



**GUARDA NACIONAL REPUBLICANA
PORTUGAL**

2022 FIEP PUBLICATION

OVERCOMING SECURITY THREATS ARISING FROM GLOBALIZATION 4.0



FIER²²
PORTUGUESE PRESIDENCY



**GUARDA NACIONAL REPUBLICANA
PORTUGAL**



2022 FIEP PUBLICATION

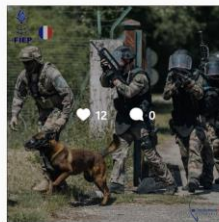
OVERCOMING SECURITY THREATS ARISING FROM GLOBALIZATION 4.0





@fiep_association

@fiep.org



www.fiep.org

TECHNICAL SPECIFICATIONS



TITLE 2022 FIEP Publication: *“Overcoming Security Threats arising from Globalization 4.0”*

COORDINATION Major-General Pedro Manuel Sequeira Estrela Moleirinho
Chairman of the FIEP22 Portuguese Presidency

Colonel Carlos João Soares Costa
2022 FIEP Publication and International Affairs Commission Coordinator

Lieutenant-Colonel Paulo Miguel Lopes de Barros Poiares
2022 FIEP Secretary-General

Major Bruno Miguel Passos Baraças
Chairman Assistant

Major Helder Manuel Gonçalves Garção
Portuguese Presidency POC

EDITORIAL STAFF Strategic Planning and International Affairs Division
Guarda Nacional Republicana





INDEX

FIEP ASSOCIATION	9
FOREWORD	9
GLOSSARY AND ABBREVIATIONS	6
Publication Framework.....	10
Introduction.....	11
Key Objectives.....	11
Common Methodology: “strategic diagnosis” as research design.....	12
COMMON EXTERNAL ENVIRONMENT ANALYSIS: A SECURITY STRATEGIC FORESIGHT	17
RESEARCH PAPERS LIST	23
I. Paper CYBERCRIME AND CYBERTHREATS	24
II. Paper PROPAGANDA AND MISINFORMATION	34
III. Paper CLIMATE CHANGE AND NATURAL DISASTERS	48
IV. Paper DISPUTES OVER SCARCE NATURAL RESOURCES	70
V. Paper FRAGILE STATES AND REGIONAL CONFLICTS	82
VI. Paper ENERGY INSECURITY	88
VII. Paper CRITICAL INFRASTRUCTURES	94
VIII. Paper MIGRATORY phenomena	112
IX. Paper HUMAN TRAFFICKING	128
X. Paper TERRORISM	140
XI. Paper TRANSNATIONAL CRIMINAL NETWORKS	152
XII. Paper COUNTERFEITING	164
XIII. Paper TRAFFICKING OF ARMS	172
XIV. Paper ENVIRONMENTAL CRIME	184
XV. Paper HEALTH (PANDEMIC)	194
XVI. Paper CBRN	210
KEY TAKEAWAYS AND RECOMMENDED STRATEGIES	224
KEY TAKEAWAYS	225
Growth strategies SO.....	226
Diversification strategies ST.....	227
Targeting strategies WO.....	228
Defence strategies WT.....	229

INDEX OF FIGURES

Figure 1. FIEP Members and Forces	8
Figure 2. Keys Strategies Cybercrime and cyberthreats	32
Figure 3. Types of information disorder	36
Figure 4. Keys Strategies Propaganda and misinformation	43
Figure 5. The landslides triggered by rainfall for the period 2007-2019	52
Figure 6. The Manavgat Fire in Türkiye on July 31, 2021	56
Figure 7. The severity of fires in Türkiye and the Mediterranean region during the summer of 2021	56
Figure 8. Key strategies Climate change and natural disasters	64
Figure 9. Countries involved in the basin (10) (COMIP – 2021) ¹³	73
Figure 10. Main rivers that form the La Plata River Basin (OAS – 2004) ¹⁴	74
Figure 11. Key strategies Disputes over scarce natural resources	79
Figure 12. GO, SO, CQ and DI	97
Figure 13. Key strategies Critical Infrastructure	107
Figure 14. Comprehensive Migration Policy	113
Figure 15. Key strategies Migratory phenomena	123
Figure 16. Key strategies Human Trafficking	135
Figure 17. Key Strategies Terrorism	147
Figure 18. Cocaine flows and transit areas	155
Figure 19. Flows of irregular migrants	156
Figure 20. Rhino poaching statistics in South Africa from 2000 to 2016	156
Figure 21. Pharmaceutical imports for eight West African countries, in millions of US\$	157
Figure 22. Key Strategies Transnational organized crime	161
Figure 23. Key Strategies Counterfeiting	168
Figure 24. Key strategies Trafficking of arms	181
Figure 25. Combating environmental crime - Italian activity 2019-2020	188
Figure 26. Key strategies Environmental Crime	190
Figure 27. Key strategies Health (Pandemic)	204
Figure 28. Key strategies CBRN	219

INDEX OF TABLES

Table.1. List of Threats or Security Challenges	11
Table 2. Global PESTEL Analysis based on key references	18
Table 3. Research Papers List	23
Table 4. PESTEL Analysis Cybercrime and cyberthreats	26
Table 5. SWOT analysis Cybercrime and cyberthreats	31
Table 6. PELTEL Analysis Propaganda and misinformation	41
Table 7. SWOT analysis Propaganda and misinformation	42
Table 8. PESTEL Analysis Climate change and natural disasters	58
Table 9. SWOT analysis Climate change and natural disasters	63
Table 10. PESTEL analysis Disputes over scarce natural resources	76
Table 11. SWOT analysis Disputes over scarce natural resources	77
Table 12. SWOT analysis Fragile States and regional conflicts	86
Table 13. SWOT analysis Energy insecurity	92



Table 14. SWOT analysis Critical Infrastructure	106
Table 15. SWOT analysis Migratory phenomena	121
Table 16. SWOT analysis Human Trafficking	134
Table 17. PESTEL analysis Terrorism	145
Table 18. SWOT analysis Terrorism	146
Table 19. PESTEL analysis Transnational organized crime	158
Table 20. SWOT analysis Transnational organized crime	160
Table 21. PESTEL analysis Counterfeiting	166
Table 22. SWOT analysis Counterfeiting	167
Table 23. PESTEL analysis Trafficking of arms	174
Table 24. SWOT analysis Trafficking of arms	180
Table 25. SWOT analysis Environmental Crime	189
Table 26. PESTEL analysis Health (Pandemic)	200
Table 27. SWOT analysis Health (Pandemic)	203
Table 28. PESTEL analysis CBRN	214
Table 29. SWOT analysis CBRN	218

INDEX OF SCHEMES

Scheme 1. Strategic Management Model (Wheelen & Hunger 2012, p. 15)	13
Scheme 2. PESTEL Framework	14
Scheme 3. SWOT Matrix (basic)	14
Scheme 4. Strategic Diagnosis. (a) Environment Scanning and (b) Dynamic SWOT Analysis (DSA)	15
Scheme 5. Strategic Diagnosis	15

GLOSSARY AND ABBREVIATIONS

A

AHP	Analytic Hierarchy Process
ARG	Argentina
ATM	Automated Teller Machine

B

BRA	Brazil
-----	--------

C

C2	Command and Control
CaaS	Crime-as-a-Service
CHL	Chile
CSIRT	Cyber Security Incident Response Team

D

DDoS	Distributed Denial of Service
DJI	Djibouti
DSA	Dynamic SWOT Analysis

E

EC3	EUROPOL's European Cybercrime Centre
EEAS	European External Action Service
EGF	European Gendarmerie Force (or EUROGENDFOR)
EMCDDA	European Monitoring Centre for Drugs and Drug Addiction
ESP	Spain
EU	European Union
EUROPOL	European Union Agency for Law Enforcement Cooperation
EUROGENFOR	European Gendarmerie Force (or EGF)

F

FIEP	International Association of Gendarmeries and Police Forces with Military Status
FRA	France

G

GNR	Guarda Nacional Republicana
GPS	Global Positioning System

I

IMINT	Imagery Intelligence
INTERPOL	International Criminal Police Organization
IOCTA	Internet Organised Crime Threat Assessment
IOM	International Organisation for Migration
IoT	Internet of Things
IP	Internet protocol
IT	Information Technology
ITA	Italy

J

JHA	Justice and Home Affairs
JOR	Jordan

K

KWT	Kwuit
-----	-------

L

LE	Law Enforcement
LEA	Law Enforcement Authority



M

MAR	Morocco
MDMA	Methylenedioxyamphetamine
MOCG	Mobile Organised Crime Groups
MSU	Multinational Specialized Unit

N

NATO	North Atlantic Treaty Organization
NDL	The Netherlands
NGO	Non-Governmental Organisation
NIS	Network and information security
NPS	New Psychoactive Substance
NSF	National Security Forces (Palestine)

O

OCG	Organised Crime Group
OLAF	European Anti-Fraud Office
OSINT	Open-Source Intelligence

P

p. pp.	page pages
P2P	Peer-to-peer
PRT	Portugal
PSE	Palestine

Q

QAT	Qatar
-----	-------

R

ROU	Romania
-----	---------

S

SASE	Safe and Secure Environment
SNE	Senegal
SOCTA	Serious and Organised Crime Threat Assessment
SOC	Serious and Organised Crime
SPU	Stability Police Unit
SWOT	Strengths, Weaknesses, Opportunities and Threats

T

THB	Trafficking in human beings
TUN	Tunisia
TUR	Türkiye

U

UKR	Ukraine
UN	United Nations
UNICRI	United Nations Interregional Crime and Justice Research Institute
UNOCT	United Nations Office on Counter-terrorism
UNODC	United Nations Office on Drugs and Crime

V

VAT	Value added tax
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VUCA	Volatility, Uncertainty, Complexity and Ambiguity

W

WEEE	Waste of Electronic and Electric Equipment
2FA	Two-factor authentication

FIEP ASSOCIATION

INTERNATIONAL ASSOCIATION OF GENDARMERIES AND POLICE FORCES WITH MILITARY STATUS

The goal of FIEP is to broaden and strengthen the mutual relationships, to promote an innovative and active reflection on the forms of police co-operation, and to value its model of organisation and structures abroad.

Founded in 1994, it then comprised the French *Gendarmerie Nationale*, the Italian *Arma dei Carabinieri*, and the Spanish *Guardia Civil*. It was quickly joined by the Portuguese *Guarda Nacional Republicana* in 1996.

Afterwards, the Turkish *Jandarma* in 1998 swelled the ranks followed by the Royal Netherlands Marechaussee and the Moroccan Royal Gendarmerie both in 1999. The Romanian Gendarmerie joined in 2002 and the Jordan Gendarmerie Forces in 2011.

The Argentinian Gendarmeria Nacional and the Chilean Carabineros 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.

For further information: www.fiep.org



Figure 1. FIEP Members and Forces



FOREWORD

In the era of Globalization 4.0, the current phenomena and challenges, whether criminal, social, political, economic or of any other nature, impose the union of efforts, which are increasingly fundamental to anticipate, prevent or respond efficiently to the emerging and crosscutting needs of the various countries.

Within the framework of International Cooperation, the creation or reinforcement of Strategic Partnerships is gradually assuming greater relevance, among which the FIEP Association stands out, particularly for its 19-member Forces, as a result of the extraordinary synergies that it has promoted, since its creation in 1994.

Throughout these 27 years, our Association has fostered the potential of Gendarmerie-type forces, highlighting the key role they have been consolidating at the global security level, as well as contributing to the appropriateness of the performance models of its partner forces, in view of the increasingly demanding challenges.

The close inter-institutional liaison, enhanced by privileged communication channels, facilitates cooperation at various levels and enables us to improve the results achieved, both nationally and internationally, optimizing resources and increasing our efficiency.

Within this framework, the Portuguese Presidency of the FIEP Association considers the development of joint initiatives and projects, aggregating the common interests of various members, as the driving force that encourages the close relationship and promotes the sharing of knowledge, experiences and best practices, which enables progress, certainly delivering benefits on a global scale.

This 2022 FIEP publication, entitled ***“Overcoming Security Threats arising from Globalization 4.0”***, is an example of such initiatives and results from the remarkable synergies generated within the FIEP Association, with a potential real impact on the security and stability of our societies, achieved through the analysis of the most pressing security threats and their associated mitigation strategies, to be considered as a way forward in the work of law enforcement institutions.



GNR
GUARDA NACIONAL REPUBLICANA

Lieutenant General Rui Manuel Carlos Clero
President of the FIEP Association
General Commander of the *Guarda Nacional Republicana*

PUBLICATION FRAMEWORK

“Security and threats arising from Globalization 4.0”

In Programme of the Portuguese Presidency, 2022

The Presidency of FIEP Association focuses on the theme **“Security and threats arising from Globalization 4.0”**. The significant changes we are currently witnessing in technology, geopolitics, environment and society are coming together to give rise to a new phase of globalization. The metamorphosis we are witnessing, deeply affected by digital transformation, entails radical changes in the way of individuals and institutions, quickly rushing towards a new phase of global dynamics: Globalization 4.0.

Globalization was a precursor of the “Volatile, Uncertain, Complex and Ambiguous” context, but the famous acronym “VUCA”, which has been used over the past four decades to describe the global reality, is no longer sufficient to give it meaning or to indicate potential future scenarios that help tackle the key challenges of today. The world has evolved and several authors suggest new terminologies to account for the disruptive mutations it is undergoing. Among others, the acronym “BANI” – “Brittle, Anxious, Nonlinear and Incomprehensible” has been advocated to respond to the era of chaos in which we are currently proceeding.

BANI is an approach that serves to articulate the increasingly common situations where simple volatility or complexity appear insufficient to understand what is happening; where conditions that characterise them are not simply unstable, but rather chaotic; where results are not simply difficult to predict, but completely unpredictable; and whose events are not merely ambiguous, but often incomprehensible.

The components of the acronym may even suggest response opportunities: brittleness requires resilience; anxiety asks for empathy and mindfulness; non-linearity calls for context and adaptivity and incomprehensibility demands transparency and intuition. These may be reactions rather than solutions, but they suggest that the necessary answers can be found.

The theme **“Security and threats arising from Globalization 4.0”**, highly up-to-date in light of the strong dynamics and global development, frames the work that we develop at each 2022 FIEP Expert Commission, subordinated to specific subthemes, which seek to promote joint analysis and reflection, thus allowing for collecting best practices and sharing knowledge to enhance evolution and joint development.

In short, the main objectives of the programme that the FIEP Presidency proposed for 2022 have been:

1. To reflect on the technological developments in artificial intelligence, applied to Predictive Policing models, as a way to enhance the capabilities and efficiency of the Security Forces;
2. To analyse the impacts that the adoption of Predictive Policing models and the use of technology have on Human Resources management, in order to increase the efficiency of Human action;
3. **To promote analysis on strategies and best practices to cope with key security threats and challenges in the era of Globalization 4.0, collating and sharing knowledge through a FIEP Association publication;**
4. To promote sharing of information and mutual knowledge on the structures that each Force has at its disposal to deal with international affairs, discussing improvements and models to follow, in order to foster efficient cooperation and networking.

In this era of Globalization 4.0, characterised by uncertainties and technological transformation, the 2022 FIEP programme aimed to stimulate the modernisation and resilience of our Forces; enhance the quality and empathy generated by our operational product; prompt an indispensable analysis of the current context and prognosis of future challenges; and also promote transparency and the sharing of information and experiences, which together enable Gendarmeries to be asserted as a Police model of excellence.



INTRODUCTION

Globalization has been a precursor of immense developments for humankind, but it has also generated complexity, chaotic dynamics and disruptive mutations, which are associated with numerous (hybrid) threats and security challenges.

Aiming to preserve the stability and well-being of societies, Security Forces shall increasingly seek to remain proactive in anticipating dangers, thus adopting strategies and appropriate measures to mitigate risks and combat criminal, as well as other security threats.

To that end, based on the emerging security challenges and key common threats, it is crucial to analyse and collect the most efficient best practices in the fight against these phenomena, aiming to foster improved security levels.

KEY OBJECTIVES

This publication aims mainly at fulfilling the 3rd objective of the 2022 FIEP work programme, prompting an indispensable analysis of the current context and **prognosis of future challenges, while developing strategies to cope with the key security challenges ahead.**

Security challenges and crime are constantly evolving phenomena, in a complex, real and dynamic context. The subject requires a holistic, yet useful and pragmatic approach. Thus, without losing sight of the whole, it is important to focus the object of this research on the main security threats with an international scope.

As such, a list of 19 key international security threats was identified and afterwards selected¹ based on different comprehensive assessments²:

Table.1. List of Threats or Security Challenges

THREAT OR SECURITY CHALLENGE		FIEP MEMBER
I	Cybercrime and cyberthreats	Spain
II	Propaganda and misinformation	Romania
III	Climate changes and natural disasters	Türkiye
IV	Disputes over scarce natural resources	Argentina
V	Fragile states and regional conflicts	Palestine
VI	Energy insecurity	Jordan
VII	Critical Infrastructures	Portugal
VIII	Migratory phenomena	The Netherlands
IX	Human trafficking	Senegal
X	Terrorism	Tunisia
XI	Transnational criminal networks	Djibouti
XII	Counterfeiting (documents, pharmaceuticals, goods and products, digital contents)	Morocco
XIII	Trafficking of arms	Chile
XIV	Environmental crime	Italy
XV	Health (pandemic)	France
XVI	CBRN	Kuwait

¹ Selection based on 3 priorities identified by each country and the principle “first come, first served” was then applied.

² Different key assessments were considered, completed with open-source analysis, notably the following:

- Global Risks Report 2022 – 17th Edition (World Economic Forum, 2022)
- 2021 Serious and Organised Crime Threat Assessment (SOCTA 2021) (EUROPOL, 2021);
- 2021 Internet Organised Crime Threat Assessment (IOCTA 2021) (EUROPOL, 2021);
- INTERPOL-UN Strategic Report on Environment, Peace and Security (INTERPOL-UN, 2016); and the
- UNODC Transnational Organized Crime Threat Assessments, from several reports available in <https://www.unodc.org/unodc/data-and-analysis/TOC-threat-assessments.html>

Based on a common systematisation and methodology, with the execution of a strategic diagnosis as a research design, each of the experts nominated by FIEP countries, focusing on a typology of threat, seeks to identify various strategies to tackle, cope and overcome the security challenge under analysis.

COMMON METHODOLOGY: “STRATEGIC DIAGNOSIS” AS RESEARCH DESIGN

1. METHODOLOGY

This is a prospective empirical study, based on hypothetical-deductive reasoning, supported by documental analysis and triangulation of sources, with a predominantly qualitative research strategy.

Based on hermeneutics, this methodological option calls for the understanding and interpretation of data and complex dynamics, thus enabling a holistic study of today’s reality, while seeking to envisage solutions for the future.

2. RESEARCH DESIGN: THE “STRATEGIC DIAGNOSIS”

According to Ribeiro (2017), strategy as a process, consists both in the science and the art of developing, arranging and employing means of coercion in a given environment and time, in order to achieve policy objectives, overcoming threats and exploring opportunities, in a given conflict environment.

Regardless of the schools of strategic thought³; its evolution and complexity of approaches; the multiplicity of concepts and methods; or the constantly evolving dynamics about strategy and its theorization; strategy is used to obtain competitive superiority.

Referring to Strategic Management, Ribeiro Ribeiro (2008, pp. 20-25) proposed a model for the National Defence strategy formulation process, duly adapted and sustained⁴, structured into four phases:

1. **"Environment Analysis"** - Which corresponds to the question "where are we?" and, as such, includes the analysis of the external environment, namely by using the PESTEL technique (Johnson and Scholes, 1999, p.104, apud Ribeiro, 2008, p.22) in order to identify the external strategic factors; as well as the analysis of the internal environment, using the method of the "7-S" from McKinsey or by functional analysis (Ibid, p.23).
2. **"Strategic Formulation"** - Which will answer the question "where should we go?", considering namely the "best conjugation between external strategic factors (Threats and Opportunities) and internal factors (Strengths and Weaknesses), to diagnose the strategic context and, therefore allowing progress towards the desired future. This analysis should be developed using the SWOT matrix (Ibid, p.23).
3. **"Strategic operationalisation"** - Which corresponds to the question "how do you get there?", linking the formulation to the operationalisation of the selected course of action through the execution of tasks, and respective responsibilities (Ibid, p. 25).
4. **"Strategic control"** - Corresponding to the question "are we getting there?", with performance monitoring and readjustment (feedback) mechanisms, where techniques such as the "Balanced Scorecard; accounting; performance evaluation; and strategic audits stand out." (Ibid, pp. 26-27).

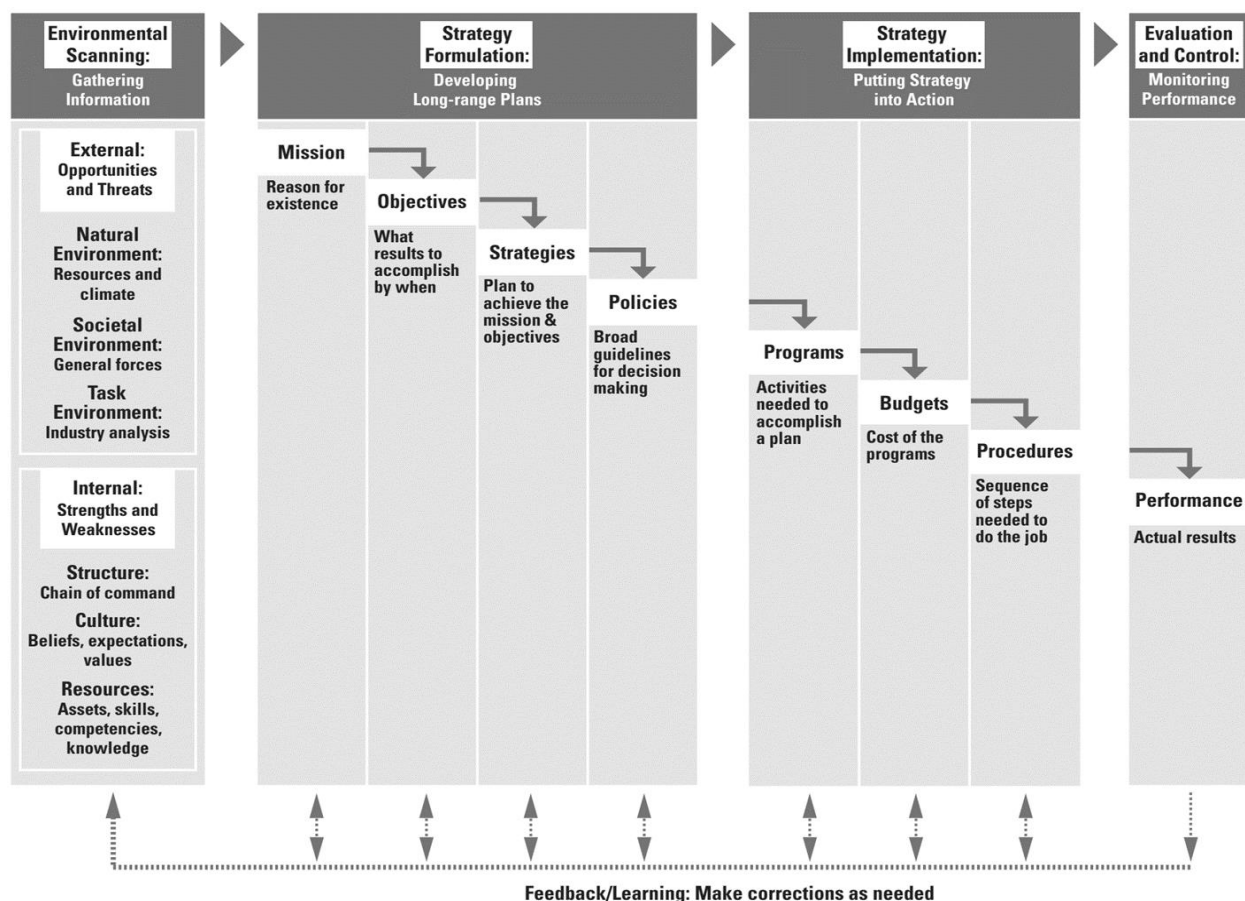
³ Mintzberg, Ahlstrand, and Lampel (1998) systematized the strategic studies into ten streams/schools of thought: between the Prescriptive ones, which encompass the "design school," the "planning school," and the "positioning school," and the Descriptive ones, which encompass the "entrepreneurial school," the "cognitive school," the "knowledge school," the "power school," the "cultural school," the "environmental school," and the "configuration school."

⁴ The author draws mainly on the strategic management model proposed by the US Naval War College, the Hunger and Wheelen model and, the Palladium Execution Premium Process™ (XPP™) model from (Kaplan & Norton, 2008, p. 2), which are essentially similar and are based on four questions: "where we are?" (environment analysis); "where we should go?" (formulation); "how do you get there?" (operationalisation); "are we getting there?" (monitoring).



In a similar approach, according to Wheelen & Hunger (2012), the basic model for Strategic Management also includes four cyclical phases, as detailed in the scheme below:

- **"Environmental Scanning"** – for improving situational awareness, both from external and internal environments, by monitoring, evaluating, and disseminating information - strategic factors - to key people.
- **"Strategy Formulation"** – for developing long-range plans for the effective management of environmental opportunities and threats, considering organizational strengths and weaknesses (SWOT). It includes defining the corporate mission, specifying achievable objectives, developing strategies, and setting policy guidelines.
- **"Strategy Implementation"** – for putting strategy into action through the development of programs, budgets, and procedures. This process might involve changes within the overall culture, structure, and/or management system of the entire organization.
- **"Evaluation and Control"** – for monitoring performance results so that actual performance can be compared with desired performance and corrective action can be taken to solve problems.



Scheme 1. Strategic Management Model (Wheelen & Hunger 2012, p. 15)

Even earlier, Michael Porter (1980), in a consistent line, when postulating a framework for structural analysis for "competitive strategy", explained that the **Strategic Diagnosis** of an organization is the first step in the collection of data that will allow for the guidance of the Strategy. This diagnosis aims to identify and monitor competitive advantages. Based on this diagnosis, the organisation will be able to anticipate changes and thus prepare itself to act in its internal and external environments.

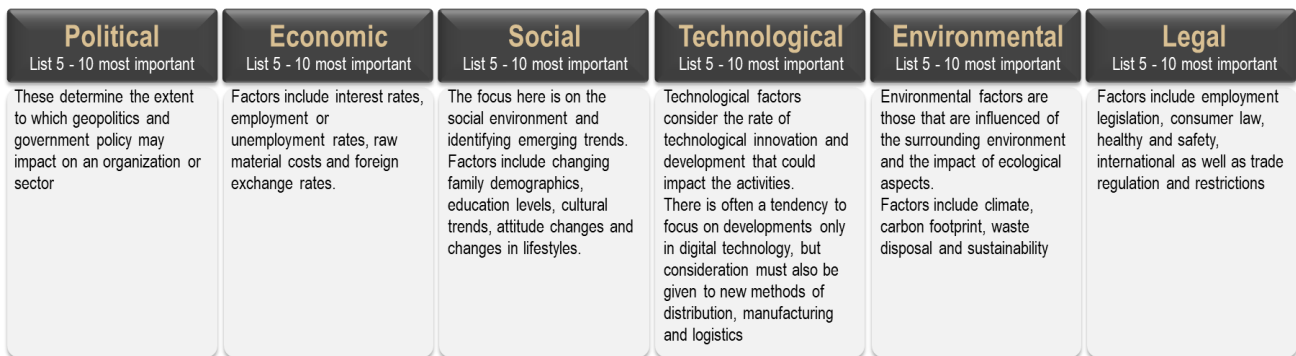
Notwithstanding the approach, the analysis of the strategic context, considering both the external and the internal environments, is a fundamental starting step, and many authors refer to this step as **Strategic Diagnosis**.

Bearing in mind that internal and external changes happen constantly, the two fundamental purposes of the **Strategic Diagnosis** and subsequent strategic planning are:

- to analyse the external environment and successfully adapt to challenges; and
- to concentrate and direct the existing internal forces towards a competitive superiority.

To analyse the endogenous and exogenous strategic environments, several methods/techniques⁵ have been used, such as PEST or PESTEL framework, the five forces model or resource-based approach. Often, internal and external factors are then presented in a SWOT matrix.

As stated by Wheelen & Hunger (2012), over the years, SWOT matrix has proven to be the most enduring analytical technique used in strategic management, conceived in the 60s, by Kenneth Andrews and Roland Christensen - professors at Harvard Business School, which became a reference mainly in the academic and business world in the 70s.

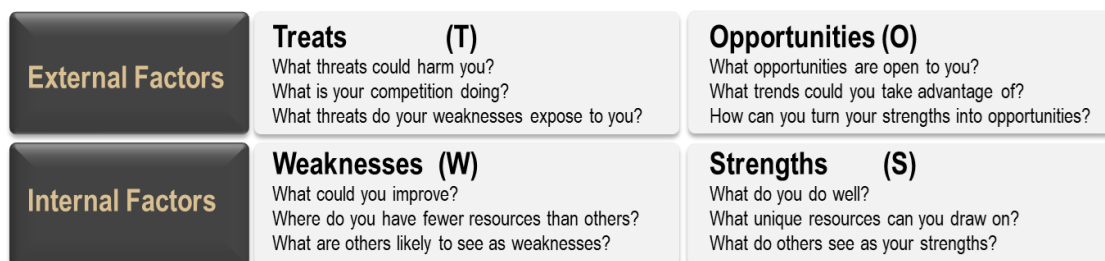


Scheme 2. PESTEL Framework

Opportunities and threats are part of the exogenous analysis of the organisation and may arise from constant technological innovation, changes in the behaviour of stakeholders, and political, social or economic changes.

In the endogenous analysis, strengths and weaknesses are listed. Strengths are related to specific organisational characteristics such as know-how and the multiplicity of the organisation's intrinsic resources, which put it at a competitive advantage. The weaknesses correspond to what may put the company at a disadvantage in relation to its competitors.

Having identified these factors, we can immediately, yet vaguely, envisage strategies based on taking advantage of strengths, eliminating weaknesses, exploiting opportunities, or countering threats.



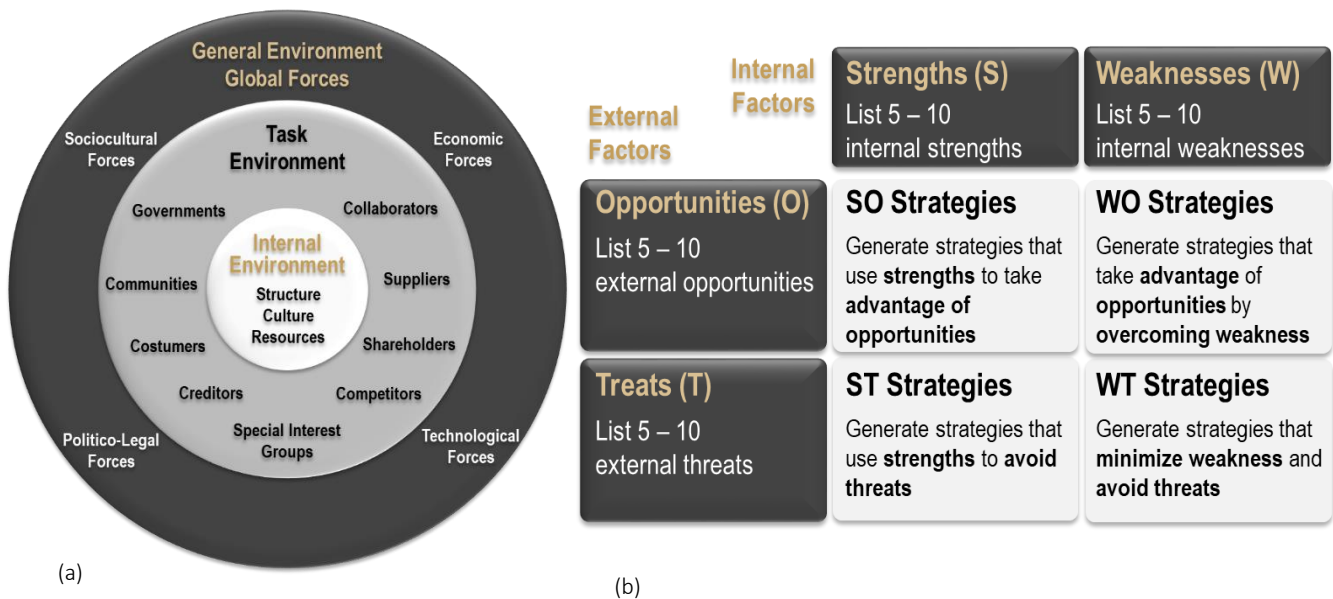
Scheme 3. SWOT Matrix (basic)

⁵ Examples: PESTEL analysis; SWOT analysis; Porter's five competitive forces; Value Chain; Boston Consulting Group Matrix; Life Cycle Model; McKinsey matrix; ADL Matrix; "7-S" from McKinsey; resource-based approach.



However, the SWOT analysis results simply list the factors or the weights of the factors and there is still a gap between strategic analysis and strategic formulation. To narrow the gap, need to correlate and select strategies through S/O, W/O, S/T, W/T areas and, ideally, use Analytic Hierarchy Process (AHP) so that the non-quantitative events in system are converted to quantitative analysis. The AHP is integrated with SWOT analysis to determine priorities for the factors included in SWOT analysis and make them commensurable (Wang, Zhang, & Yang).

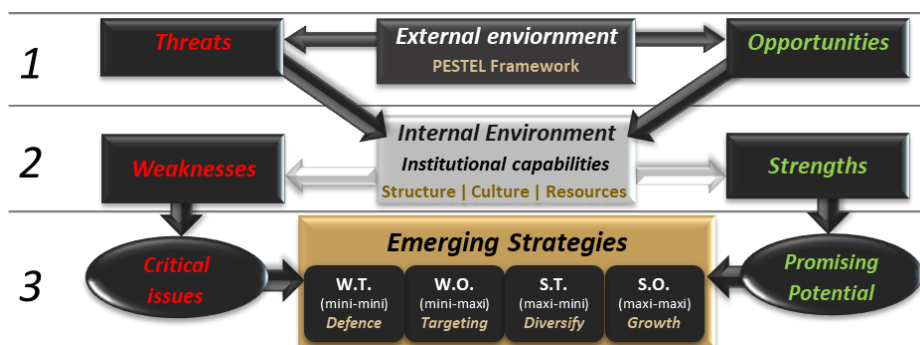
Still, from the plain correlation between key Strengths and Opportunities, Challenges can be drawn; between Strengths and Threats, Warnings can be found; from the intersection of Weaknesses and Opportunities, Risks can be identified; and from Weaknesses and Threats, Constraints can be extracted. With these correlations arises the concept of Dynamic SWOT analysis (DSA), also referenced as TOWS analysis by many researchers.



Scheme 4. Strategic Diagnosis. (a) Environment Scanning and (b) Dynamic SWOT Analysis (DSA)

The DSA process starts with the traditional SWOT matrix, but then upgrades the analysis and refines the outcome, moving it forward through several diagnostic and learning events into performance enhancing strategies and projects, by factor correlation (Dealtry, 1994).

The DAS can also be used to generate a number of possible alternative strategies as the external opportunities and threats facing a particular Institution can be matched with that organization internal strengths and weaknesses to result in four sets of possible strategic paths. This is a method for brainstorming to create alternative strategies that might not otherwise be considered as it forces strategic managers to create various kinds of growth as well as retrenchment strategies.



Scheme 5. Strategic Diagnosis

Such method development supports how the information gathered is used to support decision-making. The external environment interacts with the organisation's capabilities, producing a synthesis of critical issues and promising potentials. The combination of these dimensions constitutes the genesis of the main **emerging strategies** for: **Growth (SO), Diversify (ST), Targeting or Focus (WO) and Defence (WT)**.

3. METHOD

3.1. STAKEHOLDERS AND PROCEDURE

Each FIEP Member selected a topic from the given list of Threats or Security Challenges proposed and appointed Expert(s) accordingly, for developing the analysis and writing an academic article focused on that subject, to be integrated in this publication.

To ensure consistency among the stakeholders, a common structure and rationale for analysing the multiples Threats or Security Challenges was established.

For coordination, the Presidency of FIEP Association fostered the collaborative work among Experts, holding regular meetings every two weeks between January and April 2022.

3.2. DATA COLLECTION INSTRUMENT(S)

Scrutinizing and critically appraising, experts collect data from multiple noteworthy and reliable sources of information, either accessible to the public or reserved to institutions, ethically referencing them whenever possible, while ensuring information credibility and trustworthiness, as dictated by the best practices of writing scientific articles.

3.3. DATA PROCESSING TECHNIQUE(S)

Following the "Strategic Diagnosis" as research design and hermeneutics, the designated experts consider both qualitative and quantitative data to value and prioritise multiples sources of information, having current contextualization as a starting point, moving on to a forward-looking vision.

The papers are structured according to the methodology used for executing a "strategic diagnosis", organized in accordance with the following steps:

- *External environment analysis - by scrutinizing the changing exogenous environmental trends, considering opportunities and threats, mainly from an international perspective.*
- *Internal environment analysis - reflecting on the institutions' intrinsic characteristics and capabilities, considering their strengths and weaknesses – emphasizing, whenever appropriate, the characteristics of Gendarmeries and Police Forces with military status.*
- *The combination of the outcomes achieved, synthesizing and correlating the most relevant topics through a dynamic SWOT matrix.*
- *The analysis model allows to infer on the strategies to be adopted (growth, diversification, targeting and defence strategies).*
- *As a final product, a list of strategies is obtained, as well as recommendations for pursuing them.*

While developing the "strategic diagnosis", the experts:

1. *Choose key uncertainties;*
2. *Take a side and posit it as a "what-if" statement;*
3. *Identify early signals that this development could materialize;*



4. *Explore second-round effects through a handful of “if-then” statements for each “what-if” statement;*
5. *Infer implications for your particular policy area; and*
6. *Consider actions that could mitigate challenges and exploit opportunities.*

COMMON EXTERNAL ENVIRONMENT ANALYSIS: A SECURITY STRATEGIC FORESIGHT

This is a prospective empirical study, based on hypothetical-deductive reasoning, supported by documental analysis and triangulation of sources, with an eminently qualitative research strategy.

It is fundamental to conduct a full situational analysis before any strategy can be drafted.

In times of increasingly rapid change, growing complexity, and critical uncertainty, responsible governance requires preparing for the unexpected. Strategic Foresight is required whenever there is a high degree of uncertainty surrounding changes to the relevant future context.

Strategic foresight is a structured and systematic way of using ideas about the future to anticipate and better prepare for change. It is about exploring different plausible futures that could arise, and the opportunities and challenges they could present, so that those ideas can be used to make better decisions.

Strategic foresight does not attempt to offer definitive answers about what the future will hold. Foresight understands the future as an emerging entity that’s only partially visible in the present, not a predetermined destiny that can be fully known in advance (predicted). There are no hard facts about the future and the evidence base is always incomplete. The objective is not to ‘get the future right’, but to expand and reframe the range of plausible developments that need to be taken into consideration.

Foresight is an organizational competence that should be continually developed through training and practice, which includes multiple methods that can be complementary (IMF, 2021).

A strategic foresight can support policy-making in the following main ways (OECD, 2022):

- *Better anticipation: to better anticipate changes that could emerge in the future.*
- *Policy innovation: to reveal options for experimentation with innovative approaches.*
- *Future-proofing: to stress-test existing or proposed strategies and policies.*

Governments and organisations shall promote foresight exercises in high-level meetings between institutions so as to create collaborative decision making and policy ideas around them (OECD, 2020, p. 9).

The foresight toolkit includes horizon scanning for weak signals of emerging threats and opportunities, researching long-term trends and uncertainties, producing multiple manufactured narratives that illustrate how a future might play out (scenario planning), using back-casting to conceive paths to aspirational futures or alternatively using pre-mortem techniques to anticipate failure, and role-playing through policy gaming. Regardless of the specific tool employed, strategic foresight offers ways to “learn from tomorrow” (Édes, 2021).

Among other, the PESTEL analysis is a tool for developing horizon scanning and, therefore strategic foresight. PESTEL is an acronym for a tool used to identify the macro (external) forces and trends facing an institution. The letters stand for Political, Economic, Social, Technological, Environmental and Legal.

PESTEL analysis can be used as categorisation framework, while seeking for long-term trends and uncertainties in global reference documents, as it uncovers key drivers of various possible futures. (IMF, 2021).

