIEP.

This study aims to address the first three issues envisaged for the HR Commission during the Spanish Presidency concerning recruitment, enlistment and training.

The different security forces analyzed have in common that they are armed police institutions. In terms of organization and structure, they are hierarchically organized into different scales or ranks, according to the level and degree of responsibility of their members within the organization, with the Officers' Scale being the highest, followed by the Non-Commissioned Officers' Scale and the Basic Scale.

In order to carry out the study, reference was made to the different ways of access to the Guardia Civil to its different scales, direct access or professional promotion, the necessary academic requirements or the reservation of places for certain groups. Once the information received has been analyzed, it was compared with the Guardia Civil model used.

Based on the documentation provided and analyzed from the FIEP members, it can be deduced that the personnel selection processes are generally carried out through competitive examination systems in the different scales. Another specific form used is the competition system and, to a lesser extent, the direct

recruitment of qualified personnel, the latter option being reserved for the officer scales of some institutions. This process consists of several phases, including knowledge and physical tests. In addition, the merits obtained by the candidates, previous work experience, academic training and other relevant factors such as the maximum or minimum age for certain ranks are taken into account.

One indicator selected for the study is to compare the military background of their personnel, as they are police institutions of a military nature, as well as the promotion of their members. When the data is broken down into the different scales, it can be seen that all the FIEP institutions encourage professional promotion for the selection of their personnel, who subsequently make up the officer and non-commissioned officer scales.

There is more variety in the basic scales. On the one hand, like the Guardia Civil in Spain or the Arma de Carabinieri in Italy, which have reserved places for military personnel from the armies or reserve troops, respectively. On the other hand, it completely rules out the selection of personnel through the reservation of places for these groups.

Another factor used for the comparative study is the academic qualification acquired or its equivalence once training in the corresponding scale has been completed. People who enter the officer scale usually have a university degree.

As a general rule, personnel entering the non-commissioned officer scale have an academic qualification of higher vocational training technician or its equivalent. However, in the specific case of the Italian Carabinieri, they get a degree in legal sciences after successfully completing the three years of studies that make up their curriculum.

As for the basic scales, there is more difference in the academic qualifications acquired, ranging from baccalaureate to higher vocational training technician. It should be kept in mind in all the above sections that it has not been possible to process the information received, as the data is not known.

2.1. Highlights of the study in the Officer Scales

The purpose of the survey was to know the system of access to the scale of Officers, whether they have internal promotion, the period of training used, the employment achieved after completion of the training and the academic qualifications obtained, once the established study plans had been passed.

In NATO countries, and taking as a reference the military codes used by NATO, in all cases they reach a level equivalent to OF-1, even if the employment reached has a different designation.

Firstly, the different forms of access to the Officers' scale of the FIEP members who have provided data have been studied. It should be noted that there is a similarity in the studies required for access to training in this scale, with a university degree being the most required through the system of direct access by competitive examination, as can be seen in the model of the French National Gendarmerie. However, with the Spanish, Italian, Dutch or Moroccan model, it is not necessary to have a previous university degree, with students attending the corresponding training in the different military education centers such as the General Military Academy and the University Centre of the Guardia Civil (CUGC), the Military Academy of Modena in Italy, the Royal Military Academy of the Netherlands or the Royal Military Academy of Morocco, obtaining a University Degree in all cases.

With regard to professional promotion, there is also a unification of criteria in that a university degree is required to enter the scale, generally aimed at personnel with a background in the NCO scale, although with the possibility of entering from the basic scale, as in the Guardia Civil system. In other cases, as in the model of the French Gendarmerie, the Royal Moroccan Gendarmerie or the Spanish Guardia Civil, access is by competitive examination, with no previous university degree. Students follow the subsequent training plan at the National

School for Gendarmerie Officers (EOGN), the Royal Military Academy of Morocco and the University Centre of the Guardia Civil, leading to a university degree. Also within the professional promotion system, we find a competitive system, taking as an example the Royal Moroccan Gendarmerie, in which non-commissioned officers with more than twenty (20) years of service and an attitude certificate can become part of the Officers scale.

Another form analyzed in the selection of personnel for the Officer ranks is the recruitment of qualified personnel for specific jobs, as in the model of the Gendarmerie of the Republic of San Marino, where by virtue of optimal technical and professional preparation, evident qualities and experience acquired in military academies or international police forces and security agencies, they can be hired on a permanent basis or for maximum periods of three (3) years, starting with a probationary period of twelve (12) months.

There are also other possibilities analyzed in the systems of access to the officer ranks, such as the competition used by the Royal Moroccan Gendarmerie to fill officer posts with certain qualified personnel with a Doctorate in Medicine, Pharmacy, Veterinary Medicine or Dentistry. It is worth mentioning the direct access system of the French National Gendarmerie, although all officers are trained at the National School for Gendarmerie Officers (EOGN), the origin of its students is very varied. From university degrees, the scientific branch, for civil servants with category A with at least five (5) years of service in an organization, engineering degrees in specific subjects for field officers, engineering degrees in specific subjects for technical and administrative officers, and for officers from the army with the rank of Captain.

A similar approach is used by the Carabinieri Arma in Italy, where places are reserved for the officer scale for those with degrees related to environmental studies.

As a point of interest in the officer ranks, the officers of the Djibouti National Gendarmerie are trained for three (3) years at the Djibouti Military Academy,

supplemented by two (2) years at the French National Gendarmerie Officers' School (EOGN).

With regard to the training period, differences can be observed, especially in the direct access or internal promotion modality, varying from five (5) years to two (2) years respectively. Or even in the model of direct access with prior university degree, which usually has a training period of two (2) years, as is the French model, lacking direct access without a university degree.

2.2. Highlights of the study in the non-commissioned officer scale

In NATO countries, and taking as a reference the military codes used by NATO, in all cases they reach a level equivalent to OR-5, although the employment reached has a different denomination.

As in the case of the officer ranks, the study of access to the non-commissioned officer ranks of FIEP members was based on both direct access and internal promotion. It can be seen that all the institutions encourage the internal promotion of their members, drawing mainly from the basic scales, facilitating the professional career of their personnel. In some cases, such as the Spanish model of the Guardia Civil or the Gendarmerie of the Republic of San Marino, one hundred percent of the places for access to the scales are reserved for people from the basic scales. In the case of the Republic of San Marino, the competitive examination for direct access would only be opened when the places for internal promotion have not been filled.

To gain access to training for non-commissioned officer ranks, the most commonly required qualification for direct access by competitive examination is the baccalaureate or equivalent. In professional promotion, the most required academic qualification is the baccalaureate or equivalent, and the processes are carried out by competitive examination or competition within the Armed Forces,

such as the Royal Moroccan Gendarmerie. Another requirement to applicants is the need of completing a minimum time of service in the basic scales.

Specific mention with the information studied is the job of Gendarme in the French National Gendarmerie, the first job in its scale of non-commissioned officers.

As for the training period, it can be observed that there are differences, especially in the direct access or internal promotion modality, varying from three (3), two (2) and one (1) year, respectively. All this taking into account the origin and training acquired in the previous scales, as well as the time spent in them and the time of service rendered.

2.3. Highlights of the study in the Basic Scales

In the basic scales, the study has focused only on the modalities of direct access, and within this, the origin or reservation of places for certain groups.

From the verification of the information collected, it has been observed that not all FIEP members have the basic scale, as is the case of the Royal Moroccan Gendarmerie. In other cases, they do have the basic scale, such as the French National Gendarmerie, where its main purpose is to train personnel for future incorporation into the scale of Non-Commissioned Officers as Gendarmes, while they carry out work in the units with the employment of Deputy Gendarmes in the units. The above basic scale is also used to recruit personnel for a specific post in areas such as IT, telecommunications, and mechanics, clerical, among others.

The most remarkable aspect of this section is that not all staff belonging to the basic scale is career staff. Therefore, the format is based on recruitment for a limited period of time or age limit. To gain access to training for the basic scales, qualifications vary from school-leaving certificate, in the case of the Djibouti National Gendarmerie, to baccalaureate or equivalent in the majority of FIEP members.

As for the training period, it can be observed that there are substantial differences in duration, varying from three (3), six (6), twelve (12) and eighteen (18) months. All this taking into account the origin and training acquired in the previous scales, as well as the time spent in the same, and the length of service provided.

3. CRISIS RESPONSE (POLICE CAPABILITIES)

In order to be able to have the most appropriate staff to deal with a possible crisis situation, which could affect public security arising from a regional conflict, and which is related to the area of competence of the gendarmerie forces of several States, it was considered that this could take into consideration, among others, the different capabilities of each FIEP member, with the aim of analyzing the selection and training needs of the personnel that make up each Institution.

As a first indicator and reference sample to obtain a vision of the above, it is necessary to know the number of personnel available to each FIEP member, breaking down data from the eighteen (18) member Institutions together with San Marino as observer, in order to be able to infer the capacity of each one of them.

The following table shows the number of staff of each of the above-mentioned institutions, including the total number of staff of the FIEP Association:

COUNTRY	STRENGTH		COUNTRY	STRENGTH
France	130.000		Argentina	29.000
Italy	118.000		Chile	58.000
Spain	78.000		Palestine	12.400
Portugal	22.000		Ukraine	46.000
Morocco	50.000		Brazil	650.000
Netherlands	6.000		Djibouti	1.040
Romania	28.000		Kuwait	70.000

Jordan	15.000		Senegal	12.850
Türkiye	165.000		San Marino	87
Tunisia	28.000		**TOTAL**	1.519.112

Regardless of the number of troops available to each country, especially taking into account that it is linked to its size and population, it is necessary to mention and link the membership of the FIEP Forces to other International, Supranational and Regional Organizations as far as police functions are concerned, memberships based on police cooperation between different countries, and among the different Organizations, the following can be highlighted:

- **UN** (United Nations)
- **NATO** (North Atlantic Treaty Organization):
- **OSCE** (Organization for Security and Cooperation in Europe)
- **EU** (European Union)
- **EUROGENDFOR** (European Gendarmerie Force
- **FRONTEX** (European Agency for the Management of Operational Cooperation at the External Borders of the Member States of the European Union)

3.1. FIEP police capabilities in case of regional conflict.

The need to connect the Institutions and propose strategies to help face transnational threats (terrorism, organized crime, cybercrime, drug and arms trafficking, human trafficking, etc.), as well as to program crisis situations that may arise and affect public security in the area of competence of the gendarmerie forces that make up the FIEP, can be a useful tool for testing the selection/training needs of the personnel that make up the Institution.

Recognizing that, by definition, no state or organization can face these situations alone, the capabilities and thematic areas available to each member can provide a global approach to security in order to develop collective

responses. Therefore, by way of example, certain crisis situations that would affect more than one member state, the impact they could have and the capabilities that could be articulated are cited.

3.1.1. Crisis situations caused by natural disasters.

It can be defined as changes that occur suddenly in the dynamics of the environment, often resulting in loss of life and property. Earthquakes, floods, tsunamis or forest fires are natural catastrophes in which the human hand is not present, since, if it were present, we would be talking about environmental disasters resulting from irresponsibility with the environment.

Crises, emergencies and catastrophes involve the mobilization of numerous participants. Therefore, without going into detail about all the emergency services that would be involved, the initial police response in this situation is to be found in the basic public order and public safety units. These units would be responsible for guaranteeing public order and security by establishing access controls and signposting, evacuating people in danger and warning the public, among many other tasks.

In this parameter and in view of the capabilities analyzed in previous sections, it can be inferred that the level of FIEP members is more than acceptable, taking into consideration the high percentage of countries that have troops in the capacity known as Public Order, Area of General Surveillance of public security, of which a total of 15 countries have, representing 75%.

On the other hand, other types of police units that operate when an emergency situation arises are the Special Operational Units. In natural disasters, one of the tasks performed by this type of unit, among many others, is the search and rescue of missing persons. Technically, these tasks are also known as first response actions, as they are the actions that are carried out immediately once the disaster occurs. Along the same lines, in appropriate cases, Specialized

Forensic Investigation Units could also be set up, units related to the identification of living persons or corpses, using specialized methods for these tasks.

There is a certain inequality in the number of FIEP members that have Special Operational Units and Forensic Investigation Capabilities, with the majority of countries not having them, so that dealing with this type of situation in cooperation with another member state would not be feasible in many cases.

3.1.2. Situations of migration crisis caused by armed conflict.

When armed force is used between two or more states, whatever the motives or intensity of the confrontation, it leads, among other things, to significant internal and external human displacement, with the result that neighboring countries and areas are affected in terms of border control and surveillance.

The effective management of border guards in order to control refugees and mass movements of people, while maintaining a high level of security is therefore an extremely complex situation, requiring for the most part the assistance of institutions at the supranational level and partner states in international cooperation programs.

In this regard, it is worth mentioning that various countries that form part of transnational institutions and that have personnel assigned to border control and surveillance have recommendations and operational guidelines that have already been tested and have produced good results, which are listed below:

- Simplification of border controls at the borders of countries bordering countries in armed conflict.

- Flexibility in entry conditions: According to the rules of each country, border guards may authorize third-country nationals to enter the territory of a State on humanitarian grounds, even if they do not fulfill all entry conditions.

- Allow crossing through temporary border crossings, outside official border crossings, which could help reduce delays at the border.

- Facilitate access to rescue and humanitarian aid services, where the States concerned should take special measures to facilitate the entry and exit of rescue services, police and firefighters, including the provision of medical assistance, food and water to persons waiting to cross the border. They should also establish special lanes at border crossings to ensure access and return for organizations providing humanitarian assistance to people from countries in situations of armed conflict or war.

Without going into questions of specialized strategies specific to other fora and institutions, associations or police cooperation assistance programs already in place, the generic capacity of Border Control and its corresponding thematic areas is not homogeneous in terms of the number of FIEP members with staff dedicated to these tasks, and in general terms there is a significant lack in this field. This shortage would be covered in certain areas as some FIEP members are assigned to organizations with executive capacity and effective response, such as the FRONTEX Agency.

3.1.3. Crisis situations caused by war resulting in peacekeeping missions.

In the prevention, containment, moderation and termination of hostilities between or within States, through the mediation of an internationally organized and led peaceful third party intervention, multinational forces of soldiers, police and civilians are employed to restore and keep peace.

For this reason, through different transnational organizations and institutions (European Union, Eurogendfor, UN, NATO, OSCE), numerous troops from various FIEP gendarmerie corps have been deployed on peacekeeping missions in different scenarios and conflict zones on numerous occasions.

Consequently, in these deployments they have had to deal with each aspect at different stages of a crisis and can be categorized in a generic way:

- Security, replacing the initial phase, conducting stabilization and law and order operations and reinforcing weakened or non-existent local police forces.
- During the transition phase, continuing to fulfill its role as part of the expeditionary force, facilitating coordination and cooperation with international and local police units.
- During withdrawal, facilitating a smooth and continuous transfer of responsibilities from the military to the civilian chain of command.

During these missions, and through the aforementioned bodies created for such tasks, these gendarmerie corps carry out tasks for which they are responsible in their countries of origin and are divided into:

- Military police tasks. This work is carried out within the contingents of the Armed Forces of each country, supporting the security of the bases, their internal order and acting in different capacities and areas of work/specialties.
- Police tasks in a strict sense. In unstructured countries, these gendarmerie forces have participated as a multinational force, simultaneously with training tasks, so that the country's police forces could gradually take over security.
- Training and advisory tasks. These are probably the most common of the tasks carried out. They begin in training centers and continue by monitoring police action on the street. These missions ensure that the knowledge provided in training centers is put into practice, teaching by example and tutoring, ensuring that the new Security Forces internalize behavior in accordance with human rights and best practices in line with police codes of ethics.

4. GENERIC CONCLUSIONS

A series of generic conclusions are drawn in order to give an overview of the resources available to FIEP members in order to provide a simple and graphical view of their response capacity and to test the selection and training needs in certain situations that may affect public safety among various FIEP members.

Lack of homogeneity in terms of the capabilities available to all the members of the FIEP, as there is no balance or similarity in terms of having the same capabilities and areas of work defined in each of them. Factors such as the number of personnel, the specific casuistry of each area of responsibility, geographical location, specificity and division of competencies with civilian police forces in each country, all contribute to a differentiating element that explains the aforementioned lack of homogeneity and disparity of capabilities that the FIEP members are capable of assuming or having, with the founding FIEP members having the most capabilities and areas of work in common. The generic capacity of Public Order and its Areas of work is the one with the highest percentage of FIEP members.

The training needs of personnel in areas of work or specialties are usually covered by supranational bodies and institutions that are already consolidated and of proven solvency (CEPOL, Atlas Network, Interpol, Frontex), and in bilateral police cooperation programs between police forces and agencies. Having said this, it could be interesting to evaluate and explore new reciprocal cooperation projects, taking as a starting point and reference the experiences carried out by the French National Gendarmerie and the Guardia Civil, which resulted in optimum levels of satisfaction for both institutions. In these conferences, core areas were identified that could be a useful tool for homogenizing and creating a common basic profile of citizen security agents that could be a reference for a large number of FIEP members. These areas correspond to Migratory Flows (Police Cooperation, Detection of illegal immigration), Organized Crime (Operational Intervention), Terrorism (Police Self-Defense, Shooting, Physical Education) and Mutual Knowledge (Knowledge of the participating Institutions, Languages).

In peacekeeping missions, a significant part of FIEP members have the possibility to act under military or civilian command, and even to ensure the transition from military to civilian primacy in a crisis management operation, which allows for synergy of effort and consistency of action. In general, police forces of a civilian nature are not authorized to act under a military chain of command. Likewise, gendarmerie forces possess military skills and appropriate equipment that allow them to operate in destabilized environments, performing policing functions from the very outset of a crisis.

NEW TECHNOLOGIES AND LOGISTICS COMMISSION

Djibouti, 24th January 2023

Lieutenant Colonel Manuel José SILOS BRIANSO

Lieutenant José Luis PÉREZ MANZANO

1.-Introduction:

One of the phenomena observed in recent conflicts is that they have generated complexity, chaotic dynamics and disruptive mutations linked to numerous (hybrid) threats and security challenges. Cyber-threats are very real and security agencies cannot escape their responsibility to protect citizens in this dimension as well.

According to the Spanish FIEP Presidency Work Programme, during the New Technologies and Logistic Commission in Djibouti (23-26 January) the *SUB-THEME ´Adaptation of military status police forces to cyber-threats arising from regional conflicts´* was addressed.

When facing disturbing scenarios, only a coordinated and sensible response would be possible, but with the right level of ambition for the current and potential capabilities offered by FIEP Members as regards cyber-threats.

2.-Development.

Theoretically the Gendarmeries and Police Forces with Military Status may be specially qualified to be able to adapt to complex environment. Their military character and experience in crisis situations make them a decisive actor in these circumstances, while adding other capacities worth taking advantage of, such as detection and reaction to threats in the cyber field, prevention and investigation in environmental crimes and others put into practice more recently, such as the investigation of war crimes.

Cyberspace is a global common space characterised by its functionality and dynamism. Lack of sovereignty, its weak jurisdiction, ease of access and difficulty to attribute actions within it define a scenario with a wide range of serious security challenges.

Cyber-threats are very real and security agencies cannot escape their responsibility to protect citizens in this dimension as well.

When facing disturbing scenarios, only a coordinated and sensible response will be possible, but with the right level of ambition for the current and potential capabilities offered by FIEP Members as regards cyber-threats.