Table 2. Global PESTEL Analysis based on key references⁶

Factors	Key Macro Trends	Implications for Security Forces
Political & Legal	<p>P.1. Shifts in the global order and demography: The world is becoming <u>increasingly multipolar</u>;</p>	<p>1. Growing instability demands increased readiness, as well as better and wider range of capabilities</p>
	<p>P.2. Global rivalry and fragility are likely to increase;</p>	<p>2. Increased demand for national and international cooperation among other security and defence actors</p>
	<p>P.3. Rival powers will jockey to shape global norms, rules, and institutions, while regional powers and nonstate actors may exert more influence and lead on issues left unattended by the major powers. These highly varied interactions are likely to produce a <u>more conflict-prone and volatile geopolitical environment</u>, undermine global multilateralism, and broaden the mismatch between transnational challenges and institutional arrangements to tackle them;</p>	<p>3. Increased demand for international engagements</p>
	<p>P.4. Accelerating shifts in military power, demographics, economic growth, environmental conditions, and technology, as well as <u>hardening divisions over governance models</u>, are likely to further ratchet up competition between great powers;</p>	<p>4. Increased demand for situational awareness and quick reaction, leads to improved intelligence capabilities</p>
	<p>P.5. Global power is shifting from advanced to emerging market and developing countries, while <u>non-state actors</u> and sub-national authorities are gaining national and international influence;</p>	<p>5. Growing complexity in predicting and reacting to incidents</p>
	<p>P.6. Multi-dimensional competition and <u>deep interdependencies</u> are likely to be defining features of an increasingly multipolar global order. Global governance and infrastructure are at risk of fragmentation due to intensified rivalries in a range of areas. More diverse and assertive actors with increasing capacities and aspirations are likely to appear. This includes non- and intra-state actors, as well as transnational movements. While no single player will be in a position to dominate all regions and policy domains, strategic dependencies and capacities will continue emerging and evolving;</p>	<p>6. Requirement for a robust and credible deterrence</p>
	<p>P.7. <u>Zones of instability</u> and conflict are likely to persist and may even grow;</p>	<p>7. Increased role of private actors in the security field</p>
	<p>P.8. Increase in the <u>prominence of non-state actors</u> domestically and internationally;</p>	<p>8. Increasing concerns for the Protection of Civilians</p>
		<p>9. Increased requirement for partnership</p>
		<p>10. Lack of trust in governments and institutions;</p>
		<p>11. More demanding border control tasks;</p>
		<p>12. The growing body of legal framework published in areas of interest for the operational activity and employment of the Security Forces implies a need for</p>

⁶ Main sources used:

- *Global Risks Report 2022 – 17th Edition*, from the World Economic Forum, taken from https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
- *2021 Serious and Organised Crime Threat Assessment*, from EUROPOL, taken from https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf
- *2021 Internet Organised Crime Threat Assessment*, from EUROPOL, taken from https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf
- *INTERPOL-UN Strategic Report on Environment, Peace and Security and the*
- *UNODC Transnational Organized Crime Threat Assessments*, from several reports available here: <https://www.unodc.org/unodc/data-and-analysis/TOC-threat-assessments.html>
- NATO "Strategic Foresight Analysis 2017 Report", taken from https://www.act.nato.int/images/stories/media/doclibrary/171004_sfa_2017_report_hr.pdf
- *Policy guidelines for the next European Commission 2019-2024*, taken from https://ec.europa.eu/info/sites/info/files/political-guidelines-next-commission_en.pdf and *European Commission's 2021 strategic foresight report*, taken from https://ec.europa.eu/info/strategy/strategic-planning/strategic-foresight/2021-strategic-foresight-report_en#key-global-megatrends-that-will-impact-the-eu-in-the-future
- *Global Trends 2040: a more contested world*, publication of the USA National Intelligence Council, taken from https://www.dni.gov/files/ODNI/documents/assessments/GlobalTrends_2040.pdf
- *OECD Government Foresight Community - Annual Meeting Report 2020*, *Strategic foresight for future-ready public policy*, taken from <https://www.oecd.org/strategic-foresight/ourwork/OECD%20GFC%20Annual%20Meeting%20Report%202020.pdf>
- *CSDP 2020 report*, taken from https://www.clingendael.org/sites/default/files/2020-04/CSDP_Report_April_2020.pdf



	<p>P.9. <u>Large-scale misinformation</u>, powered by new tools and online platforms, will pose increasing challenges to democratic systems and drive a new type of information warfare;</p> <p>P.10. Return of power politics and tensions/conflicts with potential increase in global and regional conflicts and tensions (USA-Russia-China);</p> <p>P.11. Increasing threats from organised crime, corruption, extremism, terrorism, and hybrid threats, including the instrumentalization of migration for political purposes, and increasingly threaten our security;</p> <p>P.12. Growing discontent with current political structures and increasing <u>importance of non-state actors</u> in matters impacting security;</p> <p>P.13. Growing preponderance of supra-state actors with influence over states' policy decisions;</p> <p>P.14. Increasing global trend towards the "<u>militarization</u>" of police forces, which tend to be more robust to face internal and external threats;</p> <p>P.15. Crisis management under the aegis of International Organizations grows globally, with the use of integrated/comprehensive approaches;</p> <p>P.16. Gap between current policies across many jurisdictions and new biodigital capabilities arising through new products, platforms, services, and industries;</p> <p>P.17. International regulations shape internal legislation</p> <p>P.18. Data protection laws tend to become more restrictive</p>	<p>training and specialisation of each organisation;</p> <p>13. The need to implement strategic management mechanisms and instruments in the Security Forces that enable monitoring and control of the activity developed during a specific time frame;</p> <p>14. Considering the political effort and programmatic objectives established in the area of security, there will be a tendency for the Security Forces to be held accountable regarding the registered crime rates, traffic accidents rates and the overall feeling of security;</p> <p>15. Need for timely information sharing between national security forces and international security organisations;</p>
<p style="writing-mode: vertical-rl; transform: rotate(180deg);">Economic</p>	<p>E.1. The coming decades will be marked by an increasing redistribution of global power, with its geo-economic centre of gravity shifting eastwards;</p> <p>E.2. Financial linkages between countries have grown sharply, the rise of integrated supply chains and product fragmentation have changed the nature of trade, and improvements in information and communication technology have broadened access to information;</p> <p>E.3. Most national debts are rising, while a more complex and fragmented trading environment, a shift in trade, and new employment disruptions are likely to shape conditions within and between states;</p> <p>E.4. Many governments may find they have reduced flexibility as they navigate greater debt burdens, diverse trading rules, and a broader array of powerful state and corporate actors exerting influence;</p> <p>E.5. Asian economies appear poised to continue decades of growth through at least 2030;</p> <p>E.6. Increased inequalities, lower environmental and labour standards remain key challenges for emerging economies;</p> <p>E.7. The global employment landscape will continue to shift because of new technologies, notably automation, online collaboration tools, artificial intelligence (AI) and additive manufacturing;</p> <p>E.8. Growing urbanisation of the most developed countries, with the probable exacerbation of disputes over control of resources;</p> <p>E.9. The digital age will also influence payment, means and capital markets, with a growing role of crypto-assets and the development of digital currencies;</p> <p>E.10. Decreased investment in the security and defence sector among NATO countries, contrary to what has been seen in other regions of the world;</p>	<p>1. Development of multilateral programmes between states to share resources in specific areas (Example: Border control);</p> <p>2. Decrease in available manpower and resources in the Security Forces;</p> <p>3. To render the Security Forces more efficient with the available resources;</p> <p>4. Develop programmes aimed at tackling and preventing corruption within the Security Forces;</p> <p>5. Carry out multilateral research and development programmes of resources and equipment with common use within the Security Forces;</p> <p>6. The increase in economic inequalities increases phenomena related to crime against property;</p> <p>7. Need to establish a contingency plan that allows security forces to carry out their mission in the event of a shortage of resources;</p> <p>8. Need to adapt the way to provide security, due to the increase use of online collaboration tools and AI.</p>

	<p>E.11. Pandemic (COVID-19) dictates contraction of the record economy, and the resumption of economic growth "will exponentially increase demand for scarce natural resources", potentiating the emergence of new conflicts;</p> <p>E.12. Securing and diversifying supply of critical raw material is key as the increase in demand is expected to coincide with an upturn in the major suppliers' readiness to impose export restrictions.</p>	
<p style="writing-mode: vertical-rl; transform: rotate(180deg);">Social</p>	<p>S.1. Within societies, there is increasing fragmentation and contestation over economic, cultural, and political issues. Decades of steady gains in prosperity and other aspects of human development have improved lives in every region and raised people's expectations for a better future. As these trends plateau and combine with rapid social and technological changes, large segments of the global population are becoming wary of institutions and governments that they see as unwilling or unable to address their needs;</p> <p>S.2. People are gravitating to familiar and like-minded groups for community and security, including ethnic, religious, and cultural identities as well as groupings around interests and causes, such as environmentalism. The combination of newly prominent and diverse identity allegiances and a more siloed information environment is exposing and aggravating fault lines within states, undermining civic nationalism, and increasing volatility;</p> <p>S.3. At the same time that populations are increasingly empowered and demanding more, governments are coming under greater pressure from new challenges and more limited resources. This widening gap portends more political volatility, erosion of democracy, and expanding roles for alternative providers of governance;</p> <p>S.4. Shifts in the global order and demography: The world's population will reach 8.5 billion in 2030 and 9.7 billion in 2050, causing increased divergence and greater scarcity of resources;</p> <p>S.5. Growing globalisation, with increasing population, migratory flows and fracturing of national identities;</p> <p>S.6. Growing ethnic polarisation and religious extremism;</p> <p>S.7. Growing trend towards security challenges related to climate, food and access to water;</p> <p>S.8. Widening demographic asymmetries, which may threaten regional stability and increase the risk of conflicts;</p> <p>S.9. Criminal activities subsidize warring entities and there is growing complexity in combating organized crime;</p> <p>S.10. Growing connectedness, complexity and dynamics of information, with greater demand for transparency from state agents;</p> <p>S.11. Pandemic by COVID-19 globally affecting the population's sense of well-being (lowest in the last 40 years), accentuating all social, economic, regional and ethical inequalities, among others, also with a disruptive impact on labour markets, with massive job losses, which may result in a long-term cascading effect;</p> <p>S.12. COVID-19 brought the realisation that we depend on our neighbours, personally and internationally;</p> <p>S.13. Globalised workforces working together, realising they share global challenges;</p> <p>S.14. COVID-19 brought much more flexibility in work conditions, especially for those who can work from anywhere, with telework becoming the norm, but with dedicated physical meetings and intentionally re-created informal spaces for connection in the workplace;</p> <p>S.15. Collective intelligence is changing, and governments are playing catch-up.</p>	<ol style="list-style-type: none"> 1. More demanding tasks due to instability and migration; 2. Resources need to be adjusted to increasing urbanization; 3. Developing specific policing programmes targeted at the urban environment in accordance with the principles of social inclusion, human rights, protection of particularly vulnerable victims and prevention of drug use and trafficking in partnership with the local actors; 4. Intervention challenges faced with the mismatch between national culture and the customs and traditions of the different migrant communities settled in each state; 5. Promote training activities in the security forces with the aim of raising awareness and developing multicultural competences that increase the probability of successful interaction with different communities; 6. The increase in phenomena related to organised crime calls for concerted action between the different police forces with legal competence to intervene; 7. The new criminal phenomena require permanent articulation between the Security Forces and the Judiciary Authority; 8. Increased threats to critical infrastructures; 9. All actions can become immediately known and publicly scrutinized, demanding for a transparent and error-free action.



Technological

- | | |
|---|---|
| <p>T1. Digital hyperconnectivity and technological transformations: The number of connected devices globally might increase from 30.4 billion in 2020 to 200 billion in 2030. Increased connectivity of objects, places and people will result in new products, services, business models, and life and work patterns;</p> <p>T2. States and public organisations have lost their monopoly on technology;</p> <p>T3. Digital sovereignty will depend on capacity to store, extract and process data, while satisfying the requirements of trust, security and fundamental rights;</p> <p>T4. Big data and advanced analytics are evolving rapidly;</p> <p>T5. Technologies are being invented, used, spread, and then discarded at ever increasing speeds around the world, and new centers of innovation are emerging;</p> <p>T6. During the next two decades, the pace and reach of technological developments are likely to increase ever faster, transforming a range of human experiences and capabilities while also creating new tensions and disruptions within and between societies, industries, and states;</p> <p>T7. State and nonstate rivals will vie for leadership and dominance in science and technology with potentially cascading risks and implications for economic, military, and societal security;</p> <p>T8. Strengthening capacity in data management, artificial intelligence and cutting-edge technologies is key at state, institutional and personal levels;</p> <p>T9. Artificial Intelligence (AI) will confer strong advantages to countries that incorporate AI into their military systems. AI will enhance the performance of existing weapons, defences, and security systems, both physical and cyber, while counter-AI techniques, designed to negate or confuse AI decision making, also are likely to emerge;</p> <p>T10. Easy access to information and new communication dynamics with exponential growth, to which informal structures tend to adapt faster than public instruments;</p> <p>T11. The digital leap is part of an acceleration of technological change and hyperconnectivity, and this phenomenon has been further exponentiated by the COVID-19 pandemic;</p> <p>T12. Worldwide growth in the use of the Internet, with an increase in cyber-threats;</p> <p>T13. Data markets are becoming regulated;</p> <p>T14. The metaverse, an interconnected virtual platform where the majority of human interaction, for business or leisure, takes place, shall further transform our societies. Technology companies provide the hardware and software. States control what hardware and creative freedoms are afforded to their citizens within the virtual universe. Diplomacy is more important and more complex than it has ever been, as relationships between states, platform companies, and users need to be managed.</p> | <ol style="list-style-type: none">1. Involves the understanding and establishment of Intelligence-Led Policing;2. Considering the information that exists in the IT platforms within the security forces, these platforms become an attractive target for cyber attacks which will entail expenses and a reinforcement of the security protocols of these databases;3. Need to redirect the internal structure of each the Security Force in order to deal with criminal phenomena perpetuated through the use of technological tools;4. A need to introduce and apply tools that enable the processing of huge amounts of information with potential use in police activity;5. Imperative to enhance the use of non-lethal and develop an array of intermediate weapons as instruments of the use of force in police action;6. The use of AI by society in general, will deeply chance the way police activity is made. |
|---|---|

Environmental

<p>En.1. Climate change and other environmental challenges: Global warming will probably surpass 1.5°C in the next 20 years and head towards 2°C by mid-century, worsening the pressure on water and food safety worldwide. By 2050, 200 million people will be in need of humanitarian assistance partly due to ecological effects;</p> <p>En.2. The physical effects of climate changing are likely to gradually intensify during the next two decades;</p> <p>En.3. Growing scarcity of resources (namely water) and increasing global inequity;</p> <p>En.4. Extreme weather events increase the risk of more environmentally-induced migration;</p> <p>En.5. Attitudes toward “green” or ecological products;</p> <p>En.6. Debate will increase over how fast certain measures should be implemented;</p> <p>En.7. Governments impose regulations to fight climate change;</p> <p>En.8. Increasing frequency and impact of environmental disasters, with global amplification of the repercussions;</p> <p>En.9. The increased likelihood of extreme weather events, future pandemics, other natural and man-made disasters as well as regional conflicts reaffirms the need for a stronger response and cooperation on security, civil protection and defence, including to improve prevention, preparedness and response to disruptions.</p>	<ol style="list-style-type: none"> 1. The physical impacts of climate change are likely to lead to an array of human security challenges, primarily but not exclusively in developing countries in the near term; 2. Increase the effort on border and migration control; 3. Increasing instability, forcing police readiness; 4. Increase possibility for social conflicts; 5. Adapt resources, equipment and weapons in alignment with the overall decarbonisation objectives; 6. Major climate events (storms, floods, etc...) will force security forces to divert more resources to disaster relief, home and even abroad.
--	---



RESEARCH PAPERS LIST

Table 3. Research Papers List

N.	THREAT OR SECURITY CHALLENGE	FIEP MEMBER	PAGE
I	Cybercrime and cyberthreats Lieutenant Miguel Espejel	Spain	24
II	Propaganda and misinformation Colonel Sorin Despina	Romania	34
III	Climate changes and natural disasters Professor Elif Çolakoğlu	Türkiye	48
IV	Disputes over scarce natural resources Major Alfredo Orlando & Captain Angel Frias	Argentina	70
V	Fragile states and regional conflicts Lieutenant Ghada A. Temeiza	Palestine	82
VI	Energy insecurity Colonel Huessin Salem Al hajaya	Jordan	88
VII	Critical Infrastructures Major Ricardo Bailote & Major José Lopes	Portugal	94
VIII	Migratory phenomena Multiple Authors	The Netherlands	112
IX	Human trafficking Captain Mariétou Diop	Senegal	128
X	Terrorism Colonel Major Saber Souidi	Tunisia	140
XI	Transnational criminal networks Major Abdoul-karim Ibrahim Youssouf	Djibouti	152
XII	Counterfeiting (documents, pharmaceuticals, goods and products, digital contents) Lieutenant Colonel Abdessamade Chaid	Morocco	164
XIII	Trafficking of arms Captain Nicolás Valenzuela Urzúa & Felipe Cortés Aburto	Chile	172
XIV	Environmental crime Lieutenant Colonel Marina Bizzotto & Julian Colamedici	Italy	184
XV	Health (pandemic) Captain Sébastien Cassoré	France	194
XVI	CBRN Lieutenant Colonel Waleed Anwar	Kuwait	210

I. PAPER | CYBERCRIME AND CYBERTHREATS

Citation:

Espejel, M. Cybercrime and Cyberthreats. Overcoming Security Threats arising from Globalization 4.0 – FIEP Association, 2022

Published: October 2022

Publisher's Note: FIEP stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors.

Spain

Guardia Civil

Miguel Espejel

mespejel@guardiacivil.es

Abstract: In the last twenty years, there has been a great technological development. In addition to allowing an increase in the quality of life of citizens, this has also meant an increase in threats and crimes that make use of cyberspace.

This article defines the current environment of defence against cyber threats and cybercrime, making a strategic analysis of the capabilities that law enforcement agencies generally have. For this purpose, different tools typical of strategic analysis are used, such as PESTEL analysis, the McKinsey 7s model and the use of the SWOT matrix. Subsequently, strategies for enhancing the capabilities of the security forces are established with the help of the dynamic SWOT matrix.

The strategies finally chosen are based on improving public awareness, training law enforcement agents in cyberspace, increasing law enforcement equipment and boosting international judicial coordination.

Keywords: cybercrime; cyberthreat; technology; internet; computer.



1. INTRODUCTION

Globalization and advances in the field of technology have brought the world new opportunities but also new threats. In this publication, all the threats and crimes related to the cyber environment are going to be analysed to improve the understanding about their origin and their consequences.

As everyone implemented computers in all aspects of life, including the business world, criminals realized how profitable their actions could be with the use of these machines. Starting in the early stages of computers and internet, criminals exploited this new opportunity and started to adapt the traditional scams to the cyberspace. In the eighties, the first malware was detected and since then, the number and complexity of both scams and malware production has increased exponentially in a way that back then was unimaginable.

Due to this quantity and complexity, it is important to carry out a detailed analysis on what the main threats are nowadays and how they can be countered. To do so, this publication will focus on defining them, studying their consequences and establishing the best practices to counter them.

As the threats did increase, not only the technical measurements had to improve but the legal framework had too. In 2001, the Council of Europe drawn the Convention on Cybercrime, also known as the Budapest Convention on Cybercrime. This convention has nowadays been ratified by 66 countries (as of March 2022) and has meant that the states have had to include in their legislation all the crimes described in the text and all the tools for combating cybercrime.

The Budapest Convention the following crimes to be included in the countries' legislation:

- *Illegal access*
- *Illegal interception*
- *Data interference*
- *System Interference*
- *Misuse of devices*
- *Computer-related forgery*
- *Computer-related fraud*
- *Offences related to child pornography*
- *Offences related to infringements of copyright and related rights*

After the countries started to give priority to these threats, a lot of studies started to be carried out about the topic and currently even the most important organizations and agencies of the policial world, including Interpol, Europol and FIEP, have spent a lot of their resources on efficiently studying this phenomenon and establishing the best practices for combating cybercrime.

With Europe being one of the main technological developers, one of the publications for reference in this field is the one produced by Europol, as it does not only include the European Union member states but all of the European agency's partners. The Internet Organised Crime Threat Assessment (IOCTA) is published every year, and it is Europol's flagship strategic product that provides a law enforcement focused assessment of evolving threats and key developments in the area of cybercrime.

In the IOCTA, the approach to the problem is from the cybercrime perspective, organizing the document in four groups: Cyber-dependent crime, child sexual abuse material, online fraud and Dark Web. In contrast to the approach chosen by Europol, this publication will take a broader view, looking not only at cybercrime but also at other cyberthreats not directly related to the criminal framework, discussing concerns about threats related to military technologies, biotechnology advances or the interconnection of the data.

2. MATERIALS AND METHODS

This study is going to analyze how the cyber environment is now and how cyberthreats and cybercrime can be countered. To do this, the method that is going to be used is based on hypothetical-deductive reasoning, supported by documental analysis and triangulation of sources.

In a first part, endogenous and exogenous strategic environments are going to be analysed using the same methods as other articles of this publication. Starting with a PESTEL analysis where the factors that affect the Political, Economic, Social, Technological, Environmental and Legal aspects of the cyberthreats are going to be defined.

After that, the SWOT matrix analysis is going to be used to determine whether these factors are strongening or weakening the countries in the combat of cyberthreats and cybercrime, and what areas must be reinforced or can be disattended for now. Later, that matrix will be transformed into a dynamic SWOT matrix, to help define the strategies to adopt.

In the end, the information gathered and processed in the earlier stages, will be used to define the best strategics to follow to successfully counter cyberthreats and cybercrime according with the actual situation.

3. RESULTS

3.1. External environment analysis

Table 4. PESTEL Analysis | Cybercrime and cyberthreats⁷

Factors	Key Macro Trends	Implications for Security Forces
Political & Legal	P.1. Global rivalry and fragility are likely to increase	1. Growing rivalry between states increases the number of cyberattacks enabled by national institutions
	P.2. Spending on technology development is increasing globally by the states	2. More medias will be available for the security forces
	P.3. States are increasingly interested in having as much data as possible on anyone who is or may be connected to them	3. Increased complexity in cybersecurity of the data owned
	P.4. The control of communications networks becoming strategic priority for states.	4. More data to analyze means more useful results but more resources spent in the analysis
	P.5. Tightening of data protection policies in the western countries	5. Communication networks become more and more sensitive in the context of critical infrastructures
	P.6. Conflict between Ukraine and Russia will increase instability between western and eastern countries	6. More security on communication networks must be implemented
	P.7. Technologies are being used more and more in critical infrastructures	7. Data collection and storage will be more delicated 8. Increased threats on critical infrastructures, needing to spend more resources in their defence

⁷ Main sources used:

- 2021 Internet Organised Crime Threat Assessment, from EUROPOL, taken from https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf
- 2021 Serious and Organised Crime Threat Assessment, from EUROPOL, taken from https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf
- INTERPOL cybercrime threat response documents, taken from <https://www.interpol.int/Crimes/Cybercrime/Cybercrime-threat-response>
- NATO "Strategic Foresight Analysis 2017 Report", taken from https://www.act.nato.int/images/stories/media/doclibrary/171004_sfa_2017_report_hr.pdf



<p style="writing-mode: vertical-rl; transform: rotate(180deg);">Economic</p>	<p>E.1. The importance of economics over other aspects will continue growing</p> <p>E.2. States with national debts from other states will want to take advantage of their investment</p> <p>E.3. Companies are going to gain more power within the states where they have their headquarters</p> <p>E.4. Cryptocurrency will gain importance and more people and states will start using and accepting it</p> <p>E.5. Public and private banks will try to stop the increase on the use of cryptocurrency</p> <p>E.6. Another global financial crisis is going to affect at least the western countries</p> <p>E.7. Rebuilding of Ukraine is going to benefit the economic situation of the countries involved</p>	<ol style="list-style-type: none"> 1. More efforts will be made to curb economic threats 2. Public funds spent on security forces will be reduced 3. Need to establish a contingency plan that allows security forces to carry out their mission in the event of a shortage of resources 4. Investigation of corruption cases will have to be improved and/or increased 5. Investment in the field of cryptocurrency investigation and security will be needed 6. Creation or adaptation of the economic structure to include cryptocurrency for both payment and seizure.
<p style="writing-mode: vertical-rl; transform: rotate(180deg);">Social</p>	<p>S.1. Increased life expectancy</p> <p>S.2. Rise of extreme liberal movements, with trends like the “you only live once” as excuses to assume more risks and breaking laws</p> <p>S.3. Transmission of the importance of social life to social networks</p> <p>S.4. Education in computers field oriented to use technologies, not to know how they work</p> <p>S.5. Technologies getting more and more complex difficult the individuals to know about everything, making them specialize in a field but ignoring the others</p> <p>S.6. Increase in protests by society, any difference of thought with the government is met with an act against it.</p> <p>S.7. The identity of individuals is becoming a priority. Biometric recognition, personal data, etc.</p>	<ol style="list-style-type: none"> 1. While the average age of citizens is increasing, they are unwilling to learn new things after a certain age, such as technology, which increases the risks they take without knowing them 2. People are usually giving personal data to untrusted services on the internet. When a crime takes place, or a security breach is discovered they don't think that it is related to that data given 3. As people increasingly publicly reflect their lives on social networks, criminals can obtain free information about their victims from open sources 4. Technologies are being used more widely but without a thorough understanding of how they work, which greatly increases the scope for attacks 5. Changes should be made to the structure of the security teams. It used to be possible to have many people working on individual cases, but now teams of specialised individuals must be set up to work on cases together 6. Increased hacktivism. More resources spent on prevention, defence and remediation 7. Increased importance of personal and biometric data, leading to increased criminal interest in identity theft
<p style="writing-mode: vertical-rl; transform: rotate(180deg);">Technological</p>	<p>T.1. Increased quantity of connected devices.</p> <p>T.2. Digital sovereignty will depend on capacity to store, extract and process data, while satisfying the requirements of trust, security and fundamental rights</p> <p>T.3. Research into new computing technologies that can make old ones obsolete</p> <p>T.4. Modern cryptography will be destroyed by the development of quantum computing, creating a mismatch between users of traditional computers and users of quantum computers.</p> <p>T.5. Continued develop of metaverse with unknown consequences and threats</p> <p>T.6. Criminals are always a step ahead states in the new technologies field</p>	<ol style="list-style-type: none"> 1. More attack vectors for criminals to use 2. Complex implementation of new technologies to work with citizens' data 3. Much greater adaptability will be needed to be able to implement all technological developments in time 4. Research in the metaverse will become more important and new techniques and protocols will have to be established to combat crime in the metaverse. 5. Need for spending on police research in the field of new technologies

Environmental	<p>EN.1. Concerns about the environmental impact of technologies due to their power usage are increasing in the western countries</p> <p>EN.2. States are pushing renewable sources of energy, focusing on their development but not on their security</p>	<p>1. Criminals and national enabled actors from the eastern countries will have easier access to more power-demanding and powerful technologies</p> <p>2. Critical infrastructures related to the generation of energy will be more vulnerable</p>

3.2. INTERNAL ENVIRONMENT ANALYSIS

After analysing the external factors affecting cyberthreats and cybercrime, it is needed to analyse what the actual state of law enforcement to combat them. To do so, the study will be using the McKinsey 7S Model which focuses on determining Structure, Strategy, Systems, Skills, Style, Staff and Shared values.

3.2.1. STRUCTURE AND STRATEGY

Both, structure and strategy are going to be studied at the same time as they are closely linked in the cybersecurity field and are going to be analysed as the standard that is being followed by states, no law enforcement specific structures and strategies are going to be explained for security reasons.

The defence against cyberthreats is a matter covered by cybersecurity. In this field, threats are defined as a malicious act that seeks to damage data, steal data, or disrupt digital life in general. In order to defend against cyberthreats, there are four strategies which will force to have a structure divided in four types of specialists.

The first strategy is Prevention: it requires hardening specialists and the development of administrative policies, standards, procedures and guidelines aimed at making it more difficult to exploit threats. As for hardening we understand the collection of tools, techniques, and best practices to reduce vulnerability in technology applications, systems, infrastructure, firmware, and other areas. The goal of hardening is to reduce security risk by eliminating potential attack vectors and condensing the system's attack surface.

The second strategy is Detection: it is the practice of holistically analyzing the entirety of an organization's security stance and IT ecosystem to identify any malicious activity or vulnerability that could compromise the network. Mitigation efforts ought to be enacted upon detecting threats to neutralize them properly. To achieve this, controls must be put in place to verify that systems are functioning as intended and expected. In case of non-conformity with the usual operation for no known reason, the event should be investigated to determine whether it is part of an attack. It requires specialists. It requires specialists with a high level of knowledge of the system who can detect not only the most obvious abnormalities, but also any deviation from normality.

The third strategy is Response (or Incident Response): is an organized approach to addressing and managing the aftermath of a security breach or cyberattack, also known as an IT incident, computer incident or security incident. The goal is to handle the situation in a way that limits damage and reduces recovery time and costs. It is usually done by a team of specialists (or organization) with is commonly called computer security incident response team (CSIRT).

The fourth and last strategy is Recovery: it is defined as the need to develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cyber security event. Digital forensic specialists must be employed in this strategy, as they are the experts in tracking evidence to determine the source of the attack.



3.2.2. SYSTEMS

The organisation of systems in terms of cyber-security varies greatly, depending on the needs of each company or organisation. In the case of state structures there are also differences depending on the importance of the system for the functioning of the state. For example, in cases where critical infrastructure is involved, it is most common for the state to establish minimum standards of protection against cyber threats that are reflected in state legislation. In this respect, there is a strong culture of cybersecurity in the West and there are many standards in terms of security in the organisation of systems. One of the leading institutes in the development of these standards is NIST.

3.2.3. SKILLS

Within the defence against cyber threats and the fight against cybercrime, law enforcement agencies have different effectiveness. Normally, the most serious crimes are well responded to, as the group of experts dedicated to these types of investigations can spend the required time because there are fewer cases. However, when the simplest crimes, such as a simple email scam, are of a minimal technical nature, the effectiveness of the investigation decreases dramatically. This is because the number of specialist (not expert) staff is not large enough to combat the large number of cybercrimes that occur.

3.2.4. STYLE

The style normally followed in the security forces is a very defined hierarchy. In the specific case of the Gendarmeries and Police Forces with military status, this rigid hierarchy is even more visible. Although there is this more traditional rigidity, the style of command that has been adopted in recent years is focused on the figure of the leader, who takes advice from his subordinates but ultimately makes the decision that he believes to be most appropriate according to his own criteria.

3.2.5. STAFF

Most commonly, law enforcement agencies have few experts in the field of cybersecurity and cybercrime. These experts usually deal with the most complex threats and crimes, but for most cases there are less specialised staff. This is usually due to the fact that in the private business world, experts in this field are generally much more highly valued. Behind these top experts, there are specialised echelons who, without being considered experts, are highly capable of dealing with the most common threats and crimes very effectively. In contrast to the expert staff, specialists are sufficiently highly valued within law enforcement and are provided with training so that they can at some point be considered experts.

3.2.6. SHARED VALUES

Security forces have similar values in all countries. Analysing the Gendarmeries and Police Forces with military status, among the main values, the following can be highlighted:

- *Honour: Is the idea of a bond between an individual and a society as a quality of a person that is both of social teaching and of personal ethos, that manifests itself as a code of conduct, and has various elements such as valour, chivalry, honesty, and compassion.*
- *Sacrifice: Danger or serious work to which a person is subjected, an act of self-sacrifice inspired by a sense of duty. It means subordinating one's own life or well-being for the sake of others.*
- *Loyalty: Compliance with the demands of fidelity and honour.*
- *Austerity: Moderation of the senses and passions in the face of higher goals such as the performance of duty.*



- *Discipline: Doctrine, instruction of a person. The meaning implies the observance of principles of obedience that only knows the moral limit of honour and the material limit of the Law.*
- *Abnegation: Sacrifice of one's will, affections or interests, usually for professional reasons or altruism.*
- *Beneficent spirit: Benefactor, doing good to others. Considering the needs of others above one's own.*



3.3. SWOT analysis

Table 5. SWOT analysis | Cybercrime and cyberthreats

Internal factors	Strengths (S)	Weaknesses (W)
	<ul style="list-style-type: none"> ▪ Law enforcement personnel are committed to fighting cybercrime ▪ There is a high level of expertise in the fields of investigating the most complex cybercrimes ▪ Law enforcement agencies have privileged access to data held by agencies and companies ▪ With a warrant from the judicial authorities, they have access to measures restricting fundamental rights, for example to personal data. 	<ul style="list-style-type: none"> ▪ Rewards for cyberspace experts need to be improved ▪ More resources have to be spent in training not only specialists but also experts ▪ Cybercriminals have no working hours ▪ Cybercriminals don't have the same problems as law enforcements to get things done in other
External factors		
Opportunities (O)	<ul style="list-style-type: none"> ▪ Create more specialists in cybercrime field to investigate the simplest crimes ▪ Provide law enforcement with more equipment so that 100% of available personnel capacities can be utilised 	<ul style="list-style-type: none"> ▪ Use the increased budget to cover 24 hours a day in the fields where it is required and to improve the training of law enforcement agencies ▪ Improving rewards in cybercrime research stations
Threats (T)	<ul style="list-style-type: none"> ▪ Promote international judicial cooperation by building on relations between law enforcement agencies and judges ▪ Dedicate resources to raising public awareness 	<ul style="list-style-type: none"> ▪ Increase public awareness efforts ▪ Raise awareness among the rest of the administration on the importance of the fight against cybercrime and the increase of the budget dedicated to it
<ul style="list-style-type: none"> ▪ The attack surface is increasing because of both quantity and quality reasons. ▪ The complexity of technologies is increasing and people need to become more expert in just one field ▪ States are not investing enough resources on the cyberspace ▪ Cybercriminals are always one step ahead in the use of technologies ▪ Despite efforts in international cooperation at the police level, there is still great slowness in judicial procedures for international cooperation 		

3.4. STRATEGIES

Once the SWOT matrix is done, to establish strategies to be followed to enhance strengths and minimise threats, it is interesting to transform this matrix into a dynamic SWOT matrix, where strengths and weaknesses are combined with opportunities and threats.



Figure 2. Keys Strategies | Cybercrime and cyberthreats

4. CONCLUSIONS & RECOMMENDATIONS

As the results of the strategic analysis indicate, there are many ways to increase efficiency in the fight against cyber threats and cybercrime.

The strategies proposed in the dynamic SWOT matrix are as follows:

1. *Create more specialists in cybercrime field to investigate the simplest crimes;*
2. *Provide law enforcement with more equipment so that 100% of available personnel capacities can be utilised;*
3. *Use the increased budget to cover 24 hours a day in the fields where it is required and to improve the training of law enforcement agencies;*
4. *Improving rewards in cybercrime research stations;*
5. *Promote international judicial cooperation by building on relations between law enforcement agencies and judges;*
6. *Increase public awareness efforts;*
7. *Raise awareness among the rest of the administration on the importance of the fight against cybercrime and the increase of the budget dedicated to it;*



As can be seen, the areas where there is room for improvement are training, public awareness, materials and international judicial coordination.

Although these are areas for improvement already known to all law enforcement agencies, the importance of the fight against cyberthreats and cybercrime still needs to be emphasised, as priority is still given to other areas such as the fight against drug trafficking or crimes against property.

It is therefore advisable to continue to insist in all possible forums on the needs arising from the protection of cyberspace. Although improvements have already been made and the visibility of this problem has increased, there is still a long way to go.

II. PAPER | PROPAGANDA AND MISINFORMATION

Citation:

Despina, S. Propaganda and misinformation. Overcoming Security Threats arising from Globalization 4.0 – FIEP Association, 2022.

Published: October 2022

Publisher's Note: FIEP stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors.

Romania

Jandarmeria Romana / Romanian Gendarmerie

Sorin Despina



sorin.despina@yahoo.com

Abstract: Probably misinformation appeared with the occurrence of human communication and it took on various forms of manifestation - rumor, diversion, propaganda or more recently fake news. It has grown exponentially with the advancement of technology and the diversification of mass communication and data transmission channels. In post truth age, when communication technologies and artificial intelligence are amplifying the spread of fake news, with no interpose until the end consumer, communication passing from consumer to consumer, it is increasingly clear that the collective effort to tackle disinformation must be doubled by an individual effort of correct information.

Keywords: misinformation, propaganda, law enforces agencies



1. INTRODUCTION

In the context of contemporary conflicts, information, properly exploited and managed can decisively contribute to winning a war. The conflicts of the future will ultimately revolve around manipulating information and changing human behavior, without firing a gun.

To satisfy the “thirst” of information, modern human being uses the “vectors” of transmitting it - newspapers, magazines, radio-TV, INTERNET, etc. - becoming unconsciously increasingly dependent on them and giving them high credibility. This addiction is a great opportunity to manipulate information.

According to Toffler, the Gulf War was the end of the “Industrial Age War” and the beginning of the “Information Age War”.

In his work “Subversion”, Roger Muchielli states that “modern warfare is primarily psychological” and, at the same time, he seems to have become aware of a radical transformation in the art of war.

About information as support for psychological action:

- it implies the presence of three variables in which one cannot have absolute confidence: the informant, the means of communication, the informed;
- information never contains one hundred percent truth;
- whatever one might think, not only that there is no objectivity in terms of information, but any claim to objectivity must be treated with suspicion (objectivity exists only in scientific information);
- it is natural for each witness to have his/her own impression of the event he/she attended;
- one can notice that the information is in itself a distorted product; there will be the temptation to distort it even more.

And so, we came to DIS-INFORMATION.

Misinformation is a term that has recently appeared in the specialized language, although it has been practiced since antiquity. It is inextricably linked to information, which may be flawed in the name of well-defined purposes. Almost any information is at risk of misrepresentation. It follows that: information never contains one hundred percent truth. The term disinformation first appeared in Russian after World War II, and was intended to refer to “exclusively capitalist practices aimed at enslaving the masses of the people”. Hence the term in English means “misleading deliberate information leak”.

2. THEORETICAL AND CONCEPTUAL FRAMEWORK

Although fake news is a frequently used term, *misinformation*, *disinformation*, and *malinformation* represent more adequate terms.

The term “fake news” is increasingly regarded as inadequate, a recent study of thirty-four academic papers (Tandoc et al, 2017) concluded that “fake news” encompasses a wide range of phenomena: news satire, news parody, fabrication, manipulation, advertising, and propaganda. Moreover, “fake news” is misleading, as it is also increasingly used by politicians “to describe news organisations whose coverage they find disagreeable. In this way, it’s becoming a mechanism by which the powerful can clamp down upon, restrict, undermine and circumvent the free press.” (Wardle & Derakhshan, 2017). A French report (Jeangène Vilmer et al, 2018) by the French Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the French Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces argues for “substituting the vague and controversial notion of “fake news” for the more precise term, “information

manipulation". The latter is understood as the intentional and massive dissemination of false or biased news for hostile political purposes."

Therefore, instead of "fake news" we adopt the *information disorder* theoretical framework (Wardle, 2017; Wardle & Derakshan, 2017), which defines three types of false and/or harmful information:

- **Mis-information:** false information that is shared inadvertently, without meaning to cause harm.
- **Dis-information:** intending to cause harm, by deliberately sharing false information.
- **Mal-information:** genuine information or opinion shared to cause harm, e.g. hate speech, harassment.

TYPES OF INFORMATION DISORDER

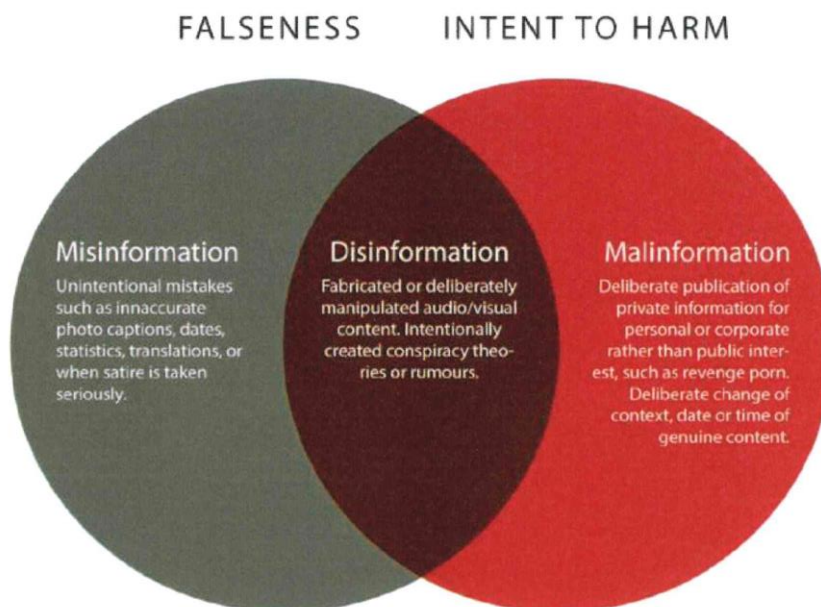


Figure 3. Types of information disorder

Source: (Wardle & Derakshan, 2017)

In practice, it is difficult to make a difference between mis- and dis-information, as the intention of the information source or amplifier may not be easily discernible, not only by algorithms, but also by human readers (Jack, 2017; Zubiaga et al, 2016). Therefore, mis- and disinformation are sometimes addressed as if they are interchangeable.

Disinformation is also related to propaganda which "*...is neutrally defined as a systematic form of purposeful persuasion that attempts to **influence the emotions, attitudes, opinions, and actions of specified target audiences** for ideological, political or commercial purposes through the controlled transmission of **one-sided messages (which may or may not be factual)** via mass and direct media channels.*" (Nelson 1996: p232-233)

Deceitful propaganda techniques (e.g., selective use of facts, unfair persuasion, appeal to fear), however, are employed much more widely, e.g. in anti-EU campaigns, post-truth politics, ideologydriven web sites,



and hyperpartisan media, often with the intent to **deepen social division, increase polarisation, influence public opinion, or impact key political outcomes.**

2.1. PROPAGANDA TECHNIQUES

What makes online disinformation even more challenging for citizens to identify and protect themselves against is not just its ubiquitous online presence, but also the way it exploits propaganda techniques around linguistic, cultural, and national differences, to create new social barriers and divisions, as well as causing financial and personal damages.

Not only are disinformation and propaganda campaigns ubiquitous, but they are also cross-border and cross-language, often using different persuasion techniques and sources.

Key propaganda persuasion techniques employed in making online disinformation more credible include (Faris *et al*, 2017):

- Ad hominem – statements attacking the opponent, rather than their argument.
- Ad nauseam – constant repetition of a slogan or an idea, to make it mainstream and accepted.
- Cherry-picking – facts and opinions are unequally represented.
- Appeal to authority – citing of prominent figures or sources, sometimes out of context.
- Appeal to fear, anger, or prejudice – building support through fear, anger, prejudice, or stereotyping.
- Deception – deceptive/misleading presentation of facts or viewpoints.
- Humour – used to discredit democratic values or politicians; involves structural manipulation of message content (NATO StratCom COE, 2017).

The rationale behind employing propaganda techniques in online disinformation campaigns is to enhance the credibility of the message.

In addition, as argued in (Wardle & Derakhshan, 2017) in order to understand online disinformation, its spread and effects, it is necessary to adopt a more sophisticated conceptual framework, which distinguishes between:

- the **Agents** involved - who are the authors or distributors of disinformation and what is their motivation;
- the **Message** - the false content that is being spread, how it is expressed, and the techniques used to enhance its credibility;
- the **Interpreters** - who are those reading the disinformation and what are its effects on their beliefs and actions.

2.1.1. FACTORS HELPING THE SPREAD OF DISINFORMATION

The first places in terms of public information are currently held, in all media, by television, radio and print media, to which is added the powerful information vector in full expansion - the Internet.

However, there is fierce competition between them because they all assume the same task in serving the public. Informing, cultivating and entertaining. Unfortunately, the emphasis is often on “entertaining” to the detriment of accurate information; the sensational prevails over the truth, and

various media channels often overlook the importance of correctly presenting information and objectivity in order to rise to the top of public opinion preferences. The same competition is intensified by the common dependence on the financial resources provided by advertising. Nor does politics lack the means to put pressure on information professionals. On the other hand, the latter are driven by the capitalization of the presentation and comments to the detriment of the fact.

Considering that the press (written, spoken, filmed) is one of the most active disinformation systems of public opinion, we can analyze the ways in which the messages conveyed are used in maintaining, consolidating or changing images, opinions and attitudes towards a stimulus situation:

- 1) influence through the source of the news - is based on the idea that using editorials to distort facts is the ideal way to persuade the audience to think or feel the way reporters want;
- 2) influencing by selecting the news appreciated as one of the most efficient and easy ways of misinformation;
- 3) influencing news orientation, which is practiced after a publisher has decided what material to publish;
- 4) influencing by placing news - is a technique by which publishers can minimize the attention given to events (small broadcast spaces, placing articles on the last pages of newspapers) or, conversely, can increase interest in these events (large spaces broadcast, first page appearances);
- 5) influencing by omitting (evading) parts or elements of the news content;
- 6) influencing by “coincidence” in the placement of news;
- 7) the influence through titles, which is based on the idea that the titles establish the disposition and the system of values of the article;
- 8) the influence by choosing the words on the occasion of different events ensures the discrediting or, on the contrary, the increase of the prestige and the respect towards the personality or social group;
- 9) influencing by selecting photographs and / or images ensures the distortion, positive or negative, of the perception on a social phenomenon or process;
- 10) influencing through the explanations that accompany the photos and / or images presented and that can significantly affect a person's attitude towards the topic.

In order to carry out manipulation through misinformation, one provides such information which, through processing, lead to psychic products that the individual considers as being his/her own, when in fact they have been ordered. Although (s)he decides for himself/herself, the decision is not his/hers.

In recent years, the Internet has become the quintessential ground for information warfare. Large companies use the Internet to inform themselves and to misinform their competitors. Mastering the channels of information circulation, disseminating as widely as possible their own points of view in order to impose them, the continuous adaptation of the methods and tools of information processing are just as many possibilities for their processing and manipulation.

The Internet is becoming the best thing in the world but also the worst one, as the user who informs himself/herself with the display imagines that the information (s)he receives is objective, which is not necessarily true.



When it comes to disinformation, the weakness of online sites and social platforms is also their main strength, i.e. the easy way in which their users can create, publish, share, and engage with online content. A typical strategy is to create a fake headline, coupled with misleading images or videos, to create an emotionally provocative story, which entices social media users to share and click, on platforms like Facebook (Silverman, 2017), Twitter, and WhatsApp (McLaughlin, 2018). Many successful disinformation campaigns tend to harness the emotional power of videos by posting them first on YouTube (Albright, 2018a) and then sharing the content through Facebook and similar channels. Their reach and impact are then amplified by the platforms' trending topics algorithms, which frequently promote misinformation (e.g. conspiracy theories) during major events and crises (Lapowski, 2018). In addition, successful propaganda and disinformation campaigns often leverage a network of websites that post disinformation or distorted, out-of-context news stories, designed specifically to invoke emotional response and online engagement

The proliferation of online misand disinformation is also affecting web search results, which further hinders users in finding and reading trustworthy online information. For example, in February 2018, Google search suggestions were showing misleading or false information (Albright, 2018) especially in the top one to five suggestions, e.g., feminists are crazy, police are evil.....

The most commonly used mechanisms for creating, promoting, and spreading online disinformation are:

2.1.2. FAKE PROFILES AND GROUPS

Social platforms are plagued by fake profiles and groups, which are created to post online disinformation and amplify its spread and perceive important Fake accounts, which can also be created and purchased to act as fake followers and thus artificially inflate the importance and popularity of genuine accounts.

2.1.3. ONLINE ADVERTISING AND CLICKBAIT

Online advertising has been used extensively to make revenues for junk news sites, as they receive payments when the adverts are shown alongside the fake content. Owners of such web sites have claimed to earn between \$10,000 and \$30,000 per month from online advertising.

A clickbait post is designed to provoke emotional response in its readers, e.g. anger, compassion, sadness, and thus stimulate further engagement by following the link to the webpage, which in turn generates ad views and revenues for the website owner. Clickbait typically omits key information about the linked content (Chakrabarti et al, 2017), to create a curiosity gap (Loewenstein, 1994) and thus entice users to click. The sensationalist and emotive nature of social media clickbait has been likened to tabloid journalism and found to provide an “alternative public sphere for users drifting away from traditional news” (Chakrabarti et al, 2017). Clickbait tweets have been found to retain their popularity for longer and attract more engagement, as compared to non-clickbait.

Promoted posts on social media are marked as advertisements and can be reposted, liked, replied to, etc. as any normal post can. Advertisers are billed by the social platform based on the amount of engagement generated, e.g. likes, shares, clicks and views. In many cases advertisers can choose which users will see the promoted post, based on information such as geographic location, gender, interests, device type, or other specific characteristics. When adverts are targeted at a very narrow set of users, with very specific profiles, the practice is called micro-targeting.

2.1.4. MICRO-TARGETING AND THIRD-PARTY DATA ANALYSIS OF USER DATA

Social platforms, such as Facebook, Twitter, LinkedIn, and Pinterest, offer advertisers the option of creating the so-called dark ads. These are online adverts that are visible only to the users that are being targeted (*e.g.* voters in a marginal UK constituency (Cadwalladr, 2017)). Dark ads do not appear on the advertiser's timeline or in the feeds of the advertiser's followers. They have been used during political campaigns to spread misinformation, with the intent of influencing election outcomes. Moreover, due to their highly personalised nature, dark ads can be used to target susceptible users with misinformation which they are likely to believe is correct. As dark ads are hidden from view of other users, misinformation within cannot be discussed or counter-evidence posted by the user's friends.

2.1.5. FAKE AMPLIFIERS: SOCIAL BOTS, CYBORGS, AND TROLLS

Social bots are programs "capable of automating tasks such as retweets, likes, and followers. They are used to disseminate disinformation on a massive scale, but also to launch cyber attacks against media organizations and to intimidate and harass journalists." (RSF, 2018) Sockpuppets are fake accounts that pretend to be ordinary human users and aim to connect to and influence real social network users. Sockpuppets are typically human controlled, but can also employ some automation, in which case they are referred to as cyborgs. Politically oriented sockpuppets, especially those controlled by governments or affiliated organisations are known as trolls.

Social bots, cyborgs, and trolls have all been employed as fake amplifiers in online misinformation and propaganda campaigns (Gorwa & Guilbeault, 2018). In Mexico, for instance, it is estimated that 18% of Twitter traffic is generated by bots (RSF, 2018), which flood the platform with manipulated content thus making high quality information hard to find. Automated accounts and trolls also engage in astroturfing - a propaganda technique which "creates the illusion of a spontaneous, popular movement on the internet started by a fake grassroots organization." (RSF, 2018).

Another kind of false amplification is the use of fake followers to inflate artificially the perceived influence of a social media account. It is linked with social media identity theft, where names, photos and personal details of real social media users were used to create more authentic-looking fake accounts. The problem is not confined to Twitter, with Facebook also acknowledging that up to 60 million automated accounts may exist on its platform (Confessore et al, 2018).

Artificial Intelligence, Synthetic Media, and "Deepfakes" In the past several years, advances in artificial intelligence and the availability of affordable high-performance computing have led to the emergence of synthetic (*i.e.* computer-generated) images, audio, and video. The so called "deepfakes", in particular, are synthetic videos and images generated using deep neural network models, which "look and sound like a real person saying something that that person has never said." (Lucas, 2018). "Deepfakes" can potentially cause significant harm, as they look credible; are harder for citizens to verify; Pornography-oriented deepfakes are also offensive to the target and can be used as part of online abuse campaigns. Until this technology came into existence, generating even simple synthetic media content required significant expertise and effort. Since off-the-shelf, easy-to-use tools for the creation of deep fakes have become widely available, they have been used to perform face swapping in images and video, lip-syncing, speech modification, or image alterations (Hui, 2018)



3. RESULTS

3.1. METHODOLOGY AND METHOD

This study maps and analyses current and future threats from propaganda and misinformation. The challenges of evaluating their effectiveness and practical adoption are also discussed. The study summarises and analyses the findings of relevant journalistic and scientific studies and policy reports in relation to detecting, containing and countering disinformation and propaganda campaigns. Also, it traces recent developments and trends.

3.1.1. PRESENTATION OF DATA AND DISCUSSION OF RESULTS

The results of the analysis of the data obtained from the different sources consulted will be presented below. First, the results of the analysis of the external environment carried out through the PESTEL method will be detailed, followed by the analysis of the internal environment through the dynamic SWOT.

3.1.2. PRESENTATION OF DATA

Table 6. PELTEL Analysis | Propaganda and misinformation

Factors	Key Macro Trends	Implications for Security Forces
Political & Legal	<p>P.1. The desire of certain countries or power groups to influence public opinion and destabilize certain societies</p> <p>P.2. The conflict between civilizations and between different models of organization of society</p> <p>P.3. States are increasingly interested in controlling the information provided through various channels of communication</p> <p>P.4. Lack of legal regulation in order to establish standards for public communication.</p> <p>P.5. Concern for a general legal framework, through which can be delimited the right to free expression from propaganda / misinformation</p>	<ol style="list-style-type: none"> 1. Increasing radicalization and the emergence of social pressure groups, which incite disobedience and create conflicts between communities 2. The emergence of hybrid, asymmetrical or even classical conflicts. 3. Demonstrations against the rules imposed by governments and social disobedience 4. Lack of tools to punish propaganda and misinformation 5. Providing legal tools to limit / combat propaganda / information
Economic	<p>E.1. The rapid progress of the media and the technology used to transmit information</p> <p>E.2. Instability and economic crises</p> <p>E.3. Availability of growing budgets for propaganda and misinformation</p>	<ol style="list-style-type: none"> 1. Widespread dissemination of truncated-false propaganda and information, which can lead to extreme social reactions. 2. Budgetary restrictions for upgrading technological resources 3. They can be used to erode trust in state institutions 4. The emergence of radical social reactions
Social	<p>S.1. Segmentation and social radicalization</p> <p>S.2. The emergence and use of communication channels only by members of certain communities</p>	<ol style="list-style-type: none"> 1. Public manifestation of desires for autonomy of certain communities; 2. Opposition to legitimate measures taken by the authorities; 3. Creating false perceptions about certain measures taken by the authorities, which lead to a decrease confidence in authorities and state

Technological	<p>T.1. Emergence and development of technologies that promote the spread of false information and propaganda</p> <p>T.2. Ease of manipulating information (including movie images) through the use of computer programs. Unrestricted creation of online, word-wide information resources and easy and unlimited access to information resources</p>	<p>1. Impossibility of law enforcement agencies to implement adequate strategies for tackling propaganda and misinformation</p> <p>2. Creating false perceptions about certain realities and social situations, with an impact on the confidence that the authorities can manage the phenomena / aim at the interest of the community</p>
Env.	EN.1. Low impact on the issue	

3.2. ANALYSIS OF THE INTERNAL ENVIRONMENT: SWOT METHOD

3.2.1. SWOT ANALYSIS

Table 7. SWOT analysis | Propaganda and misinformation

Internal factors	Strengths (S)	Weaknesses (W)
External factors	<ul style="list-style-type: none"> ▪ Existence of communication structures within the law enforcement forces ▪ Access to all communication platforms ▪ Possibility to carry out awareness campaigns and to fight propaganda and mis / disinformation ▪ The high level of trust in law enforcement agencies. 	<ul style="list-style-type: none"> ▪ Lack of legal tools to combat fake news / misinformation ▪ Limited budgetary possibilities for awareness-raising campaigns / actions to combat propaganda / disinformation ▪ Limited possibilities for the creation of automated technologies for early detection of propaganda / misinformation ▪ Insufficient staff dedicated to monitoring, analyzing the phenomenon and implementing countermeasure projects.
Opportunities (O)	<ul style="list-style-type: none"> ▪ Initiate and run communication campaigns for raising public awareness about propaganda and mis/disinformation ▪ Strengthening the PR department, in order to be able to monitor the public messages regarding public order forces and to provide an instant and strong answer to mis-disinformation 	<ul style="list-style-type: none"> ▪ Develop new means and use the latest technologies for early warning of campaigns that aim at credibility and trust in public order forces ▪ Promote more transparency and use all communication tools in order to have a better dialogue with citizens and to maintain and raise their trust in gendarmerie forces
Threats (T)	<ul style="list-style-type: none"> ▪ Develop new partnerships with NGOs, professional association of journalists, universities and influencers, in order to raise public awareness and critical thinking 	<ul style="list-style-type: none"> ▪ Design communication strategies for own personnel ▪ Create integrated answers to disinformation campaigns, together with other public institutions
	<ul style="list-style-type: none"> ▪ Promoting campaigns for raising public awareness about propaganda and mis/disinformation ▪ International concer on takling propaganda and disinformation. 	
	<ul style="list-style-type: none"> ▪ The increasing of propaganda and mis/disinformation activities ▪ The complexity and opportunities of technologies is increasing ▪ States are not investing enough resources on tackling propaganda and mis/disinformation ▪ Propaganda and mis/disinformation can be conducted/supported from territories that are not under law enforcement authorities ▪ Lack of critical thinking in case of a large number of citizens, especially among youngs. 	

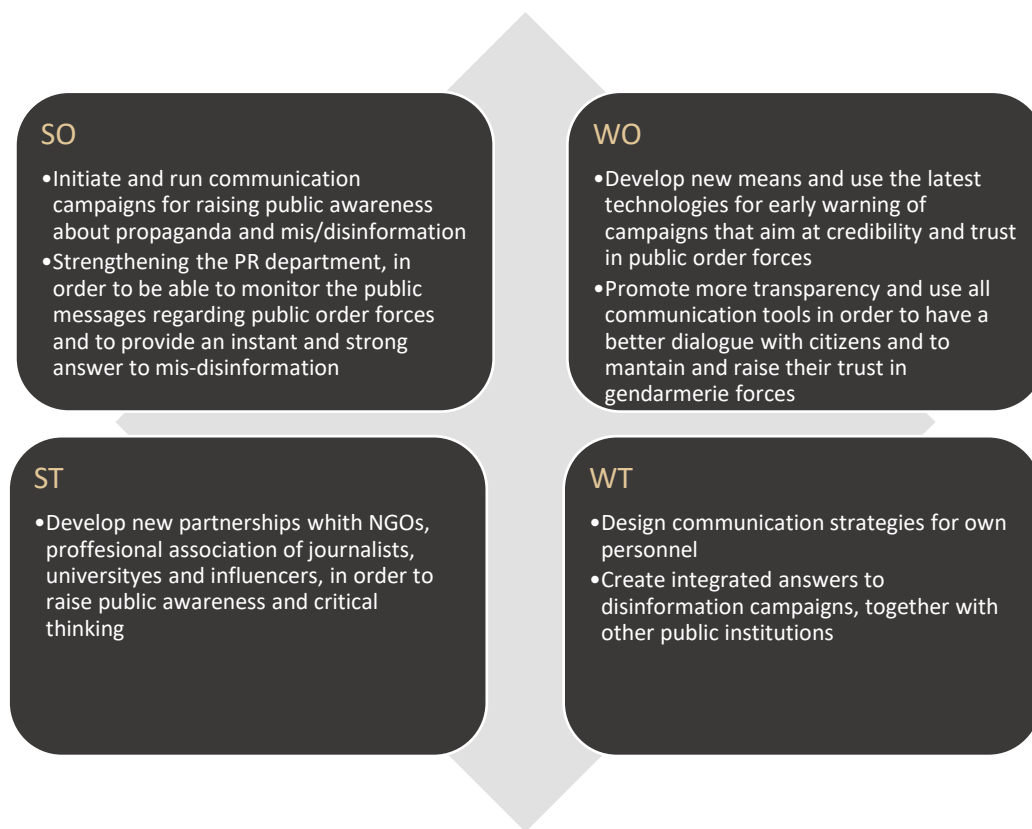


Figure 4. Keys Strategies | Propaganda and misinformation

3.3. STRATEGIES

Despite the efforts to address these diverse major challenges and develop a new generation of content verification and disinformation tackling tools, there are no certain strategies and instrument available. For law enforcement agencies, it is more difficult to promote sectorial strategies, taken in consideration that this issue has a major social impact and cannot be addressed through individual approach.

The most promoted strategies shall be about media literacy and public awareness. It should focus on empowering society, journalists and activists to enhance their media literacy and learn ways to spot disinformation and avoid spreading it further. These strategies must also involve the gendarmerie staff and their families, in order to become aware of the impact of disinformation, of the critical thinking they need to exercise and of the tools and resources available for verifying information.

The improvement of technology for fighting disinformation can be another strategy. It is a major need for the social media platform and independent researchers to develop more efficient technological tools for early warning and stop disinformation. Gendarmerie forces may participate in this effort, providing certain cases and situations faced in daily activities that can be used for machine learning technologies.

New rules and regulations are important but there will always be a topic on the protection of free speech right.

Also, the improvement of every public body's transparency may be a response and will address disinformation by offering official answers to root subjects of disinformation.

4. CONCLUSIONS & RECOMMENDATIONS

The blurring lines between interests and evidence, opinion and fact are arguably affecting journalism, academia, courts, law enforcement, science, and intelligence. This poses a fundamental risk to democracy's core structures and processes and thereby to democratic governance. From a citizen's perspective, declining confidence in the government's ability to protect people's interests affects confidence in democratic processes, leading to alienation and disengagement.

There is reportedly mounting concern at United Nations headquarters that the general pushback against human rights, combined with decreasing trust and transparency, could result in a 'secretive international environment in which multilateral institutions lack both political credibility and technical proficiency to establish the facts of major security incidents'.

Under public pressure and media articles pointing out the dangers of disinformation on our societies, there was several initiatives to draft regulatory responses to this issue.

Some social media platforms like Facebook or Twitter decided to implement voluntarily in reaction to this issue. Alongside using AI algorithms to flag false content, social platforms have also empowered their users with the ability to flag suspicious content, which is then checked manually by the platform's content moderators.

This is a reason for developing media literacy and critical thinking as the key skills required by citizens to engage more effectively with online information and social platforms.

In my opinion, law enforcement agencies will need to strengthen their communications departments and work closely with other authorities to provide an integrated response, both nationally and regionally, to threats of misinformation. This strengthening should include superior technical endowments, improved staff training as well as an allocation of resources to support classic or online communication campaigns.

Aslo is important to develop new partnerships with NGOs, professional association of journalists, universities and influencers, to be part of public campaigns for raising public awareness and critical thinking. These partnerships can be use for multiplying messages and answers to obvious disinformation and to decrease or even stop spread of fake-news.

Based on the confidence they enjoy among the population, the gendarmerie will have to design and promote transparent communication policies and actions. A better and constant dialogue with citizens is basically needed, using all communication platforms and offering a solid feed-back to all issues.

Also, due to the limited resources of specialized staff, all personnel can be used as a message multiplier in all major social media groups.



REFERENCES

- Albright, J. (2018a). Untrue-Tube: Monetizing Misery and Disinformation. Medium. 25 Feb 2018.
- Albright, J. (2018). #NotOKGoogle search suggestions: 2018 edition. Medium.
- Bentzen N, From post-truth to post-trust?
[https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA\(2018\)628298](https://www.europarl.europa.eu/thinktank/en/document/EPRS_ATA(2018)628298)
- Cadwalladr C. (2017), The great British Brexit robbery: how our democracy was hijacked, The Guardian, 7 May 2017, <https://www.theguardian.com/technology/2017/may/07/the-great-british-brexit-robberyhijacked-democracy>
- Chakraborty, A., Sarkar, R., Mrigen, A., and Ganguly, Niloy (2017). Tabloids in the Era of Social Media? Understanding the Production and Consumption of Clickbaits in Twitter. Available at SSRN:
<http://dx.doi.org/10.2139/ssrn.3034591>
- Confessore, N., Dance, J.X.A., Harris, R., & Hansen, M. (2018). The Follower Factory. New York Times. Published on 27 Jan 2018. <https://www.nytimes.com/interactive/2018/01/27/technology/social-mediabots.html>
- Draguş S, INFORMARE ŞI DEZINFORMARE ÎN MASS-MEDIA,
<https://www.armyacademy.ro/biblioteca/anuare/2004/a10.pdf>
- Gizikis A, Alexandre Alaphilippe, and Clara Hanot of EU DisinfoLab, and Kalina Bontcheva of The University of Sheffield, Automated tackling of disinformation, study at the request of the Panel for the Future of Science and Technology (STOA),
[https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624278/EPRS_STU\(2019\)624278_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624278/EPRS_STU(2019)624278_EN.pdf)
<https://ec.europa.eu/digital-single-market/en/news/synopsis-report-public-consultation-fake-news-and-onlinedisinformation>
https://en.wikipedia.org/wiki/Media_literacy
- Jack, C. (2017) Lexicon of Lies: Terms for Problematic Information, Data & Society Research Institute.
- Jeangène Vilmer, J.-B., Escorcía, A., Guillaume, M., & Herrera, J. (2018) Information Manipulation: A Challenge for Our Democracies, report by the Policy Planning Staff (CAPS) of the Ministry for Europe and Foreign Affairs and the Institute for Strategic Research (IRSEM) of the Ministry for the Armed Forces, Paris, August 2018.
- Faris, R., Roberts, H., Etling, B., Bourassa, N., Zuckerman, E. & Benkler, Y. (2017). Partisanship, Propaganda, and Disinformation: Online Media and the 2016 U.S. Presidential Election. Berkman Klein Center Research Publication 2017-6
- Gorwa, R. & Guilbeault, D. (2018). Unpacking the Social Media Bot: A Typology to Guide Research and Policy. Policy & Internet, 10 August 2018. doi:10.1002/poi3.184
- Hui, J. (2018) How deep learning fakes videos (Deepfakes) and how to detect it? Medium. 28 Apr 2018.
https://medium.com/@jonathan_hui/how-deep-learning-fakes-videos-deepfakes-and-how-to-detectit-c0b50fbf7cb9
- Lapowski, I. (2018). Parkland Conspiracies Overwhelm the Internet's Broken Trending Tools. Wired.
- Loewenstein, G. (1994) The psychology of curiosity: A review and reinterpretation. Psychological Bulletin 116, 1
- Lucas, E. (2018). Oral Evidence: Fake News HC 363.

<http://data.parliament.uk/writtenevidence/committeeevidence.svc/evidencedocument/digital-culturemedia-and-sport-committee/disinformation-and-fake-news/oral/79824.html>

McLaughlin, T. (2018). Disinformation Is Spreading on WhatsApp in India—And It’s Getting Dangerous. The Atlantic.

<https://www.theatlantic.com/international/archive/2018/09/fighting-whatsappdisinformation-india-kerala-floods/569332/>

NATO StratCom COE (2017). StratCom laughs. In search of an analytical framework

Nelson, R.A. (1996) A Chronology and Glossary of Propaganda in the United States, Westport, Connecticut: Greenwood Press, ISBN 0313292612.

RSF (2018). ONLINE HARASSMENT OF JOURNALISTS - Attack of the trolls. Reporters without Borders. 25 July 2018. <https://rsf.org/en/news/rsf-publishes-report-online-harassment-journalists>

Silverman, C. (2017) 5 ways scammers exploit Facebook to feed you false information. BuzzFeed, 28 April 2017.

<https://www.buzzfeed.com/craigsilverman/how-facebook-is-getting-played>

Wardle, C. & Derakhshan, H. (2017) Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making. Council of Europe report DGI(2017)09, October 2017, <https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-forresearch/168076277c>

Wardle, C. (2017) Fake News. it’s Complicated. First Draft, 16 February 2017.

<https://firstdraftnews.org/fake-news-complicated/>

Zubiaga, A., Liakata, M., Procter, R., Wong Sak Hoi, G., Tolmie, P. (2016) Analysing How People Orient to and Spread Rumours in Social Media by Looking at Conversational Threads. PLoS ONE 11(3): e0150989.

<https://doi.org/10.1371/journal.pone.0150989>



Page intentionally left blank

III. PAPER | CLIMATE CHANGE AND NATURAL DISASTERS

Citation:

Colakoglu, E. Climate Change. Overcoming Security Threats arising from Globalization 4.0 – FIEP Association, 2022.

Published: October 2022

Publisher's Note: FIEP stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors.

The Republic of Türkiye

Prof. Dr. Elif Colakoglu



Prof. Dr. Gendarmerie and Coast Guard Academy, The Faculty of Security Sciences, The Department of Security Sciences, Ankara (The Republic of Türkiye); elif.colakoglu@jsga.edu.tr

Abstract: As the climate changes, our living spaces become more vulnerable. Even if security risks vary depending on a country's level of development, they can quickly erupt into humanitarian crises. On the one hand, rising global temperatures cause warming of the world's oceans, rising sea levels, decreased precipitation, and melting of ice as a natural result of ecosystem deterioration, and on the other, it has consequences that will severely damage countries' critical infrastructures. As a result of the current situation, this is expected to worsen in the future.

This study focuses on the threats to national security posed by climate-related crises and natural disasters, but it also develops strategies and policies on how law enforcement should respond to its consequences, which directly threaten public safety. The main goal here is to use the dynamic SWOT matrix to improve strategies for improving security capabilities. This is accomplished through the use of various strategic analysis tools such as PESTEL analysis, the McKinsey 7s model, and the SWOT matrix.

Keywords: climate change; natural disaster; national security; law enforcement.



1. INTRODUCTION: COUNTRIES ARE STILL NOT ADEQUATELY INSURING AGAINST NATURAL DISASTERS...

Climate change is viewed as a new, direct, and multifaceted threat to national security today more than ever. Considering its effects, especially through extreme weather events, the situation seems quite serious. Therefore, the future of humanity and our planet may be jeopardized. Thunderstorms, droughts, forest fires, and floods have harmed the environment and resulted in longer-lasting droughts that have harmed the food, water, and sanitation security of millions of people, and mass migration has occurred for more than a decade. The worst and most devastating effects of these problems, which are largely the responsibility of developed countries, are mostly seen, or will be seen, in developing countries, which have scarce natural resources and limited capacity to adapt to these challenges caused by climate change. They are the most expensive and destructive natural disasters for countries. In contrast, there is a risk that the problems caused by climate change will cause conflicts and tensions among countries and communities, particularly in the world's most volatile regions, as well as endangering economic and political stability, i.e., peace and tranquility.

Climate change, defined as changes that occur over time as a result of natural changes or human activities, is primarily of human origin in our era, and the resulting damage has a negative impact on the sustainability of the earth's ecosystem and thus human life. Climate change is one of these issues, which is especially emphasized at the local level, and is one of the central discussion topics in the environment-development relationship. Excessive use of fossil fuels such as coal, oil, and natural gas, land use changes, and human activities such as deforestation all contribute to the rapid accumulation of greenhouse gases such as carbon dioxide (CO₂) and methane in the atmosphere. This situation worsens the energy balance of the system in the atmosphere, resulting in further warming of the earth and the layer of the atmosphere closest to the earth. The resulting greenhouse effect is felt more in cities and becomes an environmental problem as a result of human activities that increase its impact and severity. As a result, urban heat islands form, particularly as a result of heat inversion in living spaces. These heat islands emerge as a problem, especially as a result of unplanned and unplanned urbanization, where cities get warmer than the rural areas around them, and as a result, many environmental problems are experienced. Floods caused by sea level rise, extreme weather events such as hurricanes or more droughts, reduced water needed for agriculture and food, and the increased emergence of tropical diseases are just a few examples. In addition to increasing the frequency of severe weather events, particularly in coastal cities, it has a serious impact on infrastructure such as transportation networks, energy, water, and sewer systems, and food distribution systems, as well as posing multiple security risks.

The fourth report of the Intergovernmental Panel on Climate Change that established by the United Nations in 1988, was published in 2007, and influenced international public opinion on the effects of natural disasters significantly. (Akay, 2019: 6) For the first time, this report offers the most comprehensive and scientific assessment of the effects of climate change, the vulnerability of natural and human environments, and the potential for response through adaptation. Accordingly, the report evaluates evidence that recent observed changes in climate have already affected a variety of physical and biological systems and concludes that these effects can be attributed to global warming, as well as making a detailed assessment of the impacts of future climate change and sea-level rise on ecosystems, water resources, agriculture and food security, human health, coastal and low-lying regions, industry, and settlements. (IPCC, 2007) The IPCC's most recent report, the sixth report, published in 2021, contains the most severe statements and warnings ever issued. The report emphasizes that significant climate change is unavoidable and irreversible. In other words, scientists claim that human activities have altered the Earth's climate in unprecedented ways over thousands or hundreds of thousands of years, and that some of these changes are now irreversible. According to the Report (IPCC, 2021):

- *Human activities have an impact on all of the major components of the climate system, with some responding over decades and others over centuries. It is undeniable that human activity has warmed the*

atmosphere, oceans, and land. There have been widespread and rapid changes in the atmosphere, ocean, cryosphere, and biosphere;

- *The scale of recent changes in the climate system as a whole is unprecedented in hundreds to thousands of years;*
- *Many weather and climate extremes are already being impacted by human-caused climate change in every region of the world. Evidence of observed changes in extremes such as heatwaves, heavy precipitation, droughts, and tropical cyclones, as well as their attribution to human influence, has grown stronger;*
- *Under all emission scenarios considered, global surface temperature will continue to rise until at least mid-century. Global warming of 1.5°C to 2°C will be exceeded during the twenty-first century unless CO₂ and other greenhouse gas emissions are drastically reduced in the coming decades;*
- *Many changes in the climate system become more pronounced as global warming continues. Increases in the frequency and intensity of hot extremes, marine heatwaves, heavy precipitation, and, in some areas, agricultural and ecological droughts; an increase in the proportion of intense tropical cyclones; and decreases in Arctic Sea ice, snow cover, and permafrost are among them;*
- *Global warming is expected to exacerbate the global water cycle, including its variability, global monsoon precipitation, and the severity of wet and dry events;*
- *Under rising CO₂ emissions scenarios, ocean and land carbon sinks are expected to be less effective at slowing CO₂ accumulation in the atmosphere;*
- *Many changes caused by past and future greenhouse gas emissions, particularly changes in the ocean, ice sheets, and global sea level, are irreversible for centuries to millennia, but natural disasters such as avalanches, landslides, and storms have also become more frequent and severe since the early 1990s (Hough, 2014: 126).*

Following the IPCC's final report, all countries came together in the same year – on 31 October – 13 November 2021 – at the 26th UN Climate Change Conference (hereafter COP 26) to limit global greenhouse gas emissions and build a low-carbon economy. While the IPCC claims that temperatures have risen by about 1.1°C between 1850 and 1900 (IPCC, 2019), the Conference agreed that in order to meet the 1.5°C target (COP26, 2022), they would meet again in 2022 for planning, including emission reductions. Today, we know that we are still unable to protect the climate ecosystem, which is one of the most fundamental life support systems, and that we have passed the critical stage. We refer to “climate change”, which we initially identified as a due diligence as “global warming”, as “climate crisis”, because it has now reached very dangerous proportions and has turned into a crisis. Because it ranges from floods caused by sea level rise to extreme weather events such as hurricanes or more droughts, a decrease in the amount of water needed for agriculture and food, and the emergence of more tropical diseases. Whether it is a developed or developing country, every country on the planet is now directly or indirectly exposed to the consequences of climate change, albeit at varying degrees, and this easily becomes a national security issue. As a result, the literature discusses in greater depth all aspects of climate change and its consequences that affect the public, such as health, economy, and management. The literature on its security dimension appears to have emerged in recent years as a result of security-related institutions' efforts. This study is to start by analyzing the current situation using scientific data in general, and then discuss the implications of security-based climate change for law enforcement using a dynamic SWOT analysis.



1.1. SOME NATURAL DISASTERS CAUSED BY CLIMATE CHANGE AND PROJECTIONS OF ITS EXTREMES

For over a century, average precipitation and temperature have been rising and becoming more variable around the world. Differences between land and sea, regions, seasons, and even day and night are consistent, but statistically significant. To put it another way, humans are unquestionably to blame for the rise that cannot be explained by known natural events, and they cause numerous problems that lead to major disasters. Floods, mass movements (rockfall, landslide, avalanche, collapse), storms, extreme heat and cold waves, drought, desertification, and wildfire are among the natural disasters caused by climate change.

1.2. MASS MOVEMENTS (ROCKFALL, LANDSLIDE, AVALANCHE, COLLAPSE)

According to the AFAD (2022), mass movements are the slow or rapid displacement of soil and rock masses down slopes due to gravity. These mass movements include rockfalls, landslides, avalanches, and collapses, and in addition to the countries' geographical, geological, and meteorological conditions, there has been loss of life and property in recent years as a result of climate change.

Climate change reduces the stability of slopes in high-elevation areas of the mountains, increasing the risk for visitors. Rockfall is the rapid movement of rock or ground pieces of various sizes and types that have been distorted or fragmented by physical or chemical effects down a slope, either spontaneously or as a result of external forces such as earthquakes and heavy rains (AFAD, 2022). The main drivers of climate change impacts on slope destabilization are temperature changes and extreme rainfall events. But also, the three main factors that are likely to increase rockfall in the future are thawing permafrost during heat periods, tension concentrations, which will increase as glaciers continue to decline, and changing days of frost in the high alps (Sardi *et al.*, 2019). Changes in slope stability over time and space, for example, have been studied and linked to climate change for a high-elevation catchment in the eastern Italian Alps. Focused on small- to medium-sized rockfalls, slides, and debris flows, the study the frequency of rockfalls has increased since the 2000s, and has also found an increase in the number of debris flows triggered by rainfall events since 2010, most likely due to warmer and wetter summers. Furthermore, if temperature levels remain elevated or rise further in the future, the dynamic relationships between warming trends, permafrost degradation, changes in extreme rainfall events, and the occurrence of hazardous slope failures will become increasingly important for the higher sectors of Alpine catchments. (Savi *et al.*, 2021)

As one type of mass movements landslides occur when a landslide, rock, soil, or piece of land shifts or moves noticeably down the slope as a result of gravity or external factors such as earthquakes and heavy rainfall (AFAD, 2022). These landslides cause millions of dollars of infrastructure damage and thousands of casualties around the world every year. One example is the 2011 landslide disaster in Rio de Janeiro, which was caused by heavy rains. The United Nations has declared this disaster the world's eighth-largest landslide in the last 100 years, as well as Brazil's largest climatic and geotechnical disaster. (Sousa *et al.*, 2021) Hundreds of people lost their lives and there was a great economic loss. Official government figures put the death toll at nearly a thousand people, with an additional 500 people missing who should now be presumed dead. The latter is Brazil's worst disaster. The municipalities of Nova Friburgo, Teresópolis, and Petrópolis have been partially affected by 3,623 landslide scars larger than 30 square meters. (Lacerda, 2016: 45) In fact, this situation is a reflection of the problems that have existed in the past and continue to exist in the present. That is, most landslides and erosion today occur in areas where man has altered the natural relief of the land. Because these areas are primarily cut and fills in slopes of residual soil and decomposed bedrock. (Jones, 1973: 2) Many similar examples from around the world could be provided. In the 2014 flood disaster in Italy's Liguria region, more than 100 landslides occurred, 70 people died, and more than 200 people were forced to flee their homes (Klizista-hr, 2018). However, 88% of existing Italian municipalities are at risk of flooding and landslides, with the country estimated to have lost \$15 billion USD as a result of these natural disasters

between 2006 and 2016. (DW, 2018; Çolakoğlu, 2019) Every year, riverbank erosion causes 64,000 to 100,000 people to become homeless in Bangladesh. There may also be issues that lead to internal unrest and protests. In 2011, floods caused by heavy monsoon rains in Thailand affected 2 million people, sparking anti-government protests. (Germany’s G7 Presidency, 2015).

In this regard, knowing when and where landslides are likely to occur can assist countries in preparing for these natural disasters. NASA has created a global scale landslide inventory – Cooperative Open Online Landslide Repository (The Landslide Reporter)– for this purpose. The main goal here is to create a good inventory of landslide occurrences and improve science-based prediction models. In Map 1, the visualization shows the locations of landslides during the period 2007-2019.



Figure 5. The landslides triggered by rainfall for the period 2007-2019

Source: (Kostis, 2022)

Avalanche is a sudden and rapid flow movement in the slope direction caused by the deterioration of the balance of large snow masses accumulating on sloping surfaces such as mountain slopes, either spontaneously or as a result of a triggering effect (AFAD, 2022). Avalanches pose a threat to many countries around the world, including the United States, Japan, and Australia. However, avalanches are most common in Europe, with the top four countries receiving the most avalanches in Europe being Switzerland, Austria, Italy, and France. Switzerland is probably the most well-known country for avalanche victims, not only because of the numerous disasters, but also because of the extensive snow avalanche research that has been conducted for more than 60 years. According to its statistics, approximately 25 people are killed each year in snow avalanche accidents, and approximately twenty living houses are damaged each year on average. Every year, nearly 100 other types of buildings are affected, and several roads are closed. Avalanches of snow are a major natural hazard in Austria. Avalanches kill 20–25 people each year in Switzerland, as well. The majority of these visitors are skiers. A deadly avalanche in Rigopiano, Italy, destroyed a luxury hotel and killed 29 people. The disaster was Italy’s deadliest avalanche in nearly a century. In 1970, an avalanche struck a ski resort in Val d’Isere, France, killing 42 people, the majority of whom were young skiers. This was the worst Avalanche disaster in French history. (Snowsafe Blog, 2022) Avalanche-related consequences are also more severe in developing countries. The 2015 Afghanistan avalanches are, for example, some of the worst ever recorded and by far the worst that the country has ever seen. A lethal series of avalanches killed at least 310 Afghans. Approximately 1,000 Afghan soldiers were dispatched to the area to assist with search and rescue efforts. Roads were closed, cars were stuck, power was out, and approximately 100 homes were destroyed. (Snow Brains, 2022)



The vertical displacement of the cover material lying over the underground cavity in the downward direction, as well as the collapse of a portion of the earth's crust, is referred to as collapse (AFAD, 2022). The movement of plates in the earth's crust, as well as localized heat concentrations, are a constant source of danger for people and their structures. For examples, drought-induced changes in stress loads on the Earth's crust can be significant. The 2017 study (Rasmussen, 2022), which used data from a network of high-precision GPS stations in California, Oregon, and Washington, discovered that alternating periods of drought and heavy precipitation in the Sierra Nevada between 2011 and 2017 caused the mountain range to rise by nearly an inch and then fall by half that amount, as the mountain rocks lost and then regained water during the drought. (Buis, 2022)

1.3. STORMS

A storm is defined as a wind with a speed ranging from 23 to 26 m/s that causes damage to both nature and people. As wind speed and intensity increase, so does the damage it causes to nature and people. (AFAD, 2022) Thunderstorms, tornadoes, hurricanes, hail, blizzards, ice storms, high winds, and heavy rain can form quickly and endanger people and property. Severe storms of these types occur in all parts of the world and at all times of the year. However, climate change is causing a significant increase in the number of these storms. Every day, up to 40,000 thunderstorms can occur around the world (NSSL, 2022). But the top ten countries with the most hurricanes since 1970, according to the National Oceanic and Atmospheric Research Administration, are China, the Philippines, Japan, Mexico, the United States, Australia, Taiwan, Vietnam, Madagascar, and Cuba (Belles, 2022). Historically, floods and droughts were the most dangerous natural hazards to human life, but storms have claimed more lives since the 1990s (Hough, 2014: 118-119). Even in areas where average precipitation is expected, storm intensity is expected to increase today.

Every three years, about five hurricanes hit the US coastline. These two are usually major hurricanes with winds exceeding 110 miles per hour. Every year, hurricanes kill between 50 and 100 people. (Disaster Center, 2022) Despite the fact that it has been seventeen years, Hurricane Katrina, which was active in seven states in the United States and killed approximately 2,000 people as a result of the humanitarian crises it caused, is one of the most well-known examples. This hurricane cost the country a total of \$128 billion USD in damage. (Çolakoğlu, 2016: 162) Only 80% of the city of New Orleans was flooded in the region where the state of emergency was declared. (Haddow *et al.*, 2011: 36) Oil and gas pipelines were among the critical infrastructures damaged. (Amadeo, 2020) Since 2005, the country has been hit by 103 hurricanes (Insurance Information Institute, 2020), including Hurricane Katrina. Hurricane Sandy in 2012 was the deadliest hurricane since Hurricane Katrina. It killed 44 people in the New York metropolitan area in one day, resulting in massive financial losses (over US\$50 billion). It was also reported that 88,700 buildings were flooded with flood water, and nearly 2 million people were left without power for days. (Rosenzweig & Solecki, 2017; Çolakoğlu, 2016: 162)

1.4. EXTREME HEAT WAVES

Extreme heat waves are defined as intense heat that occurs in the atmosphere and affects a specific geographic area (AFAD, 2022). According to one study, even a 1.5°C increase in temperature will result in a significant increase in the size of heat waves in Africa, South America, and Southeast Asia. As a result, in a 1.5 °C world, 13.8% of the global population will be subjected to severe heat waves at least once every five years. Under 2°C warming, this fraction is nearly three times larger (36.9%), a difference of approximately 1.7 billion people. Limiting global warming to 1.5°C would also result in approximately 420 million fewer people experiencing extreme heat waves and approximately 65 million experiencing extreme heat waves. (Dosio, 2018: 7-8)

Climate change is causing heat waves in many parts of the world. Dangerous heat waves have become more common in various parts of the world in recent years. Extreme heat is also harmful to human health; heatstroke can be fatal if the temperature rises dramatically in a short period of time. Heat waves can worsen air pollution, aggravate cardiovascular and respiratory diseases, and even cause death in some cases. As a result, the risk of death rises, particularly among the elderly living in cities. (European Environment Agency, 2015: 5). Every year, for example, extreme heat kills over 600 people in the United States (Centers for Disease Control and Prevention, 2022). Similar situations exist in Europe. Over 70 thousand people, mostly elderly people, died in European countries alone during the summer of 2003. (WHO, 2017). It is predicted that until the end of the century, an average of 150 thousand people will die each year in European cities, primarily as a result of heat stroke, heart and respiratory problems, and floods (Griffin, 2017). This is a more serious problem in developing countries. In June 2015, for example, it was reported that over a thousand people were killed in Karachi, Pakistan (Astor, 2018).

1.5. EXTREME COLD WAVES

Cold waves are becoming less common as a result of climate change, and the number of new cold temperature records has decreased as a result of global warming. However, cold temperatures and snow will continue to be a part of our typical northern hemisphere winter weather patterns. (World Meteorological Organization, 2022) As a term, an extreme cold wave is defined as weather that causes a significant and rapid drop in temperature within 24 hours, necessitating increased protection measures in agriculture, industry, trade, and social life. The lowest value of the year must be experienced in that region in terms of the season or month, the decrease in air temperatures must last at least two days, cover a large area, and the weather must be 15 degrees colder than normal. (AFAD, 2022) As an example, record-breaking cold waves in eastern China in the last two years can be cited. Extreme cold waves, which are common in eastern China, have put ecological agriculture, energy infrastructure, and human life in jeopardy. (Zhang et al., 2021: 1-2)

Extreme cold, as well as extreme heat, have both resulted in fatalities. Cold waves can cause hypothermia or frostbite, which can be fatal. According to a study conducted in 13 countries, deaths in moderately cold weather are higher than deaths in moderately warm weather, with over 74 million deaths recorded from 384 residential areas between 1985 and 2012. (Gasparrini *et al.*, 2015: 373; Kiraz, 2019, p. 8) The elderly and those in poor health are particularly vulnerable to extreme cold.

1.6. DROUGHT

Drought is defined as a temporary period in which precipitation falls below 80% of seasonal average values in meteorology, as a temporary period in which dams, lakes, ponds, and groundwater levels fall below long-term annual averages, and as a period in agriculture in which the water and moisture required by humans and other living things cannot be found in sufficient quantities. (AFAD, 2022) Drought must occur due to repeated, spreading over one or more seasons, decreasing precipitation, and increasing temperatures, in addition to affecting all natural resources that rely on the presence of water. However, drought, which is a current environmental security issue, has evolved into a full-fledged ecological disaster, with human-caused increases in frequency, severity, and consequences. Its risk is increased by anthropogenic climate change in several ways.

Droughts affect an estimated 55 million people worldwide each year, and endanger their livelihoods, raise the risk of disease and death, and drive mass migration. (WHO, 2022) Its conditions can have a negative impact on agriculture, water supplies, energy production, human health, and a variety of other societal aspects. The effects of a drought vary depending on its type, location, intensity, and duration. The effects on agriculture, for example, can range from slowed plant growth to severe crop losses, while the effects on water supply can range from lower reservoir levels and dried-up streams to major water shortages. Because



of their economic and cultural reliance on land and water supplies, prolonged droughts pose a particular threat to indigenous populations. Warming and drought can endanger medicinal and culturally significant plants and animals, as well as reduce water quality and availability, putting tribal populations at risk of waterborne diseases. Lowering streamflow and groundwater levels can also have a broader impact on ecosystems, harming plants and animals and increasing the risk of wildfires. (EPA, 2022) Water scarcity affects 40% of the world's population, and up to 700 million people may be displaced as a result of drought by 2030 (WHO, 2022). The years 2000–2021 in North America were the driest in at least 800 years, with the drought expected to last until 2022 (Park Williams *et al.*, 2022).

1.7. DESERTIFICATION

Desertification is the degradation of fertile soil quality caused by climate change, human activities, and natural factors in arid, semi-arid, and low rainfall regions. This problem is widespread across the globe, covering an area of 11.9 million km². This region is home to approximately 1.4 billion people. Climatic changes caused by excessive soil use, overgrazing, faulty irrigation methods, forest destruction, and deterioration of ecological balance are among the primary causes of desertification. (AFAD, 2022) But also, major national conflicts are linked to the land's diminished ability to support people, particularly in agriculture-based economies. It is difficult to establish causal relationships between conflicts and the land's ability to feed the people. Civil wars in Rwanda, Burundi, Ethiopia, Somalia, Kampuchea, and parts of Sri Lanka, Angola, Mexico, and the former Yugoslavia may have different causes. It is almost always triggered by communities threatened by land scarcity. Race, religion, population origin, and even caste may be used as justifications for the conflict, but the underlying cause is generally land and its quality. (Eswaran, 2022) It is estimated that approximately 50 million people will be displaced globally over the next ten years as a result of this reason (Başer, 2020).