The New Technologies Commission aimed to analyse cyber-threats to Public Order and how to deal with them, both from the point of view of the influence of the Gendarmeries and Police Forces with Military Status in the new legislation necessary to face these threats, and from the operational and organizational perspectives.

2.- Development of the assigned duties:

2.1.- Cyberthreats.

Currently there is no unanimous definition or classification, due to the different perceptions and even regulations, as was verified in the different discussions between experts during the NTL Commission.

Cyberthreats are in some places defined as malicious disruptions or manipulations that affect technological elements. They encompass a wide range of actions. Cyberthreats are characterised by their diversity in terms of both capacity and motivation.

They affect practically all fields of National Security, such as National Defence, economic security or protection of critical infrastructures, among others, and they do not respect borders.

The same qualities that help cyberspace drive progress can be exploited for harmful purposes when combined with how exceptionally easy it is to remain anonymous, steal identities and amplify effects.

In order to be able to work with solid bases that allow the development of the rest of the lines of work, the different experts were requested to complete the following table, taking into account that it was not a closed classification and that it was open to different opinions.

DEFINITION	malicious disruptions or manipulations that affect technological elements, and that encompass a wide range of actions					
GROUP	**SUBGROUP**	**AGENTS**	**EFFECTS**	**TYPES**	**REGIONAL CONFLICT**	**HYBRID STRATEGY**
CYBERESPIONAGE		APTS, AGENTES ESTADO-NACION, malicious insiders, corporate spies	DATA LEAKS		YES	YES
CYBERCRIME	CYBERTERRORISM	terrorist groups		DDOS	YES	YES
	HACKTIVISM	APTs, hacktivists		DEFACEMENT	YES	YES
				DATA LEAKS		
				DDOS		
	CYBERCRIME	criminal groups, hackers, APTs, terrorist groups		Theft of financial or payment related information	NO	NO
				cyber exrtortion		
				email anda internet based fraud		
				ransomware		
				identitiy fraude		
				cryptojacking		

Thanks to the Internet revolution, States, organised groups, collectives and even isolated individuals can attain a so-far unprecedented level of power and capability to influence. Digital connectivity means that global social movements take on strategic importance that has been underestimated until now.

The actions that cyberspace uses to carry out malicious or illicit activities include cyber espionage and cybercrime.

Cyber espionage is a relatively cheap, fast method with fewer risks than traditional espionage, given the difficulty of attributing authorship. The greatest capabilities are mainly held by State players (intelligence or military organisations), that fundamentally operate via what are known as Advanced Persistent Threats (APT). This type of threat means that the opponent has sophisticated knowledge levels plus resources and infrastructures so that, by deploying multiple types of attacks, they can interact on their targets over a long period of time, adapt to defence strategies, and maintain the interaction level to meet its end.

In addition, a growing trend is now seen in what are known as hybrid threats, coordinated and synchronised actions aiming to deliberately attack systemic vulnerabilities in democratic states and institutions, through a wide range of media, such as traditional military actions, cyber-attacks, information manipulation operations or elements of economic pressure. State and non- state players, either directly or through intermediaries, exploit the Internet's propensity for disinformation and propaganda and a generalised interest in obtaining and developing military capabilities to operate in cyberspace, including offensive capacities in many cases.

Cybercrime, in turn, is a top-level citizen security issue, representing one of the widest-spread and generalised threats, continuously arising and increasingly victimising thousands of institutions, companies and citizens. The term Cybercrime refers to illicit activities in cyberspace, targeting elements, computer systems or any other legal property, whenever its planning, development and performance is determined by use of technological tools; depending on the nature of the actual punishable act, authorship, motivation, or damage inflicted, this might refer to cyber terrorism, cybercrimes or, when appropriate, hacktivism.

Use of new financial and economic transaction methods, such as cryptocurrency, for illicit trafficking and trading of goods and providing services or extortion, fraud and forgery of non-monetary means of payment, poses a serious security challenge because they are both sophisticated and complex.

They can be used for money laundering and tax evasion and they represent a source of income for organised crime; therefore, they facilitate other activities such as financing terrorism, making the most of how difficult it is to monitor these new techniques.

Cybercriminals operate under organised-crime frameworks and incessantly explore techniques for building low-risk lucrative business models, sheltered by the fact their actions are difficult to trace.

Terrorist groups attempt to make the most of cyberspace vulnerabilities to launch cyberattacks or activities to radicalise individuals and collectives, for financing, disseminating techniques and tools to commit a terrorist attack, and for recruitment, training or propaganda. Intimately linked to this, there is the threat against critical infrastructures, with the clear chance of using networks to bring about a collapse as essential services fall like dominoes.

Hacktivist groups carry out cyberattacks for ideological reasons and sometimes, making the most of products, services and tools available in cyberspace, they seek to develop attacks with a major media or social impact.

Nor can we ignore threats from the continuous surge of organisations contracting cybercriminal services to damage their competitors and their in-house technological and human resources that might be detrimental for the organisation, without forgetting all emerging threats and actions resulting from lack of cybersecurity culture.

On the other hand, digital information has become an asset with high added value. Analysis of personal data on the Net is used for a wide range of purposes from sociological studies to advertising campaigns. Malicious use of personal data and disinformation campaigns have high potential to destabilise society.

Furthermore, exploiting personal data breaches represents infringement of this data's security, affecting people's privacy and their data's integrity and confidentiality.

As far as disinformation campaigns are concerned, they use elements such as fake news to influence public opinion. Internet and social media amplify the effect and scope of the information being sent out, with potential application against targets such as international organisations, States, political initiatives or public personalities or even democratic electoral processes.

With the valuable contributions imparted by the experts during the NTL Commission, the tabular presentation has been comprehensively compiled in the ensuing manner:

DEFINITION	malicious disruptions, data leaks or misuses that affect information systems, and that encompass a wide range of actions					
CLASSIFICATION						
GROUP	**SUBGROUP**	**AGENTS**	**ACTIONS**	**EXAMPLES**	**REGIONAL CONFLICT**	**HYBRID STRATEGY**
CYBERWARFARE		state actors	DISRUPTIONS DATA LEAKS MISUSES		YES	YES
CYBERESPIONAGE		APTS, state actors, malicious insiders, corporate spies	DATA LEAKS		YES	YES
CYBERCRIME	CYBERTERRORISM	terrorist groups (or individuals)	DISRUPTIONS	DDOS	YES	YES
			MISUSES	illegal contents		
	HACKTIVISM	APTs, hacktivists	DISRUPTIONS	DEFACEMENT, DDOS	YES	YES
			DATA LEAKS	DATA divulgation	YES	YES
			MISUSES	disinformation, misinformation	YES	YES
	CYBERCRIME	criminal groups or individuals, hackers, APTs, terrorist groups or individuals	DATA LEAKS	Theft of financial or payment related information, Theft of identity	NO	YES
			DISRUPTIONS	cyber extortion and ransomware, cryptojacking	NO	NO
			MISUSES	email and web based fraud, illegal gaming, forgery, traffics, laundering, sexual violence, other violence, identity fraud, other frauds, etc.	NO	NO

The use of hybrid strategies has increased; though coordinated, multidimensional actions, such strategies seek to exploit the vulnerabilities of States and their institutions, targeting their political, social, or economic destabilization or coercion. It is difficult to identify the perpetrators of such strategies, and the methods they use may include not only conventional actions but also others, such as disinformation campaigns, cyberattacks, espionage, social subversion, sabotage, economic coercion, and the asymmetrical use of military means.

3.2.-Training.

In order to have a catalogue of training actions that are carried out in the cyber field in the different FIEP forces, it was considered necessary to identify the different profiles towards the different training actions should be directed.

As an example, the following profiles, grouped by the digital skills that each one should possess, could be established:

- Law Enforcement Management
- Heads of Cybercrime Units
- General Criminal Investigators
- Intermediate and Advanced Criminal Investigators
- Cybercrime Analysts
- Cyber-Intelligence Officers
- Online Investigators
- Digital Forensic Investigators
- First Responder
- Cyber Management
- ICT/IV Specialist
- Hacker
- Developer
- OSINT Specialist
- INTEL Specialist

Given the sheer size of the force in terms of personnel, in the GENDARMERIE CORPS of San Marino the Operative and Judicial Police Department (OJPD), acts as the reference point for all intelligence, analysis and investigative activity in the field of cybercrime, and it is staffed with online investigators, intermediate and advanced criminal investigators and digital forensic investigators.

General cybercrime awareness is to be found among all members of the force, especially at local level (Brigate), while emergency phone operators collect and forward relevant information on, for example, widespread phishing and fraud campaigns.

As the expert of the NATIONALE GENDARMERIE of France stated, this work has already been carried out by the European Cybercrime Training and Education Group (ECTEG), whose "TCF" Matrix crosses profiles and digital skills indicating the level required (none, basic, intermediate, advance).

As the elements in question are considered of interest, the most noteworthy aspects of the aforementioned research by Nationale Gendarmerie of France were set out below:

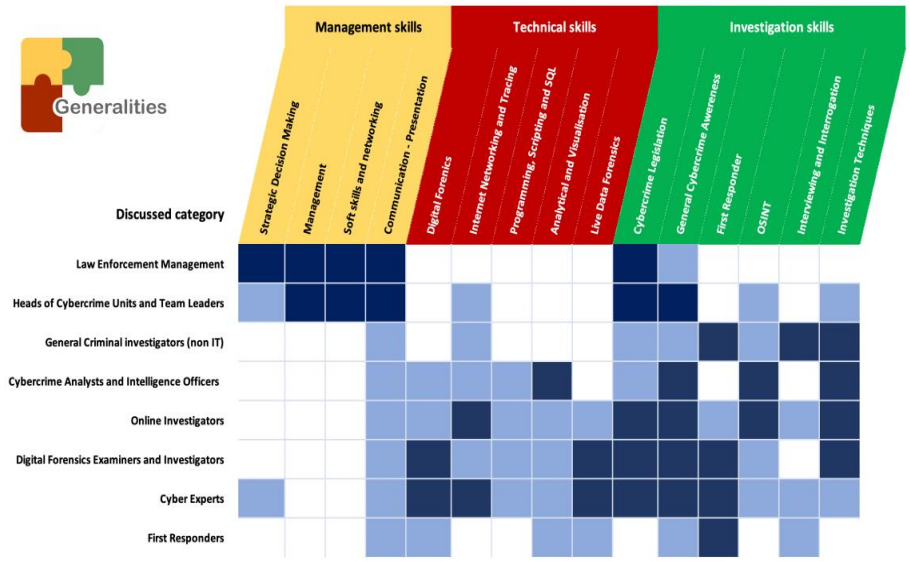
- The Cybercrime Training Competencies Framework (TCF)1 identify the required competencies, skills and training needs of the key actors involved in combating cybercrime at EU level, focusing on both LE and the judiciary.
- Drawing on the contributions and the analysis of stakeholder input, it outlines a TCF on cybercrime based on identified categories of actors, and presents a set of key findings and recommendations.

[1] https://www.ecteg.eu/tcf/co/TCF_4.html

- TCF report is one of the operational action items agreed within the EMPACT policy cycle. It is the joint effort of CEPOL, Eurojust, Europol, EJTN and ECTEG and presents the results of a one-year project. While the main focus is on the competency and skill sets of the main roles identified. The key roles identified range from entry level investigators and examiners, judges and prosecutors, to managers, decision makers and policy makers; the different needs per role in terms of knowledge, skills and expertise establish the main building blocks of the TCF.

The considered profiles included in TCF are:

- Head of Cybercrime Unit of Team Leader
- Online Investigator
- Criminal Investigator
- Cybercrime Analyst and Intelligence Officer
- Digital Forensics Examiner
- Cyber Expert
- First responders



Cybercrime Training Competencies Framework (by the French National Gendarmerie)

Conclusion: The fight against cybercrime cannot be addressed in isolation but requires a cross-border approach involving all relevant stakeholders. Particularly in the areas of capacity building, training and education, there is a need for a standardised and harmonised approach that leverages productive partnerships with industry and academia. The latter is essential for LE and the judiciary to gather and exchange information on the latest threats and trends in cyberspace and to allow for efficient and effective investigation and prosecution.

Cooperation with the public and private sectors and academia is considered essential in realising synergies in terms of skills and expertise, ensuring coherence and helping to avoid duplication of effort when developing training courses and educational programmes for LE and the judiciary.

It has been detected that there is a need for a more comprehensive, complementary and sustainable approach to training and education at EU level, ideally embedded in an agreed governance model whose realisation will be the further step to take after this report, through a concerted plan amongst the relevant partners.

Informed by stakeholder input, the TCF identifies ten key actors in LE and two in the judiciary that are involved in the fight against cybercrime. For each actor, the report identifies the required skills and expertise. The necessary competencies and skills identified fall into three main categories – management skills, technical skills, and investigation skills.

When developing new training courses or updating the existing training portfolio, contemporary education methodologies and approaches such as e-learning or blended learning, which combines e-learning elements with classroom or hands-on training, should be considered as they provide a number of advantages in terms of scalability, flexibility and consistency.

The increase in cybercrime requires a coordinated and commensurate response that is based on a sustainable and forward-looking approach, an important element of which is investment in capacity building, supported by a long-term financial strategy at EU level.

Within the proposed TCF, and leveraging existing platforms such as ECTEG, EJTN and CEPOL, the development of a centralised repository of available training resources and trainers should be considered to help facilitate access to relevant materials and information, and to allow for harmonisation, standardisation and reuse at EU level.

3.3.-Digital Proximity.

The term *proximity* is oriented towards a reciprocal and participatory relationship between the Police and the community, through permanent contact and continuous dialogue whose purpose is the proactive participation of citizens in their security, promoting the solution of priority problems for the community and promoting their participation in the identification and solution of those problems.

Information, police intelligence and new tools that facilitate the approach to citizenship are considered necessary, currently highlighting the potentialization of social networks and new information and communication technologies.

The concept of proximity pertains to a mutually beneficial and collaborative relationship between law enforcement and the community. This is achieved through consistent engagement and ongoing discourse, with the aim of fostering proactive involvement of citizens in matters of security. This approach seeks to prioritize addressing the most pressing issues for the community, and encourages their active participation in identifying and resolving such concerns.

To achieve this goal, there is a need for information sharing and the utilization of police intelligence, as well as the incorporation of novel tools that facilitate effective communication with the public. At present, the potential of social media and emerging information and communication technologies is especially noteworthy.

The experts during the New Technologies Commission in Djibouti shared the different ways in which the police forces approach their citizens in relation to the fields of action and missions assigned to each one of them.

In relation to cyber issues, both in the preventive and in the investigative facet, the different Forces communicate their actions or experiences or what is considered as elements or form of action that would form part of an ideal proximity model in relation to cyberthreats.

FRENCH NATIONAL GENDARMERIE

The French National Gendarmerie has recently established the Digital Brigade, a service set up within the framework of community policing and which aims to provide, in a dematerialized way, the advice and support necessary for populations outside of emergency situations.

Its personnel, judicial police officers holding national security clearance, may on their own initiative seize facts constituting criminal offenses of which they are aware and transmit them to the competent gendarmerie or police unit within the framework of the "one-stop shop".

The gendarmes of the Digital Brigade can be reached 24/7 via an application or a dedicated website and provide an immediate response to users, businesses and local elected officials.

The primary objective of the digital brigade is to foster interactions with the populace through digital means, by enhancing accessibility and streamlining certain administrative functions.

Since the year 2014, the Institution has been immersed in a comprehensive introspection of its proximity to the public. The ongoing digital transformation, as exemplified by the Néogend connected equipment project, is a crucial contributory factor to this endeavor.

The provision tailored to the anticipations of the populace is evidenced by the formation of "contact brigades," which likewise fosters a closer relationship with citizens. In the future, the formation of the "digital brigade" will also advance this revitalized proximity. Its aspiration is to further streamline processes for users by providing them with a novel platform for communication. The digital brigade's officers will thus augment and proliferate the reception capacities of our regional entities.

The integration of novel technologies with interpersonal interaction allows for individuals, barring emergent situations, to connect with the gendarmerie at their discretion through a variety of mediums, including but not limited to smartphones, tablets, computers, and digital access points. A plethora of communication channels are available for use, such as chat, video, telephone, SMS, emails, and social networks. Following an evaluation of the citizen's request, a gendarmerie operative may provide online assistance or arrange a meeting with a gendarme at a location of the citizen's choosing.

ITALIAN ARMA DEI CARABINIERI:

In terms of digital proximity, Carabinieri move in the direction of extending the traditional proximity approach to the digital world.

In this regard, we implemented in the first place the possibility of reporting certain types of crime online with the DENUNCIA VI@ WEB.

Other initiatives are taken in the areas of the Carabinieri Special Departments to counter the growing digital dimension of criminal phenomena. Investigations proved that both legal and illegal online market host illicit trafficking of pharmaceuticals, wastes, and cultural artifacts. In the years we have developed specific expertise in these fields and we are enforcing dedicated projects.

The Carabinieri Unit for Health Protection implemented the NPS-ONLINE project, to fight against the spread of new drugs online. In the last 2 years, 412 websites have been shut down and traced drug shipments for 3 mils. € arresting 50 suspects and identifying 42 new narcotic molecules, signaled to the International Health Authorities.

In addition, the 'PREDICTION' project is being implemented to integrate the monitoring of the virtual world with the development of software (App) to prohibit minors from accessing web content containing new psychoactive substances.

The Carabinieri Unit for the Protection of the Environment are exploiting image recognition in the fields of forest fire prevention and studying technical solutions to prevent the traffic of protected or endangered species by being able to detect their origin.

The Carabinieri Unit for the Protection of Cultural Heritage completed the Stolen Works of Art Detection System project for the online detection of stolen works of art, matching online images (social media deep and dark web) with the Database of Stolen Cultural Goods, managed for the Ministry of Culture.

All these projects are aimed at protecting both the communities and their territories exploiting digital innovations to enforce an effective proximity model with a powerful outreach also.

PORTUGUESE GUARDA NACIONAL REPUBLICANA:

Recently the pilot project E-Guard, was developed by the Portuguese Guarda Nacional Republicana to ensure the security and safety conditions of the elderly people.

The GNR´s Special Policing program, namely the Support 65 – Secure Elderly People Program, in which the E-Guard program was developed to provide an efficient response.

The GNR´s E-Guard program allows elderly people to be in direct and permanent contact with GNR´s District Command and Control Centre.

The pilot project is based on a easy, portable and handy mobile device with communication capacity via GSM, besides GPS signal and several other sensors, which in case of an event will send alerts to the GNR´s Command and Control

Centre, allowing an early identification of a potential victim as well as contributes to a more effective use of police resources and proactive measures.

The project has been developed in collaboration with civilian partners, allowing the cost of the project to be totally free for elderly people and for GNR.

SPANISH GUARDIA CIVIL:

Two main initiatives were included regarding the Guardia Civil, the @ TEAMS, and on the other hand the ALERTCOPS app.

-@ TEAMS:

The Guardia Civil´s commitment to countering cybercrimes is reflected in its dedicated teams focused on cybersecurity. These teams have specific objectives ranging from preventing cyberattacks, investigating and prosecuting cybercriminals, to providing support and assistance to victims. The Guardia Civil's Cybersecurity Unit, Cybercrime Central Unit, and Technological Investigation Group are among the key units driving the agency's efforts in tackling cyber threats.

Looking to the last report about cibercrime, there are several key findings:

- Increased cybercrime incidents: The report reveals a significant increase in cybercrime incidents compared to previous years. This can be attributed to the growing reliance on digital technologies and the expansion of online activities due to the COVID-19 pandemic.
- Types of cybercrimes: The report identifies various types of cybercrimes, including phishing attacks, ransomware, identity theft, online fraud, and child exploitation.
- Impact on society and the economy: Cybercrimes have wide-ranging consequences, impacting both individuals and organizations. Furthermore, the report emphasizes the importance of protecting critical infrastructure and national security from cyber threats.
- International cooperation: The report highlights the necessity of international collaboration in combating cybercrimes. Given the borderless nature

of cyber threats, effective cooperation between countries is crucial for sharing intelligence, coordinating investigations, and bringing cybercriminals to justice.

- Efforts to combat cybercrimes: The report discusses the measures taken by law enforcement agencies, including the Guardia Civil, to tackle cybercrimes.
- Prevention and awareness campaigns: The report underscores the significance of prevention and raising awareness among individuals and organizations.
- Legal frameworks and legislative developments: The report discusses the importance of robust legal frameworks to address cybercrimes effectively.

Dealing with the digital evidence requires more and more personal and tools. Crime is always evolving and Guardia Civil needs to improve at least, at the same pace than cybercrime actors. The importance of digital evidence in cybercrime cannot be overstated. In the digital age, criminals leave behind a trail of electronic footprints that can be crucial for identifying, investigating, and prosecuting cyber offenders. Digital evidence provides a comprehensive and objective record of cybercriminal activities, including the methods employed, the identities involved, and the impact on victims.

The Strategic Plan of the Guardia Civil 2021-2024, dedicates an exclusive Strategic Line to the Cybersecurity, including objectives related to the provision of personnel specialized in new technologies used by cybercriminals.

One way of relieving the more technical levels of work is to create a series of first response and citizen service teams to act as a first filter so that the highly specialized personnel is not saturated, and on the other hand, so that the citizen receives careful and careful attention when filing a complaint in this area. Under the name of Cybercrime Advisory, Prevention and Response Teams (Equipos@), the police stations will set up functional teams responsible for reinforcing the

response to cybercrime, in particular to cybercrime, particularly in the face of online scams, which are one of the main problems in this area.

These teams will provide a first specific basic response, supporting or transferring responsibility to the Judicial Police units, when the entity or complexity of the crimes to be investigated so requires.

At least one team will be established in each police station, which will be integrated and will depend technically and functionally on the Judicial Police Organic Unit, and which will be located where the Chief of the Command will determine.

At the central level, integrated in the organic structure of the Judicial Police Headquarters, a @ National Team has been established, responsible for guiding, promoting and homogenizing the work procedures of the territorial teams.

These 84 territorial @ Teams located in the police stations work in technical coordination with the @ National Team, which in turn is part of the structure of the Judicial Police Headquarters. They will be in charge of:

1. Reinforce the response of the Corps in cybercrime, in particular, before the scams on the network, which constitute one of the main problems in this area.

2. Receive those cybercrime complaints that, due to their degree of complexity, require specific intervention, in addition to preparing the reports established and supervising the quality of the recording of the complaints received.

3. Ensure attention to the victims and injured parties of cybercrime.

4. To offer advice and provide specific attention to citizens and companies on everything related to cybercrime, specifically with online scams.

5. Advise and guide the members of the Corps of the territorial units that receive complaints of cybercrime, especially scams on the network.

6. Generate a deployment of units, the Teams @ that favors the early knowledge of cybercrimes committed in the territory, which multiplies the capacities of investigation and attention to victims.

7. To carry out basic investigations related to cybercrime in accordance with the Judicial Police Action Plan of each police station, and to refer the most complex investigations to specialized teams.

-ALERTCOPS:

AlertCops is a free mobile application, created by the Secretary of State for Security of the Ministry of the Interior of Spain, whose main purpose is to improve and facilitate access to certain public citizen security services, so that any person, regardless of their language, origin or their hearing or vocal disabilities can communicate to the State Security Forces and Corps (Guardia Civil and Police) an alert, information, data or news about a criminal act or security incident of which you are being a victim or witness.

Its Mission:

1. Facilitate a new communication channel between citizens and the LEAs.
2. Streamline the information request and response protocol, obtaining information from the person seeking help from the beginning, such as: positioning, type of incident that is being suffered, people involved, or other relevant data.
3. Improve citizen response times and the information process and open a new channel for citizen collaboration.
4. Offer foreigners who visit or reside in Spain a channel in their language to access the security services of the LEAs.
5. Guarantee accessibility to these services for people with communication disabilities.
6. Serve as a platform for future internal and / or external management and communication uses.

AlertCops Services for citizens:

- Chat: If you are a victim or witness of a risk situation, you may contact through the chat or send us photos and videos. You will get immediate attention from the Law Enforcement Agencies.
- Guardian: Whenever you want, you may share your location with whoever you want. In case of emergency, the rescue will be faster and more accurate.
- Button SOS: Allows you to send an immediate notice to your guardians with your location and a 10-second audio. Offers reinforced protection for vulnerable groups: instantly alerts the nearest police forces for urgent attention.
- Service Centre: 99 active centres attended by the Guardia Civil and National Police.
- Forces: 4.122 Registered Forces
- Sending alerts to LEAs: You can talk by chat or by phone with the nearest service centre to report a crime of which you are being a victim or witness.

Moreover, deaf people can request emergency services (medical assistance, police, firefighters, etc.) through a specific alert.

- Private guardian: It allows you to share your position with people you trust for greater security. Any family member or close friend in the mobile phone's "Contact Book" can be your GUARDIAN. Configuring this function, you become PROTECTED: your GUARDIAN will be able to see your latest locations on the MAP of the app.
- SOS Guardians button: You can ask for help just by pressing an icon on the main screen of the mobile, with hardly any interaction. Forward the alert to your Guardians. 10 seconds of audio will be recorded and sent as an attachment to the alert.
- Guardian - Security Forces: It allows you to share your position with the Law Enforcement Agencies. You may share your location with whoever you want. In case of emergency, the rescue will be faster and more accurate.
- SOS button for vulnerable groups: It offers reinforced protection for vulnerable groups: victims of gender violence and health personnel. You can ask

for help just by pressing an icon on the main screen of the mobile. Instantly notify the nearest police forces for urgent attention. 10 seconds of audio will be recorded and sent as an attachment to the alert.

- Located warnings and geolocated security warnings.
- Receive notifications from the Law Enforcement Agencies informing of an emergency that is occurring in the area where you are. You can also receive advice and alerts from the special security devices deployed when you attend a mass event.

3.4.-Governance.

3.4.1. SPANISH GUARDIA CIVIL:

The Spanish National Security Law contemplates CYBERSECURITY as a field of special interest.

The National Security Strategy, details the objectives of each of its areas, among which is CYBERSECURITY, highlighting the mentions made of the capacities necessary to guarantee it: prevention, detection and response against cyber-attacks and prevention, detection, reaction, analysis, recovery, response and investigation against cyber threats.

The National CYBERSECURITY Strategy understands that "the new cybersecurity extends beyond the field of merely protecting technological heritage", and considers that there must be an evolution from a "preventive and defensive CYBERSECURITY model" to one that contemplates cyberspace as a domain of confrontation, with a more proactive approach to cyber-intelligence, to achieve the necessary knowledge of the situation and the consequent early warning that allows anticipating the actions of potential adversaries, as well as promoting the use of mechanisms and means that allow a timely investigation and prosecution of the perpetrators.

In this way, and in relation to cyber-threats, it characterizes CYBERSECURITY as transversal, and a comprehensive perspective is needed to deal with it, which includes both Public Administrations and the public and private sectors and society at large.

Specifically, Cybercrime is defined as the set of illegal activities committed in cyberspace that have as their object the elements, computer systems or any other legal assets, provided that the use of technological tools is decisive in their planning, development and execution; Depending on the nature of the punishable act itself, its authorship, its motivation, or the damage inflicted, we can thus speak of cyber-terrorism, cybercrime, or, where appropriate, hacktivism.

One of the objectives of the Spanish National CYBERSECURITY Strategy is a safe and reliable use of cyberspace against its illicit or malicious use, for which it is considered essential to allocate sufficient resources to the competent bodies in the matter and the training of professionals who work in this field. Strengthening capacities for investigation and prosecution of cybercrime, to guarantee citizen security and the protection of rights and freedoms in cyberspace, are included among the measures to be adopted.

The National Strategy against Organized Crime and Serious Crime 2019-2023, warns about "the new modalities of money laundering, with special incidence of the use of cryptocurrencies, and the appearance of criminal markets managed through the Internet, mainly through the deep web. Another factor to keep in mind is "the globalization of communications, its fraudulent use, anonymity and the lack of regulation, together with the difficulties of research in the field of new technologies, are giving important opportunities to crime, since be organized or serious".

The 2019 Spanish National Strategy against Terrorism states that "*another trend noted in recent years has been the extensive use by terrorists of the Internet and social networks, through the construction of false narratives far removed from social reality, with which they have tried to recruit new terrorists to undermine our democratic society*". Among other measures, it identifies the need to "*strengthen*

and improve critical infrastructure protection plans against terrorist attacks through cyberattacks, optimizing public and private coordination through the competent bodies."

The Guardia Civil Institutional Strategy 2030 includes, among its strategic objectives, one dedicated to orienting the service potential and the organizational structure to the new security challenges, challenges among which is cybersecurity and the fight against cybercrime.

This strategic document has its development in the most operational sphere through the Strategic Plan of the Guardia Civil 2021-2024, dedicating an exclusive Strategic Line to Cybersecurity, including objectives related to:

- The culture of cybersecurity.
- Strengthening capacities in the fight against cybercrime in its different forms.
- The provision of trained and specialized personnel.

3.4.2. ITALIAN ARMA DEI CARABINIERI:

There are many relevant actors in the cyber domain that require coordination.

The Law Decree of 21 September 2019, no. 105, established the Italian National Cybersecurity Perimeter (NCSP), for the protection of the Italian ICT critical infrastructures, by imposing specific obligations on essential operators to safeguard networks, information systems, and IT services that are pivotal to the life and functioning of the nation, and strengthening the incident notification mechanism.

The Law Decree 82/2021 redesigned the national cybersecurity architecture establishing the National Cybersecurity Agency (ACN) to protect the national cyberspace by coordinating all public stakeholders (recruitment, training, competence and skills evaluation, research and development, resilience) and promoting public-private partnerships in Italy and abroad.

The decree law 13 September 2022, no. 115 (aiuti bis), art. 37 strengthened the detection and response mechanism. The Prime Minister, in emergencies, may authorize the intelligence agencies, to intervene and actively respond to identified cyber threats (in case mere protection may not suffice), exploiting when necessary the capacities of the Armed Forces. The operators acting in these operations are granted the same legal immunity as intelligence agents.

Carabinieri are involved by pursuing the Military Police function to ensure Force Protection and investigating as law enforcement authority with civil and military Prosecutors.

3.4.3. FRENCH NATIONAL GENDARMERIE (GNF):

The GNF has got a quite advanced multilevel training model, supported by a national cyber training centre (CNF-CYBER), which also provides courses for other French administrations as well as international courses (see below).

The GNF has set up a dedicated training course (FINTECH), with national sessions and some international ones (in EN), organised by the CNF-CYBER.

The GNF is looking forward to lead soon a joint national service at ministerial level (Interior), on the model of its Command for the cyberspace.

The French National Gendarmerie (GNF) cyber strategy constitutes a synthetic roadmap allowing the GNF to integrate its actions in the interministerial cyber ecosystem and to develop its poles of excellence, thus providing the Ministry of the Interior with the necessary assets to take into account the cyber vector, whose territory and capabilities are increasingly used by delinquents as well as organized criminal groups.

In this respect, the present action plan meets the 5 objectives set by the GNF cyber strategy:

- prevention at the heart of the action. In order to infuse a cyberculture within all GNF units and to develop a prevention and contact policy that is visible and accessible to all;

- watch to protect. In order to improve its knowledge of the threat, the GNF is strengthening its research, analysis and cross-checking capabilities for technical data and intelligence of cyber interest, relying on strong partnerships with institutional and private actors of the cyber ecosystem and InterCERT-FR network;

- supporting victims in the fight against cybercrime. In order to face the criminal organizations developing their own capacities, the GNF is intensifying its offensive action and consolidates its investigative capacities;

- cooperating to succeed, the operational requirement of international cooperation. In order to develop and animate the links, which are essential to take into account the transverse and borderless nature of cyberspace, with private and institutional, European and international partners, and to develop the capabilities of the GNF within the privileged networks contributing to the elaboration of the cyber investigation doctrine;

- participate in the resilience of the nation, the ultimate mission. In order to be able to deal with the cyber dimension of traditional crises, or crises that are cyber in nature, the GNF has strengthened its operational crisis management model, relying on its national operations centre and a digital task force, and has developed a digital crisis management doctrine.

3.4.4. THE ROYAL NETHERLANDS MARECHAUSSEE:

The Dutch Cybersecurity strategy currently focusses on 4 main points:

1. Better visibility of the threat. The government invests in people and systems that provide a clearer picture of the origin of threats and who they are aimed at.

2. More cybersecurity specialists. We are taking various actions to get more ICT specialists on the labor market.

3. Government and sector responsibility. The necessary requirements for safety and supervision will be set for the entire government itself. In addition, within the

legal frameworks, the government will use the possibilities even more than now to detect, tackle, disrupt and prosecute malicious actors and their facilitators (digitally).

4. Better supervision and the associated laws and regulations. Rearrangement of responsibilities requires expansion of legal rules and supervision. Safety must become the foundation on which new systems are designed. New rules will be introduced that governments, vital suppliers and reliable digital products and services must comply with.

Nederlandse Cybersecuritystrategie 2022-2028

3.4.5. GENDARMERIE CORPS OF SAN MARINO

Intelligence, analysis and investigative activity on possible existing cyber threats lie within the competence of the Operative and Judicial Police Department (OJPD), working in close collaboration with the National Central Bureau-INTERPOL San Marino.

Protection of critical infrastructure, including critical information infrastructure, is regulated by the legal framework on counterterrorism. The Commander of the Gendarmeria is either a member or the president of the bodies in the counterterrorism network, i.e. the Permanent Counterterrorism Committee, the Counterterrorism Task Group and the Crisis Unit on Counterterrorism. Established by Law 31st January 2019 no. 21. the three bodies are entrusted with different functions, from the drafting of the National Strategic Plan on Terrorism to incident classification and response, including cyber threats and cyberattacks.

4.-Conclusions.

The forthcoming decades are expected to be distinguished by a surge in the process of digitization, heightened interconnectedness, and an exponential upsurge in data volumes. The confluence of diverse spheres is anticipated to increasingly obscure the demarcation lines between the tangible, intangible, and

biological domains, thereby giving rise to novel hazards, complexities, and prospects for law enforcement.

Collectively, the worldwide tendencies that have been recognized are altering the fundamental basis upon which law enforcement operates, thereby engendering novel circumstances in policing's sphere of operation. These circumstances represent interdependent collections of trials and prospects that Gendarmic Forces will be required to acclimate to.

Cyberthreats

In the coming decades, it is highly probable that the Gendarmic Forces will encounter a growing need to respond to an array of diverse and complex locations and scenarios, ultimately placing a strain on their pre-existing capacities. Nonetheless, it is imperative to acknowledge that none of these expansions can be assumed, as they may be met with potential opposition from non-state actors or the general public.

As the capabilities of policing continue to advance, the recruitment, training, and retention of police officers for future endeavors will pose a substantial strategic challenge to law enforcement. This may necessitate the implementation of inventive approaches to the workforce, such as modifications to job design, recruitment methods, and training and development programs.

Given the significant input from experts in the field, it is deemed worthwhile to establish a unified and current taxonomy and grouping of cyber hazards. This will facilitate seamless communication among various entities in the exchange of critical information and implementation of best practices, within the ambit of worldwide law enforcement collaboration.

Continual refinement of the cyberthreat repository will enhance the decision-making processes of individual organizations in operational, training, and technical spheres.

Training

To fully capitalize on the potential of digitalization, it is imperative to cultivate novel digital inquiry and information administration competencies, implement widespread digital conversion, develop new proficiencies and expertise, and augment these efforts with innovative AI-driven instruments.

In order to effectively monitor, comprehend, and utilize the multitude of innovative advancements affecting communities, it is imperative to secure sufficient funding, attract individuals possessing the appropriate skillset, and impart rudimentary technological training to all personnel. Additional noteworthy factors encompass transitioning from a reactive approach to proactive methodologies, facilitating a more cohesive integration of foresight and innovation teams, and augmenting procurement and other corporate competencies.

In contemporary times, a majority of criminal activities leave behind a digital footprint. As a result of this development, investigators must acquire specialized skills and tools to conduct thorough investigations in the online realm, including the application of social media. In this regard, AI-based solutions can prove to be a valuable resource for rapidly gaining insights from voluminous data.

The retrieval of digital evidence from an increasing array of devices, including but not limited to laptops, smartphones, automobiles, home appliances, and the Cloud, may necessitate the involvement of law enforcement forensics. Emerging developments in cryptography and deep fake technology, coupled with public apprehensions regarding surveillance and corresponding shifts in legislation, could engender mounting obstacles.

Both facets are indispensable to any law enforcement body. However, in situations where resources are scarce, organizations may be compelled to opt for either a generalist or specialist approach to recruitment. Moreover, the areas of specialization are highly prone to significant alterations.

Generalist models that incorporate a substantial proportion of officers possessing a fundamental set of policing skills can augment resilience, whereas specialist models can amplify efficacy. Despite the fact that uniformed officers will persist as the foundation of policing, in light of the escalating intricacy of (digitally mediated) crime, an expanding array of in-house and external specialists are anticipated to join their ranks. Law enforcement organizations may consider mandating a requisite minimum of technological training for all officers.

Considering the rapid rate of advancements, there will inevitably arise an augmented necessity for perpetual education.

The possession of a Digital Police Competences Framework of Reference, which consists of a pre-established assortment of profiles, categorized according to the aforementioned competences, permits the customization of the decision-making process to suit the required analysis of needs in the creation of training activities that meet the demands of the organization.

Moreover, it facilitates, when applicable, the procedure of student exchange among various police forces, due to the availability of information pertaining not only to the name of the training activity, but also to the individuals to whom it is directed, distinguished by their function and level of competencies to be acquired.

Digital Proximity

Maintaining the confidence and reliance of the public both in the virtual and physical realms will be of utmost importance for the forthcoming policing endeavours, which will have significant consequences for the inquiries, enlistment, acquisition, and financial plan. In the age of digitalization, the methods of civic involvement might have to adapt to keep pace with the online communities, whereas the offline methods of varied recruitment policies and ongoing education

could play a vital role in meeting the rapidly changing societal norms and anticipations.

In contemporary society, it is becoming progressively crucial for law enforcement to broaden their virtual channels of communication with the community and enhance their mechanisms for online crime reporting.

Establishing a robust rapport with communities, for instance, by deploying specialized community teams, has always been a critical determinant of effective policing. Presently, technological advancements are offering novel avenues for constructive engagements. Diversified communication channels, such as crime reporting applications, can augment civic involvement and satisfaction, concurrently affording instantaneous cognizance to law enforcement agencies and facilitating their prompt responsiveness to the demands of their constituents.