1.8. WILDFIRES

As a result of natural causes, human neglect, or other factors. (AFAD, 2022) The increased frequency of forest fires, particularly in recent years, has drew attention. Fires have burned through millions of hectares of land, causing tragic consequences for wildlife and habitat loss, as well as financial losses for property owners. The economic losses from these fires reached millions of dollars. Rising temperatures in the Northern Hemisphere increase the risk of wildfires. In 2021, Northern India and Nepal will experience the worst forest fires in 15 years. These fires caused havoc on much of Australia in 2019, and the American West Coast, from California up to Oregon and Washington State, and later Colorado, in 2020. They are significant contributors to greenhouse gas emissions. According to Cal Fire, six of the top twenty largest wildfires in California history have occurred this year. Also, eight of the top ten largest wildfires occurred in the last ten years, and seventeen of the top twenty occurred since 2000. Since 2015, seven of the top ten most destructive wildfires have occurred. (WMO, 2022) For example, these wildfires were the largest in recorded history, and Hurricane Harvey in Texas in 2018 produced the most rainfall total in a single storm in the continental United States (Garfin, 2021: 1). The Amazon, the world's largest tropical forest, is also on fire, with a 60% increase in fire locations compared to 2019. (Uitto, 2021: 99) Summer temperatures in the Mediterranean and central Europe have been particularly high in 2021. In Türkiye and Greece, wildfires have wreaked havoc. (Frost, 2022) 275 forest fires erupted in Türkiye's 53 provinces during this time period (Remonews, 2022). For example, the Manavgat Wildfire, which began on July 28, 2021 and killed eight people, could be extinguished on August 12, 2021. More information about a wildfire near the town of Manavgat, east of the resort city of Antalya, Türkiye, on July 31, 2021, can be found on Map 2. Copernicus data (2022) show that the Mediterranean region is evolving into a hotspot for wildfires, with fire intensity reaching new highs in Türkiye this year. For more information, see Map below.

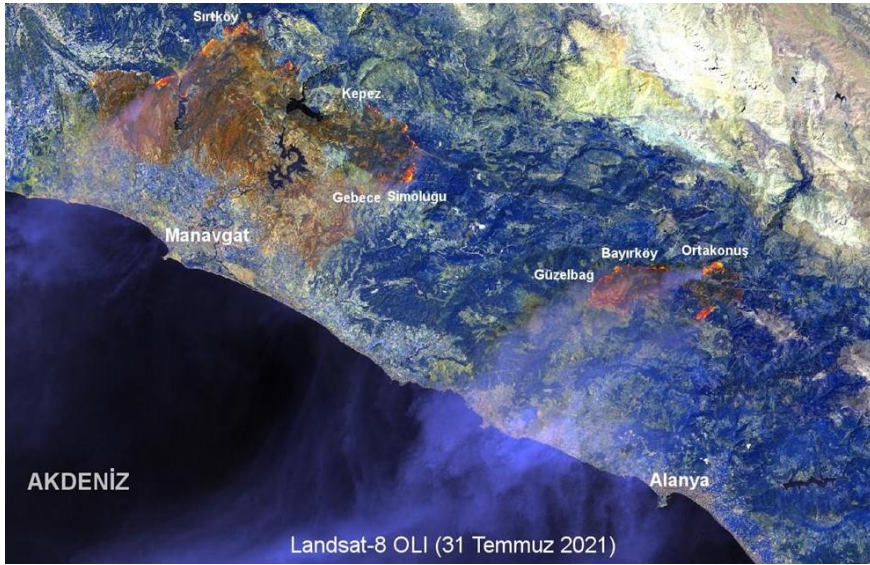


Figure 6. The Manavgat Fire in Türkiye on July 31, 2021
Source: (Gebze Technical University, 2022)

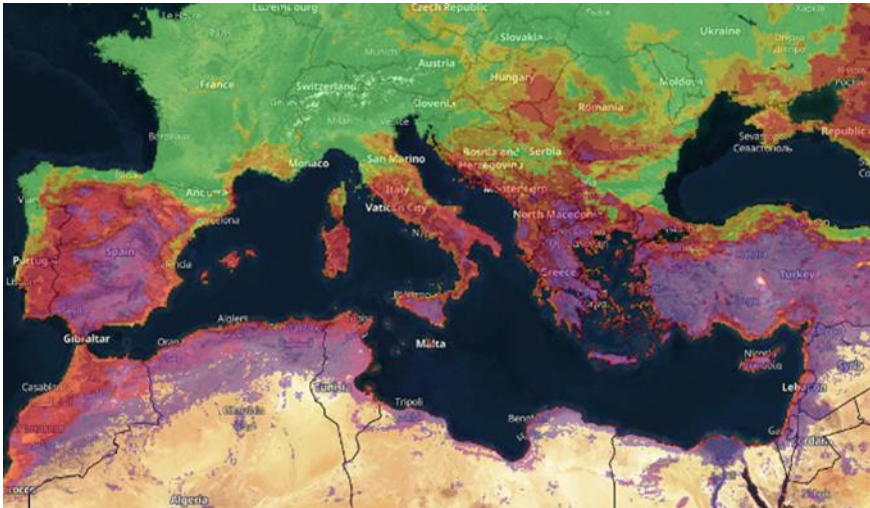


Figure 7. The severity of fires in Türkiye and the Mediterranean region during the summer of 2021
Source: (Copernicus, 2022)

Between 2008 and 2020, an average of 20,760 hectares of land was burned in Türkiye, a figure that increased by 75%. Greece, which was dealing with forest fires at the time, suffered a much higher loss, accounting for 1073% of the total. The average area lost in fires between 2008 and 2020 was 9.919 hectares, but the amount of burned area in Greece during this time period was 116.365. (Koyuncu & Altunkaya, 2022)



2. MATERIALS AND METHODS

When climate insecurity is combined with potential humanitarian, political, and economic issues, the country's insecurity and instability inevitably worsen. Climate change is considered an environmental crime by Interpol (2022), and it is recognized that it will harm ecosystems, including the human environment. From now on, law enforcement officers should implement strategies and policies aimed at mitigating and adapting to the climate security issue as part of their preventive law enforcement duties beyond the detection of environmental crimes. Because natural disasters strike our states on an irregular and unexpected basis, taking various forms and affecting us in various ways, exacerbating fragility. To be ready, the gendarmeries with military status, which are primarily responsible for maintaining public order and security in the majority of our countries, must develop institutional flexibility, which is defined as the ability to anticipate and respond to multiple threats and risks on both short and long-term perspectives, as well as the ability to welcome new analysis and competencies in terms of building resilience and reestablishing consistency. The gendarmerie and related its units must strengthen and increase their capability preparedness to respond to disasters wherever and whenever they occur, as well as undergo an internal transformation to become adaptable and capable of dealing with changing circumstances, in order to strengthen their role in disaster management.

In the face of the consequences of climate change, the gendarmeries have three basic responsibilities. These responsibilities include searching for and rescuing people in disaster areas caused by climate change, evacuating and relocating disaster victims, ensuring security in the disaster area, and providing disaster relief. However, there are few studies in the literature on climate-related disasters for law enforcement officers' critical infrastructures (airports, ports and harbors, roads, rail lines, tunnels, and bridges etc.), as well as the activities carried out by law enforcement officers who devote their lives to climate security. Briefly, it is critical that law enforcement officers adopt new strategies and policies that are consistent with precautionary environmental policies, in addition to their current basic responsibilities. This study is thought to be a pioneering study in this regard. The method used here is hypothetical-deductive reasoning supported by documental analysis and source triangulation.

Endogenous and exogenous strategic environments are be analyzed using the same methods as other articles in the first part of this study. Beginning with a PESTEL analysis, the factors influencing the Political, Economic, Social, Technological, Environmental, and Legal aspects of climate change are be identified. Following that, the SWOT matrix analysis is be used to determine whether these factors are strengthening or weakening the countries in their fight against the climate crisis, and what areas must be reinforced or can be ignored for the time being. Later, that matrix is transformed into a dynamic SWOT matrix to aid in the formulation of strategies. Finally, the information gathered and processed in the earlier stages is used to define the best strategies to follow in order to successfully counteract climate change based on the current situation.

3. RESULTS

3.1. EXTERNAL ENVIRONMENT ANALYSIS

The PEST analysis is presented in this study as one potential tool for understanding what the climate crisis may mean for law enforcement. The analysis is a method of examining political & legal, economic, social, and technological factors in order to identify what is important and to take immediate action, as well as to reveal who these factors affect positively or negatively, and provides a framework for considering macro-environmental factors that may arise as a result of climate change.

Table 8. PESTEL Analysis | Climate change and natural disasters ⁸

Factors	Key Macro Trends	Implications for Security Forces
Political & Legal	P.1. Return of power politics and tensions/conflicts, potentially leading to an increase in global and regional conflicts and tensions	1. Strengthening institutional adaptation and implementation strategies
	P.2. Persistence and expansion of areas of insecurity, conflict, and war	2. Ensuring that the issue of climate change adaptation is incorporated into existing strategies, plans, and legislation
	P.3. The formation of large groups of people in border regions as a result of large population movements caused by wars and conflicts	3. Increased energy efficiency standards and regulations for vehicles, appliances, and other items
	P.4. A greater emphasis and regulation on climate-related disclosure in terms of emissions as well as institutional adaptation and implementation strategies	4. Improved building regulations and standards for security forces' climate resilience and energy efficiency
	P.5. Increased energy efficiency standards and regulations for vehicles, appliances, and other items	5. Increasing and supporting policy support for renewable energy and energy efficiency
	P.6. Adopting policies that regulate different geographies and land uses, as well as providing incentives for climate-smart agriculture and afforestation	6. The impact of immigrants on natural resource security in destination or transit countries. People fleeing the Syrian Civil War, for example, were caused a water crisis in Jordan
	P.7. Increased air quality and CO2 regulations for vehicles and power plants, as pollution is becoming more regulated globally	7. More difficult border control tasks due to climate refugees, and taking precautions to protect civilians
	P.8. Enhanced building regulations and standards – for both climate resilience and energy efficiency	8. With an increasing demand for national and international cooperation among other security and defense actors such as NATO, OSCE, and the UN, a common mode of operation, similar to the C40 Cities Climate Leadership Group, can be adopted.
Economic	E.1. Because of unbalanced shifts in the global order and demography, global rivalry and fragility are likely to increase	1. Increased investment in new low-carbon technologies and business models like renewable energy, energy efficiency, electric vehicles, etc.
	E.2. The growing urbanization of the most developed countries, which is likely to exacerbate disputes over resource control	2. Increased research and development funding and incentives for renewables, energy efficiency, and clean-tech industries
	E.3. Pandemic (COVID-19) dictates contraction of the record economy, and the resumption of economic growth “will exponentially increase demand for scarce natural resources”, potentiating the emergence of new conflicts	3. Long-term shift to ultra-low-carbon vehicles and alternative modes of transportation
	E.4. Climate change may have a negative impact on trade because extreme weather events raise trade costs by destroying or degrading transportation infrastructure and reducing agricultural production	4. Enhanced incentives for resource efficiency and recycling, as well as increased penalties for inefficiencies
	E.5. The direct cost of climate change (about US\$7.9 trillion ⁹) to the global economy by mid-century is high as increased drought, flooding and crop shortages stunt growth and compromise infrastructure.	5. Increased reliance on carbon management as a proxy for organizational efficiency and productivity
	E.6. Rising capital costs for the development of high-carbon infrastructure, as well as projects that fail to address future climate impacts	6. Increased threats to critical infrastructures such as airports, ports and harbors, and roads, necessitating increased defence spending.
	E.7. Climate change and its consequences have a negative impact on our ability to effectively manage the risks associated with natural disasters.	

⁸ Main sources used: (Europol, 2021; NATO, 2017; The World Bank, 2022)

⁹ See also: (Galey, 2022; UCL News, 2022; Kikstra, 2021; UNEP, 2022)



Social	<p>S.1. At the same time that populations are becoming more empowered and demanding more, governments are under increasing strain from new challenges and limited resources. This widening chasm portends increased political volatility, deterioration of democracy, and expanded roles for alternative governance providers.</p> <p>S.2. Segregation and resource scarcity are being exacerbated by changes in global order and demographics</p> <p>S.3. Globalization is becoming more prevalent, as evidenced by rising population, migration flows, and the fragmentation of national identities</p> <p>S.4. The growing trend of climate-related security challenges, such as access to water and food</p> <p>S.5. Widening demographic disparities that may jeopardize regional stability and increase the likelihood of conflict</p> <p>S.6. Increased societal connections and links between lifestyle, well-being, and health, as well as lower emissions and cleaner cities in developed countries, as well as their best practices</p>	<ol style="list-style-type: none"> 1. Tasks that are more difficult to complete as a result of insecurity, migration, and scarcity 2. To increase urbanization, resources must be adjusted 3. Increased threats to critical infrastructures used for public service delivery 4. Continued and stepped-up efforts to establish links between the effects of climate change and the need for climate action. 5. Closer examination of institutional behavior and investments 6. Green organizational culture dissemination and internalization as a strategy for environmental sustainability
Technological	<p>T.1. An expanded role for information and communication technology and “big data”, as well as the rapid evolution of advanced analytics</p> <p>T.2. Stronger drivers and opportunities for relevant innovation</p> <p>T.3. Increased research and development in clean technologies and energy-efficient products and services</p> <p>T.4. New approaches to innovation – in response to Paris, responses are increasingly focusing on new business models such as the circular economy, which necessitates different economic actor relationships</p> <p>T.5. Smart cities, smart power grids, smart technology, and increased interactivity between individual lifestyles and technology</p> <p>T.6. New materials and processes, with a trend toward using fewer and recycled materials in the manufacture of new products.</p>	<ol style="list-style-type: none"> 1. Need for spending on police research in the field of new technologies 2. Increased interest in and support for clean technologies, use of solar panels, recycling of used equipment, uniforms and materials, use of electric vehicles 3. Increased research and development funding and incentives for renewables, energy efficiency, and clean-tech industries

Environmental	<p>EN.1. Climate change and other environmental challenges: Global warming is expected to exceed 1.5°C in the next 20 years and reach 2°C by mid-century, putting additional strain on water and food security around the world. By 2050, 200 million people will require humanitarian assistance, owing in part to environmental effects.</p> <p>EN.2. The physical effects of climate change are expected to worsen gradually in the near future.</p> <p>EN.3. The growing scarcity of resources and increasing global inequity</p> <p>EN.4. Extreme weather events that increase the likelihood of further environmental migration</p> <p>EN.5. Attitudes toward “green” or environmentally friendly products</p> <p>EN.6. The disparity in development between countries, as well as their desire for development, heightens the debate over how quickly certain measures should be implemented</p> <p>EN.7. Regulations are imposed by governments to combat climate change</p> <p>EN.8. Increasing frequency and severity of natural disasters, with global amplification of the consequences</p> <p>EN.9. Critical infrastructures related to energy generation are more vulnerable</p> <p>EN.10. The increased likelihood of extreme weather events, future pandemics, other natural and man-made disasters, and regional conflicts reaffirms the need for a more robust response and cooperation in security, civil protection, and defense, including improved prevention, preparedness, and response to disruptions.</p>	<ol style="list-style-type: none"> 1. Getting security forces ready for climate-related security threats, and its evaluation and analysis in the field of human security in particular 2. The need for security forces to address environmental issues related to climate change, as they affect social and environmental determinants of health such as clean air, safe drinking water, adequate food, and safe shelter. 3. Forests are critical in the fight against climate change, and their preservation is an important climate solution. 4. The direct negative impact of bases and infrastructures where security forces primarily operate in nature 5. Extreme weather conditions increase migration movements and raise the issue of border security 6. Because climate change has now become a national security issue, it is necessary for the institution’s personnel to be informed about the security implications and potential solutions to the issue, as well as to receive in-service training in this area. 7. The security forces’ field operations may suffer as a result. On the one hand, increasing extreme weather conditions can make working conditions difficult for personnel (extreme heat, disease spread, etc.); on the other hand, it can cause equipment to wear out faster. Furthermore, humanitarian crises and the insecurity caused by climate change can have an impact on logistics capacity.
---------------	---	---

3.2. INTERNAL ENVIRONMENT ANALYSIS

Following an analysis of the external factors affecting climate security, the McKinsey 7S Model is used to analyze the current situation of law enforcement in order to address them. This model identifies Structure, Strategy, Systems, Skills, Style, Staff, and Shared Values.

3.2.1. STRUCTURE AND STRATEGY

In the study, both structure and strategy are studied concurrently because they are closely linked in the field of climate change, and they are analyzed as the standard that states follow, and no law enforcement-specific structures and strategies are explained for security reasons.

The addition of greenhouse gases to the atmosphere in the fight against climate change, as is well known, increases the greenhouse effect, which is a natural process that causes the Earth to warm and the climate to change. The fundamental solution is to reduce global greenhouse gas emissions, particularly carbon dioxide. This entails making better use of natural resources, particularly energy. Because fossil fuels used in heating, cooling, and transportation, such as gasoline, natural gas, and coal, are major contributors to greenhouse gas emissions. Fossil fuels must be used in smaller quantities and with greater efficiency. As a result, the most effective way and strategy for law enforcement is to implement an effective energy and climate change policy, because the use of fossil fuels for energy is one of the primary causes of climate change. All law enforcement must transition away from the use of fossil fuels as soon as possible. As a policy and strategy, the security forces appear to be primarily



focused on clean and renewable energy, which includes technologies such as solar, wind, wave, tidal, and geothermal power. However, law enforcement officers are required to implement policies and measures in areas such as land use, transportation and waste in order to combat climate change.

In addition to the aforementioned efforts of law enforcement officials to reduce emissions from military activities and installations, because climate change is unavoidable, complementary actions to adapt to its effects are required. By predicting the effects of climate change, alignment is required, as are strategies and actions to take appropriate measures to prevent or mitigate these impacts. These actions should include technological measures, ecosystem-based measures, and behavioral change measures.

FIEP, like NATO, can actively participate in negotiations to establish comprehensive and functional international cooperation mechanisms in the fight against climate change, mitigation, and adaptation efforts. Members of the FIEP can adapt to climate change either individually or collectively. It has the ability to act within the framework of the collaborative approach. NATO's environmental community, for example (NATO, 2022), has been active in collaborative efforts with other international organizations such as the United Nations and the European Union. Discussions with industry, academia, and government agencies are also part of this approach. For its members, FIEP may develop a common strategy and action plan. They will be able to carry out their own processes using the units that the law enforcement forces will establish within their own body. It is possible to ensure that the appropriate emission inventory is prepared more thoroughly and that actions are taken within this framework. Law enforcement officers must understand the changes in the climate ecosystem as soon as possible, act against them, and adapt their institutional capabilities accordingly. Indeed, climate change and extreme weather conditions have a significant impact on the tactical, operational, and military-strategic levels (Goodman & Kertysova, 2022) of FIEP in terms of safety and security, ranging from increased storm frequency and intensity to extreme heat and cold, reduced drinking water supplies, and faster wear and tear of military equipment.

3.2.2. SYSTEMS

The Intergovernmental Panel on Climate Change (IPCC) may provide assistance in adapting FIEP's climate change strategies and capabilities. Because the FIEP's member countries are members of the IPCC, a United Nations body that evaluates the scientific aspects of climate change. IPCC scenarios based on representational concentration routes should generally serve as a guide for political action because they demonstrate strong scientific and national consensus. FIEP, like NATO, should thoroughly assess this consensus, which includes extreme scenarios and the dynamics of climate change processes, along with all of their risks. (Heise, 2022)

3.2.3. SKILLS

In order to adapt its capabilities to climate change, law enforcement agencies must incorporate climate change considerations into their work on resilience, civil preparedness, defense planning, capability delivery, assets and installations, standards, innovation, training, exercises, and disaster response. (NATO, 2022)

3.2.4. STYLE

In the security forces, the standard operating procedure is a well-defined hierarchy. This rigid hierarchy is even more visible in the case of law enforcement officers with military status. Despite this more traditional rigidity, the command style that has been adopted in recent years is centered on the figure of the leader, who takes advice from his subordinates but ultimately makes the decision that he believes to be most appropriate based on his own criteria.

3.2.5. STAFF

In general, there are few climate change specialists in law enforcement. In fact, all law enforcement agencies have some institutional arrangements in place to protect the environment and natural resources. However, because today's climate change issues have become a crisis, there is a need for security-based climate experts. During this transition period, assistance can be obtained from the IPCC's specialized personnel. In contrast to expert staff, specialists are sufficiently valued within law enforcement and are given training to the point where they can be considered experts. Disaster training for the gendarmerie should be expanded to include all personnel in this context.

3.2.6. SHARED VALUES

Security forces in all countries share similar values. The basic values of law enforcement officers with military status include honor, sacrifice, loyalty, austerity, discipline, abnegation, beneficent spirit, and service mentality. According to this:

1. *Honour*: The concept of a bond between an individual and a society as a quality of a person that is both of social teaching and of personal ethos, manifests itself as a code of conduct, and includes elements such as valour, chivalry, honesty, and compassion.
2. *Sacrifice*: A person's exposure to danger or serious work, as well as an act of self-sacrifice motivated by a sense of duty. It entails putting one's own life or well-being aside for the sake of others.
3. *Loyalty*: Obeying the demands of fidelity and honor.
4. *Austerity*: Moderation of one's senses and passions in the face of higher goals such as duty performance.
5. *Discipline*: Doctrine, a person's instruction. The meaning implies adherence to obedience principles that only know the moral limit of honor and the material limit of the Law.
6. *Abnegation*: The act of sacrificing one's will, affections, or interests, usually for professional or altruistic reasons.
7. *Beneficent spirit*: A benefactor who helps others. Putting the needs of others ahead of one's own.
8. *The service mentality*: Based on the principles of the rule of law, observing the public interest, impartiality, participation, transparency, accountability, focusing on the service result, and continuous improvement, it performs its duties and provides its services.



3.3.SWOT analysis

Table 9. SWOT analysis | Climate change and natural disasters

Internal factors	Strengths (S)	Weaknesses (W)
<p>External factors</p>	<ul style="list-style-type: none"> ▪ Existing climate change research ▪ Planning for land use ▪ Protected areas have been established ▪ Environmental balance that is favorable ▪ Scientists and policymakers will benefit from this information. ▪ Knowledge integration and international cooperation 	<ul style="list-style-type: none"> ▪ Low climate change awareness level ▪ Weak institutional capacity ▪ Inadequate climate change expert ▪ Inadequate strategy popularization ▪ Lack/insufficiency of existing norms ▪ Inadequate infrastructure
<p>Opportunities (O)</p> <ul style="list-style-type: none"> ▪ Mitigation and adaptation to climate change ▪ Better air quality ▪ Updating the legislation and regulations ▪ Preference for eco-friendly or eco-sustainable materials ▪ Establishment of climate change secretariat ▪ Establishment of authorities for protected areas ▪ New and low-carbon technologies ▪ Increasing organizational awareness and evolving the security forces' mission and vision 	<ul style="list-style-type: none"> ▪ Fulfilling the institutional structure, and updating the legal regulation for mitigation and adaptation ▪ Conducting climate change research ▪ Implementing environmentally friendly practices ▪ Increasing preventive observation (patrol) activities for environmental and wildlife protection 	<ul style="list-style-type: none"> ▪ Strengthening institutional capacity ▪ Recruiting qualified specialist personnel ▪ Developing a climate change strategy and releasing a road map ▪ Eliminating legal loopholes
<p>Threats (T)</p> <ul style="list-style-type: none"> ▪ The major problems of climate change: heatwaves, rising ocean temperatures, melting polar ice, increased storm activity, animal extinction and biodiversity loss, water shortages, deforestation and land degradation, more extreme and frequent droughts, floods etc. ▪ Displaced communities ▪ Critical infrastructure vulnerability ▪ Security aspects and conflicts ▪ Harming military power and the national economy ▪ High costs and limited financial resources 	<ul style="list-style-type: none"> ▪ Based on scientific data, being able to reveal and observe the problems caused by climate change ▪ Ensuring collaboration with relevant institutions based on existing problems ▪ Reducing loss through mitigation and adaptation strategies and policies ▪ Protecting critical infrastructure 	<ul style="list-style-type: none"> ▪ Increasing public awareness efforts ▪ Decreasing pressure on scarce resources ▪ Increasing the efficiency of scarce resource use ▪ Decreasing natural resource scarcity and disaster-induced migration mobility ▪ Reducing the risk of conflict ▪ Updating legal regulations

3.4. Strategies

When the SWOT matrix is finished, it is transformed into a dynamic SWOT matrix, in which strengths and weaknesses are combined with opportunities and threats to develop strategies to strengthen strengths and minimize threats.



Figure 8. Key strategies | Climate change and natural disasters

4. CONCLUSIONS & RECOMMENDATIONS

Climate change is having a negative impact on today's countries, making our living spaces unsafe. Despite the fact that they differ in terms of the development level of the countries in which they are located, they are affected by security risks. Climate change, in addition to severe meteorological events such as increased floods, storms, droughts, earthquakes, forest fires, and heatwaves, has serious consequences for our living spaces' critical infrastructures such as transportation networks, energy, water, and sewerage transmission lines, and food distribution systems, posing multiple risks to national security, which can lead to various crises.

The countries of the developed and developing worlds, which are vulnerable to the effects of climate change, promised to act in accordance with the targets they set in order to reverse this negative trend, particularly at all international meetings held under the leadership of the United Nations. However, the countries in question realized that they would not be able to meet the goals they set in these meetings if they did not abandon their development objectives, and they changed their policy in the 1990s. They adopted the policy of sustainable development, which is the policy of achieving development goals while protecting the environment, taking into



account society's development, and ensuring its continuity. Even today, despite the fact that this policy is still valid, there is a presumption that the climate has changed and will continue to change. As a result, when adverse climate conditions become severe and frequent enough to constitute a crisis, governments must strengthen and harden the measures in place to combat natural disasters. In many developed countries, it began at the national or local level. They have had a lot of success by focusing on the issue of sustainability with their reduction and adaptation policies. They act amongst themselves at times, particularly with new organizational models and networks, but they always act in accordance with climate action plans. However, reaching the desired level will be impossible unless these efforts at the local and regional levels are supported by comprehensive policies at the national, regional, and international levels. What to do in this case; is the adaptation of governments to the changing climate conditions.

In doing so, it is critical that law enforcement officers, who are viewed as indispensable members of society, mainly play a role in maintaining public order and security in the face of disasters caused by climate change. In accordance with the goal of protecting individuals' and society's rights and freedoms, these forces are tasked with assisting those in danger in the event of a disaster, including ensuring security, conducting search and rescue operations, and evacuation and resettlement activities. However, as the frequency, severity, and size of disasters increase, so does the importance of increasing the power and capacity of law enforcement officers. In this regard, in addition to the professional level in-service training that will be provided in law enforcement structures, it is also critical to take precautions to protect all types of law enforcement officers' buildings, facilities, and other structures from these disasters.

As the results of the strategic analysis based on the SWOT analysis show, there are many ways to increase efficiency in the fight against climate change, in line with the position and capacity of law enforcement, which plays a critical role in ensuring public safety. Accordingly, the following are the strategies proposed in the dynamic SWOT matrix for the law enforcements:

1. *Fulfilling the institutional structure, and updating the legal regulation for mitigation and adaptation*
2. *Conducting climate change research*
3. *Implementing environmentally friendly practices*
4. *Increasing preventive observation (patrol) activities for environmental and wildlife protection*
5. *Strengthening institutional capacity*
6. *Recruiting of qualified specialist personnel*
7. *Developing a climate change strategy and releasing a road map*
8. *Eliminating of legal loopholes*
9. *Based on scientific data, being able to reveal and observe the problems caused by climate change*
10. *Ensuring collaboration with relevant institutions based on existing problems*
11. *Reducing loss through mitigation and adaptation strategies and policies*
12. *Protecting critical infrastructure*
13. *Increasing public awareness efforts*
14. *Decreasing pressure on scarce resources*
15. *Increasing the efficiency of scarce resource use*
16. *Decreasing natural resource scarcity and disaster-induced migration mobility*
17. *Reducing the risk of conflict*
18. *Updating legal regulations*

In a nutshell, climate change will have an impact on all security forces and their tactical, operational, and military-strategic actions, albeit to varying degrees and at different times. Given the stakes of the changing, it is incumbent on each of us to do everything in our power to mitigate the harm. All of these strategies and policies, which are based on training, strategic planning, capacity building, and financing for successful implementation, can assist law enforcement in dealing with the effects of climate change and strengthening climate resilience.

REFERENCES

- AFAD. (n.d.). *Aşırı Sıcak*. In Açıklamalı Afet Yönetimi Terimleri Sözlüğü. Retrieved February 10, 2022, from <https://www.afad.gov.tr/aciklamali-afet-yonetimi-terimleri-sozlugu>
- AFAD. (n.d.). *Aşırı Soğuk*. In Açıklamalı Afet Yönetimi Terimleri Sözlüğü. Retrieved February 10, 2022, from <https://www.afad.gov.tr/aciklamali-afet-yonetimi-terimleri-sozlugu>
- AFAD. (n.d.). *Çiğ/ Çiğ Düşmesi*. In Açıklamalı Afet Yönetimi Terimleri Sözlüğü. Retrieved February 10, 2022, from <https://www.afad.gov.tr/aciklamali-afet-yonetimi-terimleri-sozlugu>
- AFAD. (n.d.). *Çökme*. In Açıklamalı Afet Yönetimi Terimleri Sözlüğü. Retrieved February 10, 2022, from <https://www.afad.gov.tr/aciklamali-afet-yonetimi-terimleri-sozlugu>
- AFAD. (n.d.). *Çölleşme*. In Açıklamalı Afet Yönetimi Terimleri Sözlüğü. Retrieved February 10, 2022, from <https://www.afad.gov.tr/aciklamali-afet-yonetimi-terimleri-sozlugu>
- AFAD. (n.d.). *Fırtına*. In Açıklamalı Afet Yönetimi Terimleri Sözlüğü. Retrieved February 10, 2022, from <https://www.afad.gov.tr/aciklamali-afet-yonetimi-terimleri-sozlugu>
- AFAD. (n.d.). *Heyelan*. In Açıklamalı Afet Yönetimi Terimleri Sözlüğü. Retrieved February 10, 2022, from <https://www.afad.gov.tr/aciklamali-afet-yonetimi-terimleri-sozlugu>
- AFAD. (n.d.). *Kaya Düşmesi*. In Açıklamalı Afet Yönetimi Terimleri Sözlüğü. Retrieved February 10, 2022, from <https://www.afad.gov.tr/aciklamali-afet-yonetimi-terimleri-sozlugu>
- AFAD. (n.d.). *Kuraklık*. In Açıklamalı Afet Yönetimi Terimleri Sözlüğü. Retrieved February 10, 2022, from <https://www.afad.gov.tr/aciklamali-afet-yonetimi-terimleri-sozlugu>
- AFAD. (n.d.). *Kütle Hareketleri*. In Açıklamalı Afet Yönetimi Terimleri Sözlüğü. Retrieved February 10, 2022, from <https://www.afad.gov.tr/aciklamali-afet-yonetimi-terimleri-sozlugu>
- AFAD. (n.d.). *Orman Yangını*. In Açıklamalı Afet Yönetimi Terimleri Sözlüğü. Retrieved February 10, 2022, from <https://www.afad.gov.tr/aciklamali-afet-yonetimi-terimleri-sozlugu>
- Akay, A. (2019). *İklim Değişikliğinin Neden Olduğu Afetlerin Etkileri*. İklim Değişikliği Eğitim Modülleri Serisi 15. T.C. Çevre ve Şehircilik Bakanlığı.
- Amadeo, K. (2020, February 10). *Hurricane Katrina Facts, Damage, and Costs: What Made Katrina so Devastating*. <https://www.thebalance.com/hurricane-katrina-facts-damage-and-economic-effects-3306023>
- Başer, H. F. (2020, February 12). *Çölleşme 10 yıl içinde 50 milyon insanı göçe zorlayabilir* (17.06.2020). <https://www.aa.com.tr/tr/dunya/collesme-10-yil-icinde-50-milyon-insani-goce-zorlayabilir/1879783>
- Belles, J. (2022, February 11). *Which Countries Get Hit the Most by Tropical Cyclones?* <https://weather.com/storms/hurricane/news/tropical-cyclone-hits-by-country-typhoon-hurricane>
- Buis, A. (2022, February 10). *Can Climate Affect Earthquakes, or Are the Connections Shaky?* <https://climate.nasa.gov/news/2926/can-climate-affect-earthquakes-or-are-the-connections-shaky/>
- Centers for Disease Control and Prevention (2022, February 11). *Extreme Heat*, Retrieved from February 11, 2022, from <https://www.cdc.gov/disasters/extremeheat/index.html>
- Copernicus. (2022, March 23). *Copernicus: Mediterranean region evolves into wildfire hotspot, while fire intensity reaches new records in Türkiye*. <https://atmosphere.copernicus.eu/copernicus-mediterranean-region-evolves-wildfire-hotspot-while-fire-intensity-reaches-new-records>
- COP26 (2022, January 23). *COP26 Goals*, Retrieved from January 23, 2022, from <https://ukcop26.org/cop26-goals/>
- Çolakoğlu, E. (2019). *İklim Değişikliği, Sürdürülebilir Kentler ve Kentsel Planlama Etkileşimi*. İklim Değişikliği Eğitim Modülleri Serisi 11. İklim Değişikliği Alanında Ortak Çabaların Desteklenmesi Projesi (iklimİN) (Avrupa Birliği ve Türkiye Cumhuriyeti tarafından finanse edilmektedir.). T.C. Çevre ve Şehircilik Bakanlığı.



- Çolakoğlu, E. (2016). Adapting to Climate Change in New York City and Regulatory Background, *Alternative Politics*, 8(1), 160-181.
- Disaster Center (2022, February 11). *Hurricanes and Tropical Storms*, Retrieved from February 11, 2022, from <https://disastercenter.com/New%20Guide/Hurricanes%20and%20Tropical%20Storms.html>
- Dosio, A. L. M., Fischer, E. M. & Wyser, K. (2018). Extreme heat waves under 1.5°C and 2°C global warming, *Environmental Research Letters*, 13, 1-10.
- DW (2018, June 22). *Italy's flooding crisis eases, leaving trail of death and destruction*, Retrieved from June 22, 2018, from <http://www.dw.com/en/italys-flooding-crisis-eases-leaving-trail-of-death-and-destruction/a-36537967>
- EPA (2022, February 12). *Climate Change Indicators: Drought*, Retrieved from February 12, 2022, from <https://www.epa.gov/climate-indicators/climate-change-indicators-drought>
- EPA (2022, February 20,). *Sources of Greenhouse Gas Emissions*, Retrieved from February 20, 2022, from <https://www.epa.gov/ghgemissions/sources-greenhouse-gas-emissions>
- Eswaran, H., Reich, P. & Beinroth, F. (February 12, 2022). *Global Desertification Tension Zones*. https://www.nrcs.usda.gov/wps/portal/nrcs/detail/soils/use/worldsoils/?cid=nrcs142p2_054030
- EUROPOL (2021). *A Corrupting Influence: The Infiltration and Undermining of Europe's Economy And Society by Organised Crime*, https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf
- Frost, Rosie (2022, February 13). *Turkiye, Greece and Italy: Which countries are being affected by wildfires and why?*. <https://www.euronews.com/travel/2021/08/12/european-heatwave-which-countries-face-the-biggest-risk-from-wildfires>
- Galey. P. (2022). *Climate impacts 'to cost world \$7.9 trillion' by 2050 (November 20, 2019)*. <https://phys.org/news/2019-11-climate-impacts-world-trillion.html#:~:text=Climate%20change%20could%20directly%20cost,infrastructure%2C%20new%20a%20analysis%20showed%20Wednesday>.
- Garfin, G., Falk, D. A., O'Connor, C. D., Jacobs, K., Sagarin, R. D., Haverland, A. C., Haworth, A., Baglee, A., Weiss, J., Overpeck, J., & Zuñiga-Terán, A. A. (2021). A new mission: Mainstreaming climate adaptation in the US Department of Defense, *Climate Services*, 22, 1-13.
- Gasparrini, A., Y. Guo, M. Hashizume, E. Lavigne, A. Zanobetti, J. Schwartz, A. Tobias, S. Tong, J. Rocklöv, B. Forsberg, M. Leone, M. Sario, M. Bell, Y.L. Guo, C. Wu, H. Kan, S. Yi, M. S. Zanotti, S. Coelho, P. Hilario, N. Saldiva, Y. Honda, H. Kim, & B. Armstrong (2015). Mortality Risk Attributable to High and Low Ambient Temperature: A Multicountry Observational Study, *The Lancet*, 386 (9991), 369-375.
- Gebze Technical University. (2022, March 23). GTU Maps Manavgat Fire. <https://www.gtu.edu.tr/icerik/8/12549/display.aspx?languageld=2>
- Goodman, S. and Kertysova, K. (2022). *NATO: An unexpected driver of climate action? (February 01, 2022)*. <https://www.nato.int/docu/review/articles/2022/02/01/nato-an-unexpected-driver-of-climate-action/index.html#:~:text=From%20higher%20frequency%20and%20intensity,tactical%2C%20operational%20and%20strategic%20levels>.
- Haddow, G. D., Bullock, J. A., Coppola, D. P. (2011). *Introduction to Emergency Management*, Burlington: Elsevier.
- Heise, R. (2022). *NATO iklim değişikliğinin getirdiği yeni sorunlara karşılık veriyor (April 01, 2021)*. <https://www.nato.int/docu/review/tr/articles/2021/04/01/nato-iklim-degisikliginin-getirdigi-yeni-sorunlara-karsilik-veriyor/index.html#:~:text=%C4%B0klim%20de%C4%9Fi%C5%9Fikli%C4%9Fi%20asker%C3%AE%20loji%20istik%20i%C3%A7in,a%C5%9F%C4%B1r%C4%B1%20de%C4%9Fi%C5%9Fikliklere%20kar%C5%9F%C4%B1%20%C3%B6zellikle%20hassast%C4%B1r>.

- Hough, P. (2014). *Environmental Security: An Introduction*, Routledge: Oxon.
- Insurance Information Institute (2020, February 10). *Facts + Statistics: Hurricanes*. <https://www.iii.org/fact-statistic/facts-statistics-hurricanes>
- INTERPOL. (2022, April 24). *INTERPOL marks a decade of tackling serious organized environmental crime* (23.11.2020). <https://www.interpol.int/News-and-Events/News/2020/INTERPOL-marks-a-decade-of-tackling-serious-organized-environmental-crime>
- IPCC (2021). *Climate Change 2021: The Physical Science Basis*, Working Group I Contribution to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change.
- IPCC (2019). *2018: Global Warming of 1.5°C. An IPCC Special Report on the impacts of global warming of 1.5°C above pre-industrial levels and related global greenhouse gas emission pathways, in the context of strengthening the global response to the threat of climate change, sustainable development, and efforts to eradicate poverty* [Masson-Delmotte, V., P. Zhai, H.-O. Pörtner, D. Roberts, J. Skea, P.R. Shukla, A. Pirani, W. Moufouma-Okia, C. Péan, R. Pidcock, S. Connors, J.B.R. Matthews, Y. Chen, X. Zhou, M.I. Gomis, E. Lonnoy, T. Maycock, M. Tignor, and T. Waterfield (eds.)].
- IPCC (2007). *Climate Change 2007: Impacts, Adaptation and Vulnerability* (Edit. Martin Parry, Osvaldo Canziani, Jean Palutikof, Paul van der Linden, and Clair Hanson). Cambridge University Press.
- Jones, Fred O. (1973). *Landslides of Rio de Janeiro and the Serra das Araras Escarpment, Brazil*, GEOLOGICAL SURVEY PROFESSIONAL PAPER 697, Prepared in cooperation with the Departamento Nacional da Producao Mineral of Brazil under the auspices of the Agency for International Development, United States Department of State, Washington, D.C.
- Kikstra, J.S., Waidelich, P., Rising, J., Yumashev, D., Hope, C. and Brierley, C.M. (2021). "The social cost of carbon dioxide under climate-economy feedbacks and temperature variability". *Environmental Research Letter*. 16(094037): 1-33.
- Kiraz, D. E. (2019). *İklim Değişikliğinin İnsan Sağlığına Etkileri*. İklim Değişikliği Eğitim Modülleri Serisi 11. İklim Değişikliği Alanında Ortak Çabaların Desteklenmesi Projesi (iklimiN) (Avrupa Birliği ve Türkiye Cumhuriyeti tarafından finanse edilmektedir.). T.C. Çevre ve Şehircilik Bakanlığı.
- Klizista-hr (2018, June 22). *Croatian Landslide Portal*. <http://www.klizista-hr.com/en/severe-weather-in-liguria-italy-caused-100-landslides/>
- Kostis, H. (2022, February 10). *Global Landslide Catalog (update 2019)*. <https://svs.gsfc.nasa.gov/4710>
- Koyuncu, H., & Altunkaya, T. (2022, February 15). *Türkiye’de 2021’de ne kadar ormanlık alan yandı? (16 August 2021)*. <https://tr.euronews.com/2021/08/15/turkiye-de-2021-de-yanan-ormanlik-alan-miktar-gecen-y-lara-gore-yuzde-755-artt>
- Lacerda, W.A., Coelho Netto, A.L., Sato, A.M. (2016). Technical report on landslide related disasters in Brazil, *Slope safety preparedness for impact of climate change* (Edited by Ken Ho, Suzanne Lacasse, and Luciano Picarelli), London: Taylor & Francis Ltd., 45-70.
- NATO (2022). *Environment, climate change and security* (December 03, 2021). https://www.nato.int/cps/en/natohq/topics_91048.htm
- NATO (2017). *Strategic Foresight Analysis, 2017 Report*, https://www.europol.europa.eu/cms/sites/default/files/documents/socta2021_1.pdf
- NSSL (2022, February 11). *Severe Weather 101*, Retrieved from February 11, 2022, from <https://www.nssl.noaa.gov/education/svrwx101/>
- Park Williams, A., Cook, B. I., & Smerdon, J. E. (2022, February 16). *Rapid intensification of the emerging southwestern North American megadrought in 2020–2021*. <https://www.nature.com/articles/s41558-022-01290-z.pdf>



- Rasmussen, C. (2022, February 10). *Sierras lost water weight, grew taller during drought*. <https://climate.nasa.gov/news/2663/sierras-lost-water-weight-grew-taller-during-drought/>
- Remonews (2022, February 15). *Breaking news ... Milas fire under control! This was announced by Minister Pakdemirli!*, Retrieved from February 15, 2022, from <https://remonews.com/Turkiyeeng/breaking-news-milas-fire-under-control-this-was-announced-by-minister-pakdemirli/>
- Rosenzweig, C. & Solecki, W. (2017, March 30). *Building climate resilience in cities: lessons from New York*. <https://www.newclimateforpeace.org/blog/building-climate-resilience-cities-lessons-new-york-0>
- Sardi, M., Volkwein, A., & Geilhausen, M. (2019). Connections between climate change and rockfall, *Geophysical Research Abstracts*, 21, 11421.
- Savi, S., Comiti, F., & Strecker, M. R. (2021). Pronounced increase in slope instability linked to global warming: A case study from the eastern European Alps, *Earth Surface Processes and Landforms*, 46, 1328 – 1347.
- Snow Brains (2022, February 10). *The Top 5 Deadliest Avalanches Ever Recorded (July 8, 2021)*, Retrieved from February 10, 2022, from <https://snowbrains.com/the-top-5-deadliest-avalanches-ever-recorded/>
- Snowsafes Blog (2022, February 10). *Which countries in Europe receive the most avalanches?*, Retrieved from February 10, 2022, from <https://www.snowsafes.co.uk/common-avalanche-countries-europe/>
- Sousa, R. L., Vargas Jr., E., Chaminé, H. I., Sousa, L. R., & Karam, K. (2021). Risk assessment on landslides focused on the role of the water: examples from model regions (Rio de Janeiro State and Hong Kong), *SN Applied Sciences*, 3.
- The World Bank (2022, April 24). *Trade and Climate Change* (September 07, 2021). <https://www.worldbank.org/en/topic/trade/brief/trade-and-climate-change>
- UCL News. (2022). *Economic cost of climate change could be six times higher than previously thought (September 6, 2021)*. <https://www.ucl.ac.uk/news/2021/sep/economic-cost-climate-change-could-be-six-times-higher-previously-thought>
- Uitto, J. I. (2021). Confronting storms, fires, and pestilence: Meaningful evaluation for a hazardous World, *Evaluation Matters—He Take Tō Te Aromatawai*, 7, 96-126.
- UNEP (2022). *Global temperatures: costs continued to soar in 2021 (January 21, 2022)*. <https://www.unep.org/news-and-stories/story/global-temperatures-costs-continued-soar-2021>
- WHO (2022, February 12). *Drought?*, Retrieved from February 12, 2022, from https://www.who.int/health-topics/drought#tab=tab_1
- WMO (2022, February 15). *Northern hemisphere summer marked by heat and fires (15 September 2020)*, Retrieved from February 15, 2022, from <https://public.wmo.int/en/media/news/northern-hemisphere-summer-marked-heat-and-fires>
- World Meteorological Organization (2022, February 11). *Extreme weather hits USA, Europe (19 February 2021)*, Retrieved from February 11, 2022, from <https://public.wmo.int/en/media/news/extreme-weather-hits-usa-europe>
- Zhang, Y., Yin, Z., Wang, H., & He, Shengping (2021). 2020/21 record-breaking cold waves in east of China enhanced by the ‘Warm Arctic-Cold Siberia’ patten, *Environmental Research Letters*, 16, 1-10.