In the pursuit of the objectives of Police Proximity, the technological aspects present themselves as conducive to the creation of a lasting and uninterrupted association with the populace, subject to the unique circumstances of each member in terms of their digital proficiency, cybersecurity consciousness, and technological assets at their disposal.

The significance of the distinct components contained in the corresponding section of the digital proximity model (human/technological) will be contingent on the diverse attributes of the populace.

Given the continuous progression of technology and the emergence of dystopian factors such as the metaverse, the perpetual acquisition of means and knowledge is deemed imperative in anticipation of the potential evolution and projected escalation of security requisites in virtual domains.

Governance

In order to address the increasing levels of sophistication, intricacy and internationalization of criminal activities, it is probable that the domain of Gendarmic Forces will require novel policies, mechanisms and frameworks at the organizational level.

To effectively accomplish its mission and anticipate upcoming challenges, the field of policing may require a departure from conventional, hierarchical structures in favor of novel, robust, adaptable, and inventive models.

In particular, successful Governance models should:

- Grant law enforcement agencies the authority to effectively utilize innovative techniques, state-of-the-art technology and data to thwart criminal activities and enhance overall productivity.
- Facilitate the integration of police efforts within the broader public safety framework, which encompasses other governmental bodies, private enterprises and non-state actors, thereby generating valuable insights into the opportunities, challenges and threats related to cybersecurity.
- Enable policing organizations to allocate and position resources strategically to combat crime at the local, national and international levels in an increasingly interconnected world.

INTERNATIONAL AFFAIRS COMMISSION

Doha, 28th February 2023

Lieutenant Colonel Basilio Luis SANCHEZ PORTILLO

Lieutenant Román CLÉRICO MURIEL

BACKGROUND

One of the elements that distinguish democracies from dictatorships is the place occupied by truth and lies: democracies are articulated around truth, dictatorships around lies. In order to exist, democracies require a public space based on trust and the belief in the possibility of establishing the truth of the facts. On the contrary, dictatorships may not be able to survive exposure to facts, so they need to destroy the truth and replace the public space with propaganda, as may happen in case of a conflict.

Regional conflicts are those a priori delimited to a characteristically named area, either by geographical or strategic position. At present, there are different conflicts that occupy different territorial areas, many of them with a long time span, others of great media relevance.

All of them are defined around a specific geographical or strategic area, making up the pieces of a global puzzle that goes beyond the merely conflictual to affect many other areas, resulting in a clear destabilizing component when, in the field of international relations, its impact is increased by the action of disinformation.

Regional conflicts change the paradigm of international relations: the world of watertight blocs based on military power has become blurred since the fall of the Berlin Wall, giving way to a struggle for the correlation of forces not only based on military power, which continues to be an element of enormous interest, but also on economic, ideological, cultural and narrative power.

They are no longer fought only with weapons, but also in the field of narratives. It is not only about winning, but also about being believed that you are winning. Here disinformation plays a fundamental role on the part of those powers that can spread false narratives that lead to the confusion of public opinion, with its repercussions on the demands on decision-makers regarding the degrees of

involvement in a given conflict.

The new globalized era, branded as 4.0, has intensified proximity among world societies and a condensation process of their time, by providing public goods as faster internet connections, the increased democratization of transports and a growing open global market.

Narrowly linked, information has therefore become yet another weapon in foreign policy, with which to attack states incisively, with important consequences for public security and increasing tension in international relations between states, agencies and international organizations.

Disinformation is not an end in itself, but serves broader political objectives, which is why the gendarmeries and police forces with military status regard it as a major threat and, consequently, a major challenge.

Based on this approach, on the occasion of the FIEP 2023 Guardia Civil Presidency and within the framework of the International Affairs Committee, a meeting of experts was held in Doha (Qatar) on 1 and 2 March 2023 under the title of discussion: "*How to minimize the impact of a regional conflict on international relations. Approach to protection against disinformation*", aims to find possible solutions to help prevent, detect, minimize and combat propaganda and disinformation campaigns.

The present document is prepared with the aim of contributing to understand the impact that regional conflicts have on international police relations, and how gendarmic forces can make the necessary adjustments, at the national level or as an instrument of the State's Foreign Action, to minimize their impact from the point of view of disinformation.

Reason why, this document seeks to gather the common positions and respond to different questions raised within the International Affairs Committee, under the following general issues:

- NORMATIVE ASPECT
- SITUATIONAL ASPECT
- OPERATIONAL ASPECT

- FINAL ASSESMENT

NORMATIVE ASPECT.

• Existing regulations, in the framework of the fight against disinformation as a form of hybrid threat.

The Kingdom of Spain, as well as other FIEP Members as countries under European Union architecture, has a framework reference in the field of disinformation, developed with the aim of helping to counteract foreign interference in the community information space and progressively including new procedures and instruments.

"Particularly relevant are the initiatives taken in this area by the various authorities of the European Union which over the years has equipped itself with tools, bodies, strategies and plans to defend citizens and institutions from the proliferation of disinformation", the Italian expert stated.

The main resources of this European framework, including other supranational organisms, are the following:

- *Action Plan on Strategic Communication*, whose creation was urged by the European Council in 2015.

- East *Stratcom Task Force*. EEAS team dedicated to proactive communication of EU policies and activities, created as a first step in the fight against disinformation. Among his activities are the website EUvsDSINFO (considered as a flagship project), and the Report of FIMI[2] threats.

- *The fight against disinformation online: a European* approach, adopted by the Commission.

[2] Foreign Information, Manipulation and Interference Threats.

- *Action Plan for European Democracy*, presented by the Commission.

- *Code of Best Practices against Disinformation*, published by the Commission, created with the aim of assuming voluntary commitments against disinformation, central axis of the EU Strategy against Disinformation.

- *The Strategic Compass,* which equips the European Union with an ambitious action plan to strengthen the EU's security and defense policy by 2030, promoting, among other things, the development of a toolkit against information manipulation and interference by foreign actors.

- *Hybrid CoE*, an international and independent network-based center for practitioners and experts based in Helsinki, which focuses on responses to hybrid threats under the auspices of the European Union and NATO.

- *NATO Strategic Communications Centre of Excellence*, is a multi-nationally constituted and NATO-accredited international military organization, which is not part of the NATO Command Structure, nor subordinate to any other NATO entity.

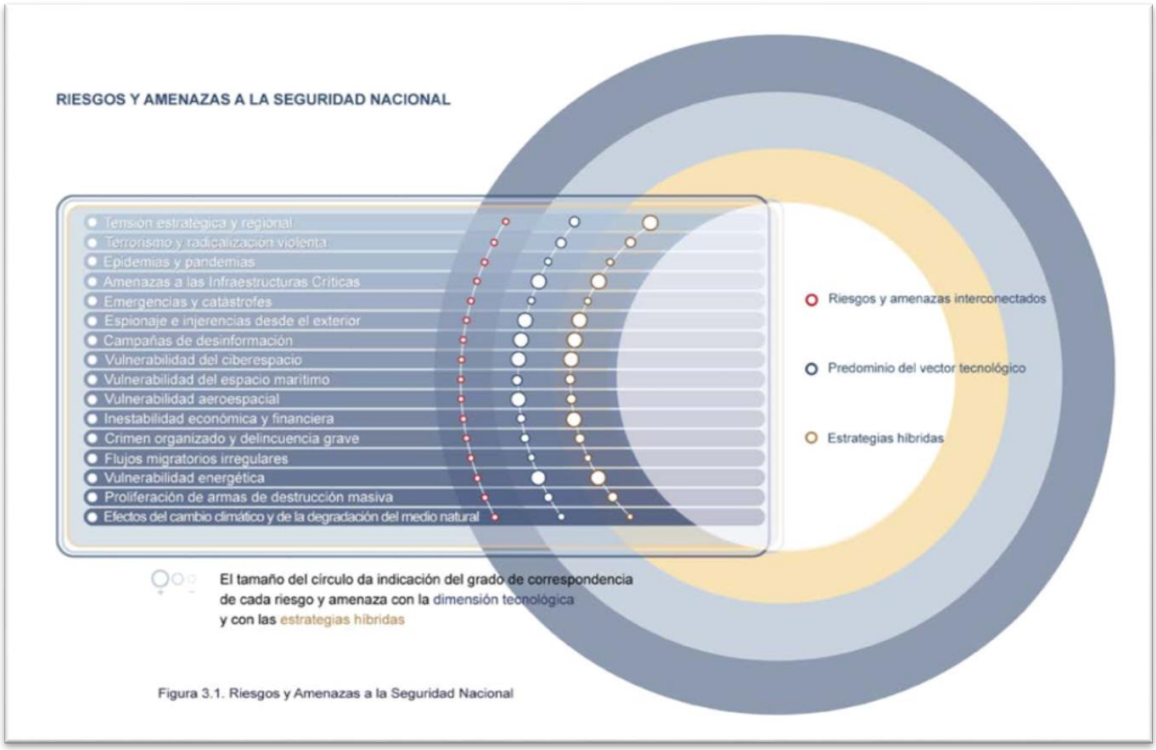
- The provisional political agreement on the *Digital Services Act*, between the Council and the European Parliament, which represent a world novelty in the field of digital regulation.

In particular, in the context of the Ukraine-Russia conflict, the European Parliament resolution of 7 April 2022 on EU sanctions against Russia has recently reiterated that Russian disinformation is part of Russia's war effort in Ukraine, and that EU sanctions against Russian state broadcasters can be easily circumvented

through virtual private networks, satellite television and smart TV functions; calls on the Commission and the Member States to fully implement the ban on Russian state-owned propaganda channels.

At the particular national level, as an example, in the recent years Spain has been developing the following regulatory and administrative structure in the fight against disinformation:

- *National Security Strategy*, where disinformation is mentioned as a threat.



Source: Spanish Security National Strategy 2021.

- *National Cybersecurity Strategy*, where cyberspace is mentioned as a strategic communication vector and potential disinformation channel.

- *Order PCM/1030/2020* publishing the *Procedure for Combating Disinformation* approved by the National Security Council, whose objectives, some achieved and others not, were:

- To identify and define the structure of bodies and authorities.
- To establish the different levels of prevention, detection, early warning, analysis, response and evaluation.
- Specific roles in the fight against disinformation.
- Define mechanisms for the exchange of information at the strategic, operational and technical levels.
- Define a methodology for the identification, analysis and management of disinformation events.

It is worth noting that, among many other Spanish initiatives, the following work in progress should be highlighted:

- Development proposal for the creation of a working group for the elaboration of the National Strategy for the Fight against Disinformation, promoted by the National Security Council.

- Paper for the Study of the Disinformation Phenomenon, with Disruptive Effects on Society, to define, in the first place, what we understand by disinformation, promoted in the Senate.

In Italy, a series of recommendations and suggestions have been elaborated, with the aim of raising awareness among the various actors interested in the adoption of good practices to recognize, resist and counter false news. An instrument of extraordinary importance is represented by the "*Anti-terrorism Strategic Analysis Committee*", set up by the Minister of the Interior in 2004, the body in charge of coordinating and exchanging information between the intelligence apparatuses and the police forces in the field of anti-terrorism.

In reference to Portugal, during the meeting the expert highlighted the GNR Strategic Guidelines and Objectives, focusing on enhancing proximity and visibility, modernizing, dematerializing, cooperating and boosting the GNR institutional dimension within the framework of internal security, as key points.

Unlike other member countries, the expert emphasized the core aspect that disinformation phenomena could be considered as a way of *"instigation of or inducement to commit a crime"* under the Portuguese Penal Code, closely link to the *"freedom of speech and information"* that the National Constitution declares.

Another important approach was made by the San Marino expert, in which the problem of fake news and disinformation was posed on the integrity of news media.

Following her words, in May 2013, the Ministry of Labour, Cooperation and News Media organised the first edition of a one-day conference titled *"Free press, free country"*, in which one of the central topics was the definition of the national guidelines to the upcoming new legal framework for press and media services in the Republic of San Marino.

In 2014 the same conference, then under the title *"Free press, free country: freedom, press and new media"*, came to its second edition. The focus on the latest trends in news industry, especially those related to new media, led to the testimony of Ukrainian journalist Viktoriia Polishchuk, who quit her job at a Crimean public broadcaster to protest the presence of Russian soldiers in front of the company's building the day before the disputed referendum for annexation. The journalist had been invited to San Marino by the government itself, and has since become a correspondent for the Sammarinese national broadcasting company (San Marino RTV) in Ukraine.

In the following two editions, held in 2015 and 2016, titled respectively *"Broken pencils? Free speech amid propaganda and truth"* and *"War and freedom, the role of the press"*, the topics converged more and more on the role of propaganda-led disinformation, and freedom of the press in post-conflict áreas.

These initiatives saw the publishing of *Law 5th December 2014 no. 211*, regulating the functioning of news industry in the Republic of San Marino. The

code of conduct for news media operators came three years later, with *Delegated Decree 31st July 2017 no. 90*. Within this framework, *art. 6 of Law 211/2014* introduced the Authority for Information, bestowed with surveillance powers on the correct application of the code of conduct, as well as that of enforcing sanctions in case of violation.

In the last few years, the attention given to the topic at hand has gradually moved from a sectoral perspective to a broader stance.

The San Marino expert continued with The *Joint Declaration on Freedom of Expression and 'Fake News', Disinformation and Propaganda*, and the *Action Plan against Disinformation*, signed in Brussels on 5th December 2018 by the European Commission and the High Representative of the European Union for Foreign Affairs and Security Policy have served as the two main reference points for the *High-level Conference on the Dangers of Disinformation*, which took place in the Republic of San Marino on 10th May 2019.

Out of the EU borders, as an example coming from Moroccan normative, the expert noted the legal and normative body in harmony with international and regional regulations, in which the main laws, were the following:

- The *Budapest Convention on Cybercrime* ratified by Morocco in 2018, whose 2nd protocol is signed in 2022;
- The *2011 Constitution* which guarantees fundamental rights such as the right to privacy, the right to freedom of thought and expression, the right of access to information and freedom of the press;
- The *Penal Code* which incriminates in its Article 447-2 the diffusion or distribution of false allegations or misleading facts;
- The *Press Code* which prohibits in its Article 72, under penalty of fine, the publication or dissemination of false news, allegations, inaccurate facts, and this, regardless of the means used;
- *Bill 22.20 on the use of social media*, which defines false information and related sanctions (Article 17), and provides for the creation of an authority to control digital platforms;

-the *Digital Development Agency* (ADD) and the *High Authority for Audiovisual Communication* (HACA), incorporating ethical provisions into the specifications of audiovisual, and introducing measures to prevent the dissemination of false information in the audiovisual media, respectively.

- The *Guide to Combating Disinformation*, published by the HACA in June 2022, deals mainly with techniques for deconstructing fake news; such as the news agency MAP, which has launched the "SOS Fake news" service, or the television channel SNRT, which has set up a "True or Fake" section that enables users to check the veracity of information by asking questions on the channel's website.
- The *Supreme Council of Audiovisual Communication* which, in the specifications of the audiovisual operators, integrates a section relating to the obligations of deontology of the programs and an article devoted to the prevention of disinformation.

The Senegalese expert also contributed to this normative aspect, stating that Article 10 of Senegalese Constitution guarantees freedom of expression in these terms: "*Everyone has the right to express and disseminate his opinions freely by speech, writing, image and peaceful march, provided that the exercise of these rights does not infringe the honour and esteem of others, or public order*". Also, their Penal Code specifies the penalty for an individual guilty of this type of offence. Finally, the new press code in Article 192, provides that "*In exceptional circumstances, the competent administrative authority [...] may, in order to prevent or stop an attack on state security or territorial integrity, or in the case of incitement to hatred or murder, order:*

- *seizure of the broadcasting media of a press company;*
- *suspension or cessation of the broadcasting of a program;*
- *temporary closure of the media organization.*"

At a regional level, Senegal participates in the African Union on the Declaration of Principles on Freedom of Expression in Africa that declares in its point II *"No individual shall be subjected to arbitrary interference with his or her freedom of expression. Any restriction on freedom of expression must be imposed by law, serve a legitimate purpose and be necessary in a democratic society."* It was declared that organizations such as Africa Check involved in fact-checking and media education, have been created.

• **Bodies or institutions responsible for deterrence, detection and response against disinformation phenomena.**

Beginning from Spain, the Procedure for Combating Disinformation approved in 2020 establishes a specific composition for the fight against disinformation:

- National Security Council
- Situation Committee[3],
- State Secretariat for Communication[4].
- Permanent Commission against disinformation[5], which includes:
  - Cabinet of Coordination and Studies of the State Secretariat for Security[6].
- Public authorities, including the National Intelligence Center.
- Private sector and organized civil society.

The procedure would be established in 4 levels of action, from a more technical or operational level to the political level. The role of the Guardia Civil as a gendarmic force, although not specifically defined but as part of the State Secretariat for Security, could contribute within the scope of its competences in the operational aspects within the first level, oriented to the detection of false news

[3] Crisis management.
[4] National contact point with EU for disinformation, as well as national communication coordination.
[5] Coordination among Ministries.
[6] Assess disinformation campaigns.

and disinformation campaigns in open sources, whose objective is destabilization or affect public security.

In general, the role of the Spanish State Forces and Corps in the fight against disinformation is relegated to a secondary role and, although necessary, its action would be limited to operational functions within the first level, coordinated by the Cabinet of Coordination and Studies of the State Secretariat for Security, specifically:

- Monitoring and surveillance for the purpose of identifying operations of influence, interference or interference through open sources, specifically in the form of sponsored disinformation campaigns, in order to analyze and disseminate them at the appropriate level so that the appropriate decisions can be taken.

- Investigation of the possible origin, purpose, monitoring of its activity, profile or media responsible for the publication or dissemination that could be classified as disinformation (an extremely complex issue when the intention is to attribute it to a State), and could affect destabilization.

- Maintain active and efficient the different channels in international relations with other services, so that the impact derived from disinformation campaigns is reduced to a minimum.

Specifically, Guardia Civil is in the process of contributing to the fight against disinformation through the following internal structure of the Corps:

- Operations Section of the Corps' General Staff.

- Cybersecurity Coordination Unit (UCCIBER) by considering cyberspace as a potential disinformation.

- Intelligence Service Command Office, responsible for transnational organized crime with destabilizing potential, as it is within its scope of responsibility, to fight against those criminal structures which, due to the seriousness of their activity and the nature of the human, technical and economic means involved, provide them with

a capacity for political, social and economic penetration of such magnitude, that could affect the normal functioning of society in general, and in the most serious cases, be a potential threat to the stability of the most solid structures of the State, in the field of public security.

Accordingly, the Royal Gendarmerie has developed an operational approach based on four phases, including:

- Monitoring the Internet and social networks, through constant surveillance for suspicious or misleading content;

- Early detection of disinformation operations, so that they can be quickly identified and dealt with;

- Rigorous fact-checking is a crucial step in distinguishing truth from false information, relying on cross-checking methods that can extend into the field;

- Reacting to proven disinformation operations, through media actions (publication of press releases) to deny or explain a situation, or through legal action when the act of disinformation is illegal.

The Royal Gendarmerie also contributes to national efforts to combat disinformation through:

- Regular exchange of intelligence with the various national security bodies to thwart disinformation campaigns;

- The conduct of investigations and judicial inquiries into cases of disinformation and manipulation of information;

- The participation of Royal Gendarmerie personnel in various training courses and workshops on combating disinformation;

- Sharing experiences and best practices in the fight against disinformation with national bodies.

So, following this lines, the Members agreed that a leading role in contrasting hybrid threats is naturally exercised by intelligence agencies, both in the search and analysis of information aimed at early warning, knowledge of the adversary's motivations and purposes; as well as the identification of vulnerabilities that it could exploit, as in covert operations aimed at neutralizing hybrid threats and in

counter-espionage and counter- interference in countering political warfare activities. Not just the work of the intelligence apparatuses, but also of the police services, is therefore crucial because through the gathering, analysis and evaluation of data it can anticipate the strategic and planned design behind the disinformation campaigns.

SITUATIONAL ASPECT

- **Regional conflicts affecting FIEP member countries, whose impact has been altered by disinformation phenomena, thus affecting the course of the conflict, especially in international police relations.**

Regional conflicts have an impact on the incidence and modes of action of public security, specifically crime, and especially serious transnational organized crime, given the international component that characterizes it, which requires the necessary international cooperation to confront it.

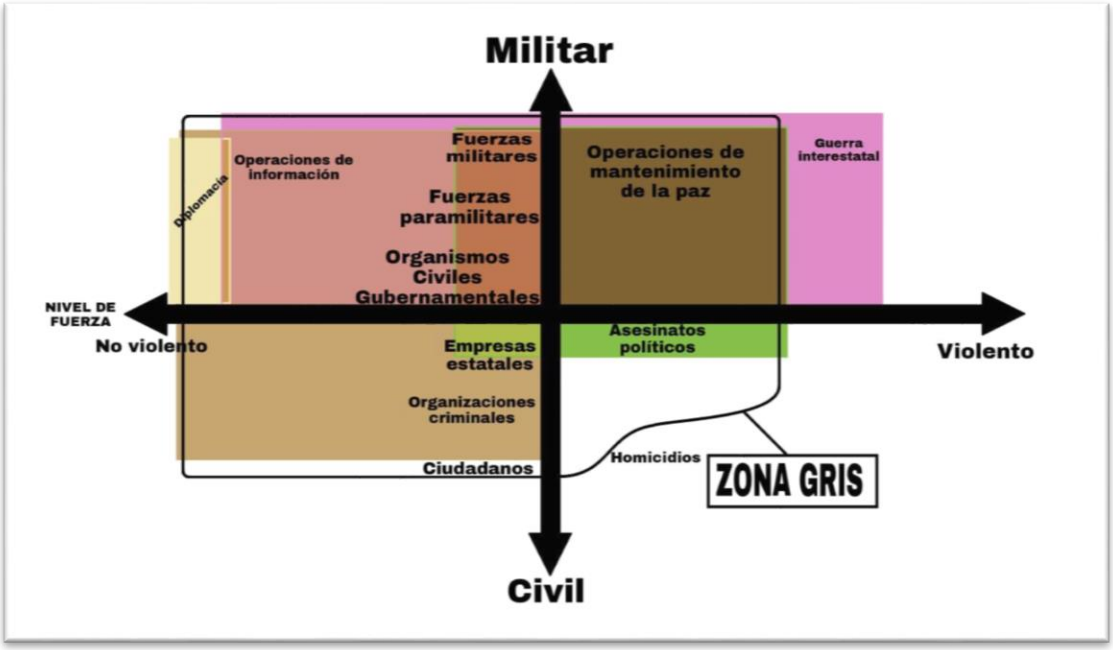
Hybrid strategies, together with technology, are configured as transversal elements to the rest of the threats to global and national security, highlighting among all these tools, disinformation, which directly affects areas such as economic, cybernetic, legal, demographic, but also and to a large extent diplomatic relations.

As part of regional conflicts, disinformation has been part of the actions used by its actors to try to justify their actions, thereby seeking to undermine the credibility and cohesion of countries. These actions, called disinformation campaigns, depending on the scheme designed (influence operations, interference operations or interference operations), have among their purposes the erosion of multilateral relations and associated geopolitical entities, trying to blame them for the actions that gave rise to the conflict, causing fissures between allied countries or countries with strong bilateral relations.

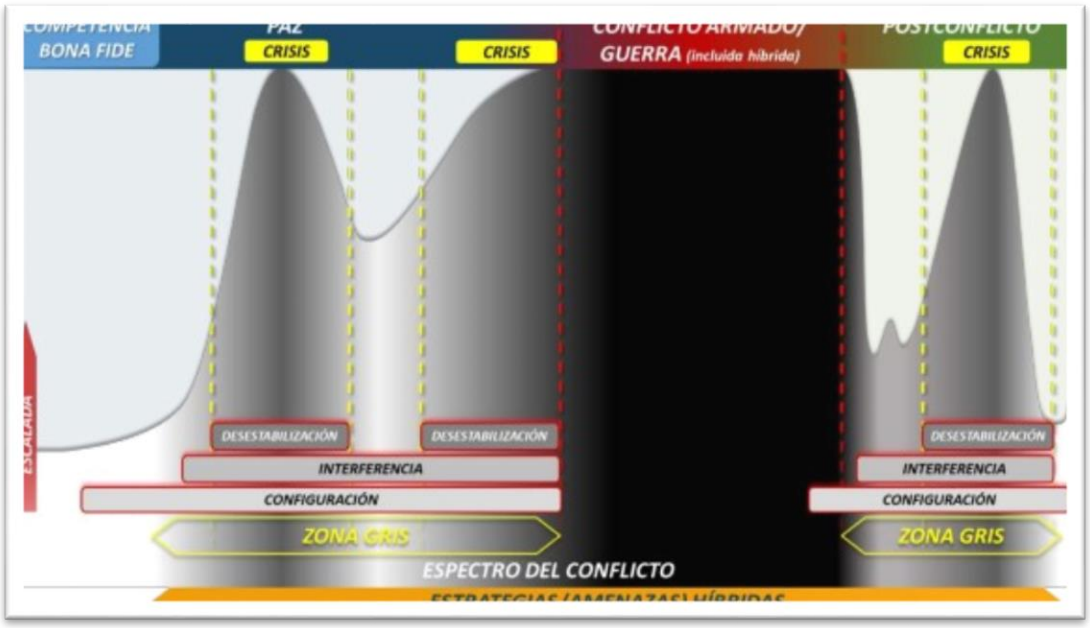
Although disinformation is usually found in what we call the gray zone, in the event of the outbreak of the conflict, current events show that it is also part of the strategy, as a way of paving the way to achieve geostrategic and geopolitical interests, at the expense of the deterioration and erosion of those called upon to collaborate and cooperate in order to face the conflict.

Three aspects of this actions should be highlighted in order to understand the role played by disinformation campaigns, both in the frame of gray zone but also as a specific action during a conflict:

- *Ambiguity*, by having a non-violent character.
- *Gradualism*, because of the interconnected actions that feed long-term operations.
- *Multidimensional or hybrid strategies*, exploiting the opponent's vulnerabilities.



Source: Open Source.



Source: Security National Strategy 2021.

The nature of the conflict and its opposing geopolitical entities, as well as the purpose of the disinformation campaign, will determine the use of one or the other active measures, configuring in a completely different way the core component of the disinformation campaign to be investigated.

- **Past, present and future of international police relations, from the disinformation approach.**

The 21st century is witnessing an unprecedented panorama of global destabilization and the battle space, in addition to the traditional dimensions of land, sea and air, has been extended to others such as the electromagnetic spectrum, space, cyberspace and disinformation.

Disinformation and propaganda, as a tool or weapon of hybrid threats, has been a part of society since ancient times, although today disinformation has been amplified by technology, becoming an efficient resource for undermining relations between countries. The ever-increasing technological dependence of today's society and a deficient education in the consumption of information

increase the risk of polarization and make it possible to exploit national tensions more efficiently, artificially generating a climate of opinion in favor of a certain power, or affecting the international recognition of others.

As the Moroccan colleague pointed out, indeed, with the help of an uninterrupted flow of untruths, disinformation is an affordable but effective tool to destabilize societies by sowing discord and amplifying internal tensions. In this context, internal security forces are prime targets for influence operations, because of the sensitivity surrounding their missions and because of their central role in the stability and social peace of a state.

When a conflict breaks out, international relations can be altered in two different ways: strengthened, with related geopolitical entities; or diminished, with respect to those they are trying to fight.

Specifically, in the negative aspect within the field of intelligence, certain services operate in the field of active measures, consisting in the secret channeling of false information, specially prepared materials and documents designed to deceive an adversary and incite him to take decisions and measures that fit in with the plans and intentions of the intelligence service, and undermine those of the other country, directly affecting relations between them.

It is therefore necessary to be aware of the impact that non-observance of these disinformation campaigns could have on relations with third countries, since in the medium term it would result in the following:

- Erosion of trust between police institutions, influencing both the individual conscience of its members and the collective conscience.

- Weakening of government systems, trying to influence decisions between them, whose political decisions will have a direct impact on international police relations.

- Undermining of social cohesion, their political communities and international organizations, with mass opinions emerging against foreign policing.

To face this scenario, international cooperation is an essential asset in the fight against destabilizing threats, which represent an extremely complex threat to combat, requiring the following actions for their effective neutralization:

- A wide network of international contacts to monitor transnational threats in their *iter criminis* outside the countries involved.

- Existence of agile information exchange channels.

- Confidence in relations with other services.

- Coordination of joint actions at the international level.

- Emphasising the importance of safeguarding reliable information on health issues.

From the Guardia Civil's point of view, disinformation would have an impact on both aspects, although it is necessary to analyze and study it in order to protect good relations with related countries, so that a disinformation operation or campaign does not alter the relations between them and, therefore, the cooperation between them remains in good health.

In the near future, the use of disinformation campaigns is expected to continue to grow, in fact, the trend is to continue improving the strategies of concealment and mimicry of disinformation content with truthful information, making it more and more difficult to detect, which is why it is increasingly necessary for detection and response mechanisms to continue to evolve and improve, especially in the field of artificial intelligence.

One aspect stated by the Moroccan expert was that in a virtual environment where the boundary between natural language and computer language is abolished, artificial intelligence (AI) plays a crucial role in the spread of disinformation. It is used extensively on the Internet and social networks to disseminate false information on a massive scale. Using sophisticated algorithms, AI is capable of creating misleading content and manipulating public opinion to

serve particular interests that could have a direct or indirect impact on public safety.

The Moroccan expert also pointed out that the Royal Gendarmerie is targeted by disinformation campaigns orchestrated by authors belonging to criminal networks who seek to discredit its actions and discourage its personnel. These campaigns sometimes come from foreign actors who aim not only to tarnish the image of the Royal Gendarmerie, but also to damage its relations with its foreign partners.

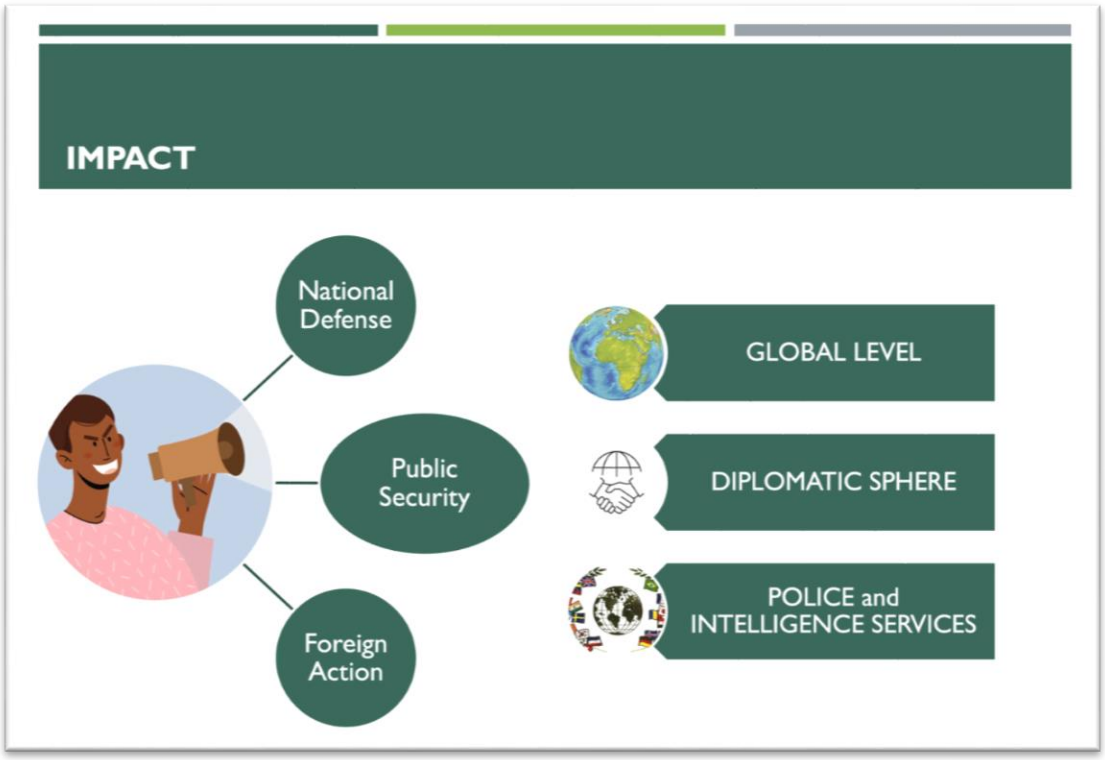
At this level, serve as an example the police cooperation existing between the Royal Gendarmerie and its different partners constitutes an effective asset in the defeat of influence operations through the permanent maintenance of communication channels and the sharing of visions and approaches in the treatment of criminal phenomena that are active in the areas of common interest.

• Impact of disinformation, especially in international relations with other countries.

In a world where derivatives are exponential, the impacts of the different regional conflicts cannot be ascribed only to their direct area of exposure, although in many situations it depends on the interests or strategic nature of the conflict in question.

It is clear that disinformation in the context of a conflict has an impact on national security, which must be protected, and affects the three main blocks that make it up: National Defense, Public Security and Foreign Action.

Breaking down Public Security into its respective spheres until reaching international police relations, it is necessary to highlight the impact on both bilateral and multilateral levels of these relations, being the police or judicial level the most palpable transcendence from the point of view of the fight against destabilizing threats, although also with quantifiable consequences from the qualitative and quantitative point of view at the institutional, training or budgetary level. Some of these areas are developed below:



Source: Intelligence Service Command Office of Guardia Civil.

At the *global level*, it becomes evident with the veto on participation in international forums and events such as summits, sports competitions or fairs of international interest, the issuance of joint declarations and even resolutions discussed in the United Nations Security Council or other regional forums such as the Council of the European Union or the Organization of Ibero-American States.

In the framework of relations with the EU, everything that is labeled as soft power (trade policy, competition, development cooperation, visas...) is being dynamized, tending to develop more gradually what affects hard power (defense, armaments, intelligence...), given its complexity.

In the *diplomatic sphere*, there may be expulsions of personnel from the embassies of unfriendly countries or the restriction of relations, as well as the reinforcement of protection for embassies that may be vulnerable on the basis of

the diplomatic positions adopted.

Police services are irremediably affected by existing conflicts, largely correlated to the country's involvement in them, although the transnationality characteristic of many of the current phenomena almost always results in, at least, knowledge of their consequences.

In words of the expert from the Moroccan Royal Gendarmerie, strengthening police cooperation, particularly with regard to the exchange of intelligence with national and foreign security bodies, appears to be of capital importance. This involves improving information-sharing channels, promoting fluid and rapid communication, and developing effective reaction mechanisms to face disinformation campaigns. Police forces can even develop shared, real-time reporting procedures for acts of disinformation that may target either force.

The case of the armed forces is even more evident, because sometimes they are forced to participate directly in the armed struggle, thus implying the reorganization of their structure and priorities, as well as assuming the consequences of the losses of their components that may occur.

The cooperative relations, so necessary for the achievement of the objectives of any police force nowadays, are diminished with those services belonging to countries over which there may be reluctance or even vetoes. This fact, whose most immediate effect reinforces the rejection of those territories where illegal, irregular or reprehensible action is considered, has a medium and long-term impact on the investigation and fight against the complex web of threats and criminality that affects the different countries, since the lack of information or the possibility of exchanges in this regard that may be necessary is obvious.

In day-to-day work, institutional and informative exchanges are reduced, there is more suspicion or direct communications are completely interrupted, either through face-to-face meetings or through the channels of contact established with these security forces, and trust is eroded, which will be difficult to re-establish after the end of the conflict.

Bilateral meetings are suspended and relations in the fight against terrorism and organized crime are frozen. Even if there is no official position on the matter, these relations are considered empty of content, given that in practice there is no effective exchange or proactive police relations.

Precisely the lack of contact with certain services or governments prevents a more exhaustive control of the creation of their narrative, which in times of conflict is confronted and must be obtained through indirect sources and specialists in the field. These monitored narratives "slip" into the countries through the multiplicity of existing forms of communication, mainly through social networks or media that move on alternative platforms.

The French colleague also highlighted a deterioration of relations between the press and police forces as "*a cyclical factor that makes grow role of image in society.*"

Other consequences with repercussions on police work:

- Increased social stress, exhausting coping resource.
- Influence on public opinion of police effectiveness.
- Obtaining economic gains, which could lead to criminal activities.
- Discredit or loss of confidence in national institutions.
- Social polarization
- In general, destabilization, *"altering a nation's foreign relations, economy and defense systems, questioning the alliances and discrediting their institutions and decisions"*, the Italian expert referred.

In a particular way, the Senegalese expert remarked that *infodemia* could have serious consequences for society, such as disinformation, polarization, division, and distrust of democratic institutions and reliable information sources.

• Societal perception and level of concern at the national or regional level.

The Procedure for Combating Disinformation approved by Spain establishes a specific composition for the fight against disinformation, in which it includes, among other components, organized civil society, contributing to the fight against disinformation by means of proposals that are echoed in the final political decision.

On the other hand, citizens, victims of the disinformation machinery itself, have a different view of the phenomenon. An ever-increasing consumption of information through new technologies, together with a lack of concern for the quality of the information consumed and a clear tendency not to contrast the information that is intentionally sent to them, means that the phenomenon itself and the actors behind its disinformation campaigns see in them an ideal target for consumption and dissemination that can hardly be stopped.

This is why FIEP members agreed in join forces to educate their societies about disinformation.

OPERATIONAL ASPECT

• Operations of interference, meddling or influence detected, and cases of "infodemia".

The biggest event produced so far is the escalation of the conflict between Ukraine and Russia, where disinformation has played a key role in escalating international relations. In the Italian expert's words: *"The Ukrainian conflict has brought to the forefront of the general public a long-known fact that had begun to be known with the invasion of Crimea in 2014: the wars of the 21st century are also fought in non-traditional fields, they are hybrid wars, ... planned and fueled by disinformation, the systematic production of false news and cyberattacks, besides sabotage and espionage."*

So, disinformation does not cause the conflict, but is part of it, contributing to:

- From the NEGATIVE point of view:

- Exploiting national or regional tensions.
- Weaken confidence in the Institutions.
- Justifying military actions.
- Promote social confrontation.
- Artificially creating climates of opinion with which to operate.
- Blurring the international order.
- Eroding international recognition.