IV. PAPER | DISPUTES OVER SCARCE NATURAL RESOURCES

The Case of the La Plata River Basin

Citation:

Orlando, A; Frias, A. Disputes over scarce natural resources. Overcoming Security Threats arising from Globalization 4.0 – FIEP Association, 2022.

Published: October 2022

Publisher’s Note: FIEP stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

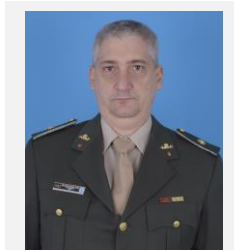


Copyright: © 2022 by the authors.

Country: Argentina

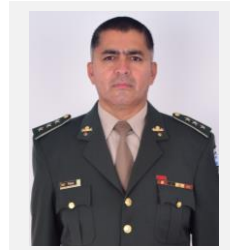
Institution: Gendarmería Nacional Argentina / Argentina National Gendarmerie

Orlando, A ¹ and Frias, A. ²



1

¹ angelorlando@gna.gob.ar



2

² angelfrias@gna.gob.ar

Abstract: Fresh water is one of the most valuable resources to maintain life on earth. Access to this resource is fundamental to preserve the biodiversity of a region and to promote its socioeconomic development. The La Plata River Basin is a water basin shared by five South American countries that use its rivers individually or collectively and with different purposes (water supply, power generation, transport, industrial or sewage discharges, etc.). The different types of uses of the Basin create potential risks that could affect the neighboring populations and cause large scale environmental and social issues. In this context, Federal Security Forces are essential actors to minimize the existing risks and to take action if anything happens. The application of the strategic diagnosis resulted in the identification of external factors, the assessment of existing opportunities and threats, and the identification of our Force’s strengths and weaknesses. This made it possible to outline the necessary strategies to anticipate and face the eventual scenarios posed as a consequence of extraordinary events that may affect the population and the environment. Finally, regional cooperation and commitment will lay the foundations for the Security Forces’ actions to prevent risks and mitigate adverse consequences on the population, to prevent the risks, provide an adequate answer, mitigate adverse effects and indirectly reduce the possibility of conflicts between States.

Keywords: natural resources; water; rivers; pollution; La Plata River Basin



1. INTRODUCTION

The topic addressed in this research work refers to problems caused by the degradation of a scarce natural resource shared by different countries. Knowing the causes and consequences of such an event would make it possible to design the course of action to reduce the damage and adopt the necessary projections to face new challenges.

The focus will be on the alteration of water quality caused by the degradation of a shared water basin (between a few countries) which, originating in one of them, affects the others downstream. The pollution of a watercourse can be caused progressively (by industrial or sewage discharges without adequate treatment) or suddenly (accidental or intentional spills of toxic substances).

The study will analyze the background and the current situation of the “La Plata River Basin”, which involves several South American countries, with the aim of identifying the challenges that the Security Forces would face in the face of a disaster situation originated by the degradation of a shared water resource. In particular, the aim is to describe possible consequences and to consider prevention and mitigation strategies.

Given the fact that many definitions exist for the terms mentioned, the following definitions will be adopted for the purposes of this work:

Water pollution: it is the introduction of any agent – chemical, physical or biological – the presence or accumulation of which has adverse effects on the natural environment, health and wellbeing of the population (FCEA - 2022)¹.

Disaster: social process, context or situation that is triggered as a result of a dangerous natural, socio-natural or anthropogenic phenomenon that, encountered with favorable conditions of vulnerability of a population or of a production structure or infrastructure, causes intense, severe and prolonged alterations in the normal working conditions of the affected country, region, zone or community, which cannot be faced or dealt with autonomously using the available resources. (González, 2022)².

Pursuant to the foregoing, the following table shows the general and specific objectives of this work, as well as the guiding questions:

OBJECTIVE	QUESTION
General: Determine the challenges to be faced by the Security Forces in a disaster situation, caused by the degradation of a shared water resource.	What challenges would the Argentine Gendarmerie face in a disaster situation caused by the degradation of a shared water resource?
Specific 1: Describe the current capacity of the Argentine Gendarmerie to take action in the face of an unexpected sudden event in the region of the La Plata River Basin.	What is the current capacity of the Argentine Gendarmerie to take action in the face of an unexpected sudden event in the region of the La Plata River Basin?
Specific 2: Identify the structural needs and the political instruments that make it possible to face new challenges efficiently.	Which resources are necessary to face new challenges efficiently?

1.1. THEORETICAL AND CONCEPTUAL FRAMEWORK

Resource depletion, environmental degradation and climate change pose fundamental threats to human security. Alone or in combination with other factors, they can destabilize livelihoods, adversely affecting ecosystems and undermining peace and development. Violent conflict can emerge where local and national institutions lack the capacity to resolve disputes that may arise from **resource degradation or depletion** (UN - Land, natural resources and conflict prevention)³.

The concept of “resource scarcity” describes a situation in which the supply of natural resources, such as water, forests, pasture and arable land, is not sufficient to meet demand. Increasing scarcity of renewable natural resources needed to sustain livelihoods can intensify rivalry between user groups. There are three main causes of increasing resource scarcity, acting individually or in combination: Demand-induced scarcity: Demand-induced scarcity arises when demand for a given renewable resource cannot be met by the existing supply [...]. Supply-induced scarcity: Supply-induced scarcity occurs when environmental degradation, **pollution**, natural variation, or a breakdown in supply infrastructure limits or **reduces the total supply or local availability of a given resource**. With a reduced supply of natural resources, options for undertaking productive livelihood strategies are undermined, **leading to potential rivalry among subsistence groups**. Structural scarcity: “Structural scarcity” occurs when different groups within a society have unequal access to resources (EU- UN Partnership)⁴.

The United Nations Environment Programme (UNEP) suggests that, over the past 60 years, at least 40 percent of all intra-state conflicts were related to natural resources and that this relationship doubled the risk of renewed conflict within the first five years. Since 1990, at least 18 violent conflicts have been driven by the exploitation of natural resources; whether “high-value” resources such as timber, diamonds, gold, minerals and oil, or low-value resources such as fertile land and water (UN - Conflicts and natural resources)⁵.

The purpose of early warning, risk assessment and scenario analysis measures is to identify threats to natural resources and potential hotspots of conflict before they escalate. These include data collection, analysis and forecasting, as well as dissemination of risk information to specific audiences, including communities and decision-makers. The use of early warnings, risk assessments, and scenario analysis to identify potential hotspots of conflict related to renewable resources should be an important cross-cutting input variable in any specific conflict prevention program (EU – UN Partnership)⁶.

1.1.1. WATER

Freshwater resources are crucial for human health and ecosystems, as well as for economic development. Almost every sector of human activity depends on water, whether for drinking, agriculture, industrial production, or power generation (EU- UN Partnership)⁷.

At the United Nations Conference on the Human Environment, held in Stockholm in 1972 it was proclaimed that “...man’s capability to transform his surroundings, if used wisely, can bring to all peoples the benefits of development and the opportunity to enhance the quality of life. Wrongly or heedlessly applied, the same power can do incalculable harm to human beings and the human environment. We see around us growing evidence of man-made harm in many regions of the earth: dangerous levels of pollution in water, air, earth and living beings; major and undesirable disturbances to the ecological balance of the biosphere; destruction and depletion of irreplaceable resources; and gross deficiencies, harmful to the physical, mental and social health of man, in the man-made environment, particularly in the living and working environment.” (UNEP 1972)⁸

Water is fundamental to life and access to safe drinking water is a human right and should be considered as such. Water scarcity, lack of access, water quality problems, and inadequate sanitation affect food



security, nutrition, and educational and economic opportunities for poor families around the world. (Torrero – 2020)⁹.

On July 28, 2010, the UN General Assembly Resolution No. 64/292 “The human right to water and sanitation” recognized that the right to safe drinking water and sanitation is an essential human right for the full enjoyment of life and all human rights. The main sources of conflict over water include: ... degradation of water quality due to pollution (industrial, agricultural, urban). (UN – 2010)¹⁰.

In terms of state and regional policy, the UN World Water Development Report 2020 states that “The challenges of development, poverty eradication and sustainability are intricately interwoven with those of climate change mitigation and adaptation, especially through water. Water is not a sector, but a connector and the impacts induced by climate change touch all aspects of our society (economic, social and environmental) (White, 2018). Strong political will and leadership are needed to highlight and mainstream water’s value in implementing the global agreements” (UNESCO – 2020)¹¹.

1.1.2. THE LA PLATA RIVER BASIN

The La Plata River Basin is one of the most important in the world due to its geographic extension and the volume of its rivers. It occupies one fifth of South America, covering the territories of five countries: Argentina, Bolivia, Brazil, Paraguay and Uruguay.

The waters of two large rivers converge in the Río de la Plata: the Paraná and the Uruguay, which in turn collect the flow of other very important rivers, such as the Paraguay, the Bermejo, the Pilcomayo and the Iguazú, among many others, as shown in figure 1. (MAyDS - 2021)¹².

It covers an area of some 3,170,000 km², making it the second largest in South America and the fifth largest in the world, after the Amazon, Congo, Nile and Mississippi.

Through its wide mouth into the Atlantic Ocean, the La Plata River Basin delivers a flow of 25,000 m³/s to the sea.

The limits of the territory do not coincide with the borders of the countries (figure 2), so the States (as administrative jurisdictions) established agreements for their management. The strong process of regional integration, initiated in 1969 with the Treaty of the La Plata River Basin and, later, with Mercosur, constitutes a model in the ties established with respect for diversity. (COMIP – 2021)¹³.



Figure 9. Countries involved in the basin (10) (COMIP – 2021)¹³



Figure 10. Main rivers that form the La Plata River Basin (OAS – 2004)¹⁴

Four of the five national capitals of the countries that make up the Basin: Buenos Aires, Brasilia, Asuncion and Montevideo, are located within the Basin, which is home to more than 50% of the population of the 5 countries... If current trends continue, it is estimated that by 2025 the population of the countries of the subregion will reach 290 million inhabitants and that the Basin will capture more than half of this growth, further increasing the pressure on the use of water resources.

In this context, it is worth mentioning that one of the facts underscored by the UN regarding Sustainable Development Goal 6 for Clean Water and Sanitation states that “Over 1.7 billion people are currently living in river basins where water use exceeds recharge” and that “More than 80 per cent of wastewater resulting from human activities is discharged into rivers or sea without any pollution removal”. (UN – ODS – 2022)¹⁵.

The needs of trade press for a better use of rivers for transportation within the framework of a common market agreed through MERCOSUR, in which Argentina, Brazil, Paraguay and Uruguay participate and in which Bolivia is associated. This situation causes an increase in water traffic, which directly affects the “Paraná – Paraguay Watercourse”.

Argentina’s river coast is a gigantic corridor of wetlands that integrates the Paraguay - Paraná system, which originates in the Pantanal and forms the southern part of it. Located in the Neotropics, the region represents the largest source of surface water and the largest inland fishery in the country. It coincides with the most important population axis of Argentina, housing seven million people without counting the city of Buenos Aires, whose fresh water supply depends on the basin and which, together with the Buenos Aires suburbs, has a population of more than 12 million people. (IUCN – 2009)¹⁶.

Recommendation 2.85, Conservation of the Middle and Lower Paraná River, of the II IUCN World Congress, Amman 2000, promoted by PROTEGER, called to “give priority to the most important wetland corridor in the world, from the Pantanal of Mato Grosso to the Rio de la Plata” (12).



The II World Conservation Congress held by the IUCN in Amman, Jordan in 2000, recalled that the La Plata Basin extends from the Pantanal of Mato Grosso to the Rio de la Plata and recommended that the Argentine Government “... give the highest priority to the implementation of conservation and rational use measures related to the maintenance of the essential ecological conditions and processes of the middle and lower Paraná River” (IUCN - 2000)¹⁷.

2. MATERIALS AND METHOD

The development of this research work was carried out from a qualitative approach to the extent that bibliographic data was collected and analyzed from 1960 to date, with the purpose of “... refining research questions or revealing new questions...” and has an inductive logic and process “...to explore and describe, and then generate theoretical perspectives”. (Hernández Sampieri, 2014)¹⁸.

For the fulfillment of the general and specific objectives set, the information and data collected were analyzed through the strategic diagnosis method. For this purpose, external (PESTEL) and internal (SWOT) environment analysis tools were used. These tools facilitated the identification of situations that imply some type of opportunity or threat and from them reflect on the strengths and weaknesses of the Institution in each case.

Based on this structured information, the analysis made it possible to outline strategies and practices that would make it possible to face the challenges posed.

3. RESULTS

The results of the analysis of the data obtained from the different sources consulted will be presented below. First, the results of the analysis of the external environment carried out through the PESTEL method will be detailed, followed by the analysis of the internal environment through the dynamic SWOT.

3.1. PRESENTATION OF DATA

3.1.1 Analysis of the external environment: PESTEL method

Table 10. PESTEL analysis | Disputes over scarce natural resources

Factors	Key Macro Trends	Implications for Security Forces
Political & Legal	<p>P.1. The La Plata River Basin Treaty promotes international cooperation.</p> <p>P.2. The main sources of water conflict include degradation of water quality due to contamination</p> <p>P.3. The creation of MERCOSUR promotes a process of regional integration</p> <p>P.4. Mercosur Framework Agreement on the Environment, which includes sustainable management of water resources and basic sanitation and drinking water.</p> <p>P.5. Need to harmonize the regulatory regime for managing water resources as river basins.</p>	<ol style="list-style-type: none"> 1. Increased cooperation with forces from neighboring countries 2. Increased requirement for resource quality monitoring 3. Demand for coordination and cooperation for the development of operational and control activities simultaneously with police and security forces of neighboring countries. 4. Basic legal framework for relations between security forces 5. Improved tools for joint control and data and information exchange
Economic	<p>E.1. Trade needs are pushing for a better use of rivers for transportation within the MERCOSUR framework.</p> <p>E.2. Increasing industrial development near watercourses increases the risk of contamination</p> <p>E.3. Regional movement of hazardous substances increases the risk of accidents and deterioration of water resources.</p>	<ol style="list-style-type: none"> 1. Increased control and supervision of river and land transportation 2. Increased quality control of industrial effluents 3. Survey and analysis of the risks of possible incidents and intervention in contingency plans. 4. Possible entry into the country of non-permitted substances
Social	<p>S.1. The freshwater supply of the city of Buenos Aires and surrounding areas (12 million people) depends on the La Plata River Basin. The alteration of the resource would provoke a social emergency.</p> <p>S.2. Possible migratory movements to unaffected areas</p>	<ol style="list-style-type: none"> 1. Need to reinforce the elements located in the vicinity of the La Plata River Basin by redeploying personnel 2. Highlight the mission to support the community as part of the National Defense System. 3. Urgent demand for specialized personnel and resources in border areas. 4. The different problems that are not addressed in the Force's areas of responsibility would have a negative impact on the Institution. 5. Increased population control and assistance functions. Increased need for personnel
Technological	<p>T.1. Early warning measures include data collection, analysis and forecasting.</p> <p>T.2. Low implementation of clean and non-environmentally degrading technologies</p>	<ol style="list-style-type: none"> 1. To monitor environmental parameters in areas that lack technology to evaluate the quality of water for consumption by their inhabitants. 2. Budgetary restrictions for upgrading technological resources 3. Enable the implementation of prevention and control tools and mechanisms that act jointly and in coordination with the different police and security forces in the region.
Environmental	<p>EN.1. Environmental degradation can negatively affect ecosystems and undermine peace and development.</p> <p>EN.2. Need to protect the region's wetland corridor</p> <p>EN.3. Global climate change generates different types of environmental emergencies.</p>	<ol style="list-style-type: none"> 1. Lack of a specialized Force for the protection and conservation of natural resources 2. The geographical and environmental characteristics of the area of interest make control and surveillance tasks difficult. 3. As a member of the National System for Integrated Risk Management (SINAGIR), strengthen institutional actions.



3.1.2 Analysis of the internal environment: DYNAMIC SWOT method

Table 11. SWOT analysis | Disputes over scarce natural resources

Internal factors	Strengths (S)	Weaknesses (W)
	<ul style="list-style-type: none"> • Rapid response capability to assemble and mobilize personnel. • Permanent border control and surveillance through the Units distributed throughout the national territory. • Relations with foreign police and security forces. • Positive image in the eyes of the population for the different tasks performed by the Force. • Personnel with specific training in environmental protection. • Stewardship of strategic objectives for the country. 	<ul style="list-style-type: none"> • The movement of personnel to locations of greater need would mean neglecting the functions currently assigned to them. • Budgetary restrictions for the updating of technological resources. • Limited material resources to cover large areas of land. • Lack of public awareness of environmental protection and community support functions. • Lack of own means for air transportation of personnel and equipment. • Prolonged staff incorporation and training processes.
<p>External factors</p> <p>Opportunities (O)</p> <ul style="list-style-type: none"> • Need to reinforce the elements located in the vicinity of the La Plata River Basin by redistributing personnel and resources. • Lack of a specialized force for the protection and conservation of natural resources. • Coordination and cooperation for the development of operational and control activities simultaneously with police and security forces of neighboring countries. • To enable the implementation of prevention and control tools and mechanisms that act jointly and in coordination with the different police and security forces in the region. • As a member of the National System for Integrated Risk Management (SINAGIR), strengthen institutional actions in the La Plata River Basin area. 	<ul style="list-style-type: none"> • Allocate human and material resources to increase the presence of the Institution in places where it is urgently needed. • As a result of its presence throughout the national territory, to position itself as a benchmark institution in the preservation of natural resources. • Through agreements with different agencies and foreign police and security forces, materialize the execution of coordinated operational activities. • Jointly with police and security forces in the region, and based on the legal framework of each country, design and implement prevention and control tools and mechanisms. • Based on the hydrometeorological information prepared by the National Emergency Alert and Monitoring System (SINAME), strengthen the actions of the different Units distributed throughout the national territory to prevent, alert and intervene in case of possible emergencies. • Strengthen, with personnel and resources, the Force's laboratories to provide them with the capacity for chemical and bacteriological water analysis. • Replicate and exchange technologies with external security and police forces on the basis of framework agreements. • Through different technological tools, disseminate the permanent action and use of human and material resources in support of the community. 	<ul style="list-style-type: none"> • Maintain a balance between the movement of personnel and resources with the incorporation of human resources and the acquisition of new materials. • Update personnel training and provide technical equipment for the development of tasks in the different areas of responsibility. • To have human and material resources available for the execution of coordinated activities. • The diversity of regulations in the region and the lack of harmonization of these regulations requires the intervention of different agencies and consensus among the parties, which will be strengthened by working together. • Train personnel in the analysis of information and data provided by specific environmental agencies. • Develop contingency plans to be established by the participating actors in the event of emergencies. • Adequate technological means to transmit and disseminate alert information quickly and accurately. • Manage material and technological resources to strengthen the laboratory's capacity for action and provide means for the collection, transfer and analysis of samples. • To broaden the concept of the Force's field of action and incorporate permanent support to the community as another activity that requires the use of material and human resources.

Threats (T)		
<ul style="list-style-type: none"> • The different problems that are not addressed in the Force's areas of responsibility would have a negative impact on the Institution. • Budgetary restrictions for upgrading technological resources • Urgent demand for specialized personnel and resources in border areas. • The geographic and environmental characteristics of the area of interest make control and surveillance tasks difficult. • Increased control and assistance to the population. Increased need for personnel and means of mobility. 	<ul style="list-style-type: none"> • Identify and analyze the risks in the areas of responsibility of the Force. Based on these risks and the available means, design actions for their prevention and/or mitigation. • Based on the projected activities and the prioritization of needs, manage the allocation of budgets that will allow completing and maintaining them in the short, medium and long term. • In accordance with the risk analysis carried out, establish mechanisms to plan the acquisition and incorporation of specialized personnel and resources. • Within the framework of existing agreements with security and police agencies and forces of neighboring countries, coordinate joint actions to minimize risks. • Provide for increased staffing requirements and the acquisition of mobility resources. 	<ul style="list-style-type: none"> • Efficient use of human and material resources currently available until the acquisition and incorporation of new elements to strengthen the planned tasks. • Optimize the use of available technological resources. • Efficient use of resources to provide an adequate response to the needs until they are updated. • Intensifying operational and prevention tasks in adjacent areas • Reformulate onboarding and training procedures for emergency situations

4. DISCUSSION

Fresh water is one of the essential resources to maintain the quality of life on the planet. Socioeconomic development, food production, climate change and global biodiversity have water as a common axis and its quality has a direct and indirect impact on human health.

Concern about the state of this natural resource and the importance of its conservation and preservation led the Member States of the United Nations to make commitments on several occasions for its proper management. The latter were embodied in the 2030 Agenda for Sustainable Development, which included 17 Sustainable Development Goals, with Goal 6 corresponding to Clean Water and Sanitation, and the proclamation of the period 2018-2028 International Decade for Action "Water for Sustainable Development", in order to promote initiatives aimed at the conservation of water resources.

The different commitments assumed over time marked a considerable advance in the management of water resources, it is within this framework that in 2002 Argentina passed Law 25.688 Environmental Water Management Regime, incorporating the concept of water basins as an indivisible environmental unit of management. Over time, this trend will allow the establishment of actions and policies agreed upon by all the jurisdictions involved.

In addition to internal management, there are regional and bilateral agreements that promote projects for the use of water resources (energy, navigation, fishing, etc.) to foster the economic growth of the region. The different uses to which the basin's watercourses are currently subjected pose risks that will increase with population and economic growth in the region.

In this sense, it is considered that regional development and its consequent increase in risks should be accompanied by policies that contemplate the conservation of the resource. Particularly the strengthening of institutions with the competence to intervene in the event of an incident that negatively impacts the resource and generates an international conflict. Although Principle 18 of Agenda 21 proclaims that "States should immediately notify other States of natural disasters or other emergency situations that may produce sudden harmful effects on the environment of those States" (UN - 1992)¹⁹, as well as in the Additional Protocol to the



MERCOSUR framework agreement on the environment regarding cooperation and assistance in the event of environmental emergencies (MERCOSUR - 2004)²⁰, it is necessary to establish regional mechanisms that allow States to act jointly to mitigate the effects of an event of these characteristics.

Based on the results of the analysis of the situation and the political, economic, social, technological, environmental and legal characteristics of the study area, the identification of related opportunities and threats, and the recognition of the institution's own strengths and weaknesses, the following strategies have been proposed to anticipate and confront possible scenarios that could result from exceptional events that put the population and the environment at risk.



Figure 11. Key strategies | Disputes over scarce natural resources

5. CONCLUSIONS & RECOMMENDATIONS

Access to drinking water is a vital need for human beings and constitutes an essential right. The alteration of the quality of this resource can give rise to emergency situations that must be dealt with immediately. Therefore, advance planning and adoption of measures are essential to successfully meet emerging demands. In this sense, considering the structure, territorial deployment and training of the National Gendarmerie personnel, as a Security Force of Military nature with the characteristics of an Intermediate Force, it is the most appropriate institution to intervene in environmental and social emergency situations that require the assistance of the State. In this context, since this is a regional problem, there is a need to implement, within the existing regional political framework, cooperation mechanisms between the institutions involved in prevention and response, which allow the execution of all the necessary actions. In particular, all foreseeable risks, their consequences and possible evolution should be considered; the necessary and available human, material and technological resources; early warning systems and mass dissemination of information. At the same time, these actions should be complemented by the regional harmonization of the regulatory framework governing the use and establishment of quality parameters for the resource.

The subsistence of the strategic resource will depend on regional cooperation, since unilateral efforts would be inefficient to manage a shared resource that does not recognize political divisions. Therefore, the commitment and action of all the actors involved is indispensable.



REFERENCES

- Fondo para la Comunicación y la Educación Ambiental
<https://agua.org.mx/contaminacion-del-agua/>
- González, Fernando Antonio Ignacio “Algunas reflexiones sobre el concepto de desastre natural”, Revista Brasileira de Geografía y Economía, número. 22, 2021
<http://journals.openedition.org/espacoeconomia/21037>
- Tierra, recursos naturales y prevención de conflictos: del infortunio a la oportunidad (UE– ONU)
<https://www.un.org/es/land-natural-resources-conflict/renewable-resources.shtml>
- Alianza UE – ONU Informe Recursos renovables y conflicto
https://www.un.org/es/land-natural-resources-conflict/pdfs/GN_Renew.pdf (p.9)
- ONU - Conflictos y recursos naturales
<https://peacekeeping.un.org/es/conflict-and-natural-resources>
- ONU - Conflictos y recursos naturales
https://www.un.org/es/land-natural-resources-conflict/pdfs/GN_Renew.pdf (p.67)
https://www.un.org/es/land-natural-resources-conflict/pdfs/GN_Renew.pdf (p.71)
- UNEP –Stockholm Declaration on the Human Environment. 1972
https://wedocs.unep.org/bitstream/handle/20.500.11822/29567/ELGP1StockD_SP.pdf?sequence=5&isAllowed=y
- Torrero, Mariana Paula. Geografía del conflicto y el acceso al agua potable como derecho humano. Revista Escuela Superior de Guerra. Marzo 2020 (p 134)
- UN – General Assembly Resolution No 64/292
https://www.un.org/ga/search/view_doc.asp?symbol=A/RES/64/292&Lang=S
- UNESCO - UN World Water Development Report 2020: Water and climate change. (p. 51)
<https://unesdoc.unesco.org/ark:/48223/pf0000373611.locale=es?msclid=2824b1d0b42611ecb662e82f31cd83fc>
- MAyDS – Política Ambiental en Recursos Naturales - Cuenca del Plata
<https://www.argentina.gob.ar/ambiente/agua/cuencas/delplata>
- COMIP – La Cuenca del Plata: La quinta del mundo.
<https://comip.org.ar/la-cuenca-del-plata/>
- The invisible resource Transboundary aquifers: an opportunity for international cooperation. Number 3 - 2004 (p. 2)
<https://biblioserver.sernageomin.cl/opac/DataFiles/12085.pdf>
- UN – Sustainable Development Goals - Goal 6: Clean Water and Sanitation
<https://www.un.org/sustainabledevelopment/es/water-and-sanitation/>
- UICN – Mapeo Preliminar de la Cuenca del Plata. (p. 4). 2009
https://www.iucn.org/sites/dev/files/import/downloads/02_argentina.pdf
- UICN – Congreso Mundial de la Naturaleza, Amman 2000. Recomendación 2.85 Conservación del río Paraná medio e inferior.
https://portals.iucn.org/library/sites/library/files/resrecfiles/WCC_2000_REC_85_ES.pdf?msclid=12773e0ab42b11eca1aedb95fb802829
- Hernández Sampieri R. Metodología de la Investigación. Ed 6ta. 2014, (p.7 y p.8)
- UN - Rio Declaration on Environment and Development. 1992
<https://www.un.org/spanish/esa/sustdev/agenda21/riodeclaration.htm>
- Protocolo adicional al acuerdo marco sobre medio ambiente del MERCOSUR en materia de cooperación y asistencia ante emergencias ambientales (art 4) MERCOSUR/CMC/DEC. Nº 14/04

V. PAPER | FRAGILE STATES AND REGIONAL CONFLICTS

Citation:

Temeiza, G. A.; Overcoming Security Threats arising from Globalization 4.0 – FIEP Association, 2022.

Published: October 2022

Publisher's Note: FIEP stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors.

Palestine

Ghada A.Temeiza

Abstract: This research paper aims to address the issue of regional conflicts and fragile states within the concept of globalization 4.0, as threats and security challenges are imposed on weak regimes creating a major challenge not only in maintaining security and civil peace, but also in continuity and an existential threat.

The SWOT strategic analysis methodology was used in this research paper to analyze the general and internal environment of the National Security Forces to show the strengths and weaknesses and the most prominent opportunities and threats facing the Palestinian National Security Forces to answer the main question of the study *“How do Israeli policy and procedures affect the work of Palestinian security in maintaining order in the state of Palestine?”*.

The results have shown that the security conditions due to the stagnation of the political process and Israel’s refusal to implement the international resolutions issued by the Security Council, the United Nations and the Human Rights Council are sufficient enough to disrupt and weaken the security work of the Palestinian security forces to maintain public order and civil peace and to carry out their tasks professionally.

The National Security Forces have professionally trained personnel who can manage matters within limited capabilities, but this requires putting pressure on the Israeli regime to implement the agreements signed by international partners, the effective regimes in international politics, and the institutions of international legitimacy.

Keywords: Fragile States; Regional conflicts.



1. INTRODUCTION

Security is considered to be one of the most important major issues that different human societies have been steadily preoccupied with until this day, which many thinkers agreed to call it the era of globalisation, and in which the security issue in its different dimensions (economic, political, social, psychological and moral) has taken the lead, as countries today are taking massive arrangements and procedures by putting the best financial and human capabilities for it. And this is supported by the saying “studies in security in the terms of its concepts, foundations, guarantees, requirements and types are the best to ensure the progress of the society”.

Among the most inclusive forms of security and most notably the issue of “national security” a concept appeared in the recent decades after it was established firstly in the United States of America after World War II and then in European countries such as France, Germany and Britain, after that it was outspread to the rest of the world. This concept took its importance from linking “security, homeland and the national state” all together.

National security is not an issue related to authority and its survival or to a group of people and their interests, it is an issue of the present and future nation. National security has many various concepts and definitions where there are some narrow concepts that concentrate on partial interests related to state security such as internal security, military capabilities, the efficiency of intelligence operations and anti-terrorism. On the other hand, we find that some of the national security concepts are broader and more inclusive, as you can see national security must include all the variables related to what countries are facing such as threats and physical violence from other counter parties, and the level of social and economic justice to achieve legitimate humanitarian needs in the country.

Over the past few years the world has witnessed a number of fundamental changes in different aspects of our contemporary life, on the level of all economic, social, political and military institutions. It also affected the values structure and social relations in many countries around the world, up to the point that it is justified to say that we are living in a world that is completely different than the one we used to live in, which lasted to the beginning of the twentieth century. and as a result of this, globalisation appeared on the scene. It allowed communications and human interaction beyond traditional borders, by making the lines between national, regional and global very narrow. In doing so, we have got rid of time and place restrictions. And surely this phenomenon and what came with it from the technological revolution, international blocs, the collapse of the bipolar system, the emersion of unipolar domination (USA) and the prominence of new global pressure factors such as: the world trade agreement, the international monetary fund and the world bank in addition to the multinational companies, all of this has led to the erosion of the concept of (state sovereignty). Also, questioning the traditional role of the state in which the government is committed to take care and protect their citizens from internal and external dangers. Achieving their social justice in addition to raising their living standard and welfare.

In fact, some thinkers believe that the State would give up this role to the cross-border multinational companies and there is no doubt that the transformation accompanied with globalisation is considered to be one of the most important factors that directly or indirectly affects all aspects of national security of any state.

Externally, there is a constant changing in the nature of international blocs, the balance of regional and global powers, and the polices of great powers. Internally, globalisation has affected the national identity and the nature of social and political movements, which could lead to provoke ethnic conflicts and sectarian wars, also affecting the loyalty of state citizens to their political system.

From this point, this study will attempt to highlight the impact of the globalisation phenomena on the concept of national security for the modern State.

Security is considered to be a free service provided to citizens without discrimination of colour, race, gender or religion.

To deliver this service to the public, the State is tasked to prepare a qualified, trained and professionally equipped body who is capable of providing this service efficiently and effectively. Hence, we have been making a lot of efforts focusing on rehabilitating and developing the security services, including the National Security Forces, which proved their ability to renew and capacity build the institutions of the Palestinian state, considering that the National Security Forces is one of the pillars of the Palestinian state and the nucleus of its Army. And it has managed to a large extent, to rebuild its system of Administrative and financial development, infrastructure, equipment, headquarters and training facilities, accompanied by the rise of serious young leaders who believe in change, took the reins of leadership, and encouraged the Commander of the National Security Forces, Major General Nidal Abu Dukhan, to make a great and constant effort to instil a new spirit in the National Security Forces, which was achieved through qualitative transformations, moving from the traditional role of the national security forces and their duties to the modern role in serving citizens and protecting their interests.

2. MATERIALS AND METHODS

To achieve the objectives of the scientific research, the SWOT strategic analysis method was used to identify the most important strengths and weaknesses of the national security forces and the most prominent opportunities and challenges to come up with the targeted results from this paper.

3. RESULTS

3.1. THE PROBLEM OF THE STUDY

Since the Oslo Peace Agreement was signed in 1993 and what followed it from other annexed agreements and protocols to organize the nature of joint relations as a transitional phase, various institutions of Palestine worked to establish State agencies to achieve the ultimate goal of ending the longest occupation in history.

However, with the stagnation of the political process and the end of the transitional period scheduled to end since 1999 and the unfortunate events that took place in 1996, as well as the outbreak of the political situation in 2000, Israel targeted the various institutions of Palestine, especially after the events of the second intifada in 2000, where it destroyed the headquarters of the Palestinian security services and weakened the work of the Palestinian security services, that restored what was destroyed with the support of multiple international parties.

However, the main problem can be summed up in the continuous undermining of the work of Palestinian security in the areas of Palestinian dominance and restricting the movement of Palestinian security to maintain public order and civil peace. Therefore, the central study question is based on the question: *“How Israeli policy and procedures affect the work of Palestinian security in maintaining public order in the State of Palestine?”*.

3.2. ENVIRONMENT ANALYSIS

3.2.1. EXTERNAL ENVIRONMENT ANALYSIS:

The Palestinian National Authority was established based on the signing of the Oslo Accords in 1993, followed by several political agreements aimed to regulate the relationship between Israel and the Palestinian Authority in different domains of economic, organizational, legal and security life.

The handover of the Palestinian territories was divided into several stages, starting with the Gaza-Jericho agreement first and then spreading to the rest of the regions. The agreements divided the regions into three categories:



- Areas A: which are fully under the control of the Palestinian administrative and security, they are concentrated in the main city areas;
- Areas B: They are areas that are administratively under Palestinian control, and police stations are allowed to open only in some of their areas, but these areas are under Israeli security control and include most of the rural sites and villages;
- Areas C: The areas under Israeli administrative and security authorities and represent 67% of the size of the West Bank and include some villages and state lands.

The border crossings and security passageways remain under the control of Israel until the final solvent agreements.

During the political stagnation and with the nature of the security situation that erupted after the events of 2000, Israel seized large areas of West Bank lands under the excuse of security and military purposes. It also built an apartheid wall inside the depth of the future State of Palestine within the 1967 borders and increased the pace of settlements in the Palestinian areas in West bank and East Jerusalem which threatens the two-state solution based on the agreements signed between the two parties, and what Israel is currently trying to do is to promote coexistence with a Palestinian entity and not just a state within an economic peace.

As for the economic aspect, the nature of economic relations has been ruled by several agreements, including the Paris Economic Agreement, as the Palestinian economy is linked to the Israeli economy and to the Israeli tax tariff, which creates a burden on the Palestinian citizen due to the difference in the rate of income between the two sides, and import and export are linked to Israeli approval and compulsory passage through The Israeli crossings, which increases the cost of import and implies restrictions on exports.

And as we mention the security condition, it is very complicated, as moving between the divided areas to maintain civil peace, as described, should pass through security coordination with the Israeli to allow movement between areas A, B and C, where coordination sometimes requires long hours, and it could affect negatively. Especially, in the event of riots or serious crimes. In addition, Israel put restrictions on the entry of various security equipment that contributes and help in controlling the security situation, they even impose complex restrictions on the entry of materials and tools that are allowed to be handled by Palestinian security. There are also security challenges created by the nature of the security relations imposed by Israel through the smuggling of weapons and drugs, and the formation of outlaw armed groups that are based in geographical areas that are difficult for the Palestinian security to reach.

The Palestinian living conditions are considered to be one of the highest living costs in the world, as the nature of the living prices does not fit with the individual income, due to linking the Palestinian prices with Israel's prices. Also, the housing cost is very high, and the price of the real estate is increasing and this is because the reduction of the areas that can be built in by Israel and the high construction costs. And for the opposing people who build in areas B and C they are punished by destroying their houses, as Israel destroyed 3884 houses during the last three years.

3.2.2. INTERNAL ENVIRONMENT ANALYSIS:

The National Security Forces were formed and developed in their current formation after the peace agreements between the Palestine Liberation Organization and Israel, where they witnessed increasing developments with legal cover, as their work was regulated by the Basic Law in Article 84 of the year 2003, and the Serving law No.8 in the Palestinian security forces was issued in 2005, in addition to

several executive regulations, the most important one is the Code of Conduct for members of the security services and rules of engagement.

The National Security Forces are considered to be a force to maintain civil peace and a main supporter for the various security agencies of law enforcement. They are the supporting forces for internal security missions, in addition to their responsibility for the Palestinian areas classified as A area according to the security divisions of the region.

The National Security Forces operate under the name of district commanders and special battalions, in addition to the presence of a special operations unit that includes a k9 unit, a bicycle unit, and an armored unit that moves to hot spots as needed.

The National Security Forces work in partnership and joint action with the rest of the security services, organized by a joint operations room that includes representatives from the different security services, and it is funded by a specific Palestinian government budget.

3.3. SWOT ANALYSIS

Table 12. SWOT analysis | Fragile States and regional conflicts

Strengths (S)	Weaknesses (W)
<ul style="list-style-type: none"> • The abundance of highly trained and qualified staff (9 battalions) trained and qualified militarily. • The presence of competencies with high academic qualifications. • The success of the forces in creating distinguished relations with the civil society. • The ability of the forces in dealing with events according to the available capabilities. • The existence of advanced training programs and sustainable courses. • The existence of an academy for creating officers. • The presence of central operating rooms equipped with the latest technologies and qualified staff. • A high and distinguished role for the Control and Inspection Department to achieve integrity, transparency and good management. 	<ul style="list-style-type: none"> • The lack of equipment and logistical supplies for the forces, which negatively affects the forces' performance on their missions. • Lack of training centers and equipment according to the international standards. • The lack of a unified mechanism for information communication between the security services and between the branches of the same forces, in terms of information transmission, voice communication and wireless communication, all of these things limited the ability and efficiency of the security services in achieving their goals. • Poor communication with the public. • Not being able to recruit new individuals due to the financial situation. • Lack of regular financial resources. • Not having modern means and appropriate technologies due to the prohibition of their entry by Israel.



Opportunities (O)	Threats (T)
<ul style="list-style-type: none"> • The growing of the international support and forming development processes within a clear methodology. • The political leadership's interest in supporting the forces. • The existence of a growing community partnership. • Benefiting from the status of Palestine as a state to deal with international partners and donors. • Benefiting from the trainees who have obtained specialized courses to develop the capabilities of the forces. • Existence of programs to attract highly qualified and distinguished competencies to work in the forces. • Existence of international programs that allow Palestine to participate and train. • The presence of effective international partners who contribute in developing performance and providing available capabilities. 	<ul style="list-style-type: none"> • Having no control over borders and crossings. • The irregular flow of financial resources and the detain of the Palestinian funds by Israel. • The political and economic instability • Assassinations and invasions of Palestinian areas, settlements and the apartheid wall. • The lack of geographic communication within and between the cities of the country due to divisions of areas according to agreements for the transitional period. • The coup in Gaza Strip and the growth of fundamentalist ideas. • Outlaw armed groups and militias that are based in areas outside the Palestinian security control. • The Israeli occupation's lack of commitment to the peace process and the agreements signed with the Palestinian Liberation Organization. • Attacking Islamic and Christian sanctities. • The high rate of unemployment in the local community, which negatively affects security. • The high rate of crime and attacks on public property. • The occupation detaining of the necessary equipment for the forces in terms of individual and collective protection. • Not introducing the necessary new weapons and equipment for special operations (automatic weapons, sound bombs and smoke bombs) and other training means. • Smuggling weapons and drugs from Israel to the Palestinian territories.

4. CONCLUSION & RECOMMENDATIONS

The SWOT strategic analysis shows us the extent of the complexities and overlaps facing Palestinian security in general and the National Security Forces in particular in the mechanism of dealing with the threats coming from the existence of an occupying force that has been doing the same practices for 74 years, as any strategy, action or development requires Israeli approval, which cannot without a continuation of the political process and carrying on the negotiating within a specific timetable to enable the Palestinians to have the right to self-determination and to form a bright picture of their future.

Here, the concept of security and strategic plans are associated with the general political situation, which Israel currently opposes under the excuse of its own security considerations and is content with promoting economic peace for the so-called Palestinian entity and not a state.

So, the interaction between the international partners to move the peace political process must be a foundation for any developments or plans, and it must work with the partners to put pressure on the Israeli system to allow freedom of Palestinian security work in order to preserve Palestinian civil peace and the development of the institutions for the future state, in addition to the importance of implementing the previously signed agreements between the State of Palestine and Israel, which deliberately obstructs the implementation of the terms related to Palestinian interests, as is the case with the failure to implement any of the international legitimacy resolutions issued by the institutions of the United Nations and the international community.

VI. PAPER | ENERGY INSECURITY

Citation:

Al-Hajaya, H. S., Overcoming Security Threats arising from Globalization 4.0 – FIEP Association, 2022

Published: October 2022

Publisher's Note: FIEP stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors.