▪ From the POSITIVE point of view:

- Raising the morale of the actors in the conflict.
- Appearing solid and serious in their international relations.
- Shaping the international order.
- Exacerbating counter-actions.
- Reinforcing police-cooperation relations in the frame of destabilizing crime and aggression, with those countries interested in defending Ukraine from aggression.

In the frame of the Ukraine-Russia conflict, the first has been the main target of Russia's FIMI operations, but also Spain in less extent. Not only Russia´s diplomatic channels regularly, but also others, serve as enablers of FIMI operations deployed across a wide range of topics. Diplomatic relations are usually influenced by the counteraction of the different intelligence services, which could be considered as hostile services due to different attacks and actions linked to them in the last times.

Source: www.miburo.substack.com

For all these reasons, and from the point of view of international relations, it should be taken into account that disinformation as a weapon or form of attack in the framework of a regional conflict can create, at the same time, chaos in Ukraine, destabilization in the Baltic countries, political influence in the Eastern countries, confusion in the Western countries, and distraction to third actors such as the USA, or China.

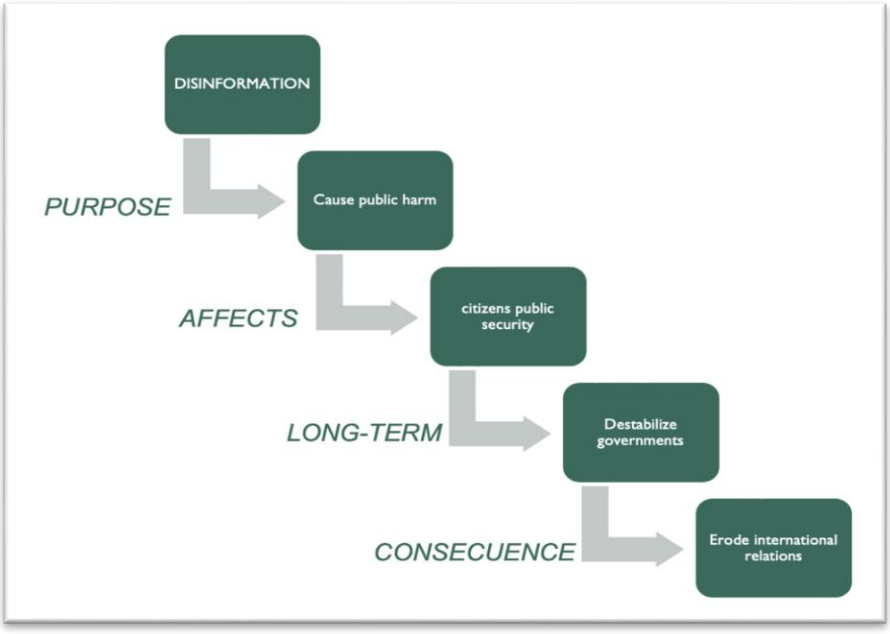
Other countries such as San Marino, linked the *infodemia* phenomena to COVID19 pandemic situation because, in this regard, the challenges posed by infodemic patterns of news dissemination during the pandemic served as immediate proof. It has been so impactful that it absorbed great attention from experts in communications studies. During the convention titled *"Digital Media and Disinformation: Politics, Journalism, Social Networks and Armed Conflicts"*, organised by the University of San Marino on 23rd May 2021, the pandemic, and the narrative thereof, was still one of the main points of discussion, because when analysing its uses for criminal and terroristic purposes (see: ISIS, Al-Sahab, Boko Haram, alt-right movements in the United States), however, the example offered

by disinformation campaigns exploiting the COVID-19 epidemic served as a connection with broader information warfare techniques (IW) and cognitive warfare (CW) at large.

- **Characteristics of disinformation phenomena observed: model of complexity, origin (sponsored or spontaneous campaign), actors, means, weapons or attacks, purpose (criminal and public security), overt or covert, dimension, scope, etc.**

In reference to Spain, the definition that the Guardia Civil position works from, has its origin in the one issued by the EU in its communication and subsequent Action Plan, where it is defined as follows:

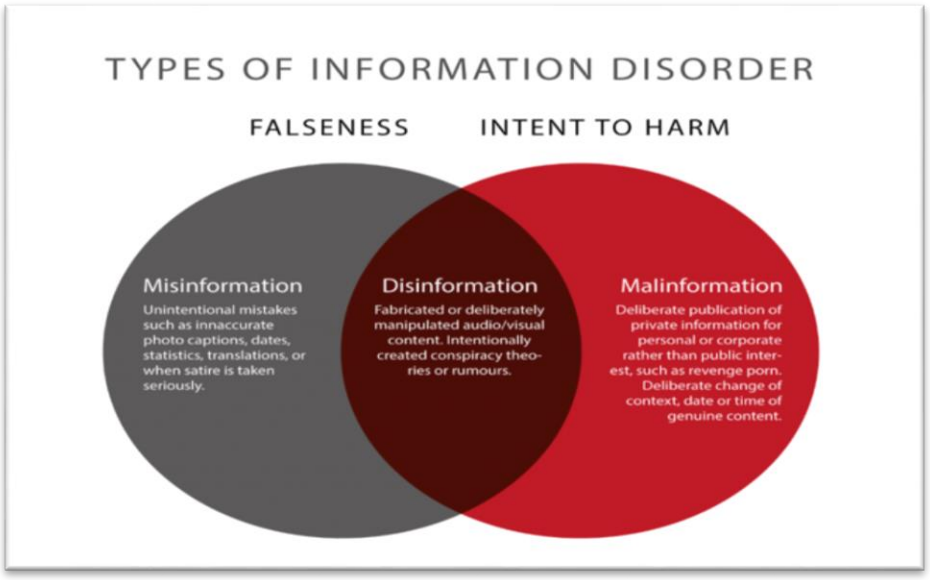
"Disinformation is defined as verifiably false or misleading information that is created presented or disseminated for profit or to deliberately mislead the public, and which may cause public harm."



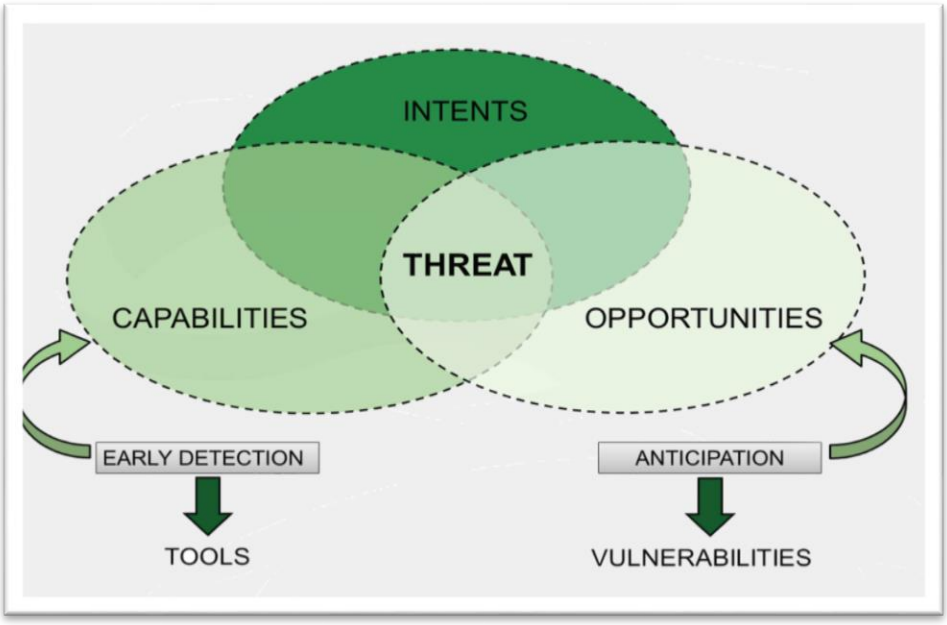
Source: Intelligence Service Command Office of Guardia Civil.

Italian colleagues, also remarked that *"public harm comprises threats to democratic political and policymaking processes as well as public goods such as the protection of citizens' health, the environment or security".*

A concept to be interpreted as an integral element of a broader entity, that of active measures (which over the years came to be called hybrid threat vectors), aimed at exerting a useful influence on aspects of the political life of a target country that are of interest, on its foreign policy and the resolution of international problems, deceiving the adversary, undermining and weakening its positions, disrupting its plans and for the achievement of other objectives. In the words of the Portuguese colleague, *"disinformation is a high-priority challenge by being considered a pathway to destabilization"*.



Source: Open Source.



Source: Intelligence Service Command Office of Guardia Civil.

From the point of view of the police function, an in-depth study of this definition leads us to evaluate the different components of disinformation that must be assessed when studying the phenomenon, detecting campaigns, analyzing their causes and investigating their origin:

Source: Intelligence Service Command Office of Guardia Civil.

- *Actors and proxies*: Differentiating between external, internal, state, non-state, or even artificial intelligence-based actors.
- *Target*: In two ways, for criminal (subversion, obstructing investigations, electoral offences, hatred, disclosure of secrets, moral integrity, public disorder, libel and slander, public health, fraud, against markets and consumers, lucrative, or other requiring medial deception) and non-criminal goals (polarization, destabilization, exploiting national tensions, influence electoral processes, undermining confidence in state institutions, exploiting vulnerabilities, control the press, promote confrontation or social unrest, political interference, interference or influence, artificially create climates of opinion, shaping international order, expansionism, international recognition, legal confusion, ideological subversion)

- *Weapon*: Chain of fake news, clandestine broadcasts of information, destruction of communications, organized crime, GPS signal spoofing, TV broadcast interference, DDoS attacks, suppression of information sources, exfiltration of information, elimination, poisoning, official public declaration, artificially create climate of opinion, centralization in a single channel or disinformation rhetoric artifices
- *Dissemination*: Social networks, social media or official documents.
- *Narratives*.
- *Intentionality* of the actors behind.
- *Evidence* of actions carried out: digital, electronical or physical.
- *Origin*: spontaneous or sponsored campaigns.
- *5 dimension purpose*: *Dismiss*: to push back against criticism, deny allegations and denigrate the source; *Distort*: to change the framing and twist and change the narrative; *Distract*: to turn attention to a different actor or narrative or to shift the blame; *Dismay*: to threaten and scare off opponents; *Divide*: to create conflict and widen divisions within or between communities and groups.
- *Scope*: Health, public administration, diplomacy, critical infrastructure, culture, policy, trade, economy, environment, public security, energy, policy and global commons.

Components that are studied in depth, assessing all their possible ramifications in order to reveal the reality behind the operation or campaign and, therefore, deepen the knowledge about the phenomenon of disinformation. Deepen in the components, the last FIMI from EEAS considers the incidents under five likely objectives of disinformation campaigns: Dismiss, Distort, Distract, Dismay or Divide.

In the specific case of Italy, the expert highlighted that the country, due to its history and geographical location, can therefore represent the picklock with which to force European Atlanticism, also weakening its Mediterranean projection in order to favor the growing Russian strategic presence in the North African quadrant, the Sahel and the Balkans.

France remembered the crucial role played by social networks, in which the society has felt *"a multiplication of information resources, where everyone can speak publicly with immediacy",* enhancing information dissemination capacity.

According to San Marino, the role of information warfare, of its products, outcomes and implications on democratic systems and international relations are usually at the forefront of many contributions from sociologists, international affairs and security studies experts. The analysis of disinformation phenomena in the context of hybrid warfare, comprises strategic and tactical use of types of aggression, under or up to the kinetic threshold, against and between state actors, sub-state actors, non-state actors, whether as 'proxy' or otherwise", reinforces the change of perspective that had emerged with the Russian annexation of Crimea (2014), later confirmed with the latest developments in the Russo-Ukrainian War (February 2022).

• Preventive and reactive measures aimed at minimizing the impact of the threat of disinformation in the field of international police relations.

The FIEP Members, aware of the phenomenon and its impact on public safety, are called upon to consider as a priority objective for the coming years, the adoption of different strategies, in order to combat disinformation and minimize the impact in police functions and competences.

In the above-mentioned meeting the Members agreed as key points, among others: to provide an updated proposal of what it is consider as disinformation phenomena and how they should address it for the benefit of public safety; make agreements in consolidated list of measures aimed at minimizing the impact of disinformation on international police relations; and increase participation of the gendarmic police forces in the national or supranational disinformation structures.

On the basis of this agreement, it was considered and discussed that in order to achieve these objectives, the following operational measures or actions should be promoted:

- Work towards a commitment to mutual cooperation, facilitate communication and dialogue, with the aim of reducing the risk of misinterpretation due to targeted disinformation campaigns.

- Contribute to the joint response system against disinformation, together with other countries, geopolitical entities and international organizations.

- Advance crisis management.

- Promote the security dimension of technological capabilities and strategic sectors.

- Develop its own capacity to contribute to the prevention, deterrence, detection and response to disinformation, creating new specific units or reinforcing existing ones.

- Increase its role as a police force and its potential in the fight against disinformation, both nationally and internationally, which will result in international recognition that will prevent international relations from being undermined. Permanent working groups should set up at an international level, was stated by the Italian expert.

- Evolve the methodology for dealing with destabilizing organized crime, adapting means and resources to the influence of disinformation.

- Design police training programs focused on disinformation, *"with experience and best practices sharing in the fight against misinformation and the awareness and training of personnel, especially on the fact-checking techniques and open-source data-mining (OSINT)"* (by Moroccan expert).

- Contribute to strengthening StratCom teams to counter foreign influence operations.

- Contribute to making public opinion aware of the phenomenon and the importance of international relations, so as to reduce the impact on it and on the climate of opinion. As Portuguese expert remarked: *"strategic communication is*

essential in this field with proximity policing programs", to which the French colleague added: *"informing in real time about police actions, and riposting immediately in the face of the emergence of disinformation"*.

- Contribute to the criminal treatment of disinformation actions and their consequences.

- Cooperate with the media and social networks in the design of strategies to detect, investigate and analyze these threats.

- Strengthen official communication channels in order to raise awareness among the population about disinformation campaigns that seek to polarize public opinion.

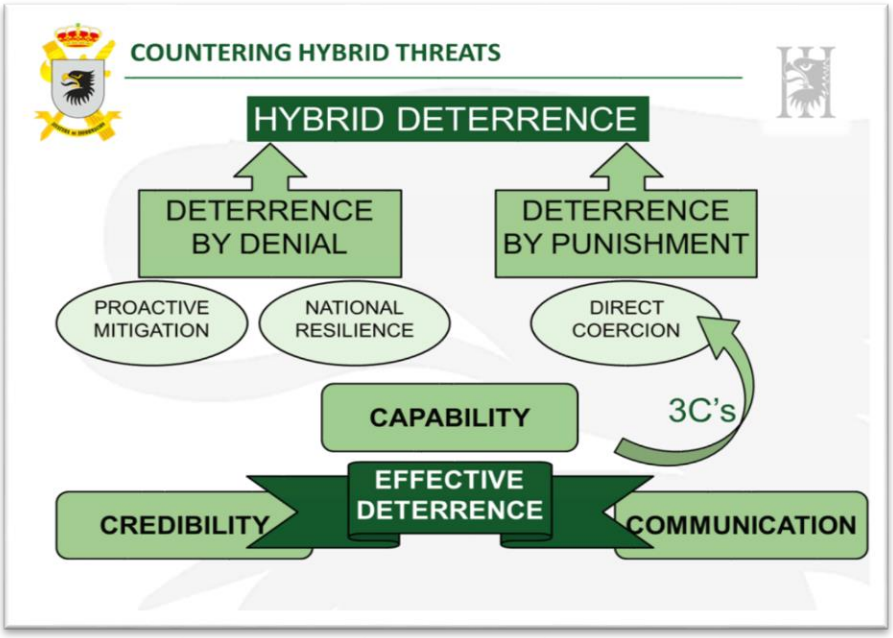
- Prevent citizens from being lured into recruitment actions based on disinformation campaigns.

- Prevent the dissemination of messages from hate and violence or clearly unfounded reports, especially those under anonymity screen.

- Promote a better accountability of social platforms, with the aim of correctly informing public opinion, by replicating what has already occurred both during the fight against international terrorism and during the pandemic phase for reasons related to the protection of public health.

- A specific collaboration between the gendarmic police forces and intelligence agencies in the fields of Artificial Intelligence (AI) for Big Data exploitation, the Internet of Things (IoT), Encryption, Blockchain and AI for image recognition.

- Strengthening of police cooperation, especially at the level of intelligence exchange.



Source: Intelligence Service Command Office of Guardia Civil.

As the French colleague from National Gerdarmerie set: *"Inform for transparency, report, prevent, alert and make counterattacks in a crisis, must be our goals in the fight against fake news and disinformation"*.

Another good approach came by Portuguese colleague, pointing that the following approach should bear in mind:

- A more transparent, trustworthy and accountable online ecosystem.
- Secure and resilient election processes.
- Fostering education and media literacy.
- Support for quality journalism as an essential element of a democratic society.
- Countering internal and external disinformation threats through strategic communication.

FINAL ASSESSMENT

In short, in a world where there were fewer conflicts, emerging problems related to crime and other threats could be addressed much more effectively. International cooperation is essential and, on many occasions, a cornerstone in the resolution of criminal actions as well as the prevention of others.

Regional conflicts do not contain any positive glimpses of working towards the specified goal, but instead lead to a loss of communication and confrontation. Moreover, even if regional conflicts are linked to a limited geographical or strategic area, they have repercussions at the international level and, depending on the importance that one wishes to attach to them, have different impacts, which have already been specified.

All this, moreover, is also influenced by the importance of the creation, control and dissemination of narratives. Under the dominance of conflict, narratives become increasingly polarized, and their defenders and detractors do so to the hilt without contemplating the capacity for listening, dialogue and even change. At the same time, it is increasingly difficult to direct a single narrative line, since there is access to a more diverse and extensive communicative world. And it is in this scenario that the different possibilities to be considered must move, without ignoring those that are around us.

In the field of international relations, as in others where disinformation has an impact, when authority or recognition is eroded, emotions fill the gap left and, therefore, dangerously, while distinguishing real facts from unreal ones becomes increasingly difficult, distinguishing between your friend and your enemy also becomes difficult, thinning the line between war and peace, between a good and a bad relationship.

Conflict has an impact, but fueled by disinformation, it has a greater impact and affects international relations to a greater extent. If we minimize the impact of disinformation, the chances of maintaining fruitful relations will increase.

In the face of regional conflicts, therefore, a broader approach is needed, taking into account global strategic dynamics, promoting meeting places and trying to get the story from the point of view of efficiency, evidence and reasoning.

Therefore, given the impact that the phenomenon of disinformation can have on gendarmerie forces affected by regional conflicts, it is essential to work in a joint and coordinated manner in order to prevent their international relations from being undermined, for the good of the institutional relations between them, which will result in the public safety of the society they serve.

SERVICE ORGANIZATION COMMISSION

Dakar, 11th July 2023

Lieutenant Colonel Basilio Luis SANCHEZ PORTILLO

Lieutenant Pablo CAL FRAGA

1. INTRODUCTION: MIGRATION AND FORCED DISPLACEMENTS

The management of migratory flows is **one of the great challenges we face in this century**. There are currently 82.4 million forcibly displaced people in the world and it is estimated that international migrants are up to 281 million.

Migrations are a natural human processes, which are due to adaptation to the environment. Generally, a distinction is made between forcibly displaced persons and economic migrants.