Jordan

Hussein Salem Al-Hajaya



hussainsalem77@outlook.com

Abstract: The aim of this paper is to define the concept of energy insecurity and its impact on national, economic and social security in Jordan. This research paper relies on Jordan as a case study. The main challenges facing Jordan were the limited natural resources, particularly energy, the large and prolonged increase in energy prices, the disruption and decline in natural gas imports from Egypt, conflicts, unrest and disputes in neighboring countries, as well as the large influx of refugees arriving in Jordan to escape conflicts, all of which placed an additional burden on the Jordanian economy and security. Based on these dilemmas, Jordan is working to address these sensitive issues so that it can explore and assess alternatives to reduce dependence on these resources; Attempts to address the use of renewable and sustainable resources had been considered, but those efforts should be reflected more firmly in Jordan's energy policy towards energy security and sustainability. The study produces a series of findings, the most important of which were the creation of alternatives to energy resources, and appropriate thinking and strategic planning to secure resources by maintaining good relations with supplier countries. Because energy security is linked to national security, privatization of this sector will jeopardize national security and have implications for social and economic development. The study also found that energy is a vital element of development, regardless of the State's approach to development, that energy security is linked to national security, social and economic development and environmental protection, and that renewable energy is the future of the energy sector worldwide.

Keywords: Insecurity; Energy; National security; economic security; social security.



1. INTRODUCTION

In a country like Jordan, which is located in one of the world's hottest political regions, which includes the Arab - Israeli conflict, the Iraq crisis, Syrian conflicts and other revolutions in the region, it is vital to define the foreign policy agenda. This identification will build a political approach in order to deal with the complexity and vitality of evolving events, where decisions are critical and have a significant impact that is unparalleled elsewhere in the world. Since the political and economic crisis threatens the political and social stability of Jordan, there is an urgent need to guide the country's foreign policy in order to achieve the highest interest of Jordan in many areas, one of which is energy security and its sustainability.

Unlike most Middle Eastern countries, Jordan's energy resources are limited; therefore, the present article appears to be vital for validating the view on energy insecurity in Jordan.

The study problem represents that Jordan is one of the poorest countries around the world in terms of its share of natural resources, and ranks as the second poorest country in terms of water resources, in addition to being fully dependent on energy imports of oil.

This paper aimed to bridge the gap in the literature on energy insecurity policies, the impact of Jordanian foreign and domestic policy on energy security and vice versa, since previous studies rarely focused on the subject. The paper therefore provided recommendations and solutions that could be very useful to help policy makers develop stable energy policies and seek alternative new sources, and could be useful to other researchers from other countries with the same situation in Jordan. Moreover, the results of this study added new methodological knowledge in the field of international relations and political science in general.

The main question of the study is, therefore, *what is the impact of energy insecurity on national, economic and social security in Jordan?*

1.1. LITERATURE REVIEW

Energy security has a complex and widely shared concept that should be viewed from different perspectives, particularly economic and national security. Energy security affects all vital sectors of the country, such as transport and electricity, affecting sustainable development.

The United States is one of the most focused countries on energy security, which made it a flexible concept that fits with its various policies, as it was often limited to oil; Although energy security is related to having sufficient supplies in time of emergency, the White House links energy security with national security, especially if problems in some oil-producing countries limit the options available to the United States to deal with its enemies.

It has been defined as providing sufficient, affordable and stable energy supply to sustain economic performance and growth, energy insecurity is exposure to prolonged supply turbulences as prices rise. Given the changes in the structure of the international system after the end of the cold war, and which affected the concept of energy security in view of the major transformations that the issue of energy has witnessed globally, as well as the expansion of the concept of security to include important issues in the field of environment and society, here there was an urgent need to reconsider the concept of energy security because of a series of transformations which are linked to national energy and it being affected by armed conflicts, terrorism and natural disasters.

1.2. THE IMPLICATIONS OF ENERGY INSECURITY IN THE HASHEMITE KINGDOM OF JORDAN

Jordan can be classified as an advanced energy importer because it imports more than 97% of its energy needs, which is also about one fifth of its GDP.

In general, the relationship between Jordanian foreign policy and energy security takes into account the relationship with energy suppliers, namely Iraq, the Gulf States and Egypt. This dates back to 1973, when the

Gulf States, particularly Saudi Arabia and Kuwait, supported Jordan with its energy needs at an appropriate price. This kind of support has made Jordan free of diligence to improve its energy plans.

By the 1990s, Iraq began to support Jordan with its oil needs at a price equal to 30% of the world price, but this concession ended in 2003, when the Gulf States again supported Jordan until 2006. After that, energy providing became a serious problem in Jordan.

The above-mentioned threats pose a challenge to the country by exploring and providing a reliable energy source essential for the country's stability and development. Recalling the year 2011, which saw revolutions in some Arab countries, including Egypt, and now called the Arab Spring. During the revolution, multiple attacks targeted the Egypt-Jordan pipeline supplies, known as the "Arab Gas Pipeline", the main source of electricity generation in Jordan, posing a serious threat to Jordan, and triggering a contingency plan to switch to diesel, as a temporary alternative, this alternative resulted in a cost increase of about seven million dinars per day, as well the gas outage also costs Jordan 11 million dinars per day, as revealed by the Director-General of the Jordanian National Electric Power Company (NEPCO). An additional financial burden was added to the national debt, as a result, Jordan was under pressure to explore other alternative solutions, one of which was the Israeli gas deal, a sensitive issue that could have a political impact.

Contrary to the stereotype of the Middle East States, the Hashemite Kingdom of Jordan does not possess oil resources and is geographically located in a semi-arid region with limited water resources. The lack of natural resources and the location of the State makes economic growth difficult to achieve and sustain. Limited energy resources exacerbate other problems, such as water scarcity, and make it difficult to explore options to address this, such as desalination.

Jordan has always relied on neighboring countries in providing the required fuel for electricity generation. Since 1939, the main source of electricity production has been fossil fuels, which is imported from neighboring countries.

In the 1980s and early 1990s, based on the good relationship between Iraq and Jordan, Iraq was the main supplier of oil to Jordan. As the oil was partially delivered to Jordan as grants (free of charge) from the Iraqi government, which has led to an economic prosperity during that period. The exchange rate of the US dollar against the Jordanian dinar was between 1.005 and 0.27 Jordanian dinars, which was the lowest exchange rate for the US dollar at that time, with an average of 0.37 dinars per dollar. Today, the exchange rate is fixed at 1.00 US dollars | 0.708 Jordanian dinars, since the exchange rate is related with the country's economic situation, and therefore fluctuates and is directly proportional to the strength of the economy. Accordingly, the energy sector, as a key driver of economic prosperity, and means and cost of obtaining it, has a strong direct impact on the achieved growth levels.

As well the repercussions of the Gulf war and the sanctions imposed on Iraq forced the Government to ease its scenarios in order to cope with the consequences of the interruption of Iraqi support and had proposed the implementation of the austerity plan to face the situation. Furthermore, it started looking for alternative solutions and suppliers.

Because of the good relationship between Jordan and Egypt, cooperation was made to provide Jordan with an affordable alternative to electricity production, Egyptian natural gas. However, this option has not solved the dependency issue.

Moreover, the subsequent instability in the region led to the "Arab Spring" uprising that overwhelmed the entire region, and had strong effects and unrest in Egypt, where people demanded the overthrow of former Egyptian President "Hosni Mubarak", which resulted in a national disturbance that affected the country's security. As a result, acts of violence escalated and resulted in several attacks on Jordan's main gas pipeline, and Jordan again witnessed another threat and interruption in the source of electricity production for several



days. A solution was sought, and an alternative was identified, but at a much higher cost up to several millions.

The government continued to explore other alternatives; it considered the Israeli option to provide gas the best option. Such an option had decisive political implications regardless of the fact that the Government had signed a peace treaty with Israel, but at the grass-roots level this option was not welcome and posed threats of opposition and further instability. However, Israel was ready to promote cooperation with Jordan to improve its security and regional stability through the natural gas agreement with Jordan.

Unfortunately, none of the explored and valued options have seemed credible or sustainable. Therefore, Jordan is still facing difficulties in providing energy at a competitive price.

Demand for primary energy consumption (raw fuel, which is used for electricity production) continued to increase significantly because of the good grid coverage, the population growth, and the change in modern and urban lifestyle. The period between 2011-2021, the cost of consumed energy was significantly high because of the several reductions in the Arab gas pipeline, and that forced Jordan to use other expensive alternatives.

However, the calculation of growth between 2010 and 2021 reflects a growth rate of 31%, which is quite a high rate. Based on an expanding economy and a population growth, the Ministry of Energy and Mineral Resources predicts an increase in energy demand by about 65% during the next 20 years.

The water and electricity sectors in Jordan are challenged by many factors, not only the lack of local energy resources, but also external factors such as regional instability and abnormal population growth which are fuelled by the influx of refugees as a result of the extreme violence in neighboring areas.

Accordingly, Jordan has collected lessons learned and experiences from the multiple crises which it faces because of its high dependence on energy imports. This heavy dependence poses a worrying threat to energy security and sustainable development, as the Government has begun to take steps to reform laws and regulations to address this area.

In 1996, the Jordan Electric Company began structural reform by decentralizing its operations on the basis of its field and location. Where three entities were founded: the National Electric Power Company (NEPCO), the Central Electricity Generation Company (CEGCO), and the Electricity Distribution Company (EDCO).

Policy makers in Jordan have demonstrated the importance of political convergence with regard to energy security. where they all share the same view that Jordan faces a major energy problem and every policy in the country should focus on diversification of energy sources at the local or international level.

Energy insecurity was also warning of danger, as some of it was because of the influx of refugees, and some because of a lack of awareness of energy discussions, so Jordan should raise awareness of energy discussions to promote energy efficiency, not only production.

2. MATERIALS AND METHODS

This research paper relied on a strategic diagnostic methodology to identify sources of vulnerability, strength, threats and opportunities based on the data provided to achieve the objectives of the paper.

3. RESULTS

3.1. SWOT ANALYSIS:

Table 13. SWOT analysis | Energy insecurity

Strengths (S)	Weaknesses (W)
<ul style="list-style-type: none"> • Search for alternative sources of energy, Jordan is looking for renewable energy sources and starting to implement them 	<ul style="list-style-type: none"> • Energy security affects all vital sectors in the country such as electricity, water and transportation. • Continued consumption of primary energy (raw fuel). • The high financial cost because of the weakness of the state's economic capabilities
Opportunities (O)	Threats (T)
<ul style="list-style-type: none"> • There are great opportunities to achieve a coherent energy policy and strategy, while relying on proper and comprehensive planning in order to achieve political, economic and social development. 	<ul style="list-style-type: none"> • Instability in the region as a result of political and military conditions in neighboring countries. • Privatization of the energy sector, which will have negative impact on the social and political development.

4. CONCLUSION & RECOMMENDATIONS

- The strategic diagnosis methodology was relied upon in order to identify the sources of weakness, strength, threats and opportunities.
- Energy is a vital component of development, regardless of the development approach adopted in the state.
- Energy security is related to national security, social and economic development and environmental protection.
- Renewable energy is the future of the energy sector worldwide.
- To achieve a coherent energy security policy and strategy, all possible scenarios that could confront Jordan must be taken into account to ensure good, proper and comprehensive planning.



Page intentionally left blank

VII. PAPER | CRITICAL INFRASTRUCTURES

The Portuguese framework

Citation:

Bailote, R & Lopes, J; Critical Infrastructures. Overcoming Security Threats arising from Globalization 4.0 – FIEP Association, 2022.

Published: October 2022

Publisher's Note: FIEP stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



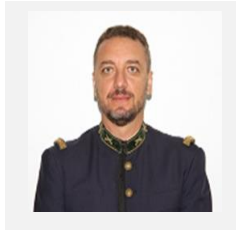
Copyright: © 2022 by the authors.

Portugal

Guarda Nacional Republicana

Ricardo Bailote ¹

José Lopes ²



¹ bailote.rmr@gnr.pt

² lopes.jmf1@gnr.pt

This study aims to analyse the processes related to the protection of critical infrastructures in a national context in light of the legislative and the European security framework by means of a Dynamic SWOT Analysis.

Abstract: This study aims to address the issue of the protection of critical infrastructures in the current security framework, focusing on the national territory and, inherently, on the international situation. Regarding the methodology used, this was based on the use of a qualitative research strategy, through the consultation of various bibliographies and legislative acquis on the subject. As a general objective, the identification of measures to protect critical infrastructures that could be implemented to increase their resilience, given the current security situation in Europe, was defined. In these terms, it was concluded that it is necessary to accompany the consolidation of the digital network of all GNR services, with the integration of computer systems on a single platform; that the GNR's Gendarmeric nature gives it a pivotal position among the Armed and Security Forces, pursuing military, police and civilian activities; and that it is urgent to develop programmes to share resources and knowledge in the area of critical infrastructures between the various Member States. In this vein, it is also observed the need to review the security plans assigned to each CI, as well as the effective conduct of drills and exercises because they are true catalysts for continuous improvement.

Keywords: Critical Infrastructure; Protection and Security; Security Plan; Resilience; Security Forces.



1. INTRODUCTION

1.1. PURPOSE OF THE STUDY

Critical Infrastructures (CI) are essential for providing vital economic and social functions to European Union (EU) citizens. The services they ensure, coupled with their cross-border nature and inter-dependencies, make them increasingly vulnerable to diversified types of threats, not only natural and accidental but also intentional.

The landscape of potential threats on EU soil has been changing and evolving with technological advancements and deep interconnectedness, paving the way for greater vulnerability to cyber attacks. For instance, with the 'cascading failure' phenomenon there is a possibility that the failure of one, single part of a given infrastructure could lead to the collapse of other components and eventually to serious damage across an entire network.

Within the landscape of challenges to CI, hybrid threats deserve a separate mention. A hybrid action exploits vulnerabilities of democracies and institutions, benefitting from ambiguity in terms of detection and attribution as well as the intrinsic difficulty in classifying a hybrid event due to the use of various measures – conventional and unconventional – in different areas – political, economic, cyber, military, civil – by the attacker. They form an effective asset in the hands of both state and non-state actors that seek to exploit the vulnerabilities of Member States (MS).

Other less evident forms of interference from state and non-state actors have also been targeting the EU. One that has recently caused widespread concerns regards Foreign Direct Investments (FDI) in the EU by third countries such as China and Russia (Tessari & Muti, 2021).

1.2. HISTORICAL FRAMEWORK

In June 2004, the European Council called for the development of an overall strategy to protect critical infrastructure (CI). In response to this request, the Commission adopted on 20 October 2004 a Communication on the protection of CI in the fight against terrorism which put forward suggestions on how to enhance European prevention, preparedness and response to terrorist attacks involving CI (European Union [EU], 2008, p. 1).

In December 2005, the Council asked the Commission to make a proposal for a European Programme for Critical Infrastructure Protection (EPCIP) and decided that it should be based on an all-hazards approach, with an emphasis on counter-terrorism. This approach should take into account human and technological threats and natural disasters in the CI protection process, although it should focus on terrorism threats (EU, 2008, p. 1).

In April 2007, the Council adopted conclusions on the EPCIP in which it reaffirmed that it was the ultimate responsibility of the Member States (MS) to ensure the protection of CI in their territories. As a result of this work, Council Directive 2008/114 of 8 December 2008 was issued. This directive constitutes the first step in a phased approach to identify and designate European Critical Infrastructures (ECIs) and assess the need to improve their protection. As such, it focuses on the energy and transport sectors and shall be reviewed in order to assess its impact and the need to include in its scope other sectors, namely the Information and Communication Technologies (ICT), and it is expected that a new Directive will be published by the end of this year (EU, 2008, p. 1).

In Portugal, Decree-Law 62/2011, of 9 May, transposed Directive 2008/114/EC into national law, recently revised with the publication of DL 20/2022, of 28 January. The revision of DL 62/2011 reinforced the holistic nature of CI protection, aligning it with the provisions of other regulations of transversal nature, such as the Internal Security Law, the National Strategy to Combat Terrorism, the National Strategy for Cyberspace

Security, the Legal Regime of Cyberspace Security, the Strategic Concept of National Defence and the National System of Civil Emergency Planning, as well as in several specific sectoral legislation (Ministry of National Defence [MDN], 2011).

DL 20/2022, of 28 January, establishes the procedures for the identification, designation, protection and increase of the resilience of national and European critical infrastructures, consolidating in national law the transposition of Council Directive 2008/114/EC, of 8 December 2008, as stipulated by article 1, DL 20/2022 (Presidency of the Council of Ministers [PCM], 2022).

2. MATERIALS AND METHODS

The general objective (GL) of this article is to identify CI protection measures that can be implemented to increase their resilience, given the current security situation in Europe. Given the defined OG, the methodology to be followed is based on inductive reasoning, since we start from the observation of particular facts, in this case in the national context, and from there generalising, pointing out changes that could be introduced, in order to improve the resilience of CIs (Santos & Lima, 2019, pp. 18-19).

The methodological path focuses on a qualitative research strategy, based on the observation of the phenomenon under study and the interpretation of patterns found in the data obtained, by consulting various bibliographies and legislative collection on the subject (Santos & Lima, 2019, p. 27). As a research design, the case study will be used, “in which one seeks to describe in a rigorous way, the unit of observation [...] and understand the object of study from the point of view of the participants in it” (Santos & Lima, 2019, pp. 36-37).

To this end, documentary collection techniques were used, based on publications from various public and private sector entities, focusing in particular on the national reality, as an EU member state. The consultation of the legislative acquis in force, referring to the object of investigation, was also fundamental in order to obtain a correct framing of the associated concepts.

Given the defined object of study, the research will be delimited at the level of time, space and content (Santos & Lima, 2019, p. 42). In temporal terms, the period after 2008, when Directive 2008/114 was published, will be considered. In spatial terms, the investigation will be limited to national space, over which, as a EU MS, Directive 2008/114 applies. As to content, the research will focus on CI protection, the respective legislative framework, the processes included in security planning and the main actors involved in CI protection and security in a national context. To be analysed in the present research, the following parameters are elaborated: OG, specific objective (SO), central question (CQ) and derived question (DQ) (Figure 12. GO, SO, CQ and DI).

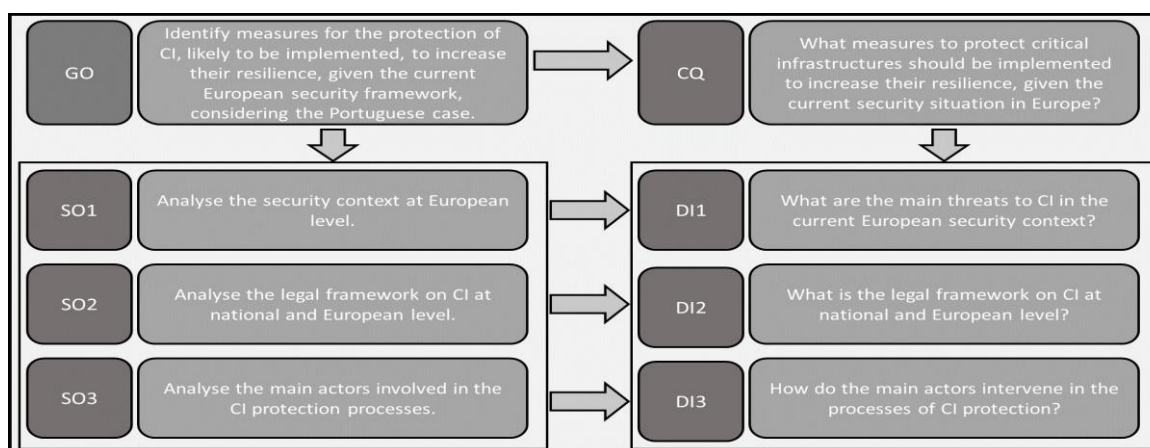


Figure 12. GO, SO, CQ and DI

3. RESULTS

3.1. CRITICAL INFRASTRUCTURES - BRIEF EPISTEMOLOGICAL FRAMEWORK IN A EUROPEAN CONTEXT

Although the United Kingdom is not currently part of the EU, at the date of publication of Directive 2008/114/EC of 8 December 2008, it was one of the Member States with the greatest preponderance and influence within this international community, so for the issues previously mentioned, it is important to recover its definition of CI. In this context, CI is characterised as the infrastructure assets, both physical and electronic, considered vital for the uninterrupted operation and integrity of essential services on which the country depends, and their loss or compromise would lead to serious economic, social or loss of life consequences (UK Government, 2010).

On the other hand, in the German context, CIs are characterised as physical, organisational structures and facilities of vital importance to the national society and economy whose failure or degradation would result in sustained supply shortages, significant disruption of public safety or other dramatic consequences (German Federal Ministry of the Interior [GFMI], 2009).

In the Portuguese case, with the entry into force of Decree-Law 20/2022, of 28 January, CI are characterised as the component, system or part thereof that is essential for the maintenance of vital functions for society, health, safety and economic or social well-being, and whose disruption of operation or destruction would have a significant impact, given the impossibility of continuing to ensure these functions, in accordance with paragraph d) of Article 2 of Decree-Law 20/2022 (PCM, 2022).

In turn, France characterises CIs as institutions, structures or facilities that provide essential goods and services forming the backbone of French society and its way of life. In this case, it is the operators themselves who draw up the list of their CIs, which can be production sites, command and control centres, network terminals or data centres (General Secretariat for Defence and National Security [SGDSN], 2017).

The European Union, through Directive 2008/114/EC, seeks a fair balance by defining ECI as an asset, system or part thereof, located in Member States, which is essential for the maintenance of vital societal functions, health, safety, economic or social well-being of people and whose disruption or destruction would have a significant impact on the Member State as a result of the inability to maintain those functions (EU, 2008).

In sum, one observes that the United Kingdom through a pragmatic characterisation seeks to characterise the CI as being the support structures to essential services on which the country depends, in fact converging with the parameters followed by France. In turn, Germany focuses on consequences and, in the Portuguese

case, one identifies an approximation to the British and French model by means of an eminently objective characterisation, replacing the term essential services by vital functions for society.

3.2. STRATEGIC DIAGNOSIS

3.2.1. EXOGENOUS ENVIRONMENT

It is important to highlight the survey already carried out in this publication, through a PESTEL analysis, which urges to identify the main threats and opportunities in face of the current international scenario in which Portugal is inserted. Thus, given the security framework in Europe, it will be necessary, for systematization purposes, to list the main trends and implications with impact on the study in question, in this case likely to influence the CI protection measures.

3.2.1.1. POLITICAL AND LEGAL

Thus, in the political and legal sphere, the following trends are identified as being the most relevant: i. the return of tensions and conflicts between the major global powers, i.e., the United States of America, China and Russia; ii. The disinformation on a large scale, enhanced by the proliferation of media and communication platforms and technological advances; iii. the way international directives influence the national legislative acquis; iv. the growth of threats related to organised crime, international crime, increase of extremist phenomena, nationalist movements, terrorism; v. the instrumentalisation of migratory flows as a form of pressure in certain territories.

In what concerns the main implications that the trends listed above presuppose in the Security Forces and Services (SFSS), the following are listed: i. instability presupposes an increase in the readiness of the Forces, as well as the development of more comprehensive capabilities; ii. an increase in international cooperation between security actors; iii. an increase in the complexity to foresee and react to incidents; iv. it presupposes the creation of information processing mechanisms aiming at a swift, efficient and effective reaction to incidents; v. the increase of private sector actors in the security area; vi. the need to share information between FFSS in a timely manner; vii. strengthening of policing and security measures in cross-border areas.

3.2.1.2. ECONOMIC

Thus, in the economic sphere, the following trends are identified as being the most relevant: i. internal indebtedness with an upward trend and a diversification of commercial exchanges and the consequent impact on the living conditions of States; ii. the COVID-19 pandemic will dictate a contraction in global economies, which may increase the demand for limited natural resources and potentiate the emergence of new conflicts; iii. the need to diversify suppliers of energy resources and raw materials; iv. a decrease in investment in the defence and security sector at the European level, contrary to what is seen in other regions of the world.

In terms of the main implications of the above trends for the FFSS, the following are listed: i. a decrease in available human resources; ii. the development of resource-sharing programmes between states; iii. the development of agreements between states enabling the research and development of resources and equipment; iv. more efficient management of available resources.

3.2.1.3. SOCIAL

In the social field, the following trends are of particular relevance: i. growing globalisation with consequences in the increase of populations and respective urban areas; ii. the impact of migratory



flows in the dilution of the national identity of States, with potential implications in the increase of nationalist movements; ii. the increase in ethnic polarisation and religious extremism; iii. as a result of the pandemic, the sense of well-being and security of populations reaches historically low levels; iv. better informed populations and an increase in the scrutiny of the actions of the FFSS.

Regarding the main implications that the trends listed above presuppose in the FFSS, the following are listed: i. reorganisation of resources in order to adjust them to the growing urbanisation of the territories; ii. considering the increase in extremist movements, the threat level to CI has tended to rise; iii. need to increase the levels of transparency and accountability in the actions developed; iv. develop specific programmes to reach out to different cultures, ethnicities and religious groups; v. develop programmes to control and prevent “internal agents”.

3.2.1.4. TECHNOLOGICAL

Technologically, the following trends with potential impact can be observed: i. hyper digital connectivity and technological transformations that enable increased interconnection of markets, people and equipment; ii. states and public organisations have lost their monopoly on technology; iii. the metaverse, as a digital platform where most people interact will transform society; iv. the increased use of the internet and consequent increased threat of cyber attacks.

In what concerns the main implications that the trends listed above presuppose in the Security Forces and Services, the following are listed: i. the implementation of intelligence-led policing mechanisms; ii. the reinforcement of protection mechanisms for the databases of the Security Forces, considering the multiplicity of information contained therein; iii. the reorganization of the internal structure in order to deal with criminal phenomena resulting from the use of technological tools; iv. the research and development of intermediary weapons with potential use in police action.

3.2.1.5. ENVIRONMENTAL

In the Environmental area, the following trends with potential impact can be observed: i. climate change and environmental challenges, materialised by the potential increase in average temperature over the next twenty years and the consequent decrease in vital resources, such as water, food; fossil fuels ii. increase in extreme weather events reflected in increased migration flows; iii. increased regulation imposed by States in order to combat the phenomenon.

In what concerns the main implications that the trends listed above presuppose in the FFSS, the following are listed: i. adapting resources and equipment in harmony with the guidelines issued by the States, towards the reduction of the environmental footprint; ii. a greater effort in border policing; iii. a potential increase in social conflicts would imply an increase in the level of preparedness; iv. the reinforcement of CI protection measures and the change of emergency planning and protection processes considering extreme weather events.

3.3. ENDOGENOUS ENVIRONMENT

3.3.1. LEGAL FRAMEWORK

Considering that Decree-Law 62/2011, of 9 May, had the desideratum to transpose into Portuguese law Directive 2008/114/EC, of the Council, of 8 December 2008, is more than a decade old, it was deemed necessary to update it, in order to correct flaws and streamline processes.

In these terms, Decree-Law 20/2022 of 28 January was published, which recently came into force on 28 February 2022, establishing the procedures for identifying, designating, protecting and increasing the resilience of national and European critical infrastructures, as per Article 1 of Decree-Law 20/2022 (PCM, 2022).

Moreover, ten sectors were added to the two provided for by Decree-Law 62/2011, of 9 May. Specifically, the sectors of communication, digital infrastructures and digital service providers, public water supply and waste treatment, food, health, industry, financial services, Sovereign Bodies and Governance, security and defence were incorporated to the energy and transport sector already provided for, according to article 3 of Decree-Law 20/2022 (PCM, 2022).

The decree-law establishes that the identification of national CI results from a selection materialised in a list, carried out upstream and under the responsibility of the sectorial entities, taking into consideration an assessment of the consequences caused by its inoperability, namely the economic impact on society and the possibility of accidents occurring, as per no. 1 of art. 8 of Decree-Law 20/2022 (PCM, 2022).

Once the CIs are selected, the identification criteria are applied, with special relevance to the types of goods produced or services provided, the available alternatives, the population and geographic area affected and the duration that an eventual disturbance will have in its operation and respective recovery time. Culminating with the submission of a final list for consideration by the National Council for Civil Emergency Planning, as per paragraph 2 of article 8 of Decree-Law 20/2022 (PCM, 2022).

At the end of this process, the respective sectorial entity, the Secretary-General of the Internal Security System and the municipality with the inherent territorial competences should be informed, in accordance with article 9 of Decree-Law 20/2022 (PCM, 2022).

For the identification and designation of ECIs, the process generally follows the same requirements applicable to national CI, however, at the time of their designation, the National Council for Civil Emergency Planning must inform the counterpart entity of the Member State of the European Union likely to be affected by the disruption of the functioning of the potential ECI, identifying it, stating the reasons for its possible designation and requesting its agreement, in accordance with Article 9 of Decree-Law 20/2022 (PCM, 2022).

Once the process of identification and designation of national CIs is completed, the operators, in this case the entities responsible for the operation of the CIs, prepare, within one year, the respective security plan and submit it to the Secretary General of the Internal Security System for appreciation and approval. As a result of this assessment, it is necessary to consult the Security Forces (FSeg), the National Authority for Emergency and Civil Protection, the National Centre for Cybersecurity or other entities with specific competences in the matter, according to article 14 of Decree-Law 20/2022 (PCM, 2022).

In this context, it is important to mention that the CI safety plan presupposes the necessary articulation with the protection and intervention plan prepared by the territorially competent FSeg, as well as with



the civil protection emergency plan prepared by the corresponding civil protection authority and, if necessary, with the due specific sectorial instruments, as per article 16 of Decree-Law 20/2022 (PCM, 2022).

The entity responsible for assessing the security threat that falls upon the CI and respective sectors is the Secretary General of the Internal Security System, with the necessary articulation with the FFSS (PCM, 2022).

The framework legal diploma on CI and specifically for the security planning processes foresees their review every five years, the holding of drills and exercises every two years and the possibility for the Secretary General of the Internal Security System to assess their execution (PCM, 2022).

However, it should be noted that the Critical Infrastructure Information Registration Platform has the potential to be an aggregating measure, in the sense that it presupposes the achievement of essential objectives, such as: i. the availability of information related to threat and risk assessments; ii. the promotion of measures, recommendations and good practices, with the desideratum of increasing the resilience of the CI; iii. the sharing of information in order to optimize the planning and prioritization processes of the interventions related to the strengthening of security; iv. the monitoring, recording and management of relevant accidents and incidents, according to article 14 of Decree Law 20/2022 (PCM, 2022).

In summary, after a comprehensive analysis of the most recent normative framework concerning CI in the national context, the following particularities that may encompass the dynamic SWOT matrix are identified:

- *Decree-Law 20/2022 is published ahead of a possible revision of Directive 2008/114/EC, so considering the time gap of the current European directive, it may happen soon, which would imply a possible revision of the Portuguese standard;*
- *The collection of entities involved in the process of identification, designation and preparation of the security plan, in this case, the operator, the sectorial entity, the National Council for Civil Emergency Planning, the Secretary General of the Internal Security System, the FSeg, the National Cyber Security Centre, the National Authority for Emergency and Civil Protection, among others;*
- *The absence of guidelines for the preparation of security plans;*
- *The implementation of a CI information registration platform;*
- *The creation of Infrastructure Contact Persons, responsible for communication with the FSeg and territorially competent civil protection services;*
- *The entity responsible for assessing the threat to CI is also the one with responsibility for approving security plans;*
- *The enlargement of the sectors covered by this regulation from two to twelve, which implies an increase in the number of national CIs;*
- *The myriad of entities consulted, for the issue of an opinion, during the approval process of the Security Plan, are the FSeg territorially competent (GNR, Public Security Police and Maritime Police), the National Authority for Emergency and Civil Protection, the respective sectorial entity and the National Cyber Security Centre.*

3.3.2. THE PROTECTION OF NATIONAL CI - SECURITY PLANS

The Security Plan shall include the identification of critical elements, the delimitation of security areas, a risk analysis, the identification, selection and priority of countermeasures and permanent and progressive security procedures according to the degree of threat, as per paragraph 1 of article 13 of Decree Law 20/2022 (PCM, 2022).

In this context, the permanent security countermeasures and procedures aggregate: i. the installation of detection, access control, protection and prevention equipment, without prejudice to compliance with the rules regarding the physical and digital security of classified information; ii. crisis alert and management procedures; iii. access control and security verification standards; iv. communication, awareness and training actions; v. cybersecurity solutions, namely a risk analysis, its implementation and the adoption of technical and organisational measures to comply with security requirements, as provided for in articles 9 and 10 of Decree-Law no.No. 65/2021, of 30 July, on the Legal Regime for Cyberspace Security; and finally, vi. the measures to minimise damages and impacts and to restore normality, in order to promote increased resilience in the event of a disruption, as per paragraph 2 of article 13 of Decree-Law 20/2022 (PCM, 2022).

Regarding CI, the regulatory framework provides an approach to safety based on two dimensions: safety and security. Although they have different meanings in their mother language, in their translation into Portuguese, both express the concept of safety. Despite this linguistic incongruence, their meanings complement each other, since safety presupposes the prevention of danger or accident risk and security incorporates the protection against threats to people, infrastructures, organizations or countries (Martinho, 2017).

As such, both dimensions are fundamental in the analysis of the specificity of each sector, and should be adequate to the twelve sectors foreseen in the Annex to the Decree-Law 20/2022, of 28 January, as well as in the elaboration of the Security Plans for each CI.

Thus, considering the aforementioned dimensions, the CI security plan should be articulated with the Protection and Intervention Plan prepared by the territorially competent Security Forces and with the Civil Protection Emergency Plan, which is the responsibility of the Civil Protection authorities.

Therefore, on the security side, the Protection and Intervention Plan must incorporate the following points in its articulation: “(i) objectives; (ii) applicable legislation; (iii) identification of important (critical) elements of the infrastructure; (iv) risk analysis; (v) permanent countermeasures and procedures - selection and priority; (vi) reaction and response to identified security incidents; (vii) progressive countermeasures and procedures - selection and priority; (viii) articulation with plans external to the facility; (ix) staff training programme; and (x) exercise programme” (Security Coordinating Office [SCG], 2011, pp.3-9).

Regarding the safety dimension, the Civil Protection Emergency Plan must integrate: “(i) objectives; (ii) applicable legislation; (iii) identification of the important (critical) elements of the infrastructure; (iv) risk analysis based on serious threat scenarios, on the vulnerability of each component and on the potential impacts; (v) identification, selection and priority of permanent and progressive countermeasures and procedures to be applied depending on the degree of threat applicable to the CI or the decreed security status; (vi) control and verification measures; (vii) communication/awareness raising and training; (viii) security of information and communications systems; and (ix) articulation of plans external to the installation” (Autoridade Nacional de Emergência e Proteção Civil [ANEPC], 2013, pp.2-6).



3.3.3. IDENTIFICATION OF THE MAIN ACTORS INVOLVED IN CI SECURITY/PROTECTION

The National Authority for Emergency and Civil Protection is the entity, in national terms, responsible for the identification and designation of CI, being also responsible for the issuing of previous opinions regarding CI security plans, as well as the definition of the national policy of civil emergency planning and the assessment of plans of this nature submitted to it (Decree-Law 20/2022). The ANEPC assumes and centralizes most of the functions intrinsic to CI, namely the promotion of forecasting, monitoring and evaluation of collective risks, the assessment of vulnerabilities to risk, the preparation of technical guidelines adjusted to prevention and rescue and the assessment and implementation of the plans submitted to it (MAI, 2014, p.5620).

The National Cybersecurity Centre, integrated in the National Security Office, whose mission is to contribute to the country's free, reliable and secure use of cyberspace, as well as the pursuit of measures and instruments essential to anticipate, detect, react and recover from situations that, given the imminence or occurrence of incidents or cyberattacks, may jeopardise the operation of the CI (PCM, 2014, p.2715).

The FSeg, according to the assigned territorial competence (in this case the GNR, the Public Security Police and the Maritime Police), are responsible for a set of tasks related to the protection of the CI, namely: i. the issue of previous opinions concerning the CI security plans; ii. the preparation of the Protection and Intervention Plan, in close articulation with the CI security plan; iii. the preparation of the Protection and Intervention Plan, in close articulation with the CI security plan; iii. promote the liaison with the Security Liaison Officers, to ensure the exchange of information on threat levels and or information coming from the CIs with impact on the security of the same; and iv. promote contacts and the proper articulation with the CI contact elements (PCM, 2022).

Considering that there are other entities involved in CI security and protection, for the purpose of systematizing information and defining priorities and focus related to the present study, it was decided to identify only those listed above, excluding the Armed Forces, the Security Intelligence Services and the Secretary General of the Security System.

3.3.4. CHARACTERISATION OF THE *GUARDA NACIONAL REPUBLICANA*

The *Guarda Nacional Republicana* is, according to its Organic Law, a security force of a military nature, composed of military personnel organised into a special body of troops and endowed with administrative autonomy, which incorporates a set of broad-spectrum capabilities arising from the characteristics arising from its nature, allowing it to strengthen the exercise of its mission as a security force, in the security dimensions of military defence and Internal Security, and also in the context of other attributions, namely in the context of emergency protection and rescue (General Officer Promotion Course [CPOG], 2020, pp.177, 178).

In this regard, it is important to bear in mind that, according to the terms of article 3 of its Organic Law, the GNR is assigned missions which fit into the two dimensions foreseen in the normative reference of CI in a national context, i.e., the safety and security dimensions. These are materialized in the following attributions: i. maintain the surveillance and protection of sensitive points, namely road, railway, airport and port infrastructures, public buildings and other critical facilities; ii. protect, rescue and help citizens and defend and preserve assets that are in situations of danger, due to human action or nature (National Assembly [AR], 2007).

Notwithstanding the identification of specific attributions in the safety and security dimensions foreseen by law, the GNR incorporates in its organization and respective organic structure two units with exclusive missions in these areas, namely, the Emergency Protection and Rescue Unit and the Security and State Honours Unit.

The Emergency Protection and Rescue Unit, as a specialised unit with the specific mission of executing prevention and intervention actions throughout the national territory in situations of serious accidents and disasters, namely in the event of rural fires, hazardous materials, floods, earthquakes, search, rescue and salvage in different environments, as well as in other emergency situations of protection and rescue, including judicial inspection in aquatic and sub-aquatic environments, eminently focused on the safety dimension (*Guarda Nacional Republicana* [GNR], 2020).

And also, the Security and State Honours Unit, more security oriented, the representation unit responsible for the protection and security of the sovereign bodies and other entities entrusted to it and for the provision of State honours, as provided in article 43 of the GNR Organic Law. As a result of the above listed duties, the Unit ensures the security of the following sovereign bodies: i. S. Bento Palace - National Assembly; ii. Necessidades Palace - Ministry of Foreign Affairs; and iii. Belém National Palace - official residence of the President of the Republic (GNR, 2020).

Besides the Units listed above, oriented towards missions of this nature, the GNR has twenty Territorial Commands with specific attributions in the security dimension, namely the Tax Posts implemented in the Ministry of Finance, in the airports of Faro, Lisbon, Porto and in the Autonomous Regions of Madeira and Azores, which, according to their inherent competences, carry out tasks at the level of security of installations (Ministry of Internal Administration [MAI], 2008).

In terms of territorial dispersion and consequent implementation at a national level, the GNR has 21,553 personnel distributed in 580 functional quarters and assumes responsibility for security in 94% of the national territory, with a total area of 86,600 km², where 54% of the population resides. It should also be noted that it is responsible for 97% of the national road network (GNR, 2020b).

The dynamics of the new threats, risks and trends with implications for the GSF, identified in the exogenous analysis, tend towards a convergence of the concepts of defence and security, bringing to light the particular attributes of the gendarmeric forces, where the GNR is included, which enable its employment in a comprehensive way, acting in each of the aspects of the security spectrum. In this context, the following issues are highlighted: i. the GNR is positioned as a hinge between the Armed and Security Forces; ii. the pursuit of military, police and civilian activities; iii. the dispersion and geographic amplitude of the GNR's action (CPOG, 2020, pp.177, 178).

According to the GNR Activities Plan for 2022, given the relevance and actuality surrounding the theme of CI protection, it becomes necessary "(...) to continue to develop and deepen the organisation, the processes, the procedures and the systems necessary for timely decision making that allow the GNR to acquire a greater capacity for intervention in terms of CI security and resilience (...) supported by a transversal approach to the risks to which these infrastructures may be exposed (...)” (GNR, 2022, pp. 17).

In this context, two areas of intervention were identified by the GNR High Command, one internal - which presupposes the development of the intervention capacity in the CI, guiding and coordinating the preparation of the Safety and External Protection Plans as well as the external one (entities that supervise this matter and respective CI operators) - which aims to promote the adoption of a common



model for the georeferencing of all CIs and the implementation of the measures foreseen in the Action Plan for the Protection and Security of Critical Infrastructures (PAPSIC), under the National Strategy to Combat Terrorism (GNR, 2022, pp. 125).

It is important to mention that today, only for the energy and transport sectors, the ANEPC has identified and classified 177 CI in the whole national territory, most of them with implementation in the GNR's territorial competence area, leaving ten other sectors, defined by Decree-Law 20/2022 (GNR, 2022, pp. 125).

In summary, after a comprehensive analysis of the actors involved in CI protection and specifically the *Guarda Nacional Republicana*, the following particularities can be identified that may be included in the dynamic SWOT matrix:

- *The GNR has attributions embodied in its organic structure in the two main dimensions in terms of CI protection, i.e. safety and security;*
- *In its organization, two Units with specific competences in both dimensions are identified: the Security and State Honours Unit, which is more security-oriented, and the Emergency Protection and Rescue Unit, which is safety-oriented;*
- *The geographical implementation of the GNR - it is responsible for security in 94% of the national territory, through 580 quarters distributed territorially;*
- *Responsible for 97% of the National Road Network;*
- *It is necessary to optimise procedures and support the Units in the development of the Safety and External Protection Plans in close articulation with the CI Operators;*
- *The existence of limited resources presupposes adequate management of the means available;*
- *The gendarmeric nature allows the GNR to position itself as a hinge element between the Armed Forces and to develop wide-ranging activities, from a more robust component to activities of a police and civil nature;*
- *The existence of a training plan, since 2020, dedicated to infrastructure protection and safety;*
- *The inexistence of an organic structure within the GNR to coordinate all matters related to cybercrime;*
- *Most of the CIs are within the GNR's territorial jurisdiction.*

4. DISCUSSION

As a result of the strategic diagnosis made in the previous chapter, where the characterisation of the exogenous and endogenous environment was carried out, it was possible to list the strengths and weaknesses, which, in turn, allowed pointing out opportunities and threats, on which a future action should focus, either from an individual or collective perspective, in order to create and explore synergies, much through the profitability of intalled capacities. It was also possible to identify threats, on which mitigation efforts should be focused, given the weaknesses identified, taking advantage of possible strengths for the same purpose. All this information is presented in the table below in the form of a Power SWOT.