Forcibly displaced persons are those who are displaced because of conflicts (war, armed conflicts) or because of a change in the original situation that makes it impossible to continue living (famine, rising sea levels, earthquake).

Generally, when we speak of forcibly displaced persons, the main cause is armed conflict. In recent years, the great geopolitical consensuses that guaranteed the coexistence of opposing systems have been in an unstable equilibrium. After years in which the shadow of traditional warfare had been displaced by asymmetric warfare, the ghosts of clashes between great powers are now reappearing. The tension is being transferred to all levels, increasing the risk of regional conflicts, which in turn serve as a backyard for the interests of third parties.

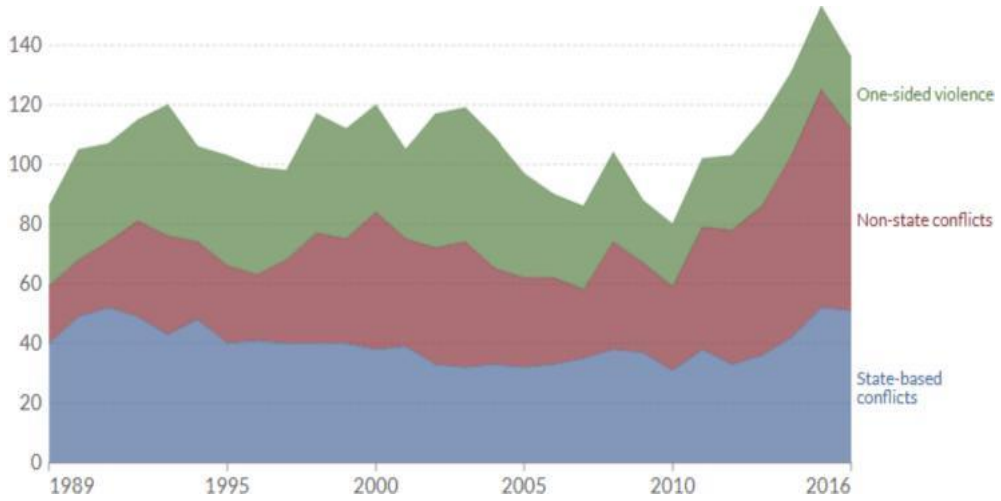


Illustration 1: Non-state and state-based conflicts, 1989 to 2016. State-based conflicts are between states, or a state and a non-state armed group. Non-state conflicts are between non-state armed groups. One-sided violence involves an armed group and civilians.

2. FORCED DISPLACEMENTS AND IMPACT ON NEIGHBOURING COUNTRIES

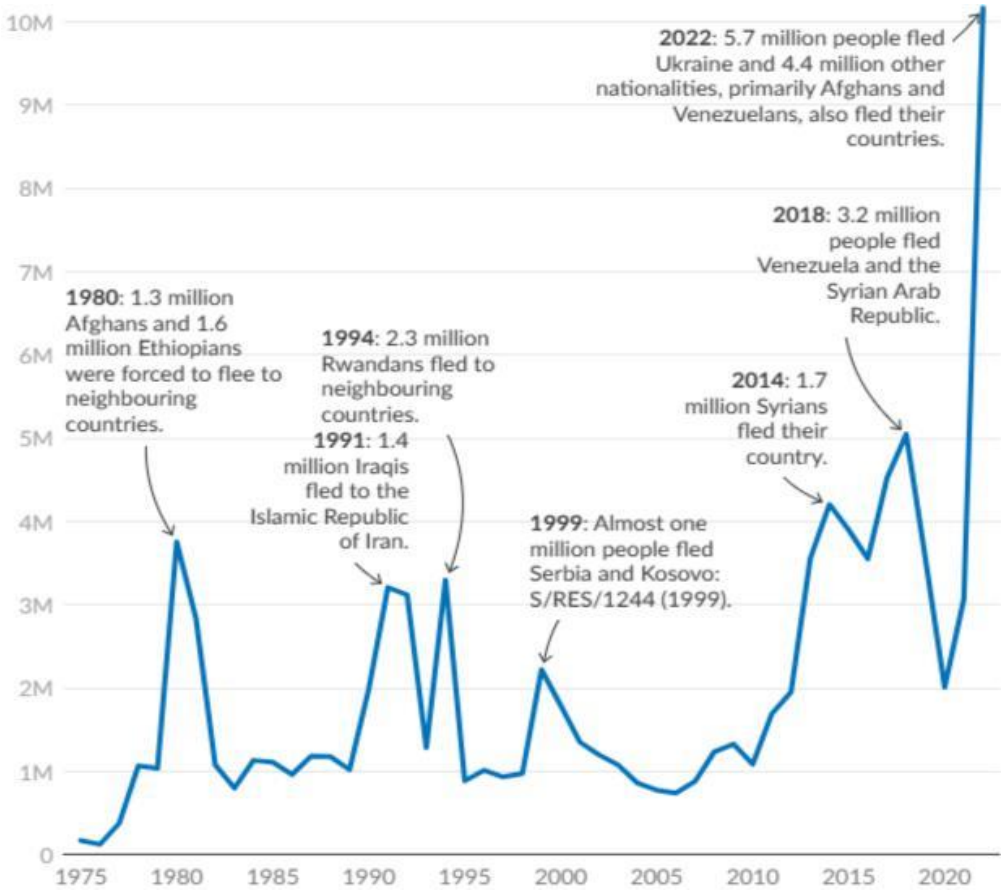


Illustration 2: https://www.unhcr.org/global-trends

In this situation, prone to conflict of interests, we can only expect an **increase in the number of forcibly displaced persons** as a direct consequence of armed conflict. And **the effects of regional conflicts are not limited to the territory in question, but affect the governance of all neighbouring countries**. The vast majority of forcibly displaced persons choose to stay in territories close to their place of origin, and only a few choose to undertake long journeys. An example of this is Afghanistan or Ukraine.

The spatial mobility of forcibly displaced persons is determined by a series of interacting structural, institutional, socioeconomic and psychological factors that vary according to context and time.

Geographical proximity is a key factor in explaining the preference of forcibly displaced persons, an example of which are the Syrian refugees mostly settled in Syria and Türkiye[7], as it allows them to maintain links with their country of origin, reduce the costs and risks of the journey, and facilitate their return in case the situation improves.

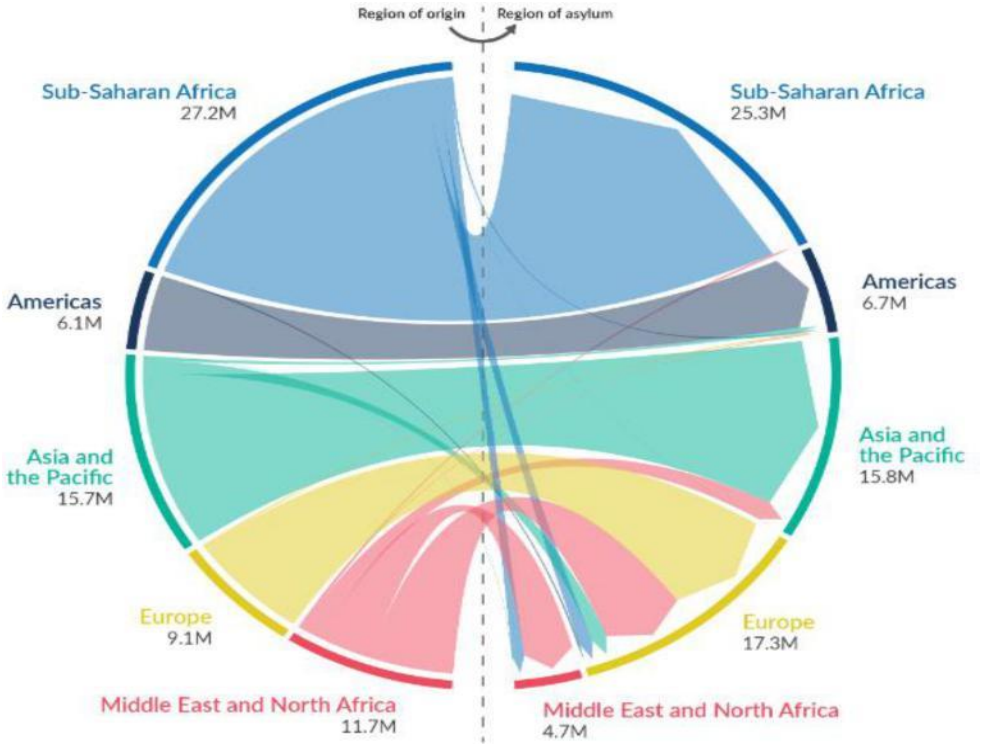


Illustration 3[8]

[7] Geographical proximity as a determining factor in the choice of destination for refugees: the case of Syrians in Türkiye], by Nuria López and María José Martínez.

[8] https://www.unhcr.org/global-trends

However, **geographical proximity also implies a number of challenges, both for the displaced themselves and for the host society**, which will see its carrying capacity put to the test.

On the one hand, despite the complexity of the issue, it can be stated that geographical distance has a negative and significant effect on refugee integration. Refugees who settle in places farther away from their country of origin are less likely to find work and to be involved in social and political activities than those who settle in places closer to their country of origin[9].

The negative effect of distance is mainly due to two factors: the reduced availability of social networks and increased culture shock. Refugees settling in more distant locations have fewer contacts with people of the same nationality or religion, making it more difficult for them to access information and support. In addition, refugees who settle in more distant locations face a greater linguistic and cultural difference with the local population, which makes it more difficult for them to adapt and integrate.

On the other hand, and although it benefits the integration of the displaced, nearby countries may find their load capacity exceeded.

2.1. LOAD CAPACITY

Carrying capacity is a concept from biology that refers to the **maximum population size that a given environment can sustainably support without irreversible damage** to natural resources. Carrying capacity depends on several factors, such as the availability of food, water, space, shelter and other ecosystem service.

---

[9] Distance matters: the impact of geographical proximity on refugee integration], by Jens Hainmueller, Dominik Hangartner and Dalston Ward.

In the context of a society receiving a massive influx of displaced persons, carrying capacity can be understood as the capacity of that society to welcome and integrate the new arrivals without generating social, economic or environmental conflicts. Social load capacity depends on several factors, such as political will, legislation, public policies, infrastructure, public services, labor market, social cohesion and culture.

Social load capacity is not a fixed or absolute value, but can vary according to context and time. Moreover, load capacity is not only a quantitative issue, but also a qualitative one. That is, it is not only the number of migrants arriving in a society that matters, but also their characteristics, needs and potential.

As a case study **we can analyze the situation in Jordan**, which despite its size and limited resources, **has been an example of solidarity**, hosting thousands of forcibly displaced persons from consecutive regional conflicts, providing them with multiple facilities and access to public services.

Between 2003 and 2007, Jordan hosted thousands of Iraqi refugees fleeing the U.S. invasion and sectarian violence in their country. Some of them returned to Iraq after the situation improved, but others remained in Jordan or resettled in third countries. Since 2012, Jordan has also hosted more than 1.3 million Syrian refugees who fled the war. In addition, it has also taken in as many as thousands of Yemeni refugees.

In economic terms, the hosting of refugees has had a mixed impact on Jordan, with both positive and negative effects. On the one hand, the presence of refugees has generated increased demand and consumption of goods and services, which has stimulated economic growth, investment and employment in some sectors, such as trade, construction, transportation and education. In addition, refugees have brought human capital, skills and social networks that can contribute to the country's development and innovation. On the other hand, the arrival of the refugees has placed a great strain on Jordan's already scarce and deficient resources and infrastructure, especially in the health, water, sanitation, shelter and energy sectors.

Undoubtedly, the reception of refugees has presented Jordan with an economic and social challenge. Although no specific data has been provided, members of the Jordanian government have spoken out in this regard, stating that the influx of displaced persons "caused a huge increase in government expenditures between the years 2011 and 2018 due to the costs involved in responding to the needs of refugees." Thus, the massive displacement is estimated to have caused "a huge decline in Jordan's economic growth" from 6.1% between the years 2000 and 2010 to 2.4% between 2011 and 2018, and an "increase in Jordanian debt" from 69% in 2010 to 95% at the end of 2018[10].

Although these data have not been verified, there are many indications that confirm the tension to which the Jordanian State has been subjected.

According to a 2016 World Bank report, the annual cost of healthcare for Syrian refugees in Jordan was about $147 million, of which the Jordanian government bore 63%. This means that the Jordanian government spent about $92.6 million per year on healthcare for Syrian refugees, which represented 4.5% of its total healthcare budget. However, this cost may have increased since then due to the increase in the number of Syrian refugees and the cancellation of health service subsidies for them in February 2018. This move resulted in Syrian refugees having to pay 80% of the Jordanian public healthcare foreigner fee, which increased the cost of healthcare for them fivefold. This caused many Syrian refugees to stop seeking healthcare services or resort to self-medication, which could have negative consequences for their health and public health in general. In turn, the demand for private healthcare has multiplied, due to the pressure on the public healthcare system, which has worsened its quality and availability.

[10] Statements by Issam Al-Majali, spokesman for the ministry in charge of supervising refugees.

The population increase has also challenged the Jordanian education system, which has had to accommodate more than 130,000 Syrian children in public schools, leading to capacity, quality and equity issues. Some schools have had to adopt a double-shift system to meet demand, which has reduced learning time and support for students.

The influx of displaced people has not only strained Jordan's services, but has also affected available resources. The current situation of Jordan's water reserves is critical, as it is one of the most water-scarce countries in the world. According to the UN, Jordan has an annual per capita water availability of 88 cubic meters, well below the absolute scarcity threshold of 500 cubic meters. In addition, water demand exceeds supply, due to population growth driven by the influx of displaced people, economic development and other climatic factors. Jordan relies heavily on groundwater, which accounts for 60% of the total water supply, but is overexploited and at risk of depletion and contamination. Other water sources are the Yarmuk and Jordan rivers, which are shared with Israel and Syria and have suffered a decline in flow and quality due to overuse and lack of regional cooperation. Jordan also has some dams and reservoirs that store rainwater, but these are insufficient and irregular. To address this situation, Jordan has resorted to measures such as desalination of water from the Red Sea and Dead Sea, reuse of treated wastewater for agricultural and industrial purposes, improved water efficiency and management, and public awareness and education to reduce water consumption and waste. However, these measures also have technical, economic, social and environmental constraints that require further investment, innovation and cooperation.

Jordan's load capacity could be measured as the ratio of available resources to the population that demands them, taking into account factors such as population growth, economic development, climatic factors and the influx of displaced persons. **As can be seen Jordan's load capacity, if not already exceeded, is close to being so**. Although given the scarcity of resources, especially water, energy and arable land, it cannot be said that the influx of

refugees is the only factor, **it has certainly generated increased pressure on Jordan's resources and infrastructure, negatively affecting the country's quality of life and environment.**

3. OTHER CAUSES OF FORCED DISPLACEMENT: CLIMATIC FACTORS

The load capacity of a society can be affected by multiple factors, not only a regional conflict or the massive arrival of displaced people. One of the most recurrent factors in recent years is climatic factors.

Migration is a process of adaptation to the environment, and the reality is that the world is constantly changing, and there are regions that are currently changing by leaps and bounds. Where it used to rain, now it is not, and vice versa. **The most of the climatic factors have subtle effects**, such as ocean acidification, loss of land profitability, or power outages. **These moderate effects have ongoing impacts that limit growth and development and can lead to the release of forced or economic migrants.**

Climate migration is projected to increase over the next few decades and then accelerate in the second half of this century. Internal migration hotspots could be generated as early as 2030, spreading and intensifying thereafter.

Internal climate migration is mainly due to long-term impacts on livelihoods and habitability in the most exposed areas, such as declining agricultural productivity, water scarcity, sea level rise, coastal erosion and extreme weather events.

Agricultural productivity is one of the main factors affecting the mobility of rural populations, especially in sub-Saharan Africa, South Asia and Latin America, where agriculture is a key economic activity and a source of livelihood for millions of people. Climatic factors can negatively affect agricultural productivity in several ways, such as reduced availability and quality of water for irrigation; reduced soil

fertility and water retention capacity; increased pests, diseases and weeds; crop loss or damage due to floods, storms, frost and fires; altered phenological and productive cycles of plants due to changes in temperature, precipitation and solar radiation.

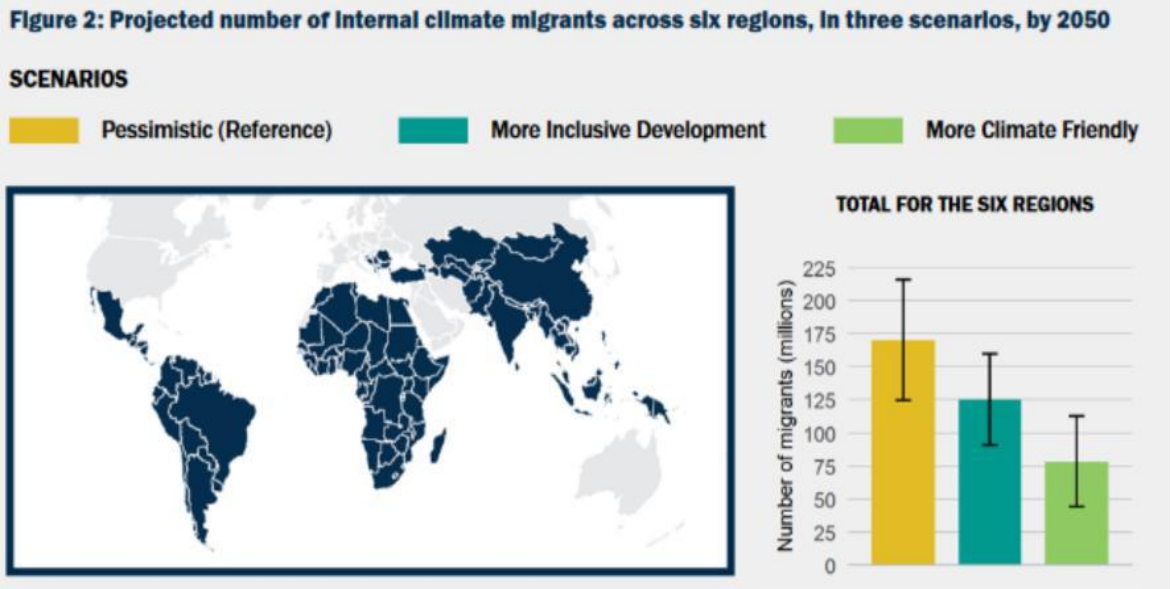


Ilustración 5[11]: Groundswell: Acting on Internal Climate Migration - World Bank

These effects may vary according to the type of crop, the region and the climate scenario. According to a World Bank report[12] , it is projected that, by 2050, agricultural productivity could decline by 2% to 9% in Sub-Saharan Africa, 4% to 7% in South Asia and 3% to 8% in Latin America.

This decline in agricultural productivity can have negative consequences for the food security, income and employment of rural populations. These populations may be forced to migrate to other areas within their countries in search of better economic and environmental opportunities. The report estimates that by 2050,

[11] https://www.bancomundial.org/es/news/feature/2021/09/13/millions-on-the-move-in-their-own-countries-the-human-face-of-climate-change.