Table 14. SWOT analysis | Critical Infrastructure

Internal factors	Strengths (S)	Weaknesses (W)
	<ul style="list-style-type: none"> • The Organic Law assigns the GNR missions framed in the two dimensions foreseen in the normative reference of CI in a national context, i.e. the safety and security dimensions; • Defined procedures for identifying, designating, protecting and enhancing the resilience of national and European critical infrastructures; • The CI safety plan presupposes the necessary articulation with the protection and intervention plan prepared by the territorially competent Security Forces; • Most of the CIs are within the GNR's territorial jurisdiction; • GNR is responsible for 97% of the National Road Network and 94% of the National Territory; • The creation by law of a registration and information sharing centre, within the scope of CI. 	<ul style="list-style-type: none"> • Slowdown in recruitment and procurement processes; • Lack of training and culture in CI protection; • The inexistence of an organic structure within the GNR that coordinates all issues related to cybersecurity; • The multiplicity of actors involved in emergency planning processes; • Lack of articulation between the Security Plans and the Protection and Intervention Plans; • Lack of safety culture
<p>External factors</p>		
<p>Opportunities (O)</p> <ul style="list-style-type: none"> • Hyper digital connectivity and technological transformations increases the interconnections of markets, people and equipment; • Need to diversify suppliers of energy resources and raw materials; • The population's sense of well-being and security is at historically low levels. • Increasing globalisation with its consequences on the increase of populations and respective urban areas. • Increased migration flows. 	<ul style="list-style-type: none"> • The creation of synergies and the implementation of information-sharing platforms, within the scope of CI, of an intra-state nature at European level, based on the Portuguese model. • Considering its gendarmeric nature and the diversity of its tasks, the GNR is the entity best placed to lead a process of research and development of resources (among member states), with applicability in the protection of CIs. • Consolidate the institutional relationships between the Operators and the competent Security Force, through training, drills and exercises. 	<ul style="list-style-type: none"> • On the basis of existing resources and in order to take advantage of territorial implementation, create a structure dedicated to the prevention and investigation of computer-related crimes. • Commitment to interoperability between systems and agents. • Develop certification processes, at the quality level, in what concerns the articulation between the Safety Plans and the Protection and Intervention Plans, increasing the levels of trust with the CI Operator. • Develop resource sharing process, with particular focus on the cross-border area.
<p>Threats (T)</p> <ul style="list-style-type: none"> • Increased threat of cyber attacks; • The return of tensions and conflicts between the major global powers; • States and public organisations have lost their monopoly on technology; • Decreased investment in the defence and security sector at European level • Increase in extremist, nationalist, ethnic and religious movements; • Increase in criminal phenomena related to terrorism and transnational organised crime; • Economic contraction, increase in poverty-related phenomena. 	<ul style="list-style-type: none"> • Develop programmes to raise awareness and prevent cyber attacks among the general population; • Develop and consolidate internal processes for resilience and protection against cyber attacks. • Implement standards to enhance the Protection and Security Plans. 	<ul style="list-style-type: none"> • Implement internal training processes to develop skills and institutional culture related to CI protection. • Optimise available resources using technological tools.



Figure 13. Key strategies | Critical Infrastructure

5. CONCLUSIONS & RECOMMENDATIONS

This study addressed the issue of CI protection in the current security framework, focusing on the national territory and, inherently, on the international context in which it is involved, as an EU Member State. The analysis of the legislative acquis on the subject, which allowed to verify the growing concern with the implementation of measures to increase the resilience of the CI, either in a safety or security context, against the identified threats, whether natural, accidental and/or intentional, was also highlighted. Regarding the main implications for the Security Forces, considering the trends identified in the strategic diagnosis, we highlight the following: i. instability requires an increase in the Forces' readiness, as well as the development of more comprehensive capabilities; ii. an increase in international cooperation between security actors; iii. an increase in the complexity of foreseeing and reacting to incidents; iv. it requires the creation of information processing mechanisms aiming at a quick, efficient and effective reaction to incidents; v. the increase of private sector actors in the security area; vi. The need to share information among the FFSS in a timely manner.

In a more holistic perspective, framed here by the geographical dimension of the EU, there is also the need to develop resource sharing programmes between MS; the development of agreements between MS that allow for the research and development of resources and equipment, as well as the sharing of knowledge and best practices.

Following the provisions of article 14 of Decree Law 20/2022, it is important to develop the necessary work for the development and implementation of the Critical Infrastructure Information Registration Platform, given the potential of constituting an aggregating measure, in the sense that it presupposes the achievement of important objectives, such as: i. the availability of information related to threat and risk assessments; ii. the promotion of measures, recommendations and best practices, with the desideratum of increasing the resilience of CI; iii. the sharing of information in order to optimize the planning and prioritization processes of interventions related to the strengthening of security; iv. the monitoring, recording and management of accidents and relevant incidents.

It was also concluded that it is extremely important to review the safety plans attached to each CI every five years, as well as to carry out drills and exercises every two years, as they are true catalysts for continuous improvement.

It was also perceived that, given the dynamics of new threats, risks and trends with implications for the SWg, identified in the exogenous analysis, they tend towards a convergence of the concepts of defence and security, bringing to light the particular attributes of the general forces, where the GNR is included, which enable its employment in a comprehensive way, acting in each of the aspects of the security spectrum. In this context, the following issues are highlighted: i. the GNR is positioned as a hinge between the Armed and Security Forces; ii. the pursuit of military, police and civilian activities; iii. the dispersion and geographical amplitude of the GNR's action.

In the development of this article, a methodology based on inductive reasoning was followed and a qualitative research strategy was used, based on the observation of the phenomenon under study and on the interpretation of patterns found in the data obtained, through the consultation of several bibliographies and legislative acquis on the subject.

As a research design, a case study was used, focusing on the national reality, with particular reference to the GNR.

Given that the object of study is the protection of military units, it was defined as an OG to identify measures for the protection of military units that could be implemented to increase their resilience, given the current security situation in Europe. In the scope of the subsequent OG and OE, it was possible to obtain answers to the formulated QC and QD.

In the answer to the questions formulated, applied to the specific case of the GNR and to the CIs in national territory, it is concluded that it is necessary to accompany the consolidation of the digital network of all GNR services, with the integration of computer systems in a single platform, contributing to the optimization of decision cycles. To this end, the following measures are planned:

- Promote the organisation, processes, procedures and systems necessary for timely decision-making that enable the linking and monitoring of the CIs;
- Ensure digital interoperability capacity of the various GNR services in the event of an incident in CI, developing *continuous and coordinated functional integration of systems, identifying gaps*;
- Certify the suitability of the equipment in ITP and make available images and alarm systems in the Situation Room and CINGOp, ensuring the compliance of the facilities, *adequate to the preparation and conduct of operations, as well as the maintenance requirements*.

Finally, the study carried out for the preparation of this article enabled us to make practical recommendations, which are presented below, on the designation of Key Take aways: i. focus on interoperability between systems and agents; ii. dissemination of good practices; iii. review of security plans; iv. carrying out exercises and simulations; v. enhancing information sharing; vi. optimisation of resources; and vii. optimisation of available resources.



REFERENCES

- ANEPC [Autoridade Nacional de Emergência e Proteção Civil], 2013. *Planos de Segurança do Operador (PSO) de Infraestruturas Críticas - Conteúdos dos PSO na Componente Safety*. Lisboa: Autoridade Nacional de Proteção Civil.
- ANEPC, 2017. *Boas Práticas de Resiliência de Infraestruturas Críticas Setor privado e setor empresarial do estado*. [Em linha] Disponível em: <http://www.procivil.pt/pt-pt/RISCOSPREV/INFRAESTRUTURASCRTICAS/Paginas/default.aspx> [Acedido em 12 Fev. 2022].
- AR [Assembleia da República], 2007. *Lei n.º 63/2007, de 11 de junho – Aprova a orgânica da Guarda Nacional Republicana*. Lisboa: Assembleia da República.
- Curso de Promoção a Oficial General (CPOG) 2019-2020 (2020). *Desafios Estratégicos para Portugal no Pós-Covid-19*. Cadernos do IUM, 43. Lisboa: Instituto Universitário Militar.
- GCS [Gabinete Coordenador de Segurança], 2011. *Infraestruturas Críticas - Conteúdos dos Planos de Segurança do Operador (Componente Security)*. Lisboa: Gabinete Coordenador de Segurança.
- General Secretariat for Defence and National Security [SGDSN], 2017. *The critical infrastructure protection in france*. [Em linha] Disponível em: <http://www.sgdsn.gouv.fr/uploads/2017/03/plaquette-saiv-anglais.pdf> [Acedido em 20 Fev. 2022].
- GFMI [German Federal Ministry of the Interior], 2009. *National Strategy for Critical Infrastructure Protection (CIP Strategy)*. [Em linha] Disponível em: <https://www.bbk.bund.de/ShareDocs/Downloads/BBK/EN/CIP-Strategy.pdf?blod=publicationFile> [Acedido em 11 Fev. 2022].
- Guarda Nacional Republicana. (2020). *Estratégia da Guarda 2025, uma estratégia centrada nas pessoas*. [Em linha] Disponível em: https://www.gnr.pt/InstrumentosGestao/estrategia_2025.pdf [Acedido em 20 Fev. 2022].
- Guarda Nacional Republicana. (2020b). *Relatório de Atividades da Guarda 2020*. [Em linha] Disponível em: https://www.gnr.pt/InstrumentosGestao/2022/PA_GNR_2022.pdf [Acedido em 20 Fev. 2022].
- Guarda Nacional Republicana. (2022). *Plano de Atividades da Guarda 2022*. [Em linha] Disponível em: https://www.gnr.pt/InstrumentosGestao/2020/PA_GNR_2020.pdf [Acedido em 20 Fev. 2022].
- MAI, 2014. *Decreto-Lei n.º 163/2014, de 31 de outubro - Lei Orgânica da ANPC*. [Em linha] Disponível em: <https://dre.pt/application/file/a/58660558> [Acedido em 12 Fev. 2022].
- MAI, 2008. *Portaria n.º 1450/2008, de 16 de dezembro - Estabelece a organização interna das unidades territoriais, especializadas, de representação e de intervenção e reserva da Guarda Nacional Republicana (Guarda) e define as respectivas subunidades, bem como os termos em que se processa o apoio administrativo pelos serviços do Comando da Administração dos Recursos Internos (CARI) e da Secretaria-Geral da Guarda (SGG) às unidades especializadas, de representação e de intervenção e reserva*. [Em linha] Disponível em: <https://dre.pt/dre/detalhe/portaria/1450-2008-443766> [Acedido em 12 Fev. 2022].
- Martinho, J.P.S., 2017. *As Infraestruturas críticas em Portugal: um modelo de abordagem*. Trabalho de Investigação Individual do CEMC 2016/17. IUM.
- MDN [Ministério da Defesa Nacional], 2011. *Decreto de Lei n.º 62/2011, de 05 de setembro - Estabelece os procedimentos de identificação e de protecção das infra-estruturas essenciais para a saúde, a segurança e o bem-estar económico e social da sociedade nos sectores da energia e transportes e transpõe a Directiva n.º 2008/114/CE, do Conselho, de 8 de dezembro*. Lisboa: Assembleia da República.

- Santos, L. A. B. dos, Lima, J. M. M. do V., Garcia, F. M. G. P. P., Monteiro, F. T., Silva, N. M. P. da, Silva, J. C. do V. F. da, Santos, R. J. R. P. dos, Afonso, C. F. N. L. D., & Piedade, J. C. L. (2019). *Orientações metodológicas para a elaboração de trabalhos de investigação* (Centro de Investigação e Desenvolvimento (ed.); 2.^a Edição). Instituto Universitário Militar.
- PCM [Presidência do Conselho de Ministros], 2018. *Decreto de Lei n.º113/2018, de 18 de dezembro - Cria a Unidade de Emergência de Proteção e Socorro na Guarda Nacional Republicana*. Lisboa: Assembleia da República.
- PCM [Presidência do Conselho de Ministros], 2021. *Decreto de Lei n.º 65/2021, de 30 de julho - Regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do Parlamento Europeu, de 17 de abril de 2019*. Lisboa: Assembleia da República.
- PCM [Presidência do Conselho de Ministros], 2022. *Decreto de Lei n.º 20/2022, de 28 de janeiro - Aprova os procedimentos para identificação, designação, proteção e aumento da resiliência das infraestruturas críticas nacionais e europeias*. Lisboa: Assembleia da República.
- PCM, 2014. *Decreto-Lei n.º 3/2012, de 16 de janeiro (2.ª alteração a coberto do Decreto-Lei n.º 69/2014, de 9 de maio)* - Orgânica do Gabinete Nacional de Segurança - Criação do Centro Nacional de Cibersegurança. [Em linha] Disponível em: <https://dre.pt/application/file/a/25343853> [Acedido em 14 Fev. 2022].
- UK Government, 2010. *Strategic Framework and Policy Statement on Improving the Resilience of Critical Infrastructure to Disruption from Natural Hazards*. [Em linha] Disponível em: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/62504/strategic_framework.pdf [Acedido em 10 Fev. 2022].
- União Europeia, 2008. *Diretiva do Conselho 2008/114/CE - Identificação e Designação das Infraestruturas Críticas Europeias e a Avaliação da Necessidade de Melhorar a sua Proteção*. [Em linha] Disponível em: <http://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32008L0114&from=PT> [Acedido em 01 Fev. 2022].
- Tessari.P & Muti.K. (2021). *Strategic or critical infrastructures, a way to interfere in Europe: state of play and recommendations*. Directorate General for External Policies of the Union. [Em linha] Disponível em: [https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653637/EXPO_STU\(2021\)653637_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653637/EXPO_STU(2021)653637_EN.pdf) [Acedido em 20 Fev. 2022].



Page intentionally left blank

VIII. PAPER | MIGRATORY PHENOMENA

Citation:

Multiple authors. Innovative, information-driven and cooperative approaches to border management and migratory affairs: Strategies for future-proof gendarmeries. *Royal Netherlands Marechaussee. Overcoming Security Threats arising from Globalization 4.0 – FIEP Association, 2022.*

Published: October 2022

Publisher's Note: FIEP stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors.

The Netherlands

Royal Netherlands Marechaussee

Multiple authors

Kalvermarkt 32, 2511 CB, The Hague (The Netherlands);
stckmar.fiep.kmar@mindef.nl

Abstract:

Technological developments are reshaping the world around us and the way we conduct our operations. Also, increasingly, information is becoming the foundation of our deployments as gendarmerie organizations. Since migration is by definition an international phenomenon that involves cross-border networks and routes, international legal frameworks and global information tools, and this will likely only increase into the future, international cooperation is key.

This article is part of the FIEP 2022 Publication and focuses on migratory affairs. It draws attention to both external drivers in migration management as well as internal developments in gendarmeries. The principal aim of this work is to generate possible strategies or options for gendarmerie organizations to deal with migratory affairs in accordance with our respective tasks, such as border management and combating human smuggling. For this purpose, strategic analysis tools such as PMESII / DIMEFIL and SWOT matrix have been used. Subsequently, the dynamic SWOT model (SWOT-TOWS) has been used to create possible strategies.

The key takeaways can be summarized as improving information-driven operations, making the most of technological innovation and the importance of international cooperation to increase effectiveness.

Keywords: migration; gendarmerie; information-driven operations; innovation; international cooperation.

1. INTRODUCTION

This article is part of the FIEP 2022 Publication and focuses on migratory affairs. It aims to draw attention to trends in the external environment of migration and human smuggling, as well as zoom in on developments within the internal environment of gendarmeries. The principal aim of this work is to generate possible strategies or options for gendarmerie organizations to deal with migratory affairs in accordance with our respective tasks.

As gendarmerie organizations, all of us deal with the influence and impact of migratory movements. Some gendarmerie organizations are involved in missions abroad to counter conflict as a root cause of migration. Many deal directly with cross-border mobility as border management authorities at land borders, airports, harbours and railroads. Most gendarmeries also take on irregular migration or human smuggling through criminal investigations, increasingly in the digital realm. And all of us, as individuals and organizations, are part of state structures, labour markets and societies that are transformed by migration and its consequences.

In the Netherlands, the Royal Netherlands Marechaussee (RNLM) approach to migration is part of the wide-ranging, whole-of-government migration policy of the Dutch government. The aim of this comprehensive approach is to ensure that migration occurs safely and in a well-managed way. Those who truly need protection must be protected. Migration movements must be in line with the needs and capacity of Dutch society. Central government, municipalities, provinces, civil society partners and countries within and outside the European Union (EU) will work together even more closely.¹⁰

The comprehensive approach to migration is based on six pillars:

1. Preventing irregular migration.
2. Improving reception and protection for refugees and displaced persons in the region.
3. Achieving a robust asylum system, based on solidarity, in the EU and the Netherlands.
4. Combating illegal residence and stepping up returns.
5. Promoting legal migration routes.
6. Encouraging integration and participation.¹¹

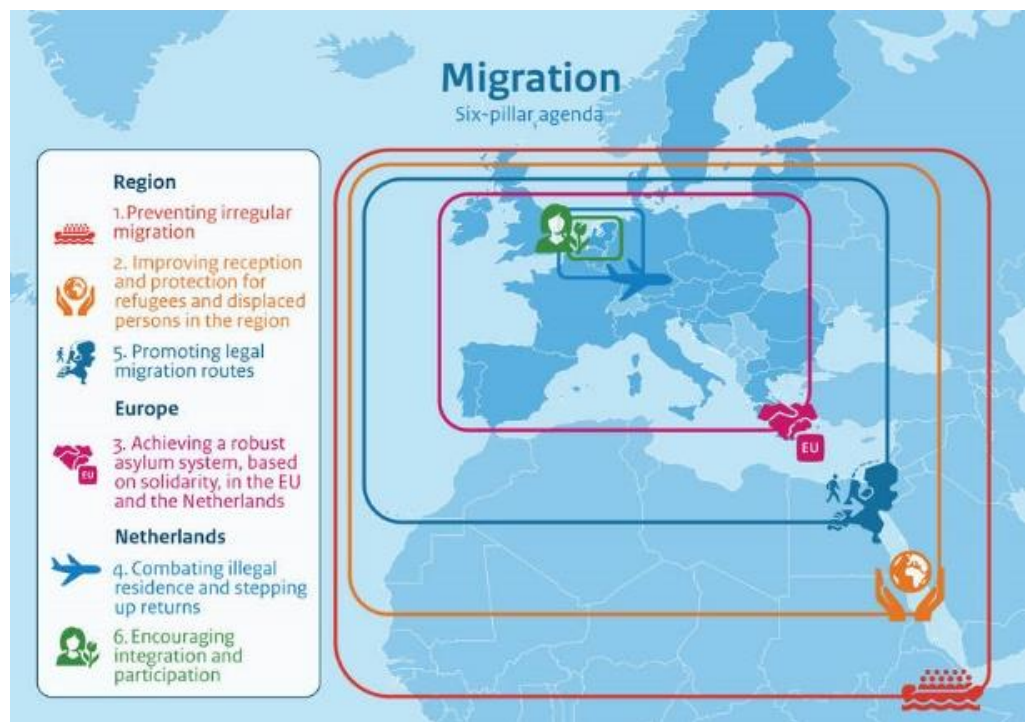


Figure 14. Comprehensive Migration Policy

¹⁰ www.government.nl/topics/asylum-policy/migration-policy

¹¹ www.government.nl/topics/asylum-policy/migration-policy

2. MATERIALS AND METHODS

This article was written from a gendarmerie strategic and operational perspective and is based on open source documentation.

For the purpose of this article, the phenomenon of migration is narrowed down to irregular migration and human smuggling. While the need to deal with the root causes of (irregular) migration cannot be overstated, within the Netherlands these efforts are generally spearheaded by the Ministry of Foreign Affairs. Furthermore, a wealth of academic articles exists on the topic of root causes of migration, including in relation to climate change. For this reason, we have chosen to focus on the role of the gendarmerie as a border management authority and a criminal investigator of human smuggling, taking advantage of our perspective as RNLM members. This focus allows us to discuss strategies for gendarmerie organizations that are operating in the changing environment of Globalization 4.0, the overarching theme chosen by the Portuguese FIEP presidency for this year's Work Programme.

The method used in this article is SWOT-TOWS analysis. The SWOT results are presented and strategies are highlighted in the results section. First, the analysis section delves into a number of trends that are relevant to the gendarmerie tasks of combating human smuggling and dealing with migratory flows.

3. RESULTS

In the era of Globalization 4.0, spurred on by the “significant changes we are currently witnessing in technology, geopolitics, environment and society”, a shift towards a world that is becoming increasingly brittle, anxious, non-linear and incomprehensible (BANI) can be observed. This theme was highlighted by the Portuguese FIEP presidency in this year's Work Programme and serves as the backdrop to our further analysis.

Furthermore, “the components of the [BANI] acronym may even suggest response opportunities [for gendarmeries]: brittleness requires resilience; anxiety asks for empathy and mindfulness; non-linearity calls for context and adaptivity and incomprehensibility demands transparency and intuition. These may be reactions rather than solutions, but they suggest that the necessary answers can be found.” These accurate conceptual notions have sadly become very real and tangible because of the events of the past few months in Europe.

Gendarmerie organizations must respond to the challenges posed to them by this changing environment. In the following three sections, trends and factors related to the management of migration and combating human smuggling by gendarmerie organizations are analyzed. Possible strategic and operational responses are explored in all three sections. These sections take both external factors (opportunities and threats) and internal factors (strengths and weaknesses) into account.



3.1. TECHNOLOGICAL INNOVATION: FROM RULE-BASED TO RISK-BASED BORDER MANAGEMENT

“Smart operations require technological innovation”

Lieutenant General Hans Leijten

Commander of the Royal Netherlands Marechaussee

Strategic level

Technological developments are reshaping the world around us and the way we organize our operations. For that reason, we ought to re-evaluate the current operational mix of technology and human efforts. What skills does the gendarme of the future need in order to perform the task at hand? A first takeaway: there will always be a need for a human factor, since not all benefits of human experience and sensing can be replaced by technology.

To arrive at fully information-driven operations in border management, the RNLM has a strategic ambition to continuously improve its array of technical resources. In the near future, that will require adopting more technical support tools, such as drones, cameras and exoskeletons. Besides the hardware, the organization is also focused on upgrading its information systems and databases. Despite significant steps forward, much work remains to be done. This transformation will require time, adaptations in legal frameworks regarding data and privacy, and indispensable investments in up-to-standard AI and data-management systems.

The RNLM ambition states that the current border control process will be developed through innovation and digitalized. Digitalization does not only refer to the use of a self-service system and e-gates, but also to applying innovation to the actual border control process. This means that routine first-line checks will be automated and there will be a move towards information-based or even risk-based border control.

The use of smart technology should lead to a better information position on the passenger prior to the border passage, which will enable us to perform risk-based border control. Routine checks will be carried out automatically as much as possible, thereby decreasing the number of physical interactions. While border guards will remain responsible for first-time decision-making, they will be supported by technology. As such, the use of smart tools should lead to a border guard being better able to weigh the risks on the basis of suspicious behaviour, such as passengers who are carrying an amount of luggage that is inconsistent with their itinerary or who are travelling into the Netherlands following an illogical travel route. Human decision-making, however, will remain crucial to the final decision.

Operational level

The ever-changing operational environment requires a gendarmerie to constantly adapt its operational concept. In order to evolve into a future-proof organization, the RNLM not only adheres to its strategic ambition to continue to invest in and adopt technology but also takes factors such as the current modernization of EU regulations and feedback from our operations into account. Existing challenges, such as limited resources and personnel, as well as requirements from commercial partners, such as transport companies, add to the mix.

Driven by the momentum of current reform in EU regulations on border management, the above factors have been translated into a Future Borders concept based on information-driven border controls. This concept aims to shift our focus from rule-based to risk-based border management. It consists of the following main elements:

- *Digitalization of the first line of border control. After their arrival in the Netherlands (for example at Schiphol Airport), passengers of both EU (free travel area) and non-EU nationalities are asked to present their documents at several points under the supervision of border guards. In the case of clearly bona fide border crossings, passengers can continue their border passage without the intervention of a border guard, in some cases by using self-service systems (ABC gates, kiosks). Information received prior to passengers' journeys enables the RNLM border guards to pick out the passengers who will then automatically be directed to border guard officers. All mandatory controls will be automated. An extra automation challenge concerns the routine check for 'sufficient means, purpose and duration of stay', as required by the Schengen Borders Code. The RNLM is currently exploring cooperation with academic research departments to possibly develop a chatbot functionality for this check. Furthermore, the RNLM will possibly take part in a pilot project initiated by the European Commission regarding the use of digital identity in the border control process. Such digitalization, brought about by new technologies to support border control, will increase data processing efficiency and thus strengthen our information position.*
- *Information-driven operations are essential. The use of indicators, watch lists and existing information, such as interactive API passenger information, allows for more information-driven operations, which enhances the effectiveness of border controls. This concept is described in more detail in section 2 on information-driven operations.*
- *The time and place of checks and interventions can be adjusted on the basis of the prevailing security risks and information risks. For example, physical and administrative checks could potentially be performed in the country of departure (pre-clearance) rather than on arrival. Furthermore, threats to national security can be identified and dealt with at an earlier stage. This includes cooperation with immigration officers in the country of departure and with air operators. On board ferries, trains and buses, the RNLM can carry out checks during the journey from A to B. For travellers, this approach results in a more seamless and faster passage, as self-service systems and touchless interaction reduces effort and increases comfort. Waiting in long queues and being subjected to intensive questioning should, for most passengers, become a thing of the past.*
- *Ethical standards, including privacy, are key principles in the use of information and the creation of profiles and watch lists. They are maintained throughout the operation.*
- *Through this process, the RNLM maintains an overview of and insight into passenger flows, both physically and digitally, for the purposes of its tasks in enforcement, investigation and intelligence. These insights are provided by human efforts and technology; by border guards when needed and by smart tools when possible. However, the human border guard maintains the final say on a traveller's border crossing, with technology supporting this process.*
- *Digital identity is the guiding element and crucial in our future-proof concept. A digital identity allows for parts of the border process to be automated, while the reliability of the data is guaranteed and identification will become smarter and faster in the future.*



3.2. INFORMATION-BASED OPERATIONS

“Increasing effectiveness through information-driven operations”

Lieutenant General Hans Leijten

Commander of the Royal Netherlands Marechaussee

Strategic level

Increasingly, information is becoming the foundation of our deployments as gendarmerie organizations. More and more, it determines what we do and where we do it. This affects the way we collect and process information, as well as the way we deploy personnel and the way they do their jobs. Our personnel play a crucial role in information exchange. Gathering intelligence has become one of our key tasks. The intended end result or effect, which we aim to achieve by using our expertise and creativity, is the principal consideration.

For the RNLM, the transition to fully information-driven operations is a major one and was embarked on in 2008. In the past few years, this long-term process has had far-reaching effects on command and control structures, intelligence gathering capabilities and investments in IT and real estate.

The National Tactical Command, a central national command, was established in 2015. This was a big leap forward from the earlier, highly fragmented regional command and control structures. The RNLM has continued to develop ever since and expects to continue this change process into the future. It recognizes that information-based operations require a strong focus on information gathering, enriching and analyzing activities.

The purpose of these extensive developments is to contribute to the achievement of government security objectives by enabling an adequate response to the professionalization of national and international criminal organizations. However, the ambition to achieve fully information-driven operations includes more than a policy programme or the necessary IT and technical modifications. It also encompasses a cultural shift in our way of thinking and acting in terms of our profession. This process will therefore remain a priority in the coming years.

Operational level

On an operational level, the ambition to achieve fully information-based operations entails a shift from capacity-driven to information-driven command and control structures. At the RNLM, this development is a work in progress and the first results have been achieved.

For example, RNLM gendarmes perform mobile checks, in addition to their routine tasks, at smaller harbours. This includes a stop at the harbour manager’s office to have an informal chat about the situation in the marina. They also conduct an awareness campaign, which includes leaflets and social media posts, to inform target groups in the maritime sector (harbour managers, boat owners, sailing equipment shops) about specific risks, such as human smuggling in or via the maritime sector. The campaign shares relevant indicators and contact details of the authorities in order to create awareness and make it possible for citizens to contact the authorities in case of any suspicious situation. At the end of such a visit, relevant information is recorded and shared. Such casual meetings have occasionally generated impressive results. The RNLM therefore aims to expand this approach and make it an integral part of its modus operandi for every gendarme.

On the other hand, however tempting it may be to always carry out routine mobile checks, which tend to always produce a hit or result, the best way of achieving a certain effect may sometimes be to take another approach. At every brigade or even gendarme level, it is therefore important to plan ahead and reflect on the best way of getting the information needed. For example, while preventing the crossing of a group of clandestine migrants at the harbour is important, the higher value lies in capturing the network behind them. A proper information-driven operation therefore requires that we plan in advance, resist our first instincts and at times opt for an alternative approach.

On the basis of this shift in thinking, RNLM checks will in the future increasingly be carried out in a hit-and-run manner. A gendarme will only be where she or he has to be and will perform indicator-based checks (based on risk profiles, modi operandi, police information, etc.) in accordance with fixed basic principles regarding selection, engagement and reflection.

3.3. INTERNATIONAL COOPERATION

Migration and human smuggling is by definition an international phenomenon that involves cross-border networks and routes, international legal frameworks and global information tools, including social media. This will likely only increase in the future. As gendarmerie organizations, at home in both the civilian and military domains, we are equipped with an international outlook, have an international work domain and often have experience in deployments abroad within multinational environments. It is essential to use this advantage and the opportunities presented by, for example, the FIEP network or existing liaison positions to increase international cooperation both on a strategic and an operational level.

Strategic level

At the RNLM, the KMar Integrated International Strategy 2021-2025 strategically shapes our current and future international activities. This strategy document is rooted in analyses of international trends, as well as policy documents of relevant ministries (Justice and Security, Defence, Foreign Affairs). It prioritises three phenomena – terrorism and extremism, irregular migration, and transnational crime such as human smuggling – as well as preferred types of engagement and geographic focus areas for the RNLM's international activities until 2025.

With regard to combating irregular migration and human smuggling, cross-border cooperation is key. In addition to a strong existing network of bilateral partners, such as with other European gendarmeries, this requires strategic-level engagement to identify possible relevant counterparts along migration routes. The FIEP network, as well as regional networks such as EUROGENDFOR, may serve as first point of contact and a platform to build acquaintance and trust.

Secondly, the RNLM maintains a network of liaison officers at embassies around the world. This network has proven to be a valuable tool. Initially positioned to enhance operational information exchange and cooperation, liaison officers also prove their worth as eyes and ears, pioneers in cooperation and representatives of the RNLM abroad. It is worth investigating how to make better use of their position and network for strategic priorities. Additionally, we work with the Dutch National Police to link our respective liaison networks, to function as each other's fall-back option and to help each other out when necessary.

Third, at the RNLM, we aim to make good use of the international network of the Ministries of Defence, Justice and Foreign Affairs. As part of the MoD, we participate in the defence attaché network stationed all over the world, with gendarmerie colleagues stationed in, for example, Jordan, Egypt and the Balkan region. Furthermore, strategic positions in multilateral organizations, such as the EU, NATO and Frontex, help us to



increase understanding, know what is on the agenda and find ways to advance our objectives in these organizations.

Fourth, the RNLM as a border management authority pro-actively engages in advising on legislative drafts, whether on a national or a European level. Border authorities, whose trump card is operational knowledge and expertise, could play an important advisory role in helping to design and enhance border management policies and legal migration frameworks on a national and a European level.

Momentum in EU regulations on external border management

In the European context, the last few decades have seen new security regulations regarding free movement of persons in the Schengen area as a result of several terrorist attacks and the COVID-19 pandemic. Furthermore, technological and societal developments have led to demands regarding digitalization of the border control process.

In response to these developments, the EU approach to external border management has been updated continuously. The mandate of the European Border and Coast Guard (EBCG) Agency Frontex for the use of passenger data has been expanded and the Frontex Standing Corps is expected to grow to 10,000 border guards by 2024. Various new European regulations, such as the EBCG Regulation (EU2019/1896) and a revision of the Schengen Borders Code, constitute a move towards processing an increasing amount of passenger information, which requires more cooperation between EU member states. Together with the implementation of the Integrated Border Management (IBM) policies of the European Commission, these processes are generating a growing level of accountability within and between EU member states, as well as in relation to the European Commission. Taken together, these developments are creating momentum – and providing the means - to intensify the transition to information-based and risk-based operations.

This policy context provides ample reason for gendarmeries to actively participate in national migration policy development of the Ministries of Defence or the Ministries of Justice/Home Affairs, or for European gendarmeries to take part in EU High Level Working Groups on the topic. In this way, a gendarmerie organization can influence all of these developments at an early stage. On a national level, it is crucial to invest in partnerships with stakeholders and play an active part in national contributions to coalitions with like-minded EU member states. While the results of EU cooperation are at times relatively intangible or difficult to measure, the power of teaming up and acting in a united way should not be underestimated, as the current crisis has illustrated.

<https://frontex.europa.eu/about-frontex/legal-basis>

Operational level

Investigative cooperation through Europol and Interpol

On an operational level, international cooperation can be fostered through use of key platforms Europol and Interpol. First, they allow for sharing operational data. Both can cross-match information and enable the secure transfer of data to member states. Secondly, they initiate and facilitate investigations and link, and if necessary align, national investigations into entities and networks. For moving investigations forward, it is sometimes of paramount importance to get together and work on analyses and targets.

Sharing specialized knowledge: maximizing the impact of scarce resources

Secondly, a valuable aspect of international cooperation on a working level is to make use of each other's niche expertise, whether technical or derived from local awareness. On the technical side, this could mean certain investigation techniques, expertise on documentation and falsifications, cyber expertise, financial knowledge, and so on. Furthermore, any country on a migration route – whether source, transit or destination – can add knowledge on local criminal networks, means of communication, language, (informal) financial channels, (informal) transport networks, housing regulations and loopholes, knowledge on what happens in smuggling hubs, and so on. All of this increases the environmental awareness of the investigators and helps to focus the investigation, or broaden it when necessary.

Whether dealing with migration at border posts or investigating a possible smuggler, such specialist knowledge is often in demand. UN and EU missions and operations, border guard organizations such as Frontex and national gendarmeries often have to fish in the same limited pond of experts. Additionally, smugglers change tactics faster than operations to counter them can adapt. To tackle this threat, it is helpful to have upfront knowledge of potential alternative means and routes.

As a way to make the most of scarce resources and to share specialized expertise, the RNLM Expertise Centre on Documentation and Identity Fraud (ECID) has developed a training curriculum on travel documents (such as passports and ID cards) and falsifications that can be provided in any location by experienced instructors and document experts. Since these courses are relatively short (about two weeks per course) and modular (basic, advanced and train the trainer), they can inject specialist knowledge exactly where it is needed. Training courses have been given to national border guard organizations that deal directly with migration flows, but also as part of the EU Border Assistance Mission (EUBAM) in Libya. Additionally, by offering a train-the-trainer course to selected candidates, a training leads to certified local instructors who can continue to distribute the knowledge to their peers and others in their own respective organizations. In this way, limited resources – two trainers per course – are maximized to have a much bigger and lasting impact.

Cooperation in the digital age

Finally, the digital age allows us to connect more easily and quickly and lowers the threshold for conversation with experts around the globe, including all of the FIEP members. While clearly not all operational discussions can take place through less secure virtual connections, they allow us to reach out and test the water before meeting in person, or to have strategic discussions with peers around the globe.



3.4. SWOT

Table 15. SWOT analysis | Migratory phenomena

Internal factors	Strengths (S)	Weaknesses (W)
	<ul style="list-style-type: none"> • International outlook and strategy • RNLM is the authority in border management and human smuggling • RNLM has institutionalized advisory role towards relevant Ministries • Availability of well-trained instructors for specific (niche) expertise • Experienced personnel for Frontex deployments • R&D / Innovation hubs for border management at staff and ops level • Operational data feed into intelligence processes 	<ul style="list-style-type: none"> • Financial limitations • Limited personnel capacity for border management operations or investigations • Limited niche expertise available
External factors		
Opportunities (O) <ul style="list-style-type: none"> • Direct links - through policy Department – to decision-making processes on new EU regulatory framework • EU context and decision-making processes are ideal for coalition-building • Good international network at EU, NATO, UN, FIEP, etc. • Part of whole-of-government approach • Extra capabilities available through Frontex • Technological innovations in border management available on the market • Platforms and databases offered by Interpol, Europol • Wide availability of digital communication tools, such as apps/smartphones • Momentum through renewal of EU regulatory framework on border management 	<ul style="list-style-type: none"> • S7x06: Make better use of data provided by technological border tools to feed into operational intelligence • S6x06/O9: Continue to invest in R&D in order to prepare for future operations • S7x06/O9: Use intelligence as the foundation for more effective operational planning and deployments • S6x06/O9: Digitalize border controls • S1x03: Use international associations and networks - such as the FIEP - to identify relevant counterparts for cooperation on/along migration routes, to share initial information, build acquaintance and trust. • S1x04: Maintain international liaison network and use Defence/Interior Attaché network • S1x08: Work on sharing operational information, using relevant channels such as Interpol and Europol • S1x08: Work together on investigations, to the extent possible • S2/S3x01/O2/O3: Proactively advise policy departments on (practical/operational aspects of) EU legislation • S7x06: Make better use of data provided by technological border tools to feed into operational intelligence • S7x06: Make better use of data provided by technological border tools to feed into operational intelligence • S6x06/O9: Continue to invest in R&D in order to prepare for future operations • S7x06/O9: Use intelligence as the foundation for more effective operational planning and deployments • S6x06/O9: Digitalize border controls • S1x03: Use international associations and networks - such as the FIEP - to identify relevant counterparts for cooperation on/along migration 	<ul style="list-style-type: none"> • W2+O7: Improve our array of technical resources: hardware, software and the ability of gendarmes to use these in daily operations • W2xO8: Work on sharing operational information, using relevant channels such as Interpol and Europol, to counter limited national resources

	<p>routes, to share initial information, build acquaintance and trust.</p> <ul style="list-style-type: none"> • S1xO4: Maintain international liaison network and use Defence/Interior Attaché network • S1xO8: Work on sharing operational information, using relevant channels such as Interpol and Europol • S1xO8: Work together on investigations, to the extent possible • S2/S3xO1/O2/O3: Proactively advise policy departments on (practical/operational aspects of) EU legislation • S6xO6/O9: Continue to invest in R&D in order to prepare for future operations • S7xO6/O9: Use intelligence as the foundation for more effective operational planning and deployments • S6xO6/O9: Digitalize border controls • S1xO3: Use international associations and networks - such as the FIEP - to identify relevant counterparts for cooperation on/along migration routes, to share initial information, build acquaintance and trust. • S1xO4: Maintain international liaison network and use Defence/Interior Attaché network • S1xO8: Work on sharing operational information, using relevant channels such as Interpol and Europol • S1xO8: Work together on investigations, to the extent possible • S2/S3xO1/O2/O3: Proactively advise policy departments on (practical/operational aspects of) EU legislation 	
<p>Threats (T)</p> <ul style="list-style-type: none"> • Human smuggling as a profitable business model • Instrumentalisation of migrants by states • Wide availability of smuggling materials (boats, engines, life jackets, etc.) and public transport (buses, trains, ferries) • Migration hubs (refugee camps, safe houses) also used as smuggling hubs • Increase in migration flow and diversity of routes • Push factors for migration, such as climate change, repression, lack of employment opportunities, etc. • Insufficient specialist expertise available for needs/vacancies • (i.e. in UN/EU missions, etc.) 	<ul style="list-style-type: none"> • S6/S7xT3/T4/T5/T6: Move towards fully information-driven and risk-based operations, supported by the necessary technological tools 	<ul style="list-style-type: none"> • W2xT3/T4/T5/T6: Move towards fully information-driven and risk-based operations, supported by the necessary technological tools • W1/W2/W3+T7: Find innovative ways to share and exchange scarce specialized knowledge where it is most needed, such as short-term expert training, study visits among experts, or plugging expertise short-term into multinational missions



Figure 15. Key strategies | Migratory phenomena

4. DISCUSSION

The SWOT diagram was developed along the lines set out in the introduction and ‘Materials and methods’ section. To recall, the scope of the phenomenon was deliberately limited to two tasks of the RNLM regarding migration:

- Effective border management
- Combating irregular migration and human smuggling

Secondly, the analysis is primarily rooted in a European context (although some factors and strategies appear to be applicable more broadly). Furthermore, root causes for migration were left out of the analysis, although a number of root causes have been listed briefly in the ‘Threats’ section under T6 for reasons of comprehensiveness.

Description of the SWOT matrix

4.1. FACTORS

Strengths (S) – Internal factors that apply to a gendarmerie such as the RNLM were chosen. Being internal, these factors are within the realm of influence of the organization itself. The factors mentioned explicitly contribute positively towards performing the two tasks, and may serve as catalysts.

Weaknesses (W) – During the brainstorm phase and the analysis, it was discovered that the factors that negatively contribute towards performing the two tasks are often more general organizational issues, such as limits in financial or personnel means. These weaknesses are considered to be more or less universal and apply to most (government) organizations. Strategies based on these weaknesses may therefore also be helpful to other gendarmeries.

Opportunities (O) – During our analysis, it was found that factors that provide opportunities can be categorized into three groups:

- *External momentum because of modernization of EU regulations on border management*
- *Availability of technological innovations on the market (and interaction with our own innovation specialists)*
- *A strong international network on border management (which is essential to the fruitful exchange of best practices between states and gendarmeries, and to the ability to fulfil an advisory role towards EU policymakers).*

Notably, the EU naturally provides a similar legal and regulatory framework for all EU member states, which encourages cross-border outreach and striving for interoperability.

Threats (T) – The threat factors were found to be wide-ranging and, probably because of the scale of the phenomenon, quite diverse. A conscious decision was made to list these diverse aspects, even though not all could be addressed by strategies.

4.2. STRATEGIES

Strengths x Opportunities – Technological innovation, moving towards information-driven operations and international cooperation were found to be the three overarching themes.

Weaknesses x Opportunities – Showing a similar picture, especially the need for technological innovation and information-driven operations stood out.

Strengths x Threats – Note that the same strategy is deliberately listed under both SxT and WxT strategies. In fact, both the positive factor (strength) of innovation hubs and the negative factor (weakness) of inherent limitations in personnel available for border management or investigations resulted in the strategy to adapt our operations to become completely information-driven and less personnel-intensive.

Weaknesses x Threats – An interesting strategy was found to be the development of ‘plug-in’ operational concepts for distributing scarce expertise, such as specialized teams of instructors or experts who distribute their knowledge exactly when and where it is needed. This strategy maximizes their impact while avoiding existing limitations and responding to the risk of a lack of expertise in, for example, EU or UN missions.



5. CONCLUSIONS & RECOMMENDATIONS

To sum up, a future-proof gendarmerie faces a number of challenges and opportunities when dealing with migration. To better equip gendarmerie organizations and increase the effectiveness of their actions, we suggest exploring the following strategies.

TECHNOLOGICAL INNOVATION

- Improve our array of technical resources in terms of hardware, software and the ability of gendarmes to use these in daily operations.
- Do not leave border checks entirely to technology: the human factor (expertise, adaptivity) remains essential to the border control process, albeit with challenges, such as personnel shortages and the need for knowledgeable and qualified staff.
- Move towards fully information-driven and risk-based operations, supported by the necessary technological tools, for example by executing first-line border checks completely digitally before arrival (pre-clearance).
- Make better use of data provided by technological border tools to feed into operational intelligence.
- Continue to invest in R&D in order to prepare for future operations.

INFORMATION-BASED OPERATIONS

- Use intelligence as the foundation for more effective operational planning and deployments.
- In order to do this, maintain a strong focus on intelligence gathering, enriching and analyzing activities.
- Design operations and command and control structures on the basis of optimizing the intended effect.

INTERNATIONAL COOPERATION

- Use international associations and networks, such as the FIEP association, to identify relevant counterparts for cooperation on/along migration routes, to share initial information and to build familiarity and trust.
- Set up or expand a liaison network. Possibly work together with a police liaison network to expand global reach in a cost-effective way.
- Use ministry-level international networks, such as defence attaché networks (for those part of Ministry of Defence) or other attachés (Interior/Justice Ministries), as well as senior-level positions in multilateral organizations.
- Proactively advise policy departments on (practical/operational aspects of) EU legislation, such as Schengen Borders Code or Europol regulations.
- Find innovative ways, such as short-term expert training, study visits among experts or plugging expertise into multinational missions, to share scarce specialized knowledge where it is most needed.
- Work on sharing operational information using relevant channels, such as Interpol and Europol.
- Work together on investigations, to the extent possible.

- Make maximum use of virtual means to maintain more frequent and informal contact with international peers.

From these, our **main takeaways** can be summarized – in SWOT-TOWS format – as follows.

SxO

- Use intelligence as the foundation for more effective operational planning and deployments.
- Use international associations and networks - such as the FIEP - to identify relevant counterparts for cooperation on/along migration routes, to share initial information, build acquaintance and trust.
- Work on sharing operational information, using relevant channels such as Interpol and Europol.