[12] Groundswell: Acting on Internal Climate Migration - World Bank. https://www.bancomundial.org/es/news/feature/2021/09/13/millions-on-the-move-in-their-own-countries-the-human-face-of-climate-change.

some 86 million people could be climate displaced from rural to urban areas in sub-Saharan Africa, some 40 million in South Asia and some 17 million in Latin America

This decline in agricultural productivity can have negative consequences for the food security, income and employment of rural populations. These populations may be forced to migrate to other areas within their countries in search of better economic and environmental opportunities. The report estimates that by 2050, some 86 million people could be climate displaced from rural to urban areas in sub-Saharan Africa, some 40 million in South Asia and some 17 million in Latin America.

Water scarcity is another major factor for population displacement and has several consequences:

– Loss of food security and livelihoods for rural populations that depend on agriculture, livestock and fisheries. These populations may be forced to migrate to other areas with greater water availability or to urban areas with better economic opportunities.

– Exposure to health and environmental risks for populations consuming contaminated or insufficient water. These populations may suffer from disease, malnutrition, stress and conflict over access to water. These populations may be forced to migrate to areas with better water quality and quantity or to areas with better health services.

– Reduced hydroelectric power generation and industrial production that depend on water. These activities can be affected by reduced water flow and pressure, which can lead to power outages, shortages of raw materials, and job losses. These situations can affect the urban and rural populations that depend on these sectors. These populations may be forced to migrate to areas with greater energy and industrial supply or to areas with greater economic diversification.

In turn, climatic factors, such as water scarcity and loss of agricultural productivity, generate and aggravate armed and social conflicts. The reasons are multiple and synergistic, but competition for access to and control of water resources and arable land between different social, ethnic, religious or political groups generates tensions, violence, forced displacement and human rights violations in many territories around the world.

In turn, they diminish the state's capacity to provide basic services, such as drinking water, sanitation, health and education, to the population, generating dissatisfaction, protests, rebellions and challenges to state authority.

Some **examples of how water scarcity and loss of agricultural productivity have fueled armed and social conflict** are:

- The conflict in Syria has been linked in part to a prolonged drought that affected the country between 2006 and 2011, among other factors. This drought caused a severe agricultural crisis, forcing millions of people to abandon their land and migrate to the cities. This increased unemployment, poverty, overcrowding and social tensions, which added to other political and historical factors that triggered the uprising against the regime of Bashar al-Assad in 2011[1].

- The conflict in Darfur, Sudan, which has been linked in part to the desertification and water shortages that have affected the region for decades. These conditions have reduced the areas suitable for agriculture and pastoralism, which has generated competition and clashes between nomadic Arab communities (engaged in pastoralism) and sedentary African communities (engaged in agriculture). These conflicts have been exacerbated by ethnic, political and ideological factors, which have led to a civil war between the Sudanese government and rebel groups since 20032.

- The conflict in Lake Chad, which has been linked in part to the lowering of the lake's level due to climatic factors, overexploitation of water and poor resource management. This decline has negatively affected the economic activities and livelihoods of more than 30 million people who depend on the lake for fishing, agriculture, trade and transport. This has led to poverty, food insecurity,

displacement and forced migration. These conditions have favored the emergence and expansion of the terrorist group Boko Haram, which has spread terror in Nigeria, Niger, Chad and Cameroon since 2009.

These are just a few examples of how water scarcity and loss of agricultural productivity can drive armed and social conflict. However, it should be kept in mind that these phenomena are neither the only nor the main causes of conflict, but are combined with other political, economic, social and cultural factors that determine the degree and form of violence.

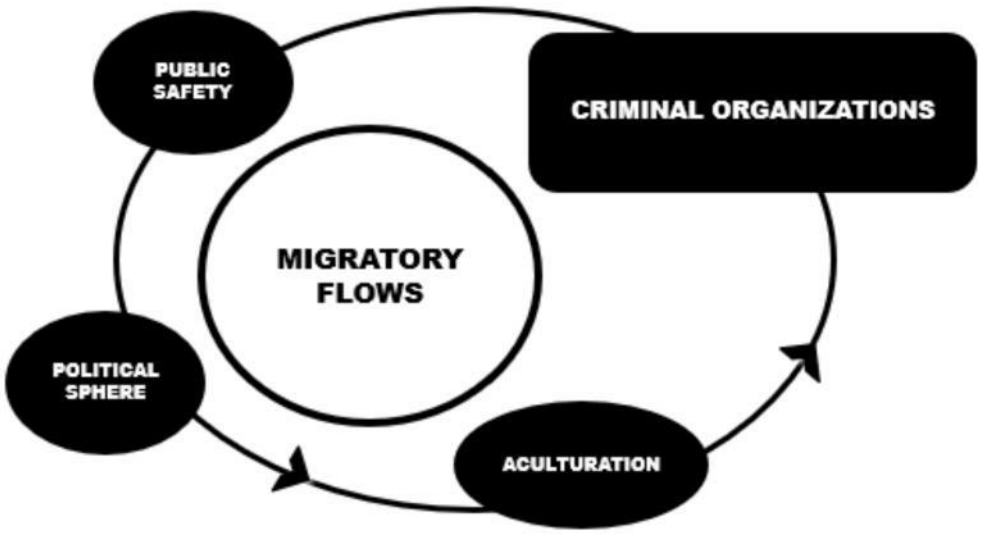
4. THE CHALLENGE OF MIGRATION MANAGEMENT

Migrations represent great opportunities for states, the expansion of labor markets, the economic development of countries of origin or training. But they also present great challenges, in which police forces have an extremely important role to play.

The challenges are not always easy to identify. There are clear consequences, such as the overflow of care systems. But there are others that are much more subtle.

Four informative objectives can be defined around which the efforts of the gendarmeries type forces and military status police forces can be focused:

- Proliferation of criminal organizations.
- Public safety.
- Political sphere.
- Acculturation.



4.1. PROLIFERATION OF CRIMINAL ORGANIZATIONS.

Mass movements of people, just as they create opportunities for States, also create opportunities for criminal organizations and armed groups, who see migrants reduced to mere commodities, which they can exploit and traffic. Unlike other natural resources, migrants pay for their smuggled through a territory, but they can also be forced to work, sexually exploited, sold as slaves, kidnapped for ransom, and even warehoused until a better used is found for them. In case of need, smugglers can also get rid of them, taking advantage of their vulnerability, and generally trusting that their administrative status will prevent them from going to the authorities.

This is a widespread phenomenon in various regions of the world, with multi-million dollar revenues. So much so, that there are entire regions and populations whose local economies have turned to migrant smuggling, covering every aspect of their exploitation.

There is an economic concept known as the "Dutch disease", which refers to the negative effects of a sudden increase in a country's income due to the discovery or exploitation of a natural resource, such as oil, gas or gold, which can be compared to the effect of the massive displacement of people in some territories.

The origin of Dutch disease dates back to the 1960s, when the Netherlands discovered large reserves of natural gas in the North Sea. This led to a significant increase in the country's revenues, which resulted in an appreciation of its currency, the guilder. As a consequence, non-gas exports lost competitiveness against cheaper imports, which adversely affected industry and agriculture. This phenomenon is known as "Dutch disease" because it is considered that **excess wealth derived from a natural resource can be detrimental to a country's economic and social development**. As with gas, migrants can be considered an untapped resource tied to a territory.

The effects of Dutch disease on a given territory can be diverse, depending on the economic structure, institutional quality and resource management of the affected country. Some of the most common effects are:

- Deindustrialization and loss of employment, due to the displacement of local production and the concentration of economic activity in the natural resource sector.
- Dependence on and vulnerability to natural resource fluctuations, which can generate boom and bust cycles that affect macroeconomic and social stability. In this case, we are talking about the demand for traffickers' services and the intensity of migratory flows.
- Corruption and institutional deterioration, due to the lack of transparency, accountability and democratic participation in the management of natural resource revenues. As criminal organizations take the lead in the exploitation of migrants, institutional deterioration is even deeper, and corruption of local institutions is a necessary step for them to operate normally.

Some theories argue that Dutch disease is not inevitable, but depends on the quality of the affected country's institutions and resource management. These

theories argue that if institutions are strong, transparent and democratic, and if resources are invested in education, infrastructure, innovation and productive diversification, Dutch disease can be avoided or mitigated. On the contrary, **if institutions are weak, corrupt and authoritarian, and if resources are wasted, concentrated in a few hands or allocated to military or clientelistic purposes, the Dutch disease can be aggravated and generate a "resource curse"** that affects the country's economic and social development. In this way, there are current and real counterexamples:

- Nigeria: The African country is the continent's largest oil producer, which has generated large foreign exchange earnings, but has also contributed to its economic and social underdevelopment. Oil has generated corruption, violence, ethnic and environmental conflicts, and an unequal distribution of wealth between regions.
- Norway: The Scandinavian country is one of the few cases that has managed to avoid or mitigate the negative effects of Dutch disease. Norway discovered significant oil and gas reserves in the North Sea in the 1970s, which has provided it with large foreign exchange earnings. However, Norway has set up a sovereign wealth fund that invests oil revenues in foreign financial assets, reducing pressure on domestic demand and government spending. It has also maintained a high level of transparency, accountability and democratic participation in the management of natural resources.

In the case of immigrant smuggling, **the proliferation of criminal organizations capable of operating with impunity on a given route takes all options for good resource management off the table, handing the initiative to criminal structures whose main motivation is self-enrichment or the quest for power.** In this way, the more wealth they obtain, the greater their capacity to achieve their objectives, and the less responsive the institutions are, which generally end up weakened and corrupted. This has been the case in certain

Libyan regions, where the main traffickers have ended up being political actors, reaching a degree of impunity only challenged by other rival organizations.

4.2. PUBLIC SAFETY

Migratory flows can affect public security in various ways, depending on the context and circumstances of each case. Some current examples of how they affect public security are:

- Public disturbances, such as assaults on the fences of the Spanish cities of Ceuta and Melilla. These two Spanish cities, located in North Africa, are external borders of the European Union and receive frequent attempts at irregular entry by migrants, who use everything in their power to overrun the contingents deployed at the border. These assaults pose a challenge to border surveillance and control, as well as to the humanitarian care and social integration of migrants who manage to gain access.
- Clashes with Security Forces and Bodies. For example, on Thursday, August 25, 2022, at around 05:00 a.m., in the Black Sea city of Burgas, Bulgaria, a bus carrying migrants ran over and killed two policemen who were trying to stop it. The bus, which had Turkish license plates, had entered the country illegally and refused to stop at two consecutive police border controls. The officers stopped their car in front of the bus, which rammed and ran over them before crashing into a bus stop. The two policemen died on the spot and no other injuries were reported. On board the bus were 47 migrants, whose nationalities have not been disclosed, but are believed to be Syrian. The bus driver has not yet been charged, but the district prosecutor said his actions were a "conscious and deliberate act." Bulgaria is a Balkan country that is part of the European Union and is on one of the main routes used by migrants from the Middle East and Afghanistan to reach Europe. Most migrants do not want to stay in Bulgaria, but use it as a transit corridor to the west.

- Serious crimes against people, such as what happened on June 14, 2023, when a fishing boat carrying between 400 and 750 migrants and refugees sank in the Ionian Sea off the coast of Pylos in Greece. It is the deadliest shipwreck in European waters so far this year. The migrants had set out from Libya bound for Italy, but the boat veered towards Greece for unknown reasons. The smugglers carrying them refused to stop at two border controls and kept the women and children locked in the hold. The ship sank for reasons still under investigation, possibly due to a breakdown or overloading. The Greek Coast Guard rescued 104 survivors and recovered 82 bodies, but hundreds are missing. Most of the survivors are men of Egyptian, Syrian, Pakistani, Afghan and Palestinian nationalities.

4.3. POLITICAL SPHERE.

Immigration has come to occupy a privileged place in global politics, due to the multiple factors that drive the movement of people across borders, as well as the challenges and opportunities they pose for countries of origin, transit and destination. According to the World Migration Report 2020, there were approximately 281 million international migrants in the world in 2020, a figure equivalent to 3.6% of the world's population. Immigration has economic, social, cultural, political and environmental implications for both migrants and the societies that host them or from which they originate.

However, immigration is also the subject of hate speech and hybrid strategies that seek to generate fear, rejection or violence towards migrants or towards certain groups or individuals based on their identity. Hate speech is defined as "any type of communication, whether oral or written, or behavior, that attacks or uses derogatory or discriminatory language in reference to a person or group based on who they are, in other words, based on their religion, ethnicity, nationality, race, color, ancestry, gender or other forms of identity". Hate speech can have negative effects on social cohesion, democracy and peace, and can incite discrimination, hostility or violence.

Hybrid strategies are those that combine different forms of political, military, economic, social or cultural action to achieve strategic objectives without resorting to open conflict. These strategies may include the use of media, social networks, cyber-attacks, propaganda, disinformation, infiltration, sabotage or support for non-state actors. Hybrid strategies may aim to influence public opinion, destabilize governments or undermine democratic institutions. Examples of hybrid strategies related to immigration include the manipulation of information on the causes and consequences of migration flows, the promotion of extremism or terrorism among radicalized migrants, or the instrumentalization of immigration as a political or diplomatic weapon.

4.4. ACCULTURATION.

Acculturation is the concept by which the process of adaptation of an immigrant to the host country is defined. Although it is a simplified model that does not capture the full complexity of the subject, it provides a theoretical framework that classifies the cultural adaptation strategies of individuals or groups that come into contact with a culture different from their own.

According to this model, there are two dimensions that influence the choice of acculturation strategy: the degree of maintenance or loss of the culture of origin and the degree of contact or isolation with the host culture. From these two dimensions, four possible strategies are derived:

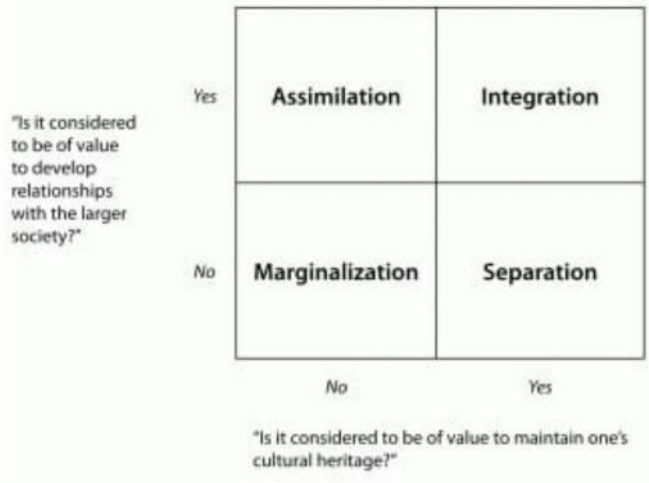
-Assimilation: implies the abandonment of the culture of origin and the full adoption of the host culture. It is typical of individuals or groups seeking to integrate into the majority society and who do not value their original cultural identity.

-Separation: implies the rejection of the host culture and the exclusive maintenance of the culture of origin. It is typical of individuals or groups that resist

changing their culture and isolate themselves from the majority society, forming ethnic or cultural enclaves.

-Integration: implies a balance between maintaining the culture of origin and contact with the host culture. It is typical of individuals or groups who value both their original cultural identity and cultural diversity and who seek to participate in the majority society without losing their culture.

-Marginalization: implies the rejection or loss of both the culture of origin and the host culture. It is typical of individuals or groups who do not feel identified or accepted by any culture and who suffer a cultural and social void. An example of this could be unaccompanied foreign minors, who have no support network either in their country of origin or in their host country.



Based on this model, it is possible to monitor the strategies employed by immigrants settled in a given territory, as well as to anticipate possible problems and solutions. Following this description, it is possible to analyze the formation of slums, the marginalization of second-generation immigrants whose parents have adopted separation strategies, or to study techniques for approaching certain social sectors.

Integration is the most beneficial strategy for the psychological and sociocultural well-being of individuals and groups facing the acculturation process. Integration makes it possible to preserve one's own cultural identity and at the same

time participate in the social life of the host country. Integration also promotes mutual respect, tolerance and dialogue between different cultures.

On the contrary, separation and marginalization are the most detrimental strategies for the psychological and sociocultural well-being of individuals and groups facing the acculturation process. Separation implies social isolation and a lack of interaction with the majority culture, which can lead to conflict, discrimination or violence. Marginalization implies a loss of cultural identity and a lack of belonging to any group, which can lead to stress, anxiety or depression.

A State that wants to facilitate the acculturation process of new arrivals must seek strategies that promote integration and avoid separation and marginalization. In this process, it is necessary to find common characteristics between cultures, with language playing a fundamental role. Assimilation policies, whereby immigrants are forced to abandon their culture of origin, have proven to have the opposite of the desired effects, mostly provoking separation strategies.

5. UNITY OF ACTION

In this scenario, in which regional conflicts are occurring with increasing frequency and intensity, with all the challenges that this entails, the Gendarmeries and Police Forces with Military Status, will have a prominent role that includes monitoring, control, coordination, and cooperation, with repression being a last resort.

The decision-making process in these areas is extremely complex, but it must always contemplate short, medium and long-term solutions, developing strategies that adapt to the evolution of the conflict.

State responses must be coordinated and multidisciplinary, encompassing different approaches, from police response to social care and the management of

emergency resources. In this sense, the Guardia Civil has the experience of being the authority in charge of coordinating actions to deal with irregular immigration. In this way, all state resources are coordinated from a single authority, avoiding duplication.

The other essential axis of action of the Gendarmeries and Police Forces with Military Status must be international cooperation. This axis can be articulated in various ways, from the exchange of experiences, to the creation of international units, or the joint investigation and prosecution of crimes. In this area, liaison officers and the promotion of communication channels play an important role.

The Guardia Civil has promoted the deployment of liaison officers and resources to support sister corps in many countries, especially on the West Coast and North Africa. This deployment has proved to be highly effective, achieving mutual benefit for all involved.

6. CONCLUSIONS

1. Regional conflicts have far-reaching implications, not only impacting the security of neighboring nations but also significantly affecting the environment. This includes land degradation, deforestation, and the exploitation of natural resources, all of which contribute to the large-scale displacement of populations. Also, in this context, migration flows can be used as a vector of hybrid threat.

2. Migratory movements, particularly those occurring in the context of regional conflicts, necessitate a multidisciplinary approach. This involves the participation of all state actors, regardless of their varying levels of responsibility. Furthermore, effective coordination between civil, military and non-governmental entities is crucial.

3. Large-scale population displacements put immense pressure on governance, security, economic, environmental and foster care systems.

4. The role of gendarmeries type forces and military status police forces in managing migratory flows includes monitoring, control, coordination, and cooperation at national and international level, with repression being a last resort.

5. In situations of regional conflict and mass displacement, it is vital to monitor the activities of criminal organizations. This includes a focus on various illegal activities such as crimes committed against the migrants themselves.

6. Environmental security is a matter of both intelligence and policing and can be leveraged to support hybrid strategies. By addressing environmental damage, we can enhance our resilience to future crises, particularly those arising from regional conflicts.

7. Responses to mass displacement must be forward-thinking, with solutions that follow the progression of the regional conflict.

8. Capacity building is needed to establish common procedures that foster international cooperation. Specialization is a priority to address this phenomenon, and the creation of specific units that arise from police cooperation is a measure to consider.

9. Common training based on best practices and lessons learned is crucial to enhance the management of migration flows.

In conclusion, a comprehensive strategy, international cooperation, and specialized training are essential to manage the mass displacement of people resulting from regional conflicts.


FIEP 2023
SPANISH PRESIDENCY