SxT

- Move towards fully information-driven and risk-based operations, supported by the necessary technological tools.

WxO

- Improve our array of technical resources: hardware, software and the ability of gendarmes to use these in daily operations.

WxT

- Find innovative ways to share and exchange scarce specialized knowledge where it is most needed, such as short-term expert training, study visits among experts, or plugging expertise short-term into multinational missions.



REFERENCES

- Anonymous (2015). "Hoe werkt dat eigenlijk? Self-service passport control". *KMar Magazine*, no. 8, ch. 12. N.p.; 24 September 2015. Last consulted on 13-4-2022. <https://magazines.defensie.nl/kmarmagazine/2015/08/12_hoe_werkt_dat_eigenlijk_8-2015>
- Boer, Henny de (2020). "KMar Futureproof. Leijters ontvouwt toekomstvisie." *KMar Magazine*, no. 5, ch. 1. N.p.; 28 mei 2020. Last consulted on 13-4-2022. <https://magazines.defensie.nl/kmarmagazine/2020/05/01_commanders_intent_05-2020>
- Damstra, H.S. (2014). "Informatiegestuurd optreden bij de Koninklijke Marechaussee". *Militaire Spectator*. N.p.; 4 November 2014. Last consulted on 13-4-2022. <<https://www.militairespectator.nl/thema/operaties-bedrijfsvoering/artikel/informatiegestuurd-optreden-bij-de-koninklijke-marechaussee>>
- Directorate-General for Migration and Home Affairs (2022). "Smart borders". *Migration and Home Affairs – European Commission*. N.p.; n.d. Last consulted on 13-4-2022. <https://ec.europa.eu/home-affairs/policies/schengen-borders-and-visa/smart-borders_en>
- European Border and Coast Guard Agency (2022). "Legal Basis". N.p.; n.d. Last consulted on 13-4-2022. <<https://frontex.europa.eu/about-frontex/legal-basis>>
- Ministry of Justice and Security. "Migration policy". *Government of the Netherlands*. N.p.; n.d. Last consulted on 13-4-2022. <www.government.nl/topics/asylum-policy/migration-policy>
- Poiaras, Paulo LtCol (2021). "Work Programme of the Portuguese Presidency of the FIEP Association 2021/2022". *Guarda Nacional Republicana*. Portugal; 2021.
- Royal Netherlands Marechaussee (2020). "Geïntegreerde Internationale Strategie KMar 2021-2025". N.p., 2020.

IX. PAPER | HUMAN TRAFFICKING

Citation:

Diop, M., Human Trafficking. Overcoming Security Threats arising from Globalization 4.0 – FIEP Association, 2022.

Published: October 2022

Publisher's Note: FIEP stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors.

Senegal

Mariétou Diop



marietou.diop@gendarmerie.sn

Abstract

The research theme raises the issue of the ineffectiveness of anti-trafficking measures. Although many efforts are being made by States and the international community to eradicate human trafficking, the crime is gaining ground. The objective of this study is to assess the effectiveness of the response provided by States in the fight against human trafficking, in order to make it more efficient. The methodology followed in the framework of this study is essentially based on a collection of documents. It gave rise to an analysis of qualitative data, collected from training materials and reports produced by organizations specialized in the fight against the phenomenon. The study shows that the struggle against human trafficking is not effective because states face a number of difficulties. First, some of the judicial actors responsible for investigating and sentencing traffickers are not sufficiently skilled. Second, it is quite difficult to gather sufficient evidence to convict traffickers. Moreover, in the case of transnational trafficking, it is almost impossible to compile the necessary evidence in the countries of origin, transit and destination in the absence of judicial cooperation. It is therefore crucial to advocate for a comprehensive and inclusive management at both the national and international levels to effectively combat trafficking in persons.

Keywords: Human Trafficking, Trafficking in Persons, Transnational organised crime, Migrant Smuggling



1. INTRODUCTION

'Human trafficking' and 'Trafficking in persons' are interchangeable but the United Nations adopted the term 'trafficking in persons' in the Protocol against Trafficking in Persons in 2000. Another term, 'trafficking in human beings' is also used by The Council of Europe in its Convention on Action against Trafficking in Human Beings of 2005. Regardless of the term used, human trafficking is a universal phenomenon that affects nearly every country in the world. These countries are either countries of origin, transit or destination. It is considered as form of modern slavery because it violates human dignity and comprises acts of terror and physical violence against victims. It is not a new phenomenon, as throughout history vulnerable individuals have been exploited by greedy people for economic gain. Slave trade and slavery are typical examples of human trafficking. According to the 2012 Global Report on Trafficking in Persons, victims from at least 136 different nationalities were trafficked and detected in 118 different countries. (UNODC, 2012)

The adoption in 2000 of the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime was a major turning point in the qualification of these acts as a criminal offence. It is the first international text to provide a definition. In fact, the definition in article 3 of the Protocol is the internationally recognized definition of trafficking in persons and is used in the legislation of many countries.

Nowadays, many countries have promulgated a national law criminalizing the acts described in article 3 of the Protocol, as required by article 5 of the Protocol. However, despite the existence of a well-developed legal framework, many people (children, women and men) continue to be trafficked in all parts of the world. The rate of prosecution for this offense is low and in many countries victims may be criminalized while impunity for traffickers prevails.

The description of this situation in the UNODC SHERLOC portal is quite illustrative: « More than a decade after the adoption of the Trafficking in Persons Protocol, most countries have criminalized most forms of human trafficking in their legislation. The 2012 Global Report on Trafficking in Persons shows that, of the 162 countries and territories concerned, only 9 do not have a specific legislation against trafficking in persons. However, the use of these laws to prosecute and convict traffickers remains limited and there is a great need to increase both the capacity and awareness of the law enforcement to better respond to trafficking. In the 2012 Global Report on Trafficking in Persons, for instance, of the 132 countries covered, between 2007 and 2010, 16 per cent did not record a single conviction for trafficking offences and 23 per cent recorded only less than 10 convictions. »¹²

It is therefore appropriate to ask why states are unable to eradicate or significantly reduce cases of trafficking in persons. The studied topic raises the problem of the ineffectiveness of measures taken to combat human trafficking. The central research question that emerges from this problem can be phrased as follows:

Do States have adequate resources to address trafficking in persons?

- Sub-question 1: Are the measures taken to combat trafficking in persons appropriate and sufficient?

- Sub-question 2: What are the obstacles met in combatting trafficking in persons?

¹² The purpose of the UNODC Human Trafficking Case Law Database, sherloc is to broaden the knowledge about human trafficking and to allow criminal justice practitioners to learn from experiences in other jurisdictions.
<https://sherloc.unodc.org/cld/en/about/index.html>

Thus, in order to attract the interest of a wider audience and to allow them to benefit more, the study does not focus on a single country. Rather, it provides a broad overview of the efforts of the various actors involved in the fight against trafficking in persons.

The study of this subject will be based on a documentary collection. It is based on an analysis of qualitative data, collected from information conveyed in training materials and international texts dealing with human trafficking. It is also based on the work done by organizations specialized in fighting against the phenomenon.

The general objective of this study is to evaluate the quality of the response provided by States in the combat against trafficking in persons, in order to make it more effective. Three specific objectives emerge from this study:

- *To determine the difficulties that States face in effectively combating trafficking in persons.*
- *To inventory the actions and mechanisms advocated by specialized international bodies to combat trafficking in persons.*
- *To make recommendations to improve the results obtained by States and the international community in the fight against trafficking in persons.*

The work will be articulated in three parts. The first part will describe the theoretical and conceptual framework of the study, the second part will deal with the methodology used, and the last part will be devoted to the presentation and analysis of the research results.

1.1. THEORITICAL AND CONCEPTUAL FRAMEWORK

The first step will be to focus on the theories already developed on the theme in order to have a better perception of the concepts. Then, an answer will be given to the central research question as well as to the sub-questions.

1.2. LITERATURE REVIEW

The Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime is the first international legal instrument to provide a consensual definition of human trafficking and demonstrates the commitment of the international community to combat this crime. It was adopted by the United Nations General Assembly resolution A/RES/55/25 in 2000. It defines trafficking in persons as follows:

"Trafficking in persons" shall mean the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organs; » (United Nation, 2000)

The same article also states that "The consent of a victim of trafficking in persons to the intended exploitation set forth in subparagraph (a) shall be irrelevant where any of the means set forth in subparagraph (a) have been used. In addition, "the recruitment, transportation, transfer, harbouring or receipt of a child for the purpose of exploitation shall be considered 'trafficking in persons' even if it does not involve any of the means set forth in subparagraph (a)" and the term "child" refers to "any person under the age of 18 years".

In legal terms, trafficking in Person should be composed of three elements:



- The action (recruitment, transportation, transfer, accommodation or reception)
- The means used (use of force, threat of force, coercion, abduction, fraud, deception, abuse of authority or of a position of vulnerability, offering or accepting benefits)
- The purpose of the exploitation (prostitution of others or other forms of sexual exploitation, forced labor or services, slavery or practices similar to slavery, servitude, organ removal).

The issue of consent in the crime of trafficking in persons deserves special attention because of its complexity. As stated in article 3 (b) of the Trafficking in Persons Protocol, consent cannot exempt a person from criminal liability if it is established that deception, coercion, force or other prohibited means were used. For trafficking cases involving children, the Protocol provides that the offence is constituted even if the means mentioned above were not used. In the case of adults, consent is nullified by the use of improper means, and in the case of children, their vulnerable situation deprives them of the capacity to give consent. (UNODC, 2009)

It should be noted that since trafficking is basically the exploitation of the vulnerability of others, certain factors can increase the risk of exploitation by traffickers. These include gender (women), age (children) and lack of proper travel documents. Women and children are particularly vulnerable to trafficking. The 2018 Global Report on Trafficking in Persons also highlights the particular vulnerability of people living in or fleeing conflict zones. These people may be trafficked within their country of origin or internationally for purposes such as forced labor, sexual exploitation, forced marriage, organ removal, and so on. Their traffickers are either members of sophisticated criminal networks or minor local offenders who operate on their own behalf.

Currently, with the development of globalization 4.0, organized crime networks as well as petty criminals are using the Internet and social media to attract more vulnerable people. The use of the Internet and social networks allows traffickers to increase their scope of action with minimal risk. Recognizing the fundamental role that information technology plays in the commission of the crime of trafficking in persons, the United Nations Office on Drugs and Crime (UNODC) has dedicated a chapter in its Global Report on Trafficking in Persons 2020 entitled 'traffickers use of the internet'. According to the report, the Internet can be used by traffickers to recruit future victims, advertise, or exploit individuals.

In this regard, addressing these three points, the report mentions: Talking about recruitment, « traffickers easily gain access to an increased pool of customers through the internet. Recruitment practices are widely reported upon, when it comes to both sexual exploitation and forced labour. » As for advertisement, « Traffickers increasingly use internet technologies to advertise the services resulting from their victims' exploitation and examples of advertisements used to exploit victims include those on classified listing sites, such as Backpage and similar, or on social media platforms and applications. ». As far as exploitation is concerned, « the internet can be used to broadcast or livestream acts of exploitation, reaching a large base of consumers in different locations throughout different regions of the world; or even be used to traffic victims to exploit them into the commission of crime. » UNODC

These days, many international organizations are committed to finding solutions to human trafficking. The United Nations is at the forefront of these efforts. As early as 2000, the United Nations General Assembly adopted the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, to supplement the United Nations Convention against Transnational Organized Crime. This Protocol, demonstrates the commitment of the international community to combat this crime.

In addition, UNODC, which is an agency of the United Nations Secretariat, is very active in the area of combating trafficking in persons. From 2006 to now, it has produced five global reports on the results of investigations in this field.

Furthermore, the Council of Europe is also active in the fight against human trafficking. On May 16, 2005, it adopted the Council of Europe Convention on Action against Trafficking in Human Beings. This convention puts the victim at the heart of the fight against trafficking in human beings, as it focuses on the protection of victims. Also, to ensure the follow-up and proper application of this legal instrument, a treaty body called the Group of Experts on Action against Trafficking in Human Beings (GRETA) has been created. (Council of Europe, 2022)

Like the Council of Europe, the Organization for Economic Cooperation and Development (OSCE) also takes a human rights-based approach to protecting victims. In 2003, it established the Office and post of the Special Representative and Coordinator for Combating Trafficking in Human Beings to assist participating States in developing and implementing effective anti-trafficking policies.

1.3. CONCEPTUAL FRAMEWORK

Human Trafficking often has elements in common with several other offences such as kidnapping, assault, fraud, immigration and labour offences, etc. It is a serious criminal conduct whose specific determination in the legislation avoids any gap that could lead to impunity of the perpetrators.

1.3.1. DIFFERENCES BETWEEN HUMAN TRAFFICKING AND MIGRANT SMUGGLING

Human trafficking and migrant smuggling are closely related, as the profile of the victims and the causes behind the two crimes are often the same. In both cases, victims are trying to escape from war, persecution, violence, poverty, in search of better opportunities or are deceived by promises of better jobs and wages.

However, a distinction must be made between the two, as the final objective of the traffickers differs. In the case of migrant smuggling, the smugglers limit themselves to a contract to convoy their clients to the final destination in exchange for a pre-defined sum. In the end, although migrants may become victims of human trafficking, generally the smuggler ceases all relations with the migrant once he has been paid. Also, human

trafficking can take place both inside and outside a country's borders, whereas migrant smuggling involves crossing international borders.

According to article 3 of the protocol against the smuggling of migrants by land, sea and air, supplementing the United Nations convention against transnational organized crime smuggling of migrants is defined as follows: 'the procurement, in order to obtain, directly or indirectly, a financial or other material benefit, of the illegal entry of a person into a State Party of which the person is not a national or a permanent resident'. (United Nations, 2000)

In human trafficking, the perpetrators seek to create a lasting dependency on their victims. They use a variety of strategies to exploit their victims for as long as possible, with maximum profit. They may use illegal immigration routes to transport their victims from one country to another.

Speaking of the fight against trafficking in persons, despite all the efforts made by States to put an end to this scourge, the number of trafficked persons continues to rise. Some may wonder if States have the necessary resources to fight effectively against human trafficking.



2. MATERIALS AND METHODS

This study is based on a SWOT analysis (Strengths - Weaknesses - Opportunities - Threats) which is a strategic diagnostic tool. It allowed us to identify the internal factors, i.e. the strengths and weaknesses of States in the fight against human trafficking, then to draw up the external factors such as the threats to which States are exposed before detecting the opportunities that they could seize to fight effectively against human trafficking. This approach has led us to formulate strategies that could bring a clear improvement in the results of the fight against this phenomenon.

The research methodology used is documentary collection. It is based on an analysis of qualitative data, collected from the reading of documents dealing with the subject on the Internet. The choice of documents used mainly focused on the work and training materials of international organizations active in the fight against trafficking in persons.

However, it was not easy to accurately describe the positive actions taken by states in the fight against trafficking in persons. This is due to the fact that in the documents consulted, the focus is much more on the shortcomings that states need to correct in order to significantly reduce cases of trafficking in persons.

3. RESULTS

The first step will be to present the results of the documentary research in a SWOT table and then analyze them to bring an answer to the aforementioned research questions.

3.1. PRESENTATION OF THE DATA

From the study carried out, the following results were obtained:

Table 16. SWOT analysis | Human Trafficking

Internal factors	Strengths (S)	Weaknesses (W)
	<ul style="list-style-type: none"> • Establishment of a legal framework to criminalize human trafficking through the integration of the offence in the penal code • Membership in organizations specialized in the fight against human trafficking • Awareness of the seriousness of the phenomenon 	<ul style="list-style-type: none"> • Low prosecution and conviction rates • Failure in early detection of potential signs of human trafficking • Lack of preventive actions • Lack of care for victims, including protection and assistance to avoid further exploitation or double victimization • Difficulty in gathering tangible evidence, especially in cases of transnational trafficking • Lack of expertise and understanding on the global stage by justice actors
<p data-bbox="146 875 579 913">External factors</p> <p data-bbox="146 913 579 952">Opportunities (O)</p> <ul style="list-style-type: none"> • Collaboration with international organizations that are active in the fight against human trafficking in the framework of training and the development of mechanisms to combat it • Mutual legal assistance between countries of origin, transit and destination to incriminate the perpetrators • of trafficking • Exchange of information to enable the dismantling of trafficking networks with a view to their conviction • Partnership with NGOs, civil society and media • Cooperation with INTERPOL in the investigation of transnational trafficking 	<ul style="list-style-type: none"> • To raise awareness of the offence of trafficking in persons among judicial actors to enable them to detect the indicators necessary to qualify exploitation as trafficking in persons • To organize information and awareness campaigns in partnership with all stakeholders • Exchange of information to enable the dismantling of trafficking networks with a view to their conviction • Partnership with NGOs, civil society and media • Cooperation with INTERPOL in the investigation of transnational trafficking 	<ul style="list-style-type: none"> • To rely on international organizations to increase both the capacity and awareness of the law enforcement to better respond to trafficking • To foster judicial cooperation between countries of origin and destination to gather as much evidence as possible that can lead to the conviction of traffickers. • Take advantage of opportunities such as World Anti-Trafficking Day to raise awareness of the extent of human trafficking and the need to report any indicators of it • Reduce the vulnerability of individuals who may be trafficked by helping them find ways to meet their basic needs.
<p data-bbox="146 1525 579 1563">Threats (T)</p> <ul style="list-style-type: none"> • Reluctance of victims to cooperate with investigations for fear of retaliation. • Reconversion of victims into traffickers due to lack of follow-up and assistance • Amplification of the phenomenon with the use of the Internet and social networks • Growing poverty and armed conflicts 	<ul style="list-style-type: none"> • To inform victims of their right to file complaints against their perpetrators and to be assisted by the courts. • To encourage victims to cooperate with investigators and to testify at trials by providing them with the necessary protection. 	<ul style="list-style-type: none"> • To adopt an approach focused on the protection and assistance of victims in the fight against human trafficking. • To raise awareness of people about the modus operandi of traffickers on the Internet and social networks so that they can be more vigilant. • To develop social support programs for individuals living in poverty or in conflict zones to make them less vulnerable to trafficking.

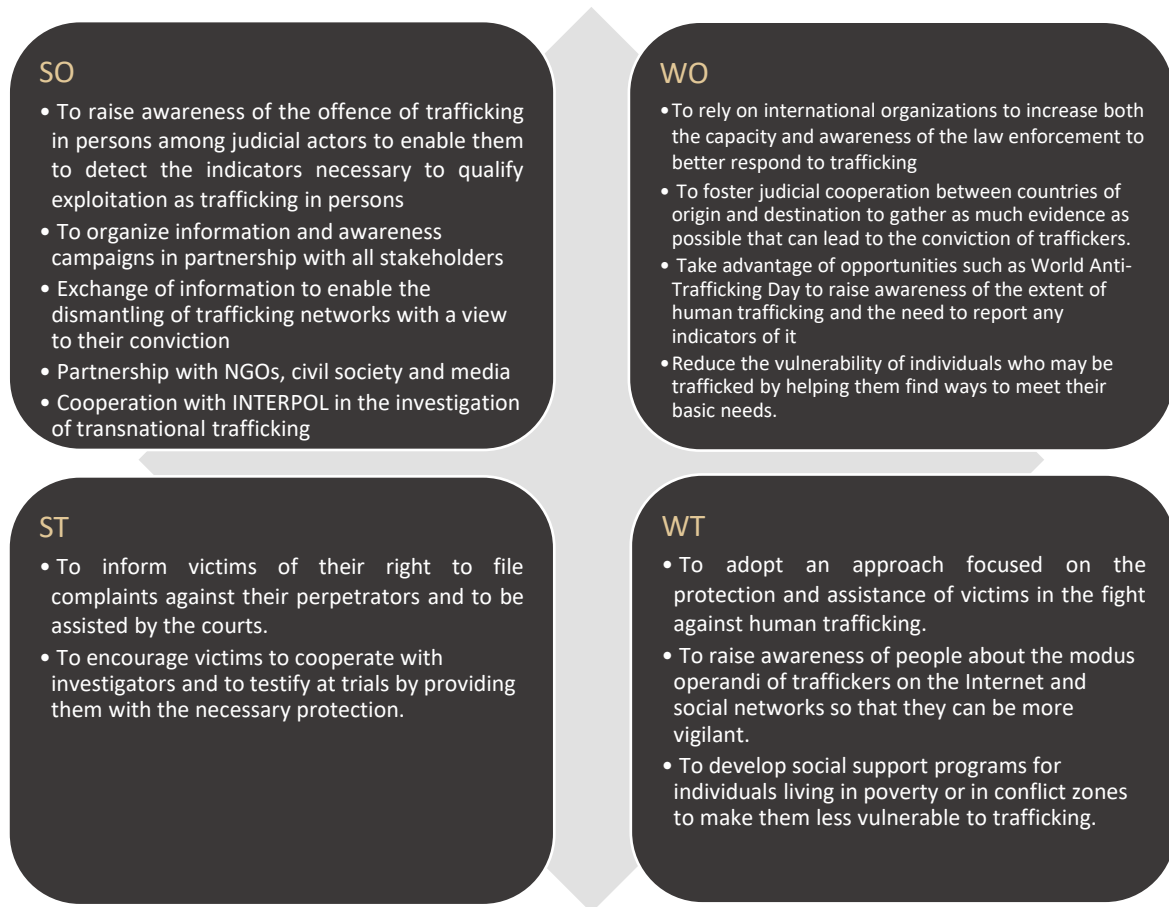


Figure 16. Key strategies | Human Trafficking

4. DISCUSSION

Since the adoption of the Additional Protocol on Trafficking in Persons, states have demonstrated their willingness to fight this heinous crime. Although many of them have taken measures in their national legislation to criminalize this offence, the number of persons convicted for this offence remains low. This situation is mainly due to the lack of experience of the justice actors in this field and the difficulty to gather the necessary evidence.

First, some police officers are not sufficiently aware of the reality of human trafficking and are not trained to identify victims when they file a complaint. This implies that the qualification of trafficking has little chance of being retained by the prosecutor's office. The subjacent offenses are thus likely to be targeted.

Second, the evidence available to the courts is often not strong enough to allow judges to make a case for trafficking in persons. This evidence is often limited to the testimony of victims. The difficulty of gathering tangible evidence is all the more noticeable in cases of transnational trafficking where several countries are involved. These countries, which may be places of departure, transit or destination, may have different laws on trafficking in persons. (MOËL, 2022)

In addition, the police need the cooperation of victims and witnesses to be able to act effectively against traffickers and hold them accountable. However, the trauma they have suffered often makes it impossible for victims to endure lengthy legal proceedings, or they fear retaliation against themselves or their relatives. This

fear even leads some victims not to attend trials, even though their testimony is crucial in the eyes of sentencing judges.

Also, the financial and material means necessary for the protection and assistance of victims are often lacking. Today, even if the authorities are beginning to realize that taking care of victims is of vital importance in the fight against trafficking in persons, many actions still need to be taken to protect them from new forms of exploitation or re-victimization.

In the face of all these shortcomings mentioned above, the actions taken by states to combat human trafficking remain ineffective. It is therefore advisable to develop new strategies to improve the response of States to eradicate the scourge. In this token, it is vital to adopt a global and international approach in the countries of origin, transit and destination, including measures of prevention, repression, but also protection and assistance to the victims; that is to say, the involvement of all the actors having a role to play in the fight against the scourge, such as governmental actors (ministries, magistrates, police services, etc.), and non-governmental actors (civil society, media, NGOs, community leaders, social workers, etc.). This assertion from the Global Report on Trafficking in Persons 2016 provides ample support for this idea. « We must, however, continue to generate much needed cooperation and collaboration at the international level, and the necessary law enforcement skills at the national and regional levels to detect, investigate and successfully prosecute cases of trafficking in persons. (UNODC, 2016)

5. CONCLUSIONS & RECOMMENDATIONS

Trafficking in human beings, sometimes referred to as a form of modern slavery, is a serious violation of people's fundamental rights. It is an ancient phenomenon, as the exploitation of man by his fellow man for economic purposes has existed for centuries. However, the qualification of the facts of exploitation of a person into an offence called trafficking in persons came with the adoption, in 2000, of the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime. It provided the first internationally recognized definition of trafficking in persons and requires states parties to enact national laws criminalizing the crime. Today, like the United Nations bodies such as the UNODC, many other international or regional organizations are active in the fight against the phenomenon. However, despite all the efforts made by States and these organizations, many people continue to be victims of trafficking throughout the world.

The study used the SWOT (Strengths-Weaknesses-Opportunities-Threats) strategic diagnostic tool to identify internal factors, such as strengths and weaknesses, and external factors, namely threats and opportunities. It is based on an analysis of qualitative data collected from the work and training materials of international organizations active in the fight against human trafficking.

The research results identified a series of obstacles that make state actions to combat trafficking in persons ineffective. Moreover, despite a well-provided legal framework, the number of prosecutions and convictions remains low. This situation can be explained by the fact that certain actors in the justice system, namely judges and police officers, are not sufficiently aware of the best practices for dealing with human trafficking cases. Secondly, there is a notorious difficulty in gathering sufficient evidence to justify the conviction of perpetrators, especially when it comes to transnational trafficking. This evidence is often limited to the testimony of the victims, while the latter sometimes refuse to denounce their torturers for fear of reprisals. Moreover, in the absence of judicial cooperation between countries of origin, transit and destination, it is almost impossible to compile the necessary evidence for the courts.



Consequently, it becomes judicious to develop new strategies of struggle to improve the response brought by States to combat the scourge. It is more than ever necessary to adopt a global and inclusive approach at both national and international levels. All the actions recommended by international organizations in each stage of the fight against human trafficking must be taken into account in the strategies to combat the phenomenon. Those strategies must imperatively include prevention measures, international cooperation mechanisms for prosecution and repression, and means of protection and assistance for victims. Moreover, beyond States that must multiply their efforts to fight human trafficking, everyone must feel concerned. A simple denunciation could save people from this villainous crime.

Based on the results of the study, the following strategies could be adopted:

For (SO-Growth)

- *To raise awareness of the offence of trafficking in persons among judicial actors to enable them to detect the indicators necessary to qualify exploitation as trafficking in persons.*
- *To organize information and awareness campaigns in partnership with all stakeholders.*

Concerning (WO-Targeting)

- *To rely on international organizations to increase both the capacity and awareness of the law enforcement to better respond to trafficking.*
- *To foster judicial cooperation between countries of origin and destination to gather as much evidence as possible that can lead to the conviction of traffickers.*
- *Take advantage of opportunities such as World Anti-Trafficking Day to raise awareness of the extent of human trafficking and the need to report any indicators of it.*

As for (ST-Diversify)

- *To inform victims of their right to file complaints against their perpetrators and to be assisted by the courts.*
- *To encourage victims to cooperate with investigators and to testify at trials by providing them with the necessary protection.*

And For (WT Defence)

- *To adopt an approach focused on the protection and assistance of victims in the fight against human trafficking.*
 - *To raise awareness of people about the modus operandi of traffickers on the Internet and social networks so that they can be more vigilant.*
- *To develop social support programs for individuals living in poverty or in conflict zones to make them less vulnerable to trafficking.*

REFERENCES

- Council of Europe. (2022, javier 25). action Against Trafficking in Human Beings. Retrieved from <https://www.coe.int/en/web/anti-human-trafficking>
- Dealtry, R. (1994). Dynamic SWOT Analysis - Developer's Guide. Birmingham.
- Édes, B. (2021). Resetting Our Future: Learning from Tomorrow: Using Strategic Foresight to Prepare for the Next Big Disruption. Winchester: John Hunt Publishing.
- EUROPOL. (2021). EU Serious and Organised Crime Threat Assessment (SOCTA) 2021. European Union Agency for Law Enforcement Cooperation. Luxembourg: Publications Office of the European Union. doi:10.2813/346806
- EUROPOL. (2021). Internet Organised Crime Threat Assessment (IOCTA) 2021. European Union Agency for Law Enforcement Cooperation. Luxembourg: Publications Office of the European Union. doi:10.2813/113799
- IMF. (2021). International Monetary Fund - Guidance Notes: How to Implement Strategic Foresight (and Why). Washington, DC: International Monetary Fund. Retrieved from <https://www.imf.org/en/Publications/analytical-notes/Issues/2021/12/22/Strategic-Foresight-at-the-International-Monetary-Fund-463660>
- INTERPOL-UN. (2016). Strategic Report: Environment, Peace and Security – A Convergence of Threats. INTERPOL & UN, International Criminal Police Organization (ICPO) – INTERPOL and UN Environment, Lyon. Retrieved from <https://www.interpol.int/content/download/5088/file/INTERPOL-UNEP%20Strategic%20Report%20-%20Environment,%20Peace%20and%20Security%20-%20A%20Convergence%20of%20Threats.pdf>
- Kurttilaa, e. a. (2000). Utilizing the Analytical Hierarchy Process AHP in SWOT Analysis—A Hybrid Method and its application to a forest-certification case. Forest Policy and Economics.
- MOËL, C. L. (2022, février 15). Retrieved from la qualification juridique de l'infraction de traite: <http://contrelatraitte.org/node/383>
- NATO. (2020). NATO - Relations with the European Union. Retrieved from https://www.nato.int/cps/en/natohq/topics_49217.htm
- ODERA, T. M., & MALINOWSKI, R. (2011). Guidelines for Assisting Victims of Human Trafficking in the East Africa Region. Geneva: OIM.
- OECD. (2020). Government Foresight Community - Annual Meeting Report 2020 - Strategic foresight for future-ready public policy. OECD.
- OECD. (2022, 01 08). OECD.org. Retrieved from Organisation for Economic Co-operation and Development: <https://www.oecd.org/strategic-foresight/>
- United Nation. (2000). Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, supplementing the United Nations Convention against Transnational Organized Crime. New York: United Nations publication.
- United Nations. (2000). PROTOCOL AGAINST THE SMUGGLING OF MIGRANTS BY LAND, SEA AND AIR, SUPPLEMENTING THE UNITED NATIONS CONVENTION AGAINST TRANSNATIONAL ORGANIZED CRIME. New York: United Nations Publications.
- UNODC. (2008). Toolkit to Combat Trafficking in Persons. New York: United Nation Publications, sale N° E.08.V.14.



- UNODC. (2009). Anti-Human Trafficking Manual for Crimonal Justice Practitioners . New York: United Nations Publication.
- UNODC. (2012). Global Report on Trafficking in Persons. New york: United Nations publications.
- UNODC. (2016). Global Report on Trafficking in Persons . New York: United Nations Publication.
- Wang, X., Zhang, J., & Yang, T. (n.d.). Hybrid SWOT Approach for Strategic Planning and Formulation in China Worldwide Express Mail Service. Journal of Applied Research and Technology, pp. pp. 230-238. doi:10.1016/S1665-6423(14)72339-9
- World Economic Forum. (2022). The Global Risks Report 2022 - 17th Edition. WEF. World Economic Forum. Retrieved from https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf

X. PAPER | TERRORISM

Citation:

Souidi, S.; Terrorism. Overcoming Security Threats arising from Globalization 4.0 – FIEP Association, 2022.

Published: October 2022

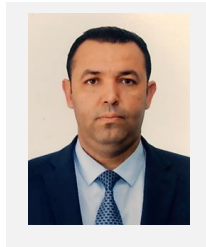
Publisher's Note: FIEP stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors.

Tunisia

Saber Souidi



saber_gn@hotmail.com;

dir.antiterrorism@interieur.gov.tn

Abstract: The aim of this paper is to tackle the phenomenon of terrorism as a violent movement of extremism, which witnessed a great development over time in different manifestations and contexts posing a threat in all parts of the world. A phenomenon that has always been a problem for all countries and governments due to the serious effects and repercussions results from and the impairments that leaves behind. Its elimination has become the obsession of all countries, as a matter of effect consolidation of efforts on the international level have become necessary to combat it and to find appropriate strategies, solutions and best practices to eradicate it, dry up its sources and eliminate the causes that paves the way for the spread of this Tumors within societies.

Keywords: Terrorism, home and global grown phenomenon, radicalization, Islamic groups, takfiri



1. INTRODUCTION

In the past, terrorist organizations included small groups moving through narrow geographical areas dominated by the harshness of nature and difficult to track in them, which usually thrive in areas of armed conflicts or in countries characterized by security, political and social instability and deteriorating economic conditions, taken as training camps (mountains in Afghanistan, Pakistan, Sudan, Yemen, Iraq, Algeria, Somalia and the coastal and desert African countries...), starting from these places extremists carry out specific operations (by executing armed attacks, bombing and simultaneous suicide attacks), using traditional means in a relatively slow pace, due to its reliance on simple and primitive mechanisms of communication. Among them, for polarization and recruitment.

On September 11, 2001, a terrorist attack on the World Trade Center in New York after two planes were hijacked executed by al-Qaeda affiliates, killing thousands of civilians, and reported by various international media outlets, constituted a qualitative leap in the war against terrorism and the joining of many extremists to the mentioned group after the contribution of this operation to the process of introducing its leaders on a larger scale. Where the impact of the phenomenon in our country during that period was limited to recording dozens of extremist elements joining the “global jihad camps” in response to the call of mobilization launched by these organizations, led by “Al-Qaeda” since its founding in 1988, and to depart from the regimes that practice a strict deterrent policy against extremism in order to receive military and combat experience. In the same context, we recorded many recruitments of Tunisian elements from countries abroad (Middle East and the European Union) involved in terrorist cells abroad. Internally, we discovered some takfiri cells that adopted al-Qaeda ideology of at the time, sought to destabilize and change the regime, and some of their remnants succeeded in carrying out some isolated and scattered operations, but they were not of great resonance and their leaders failed to attract youth due to the strict policies adopted by Tunisia during that period.

However, after 2011 and the passing of many Arab countries with major political, social and economic shocks (popular uprisings) that contributed to the deterioration of the security situation, passing through a transitional phase characterized by instability, including Tunisia, which represented an opportunity for extremists to restructure and reorganize themselves, especially after many of its leaders enjoyed a general legislative amnesty and released from prisons, in small pace of time they succeeded to control the minds of a significant number of young people by adopting direct communication (organizing advocacy tents, lessons in mosques, distributing leaflets, forums, Quranic schools and charities...) And indirectly (through media platforms specialized in propaganda and recruitment), which was embodied on the ground by the announcement of a new terrorist organization (in Syria and Iraq) after its leader, “Abu Bakr al-Baghdadi” announced the establishment of what he called a “caliphate state” from the Mosul Mosque in Iraq (in 2014). Which became the first destination for terrorists and formed the largest gathering of extremists in the world, including thousands of Tunisian takfiri elements joined its affiliates, in light of the ascension of parties with a religious background to power in the region, which adopted a policy of “tolerant of manifestations of extremism in society.” turned a blind eye to the influx of extremist preachers to our country, whose sermons contributed to influencing youth to adopt an extremist ideology.

During the last decade, our country witnessed a wide spread of takfiri and extremist ideology, which made us enter a new phase in the conflict with the phenomenon, especially after the outbreak of the situation in the Syrian and Libyan countries (lack of control over the borders, a large spread of weapons and explosives, ease of movement of fighters, and the combination of smuggling and terrorism).

This prompted us to take and activate new measures at the legislative, judicial and security levels to address the phenomenon. It made us move quickly from the stage of reaction to the stage of anticipation, in which we achieved great success in the war against terrorism. However, the security approach alone remains unable to

eradicate and abort the phenomenon and break the path of extremism within Society, which prompted us to think about updating the national strategy adopted to combat terrorism to keep pace with the new crimes and threats, by the need to create a vision to neutralize the dangerous elements, especially those that return from the hotbeds of tension, starting from inside the prison and seeking to establish an electronic monitoring system to limit their movements and seeking to activate an exemplary disengagement program Oriented these groups and to prepare a practical vision of the reintegration system along with comparative experiences in the field.

In this regard and through this overview We want to shed light on a historical background of the phenomenon and questions the reasons behind the development of terrorist activities and the approach adopted by the Tunisian government in the field of combating terrorism, and to present effective visions and solutions to address the phenomenon in light of future challenges.

The central research thesis emerges from the phenomenon which will be answered later on can be phrased as follows: *“what is the tunisian approach to fight against radicalism in terms of multidimensional remedy of the phenomenon?”*

1.1. THEORITICAL AND CONCEPTUAL FRAMEWORK

1.1.1. LITERATURE REVIEW: LOCAL DIAGNOSIS

The first step will be to focus on the theories already developed on the theme in order to have a better perception of the concepts. Then, an answer will be given to the central research question as well as to the sub-questions.

1.1.2. PRIOR TO 2011:

Tunisia witnessed, before 2011, a number of terrorist operations such as the ones that targeted the border post in Sundus in 1995 and the Ghariba Synagogue in Djerba in 2002 in addition to the terrorist incidents in Ain Tabarang, Slimane in 2006. The aforementioned incidents were undoubtedly critical and posed direct threat to social stability and cohesion. Furthermore, this threat predominantly targeted and affected the security and military institutions. However, these incidents were, in fact, isolated in place and time, for terrorism—as a nascent phenomenon back then—was marked by poor and slow-paced planning for two principal reasons. Firstly, terrorist organizations abroad were unable to attract and recruit elements inside the Tunisian soil with the exception of few clumsy attempts. Secondly, Tunisia’s strict security policy in the counterterrorism realm back then rendered domestic extremist elements’ activities crippled. As a result, some of them ended up joining tensions hotbeds overseas during that period (Afghanistan, Iraq, Sudan, Mali...).

1.1.3. AFTER 2011:

In the aftermath of the January 2011 events, Tunisia’s security situation became gravely deteriorated. The country underwent multiple turbulences on different levels that set the ground for the proliferation of terrorism.

1.2. ANALYSIS MODEL

1.2.1. CONCEPTUAL FRAMEWORK

1.2.1.1. IDEOLOGICAL FACTORS:

Circulation of revolutionary ideas especially in universities, infatuation with Arab-Islamic causes and that the collapse of tyrannical regimes is considered as a divine sign to the re-establishment of the caliphate state, rise of racism and islamophobia in economic immigration countries, radical Islamism in Tunisia has not been tarnished by civil war like what happened in Algeria.



1.2.1.2. SOCIO-CULTURAL FACTORS:

Loss of family and community solidarity and search for alternative relationships, loss of paternal authority within household, desire to discover a new identity that provides a dashed hope for better social status.

1.2.1.3. SOCIO-ECONOMIC FACTORS:

Search for better social status, economic and social marginalisation of youth, increase of unemployment due to the unstable situation locally and in neighbouring countries such as Libya which was considered as the first economic immigration destination for Tunisian youth.

1.2.1.4. INDIVIDUAL PERCEPTION:

Feelings of relative frustration and dashed revolutionary hopes, feelings of injustice and humiliation, lack of confidence towards public institutions (Schools, Universities, Organisations, Political Parties, Civil Society) which created a vacuum that has been exploited by the takfiri groups to act as the desired alternative.

1.2.1.5. RELIGIOUS FACTORS:

Use of religious space as a platform to spread takfiri ideology especially in working-class and impoverished areas, failure of supervising authority back then in drawing up a strategy to spread moderate religious ideology in order to educate and immunize the society from being drawn into takfiri ideology.

1.2.1.6. SITUATIONAL FACTORS:

Political parties with religious background on the head of state facilitated the release of many takfiri and extremist elements as they benefited from a general amnesty and whom previously were involved in terrorist cases, ease of access to funding sources, increase of advocacy tents to entice and recruit the largest possible number of youngsters who were easily persuaded through direct encounters or through promoting extremist-oriented curricula across virtual platforms, organised networks for recruitment to join tension hotbeds overseas, head in the sand policy by head of the state back then in relation to recruiting, funding and promoting extremist-oriented curricula.

Amid this climate and in the beginning of 2012, extremist elements managed to take control of mosques, particularly in working-class and impoverished areas. They additionally managed to establish associations with a seemingly charitable and advocacy dimension, which was nothing but a camouflaged front to finance takfiri groups' activities. At a later stage, extremist elements became active within the framework of clearly defined and structured organizations (advocacy wing, media wing, security wing and military wing), thus adopting a Modus Operandi similar to the terrorist organization Ansar al-Sharia (affiliated with Al-Qaeda in the Islamic Maghreb). Furthermore, we witnessed the emergence of the so-called "Islamic State in Iraq and the Levant" the extremist ideology of which did spread at a dizzying speed, particularly after the crisis in Libya, Syria and Iraq dramatically deepened. The result landscape constituted an arena for international terrorism comprising the largest number of terrorist elements throughout history.

Some of ISIL supporters/sympathizers managed to go to the aforementioned countries where they received training courses in shooting, booby-traps and the manufacture of explosives. They were additionally able to smuggle weapons and explosive materials to our country (some of them were deceased there whereas some returned to Tunisia).

1.2.1.7. THE TUNISIAN COUNTER-TERRORISM APPROACH:

In reference to the above-mentioned points, and in light of the heightened threat of terrorist attacks, we ensured—at the level of the Counter-Terrorism Department of the National Guard General Directorate—to keep ourselves abreast of the rapidly evolving developments that posed great challenges that almost ravaged the stability of the State. In essence, we swiftly shifted our paradigm from merely reacting to specific operations targeting security headquarters, military units, sensitive facilities, civilians and foreigners (this was the stage of curbing terrorist attacks) to the stage of carrying out pre-emptive intelligence-led operations that enabled us, for instance, to dismantle the Ansar al-Sharia organization (banned since 2013). Our new approach additionally enabled us to identify ISIS terrorist affiliates who were active in sleeper cells, thwart their plans, arrest and eliminate most of their leaders, uncover radicalization cells and prevent extremist elements from joining the hotbeds of tension overseas. Furthermore, we managed to seize many weapons and explosives that were brought through the smuggling routes into our country.

2. MATERIALS AND METHODS

This research papers derived its importance from using two scientific paradigms diagnosis to analyze issues, tackle targetes, and to open new horizons as well as to seize new openings. For instance, we used the PESTEL model and the SWOT (Strengths - Weaknesses - Opportunities - Threats) analysis paradigm, these two tools helps better understanding and to identify sources of vulnerability to to fight against the phenomenon of terrorism that hampers the Nation wide starting from the narrow example of Tunisa.



3. RESULTS

3.1. PRESENTATION OF DATA AND DISCUSSIONS OF THE RESULTS: PESTEL AND SWOT ANALYSIS

Table 17. PESTEL analysis | Terrorism

Factors	Key Macro Trends	Implications for Security Forces
Political & Legal	<p>P.1. dominant position of political instability as a determinant of terrorist activity</p> <p>P.2. lack of citizen satisfaction, electoral participation, and political efficacy.</p> <p>P.3. government ineffectiveness has a major negative impact of the dynamics of terrorist activities.</p> <p>P.4. Political instability.</p> <p>P.5. War and violent conflic.</p> <p>P.6. States engaged in democratic transition rather than democratic or authoritarian regimes.</p> <p>P.7. A lack of political legitimacy and continuity, as well as a lack of integration for the political fringes.</p>	<ol style="list-style-type: none"> 1. Levels of transnational terrorism are highest in semi-authoritarian states. 2. Increased threats on critical infrastructures, needing to spend more resources in their defence. 3. Democratic governments can reduce the number of terrorist incidents.
Economic	<p>E.1. economic change translates into higher terrorist activity</p> <p>E.2. economic success exerts no independent effect of on terrorist attacks.</p> <p>E.3. Unemployment in general is a highly statistically significant predictor of terrorism.</p> <p>E.4. The rise of prices is an indicator of positive correlation between inflation and terrorist activities.</p> <p>E.5. the quality of public services, the quality of the civil services and the degree of its independence from political pressure, the quality of policy formulation and implementation, and the credibility of the government's commitment to such policies.</p> <p>E.6. Poor societies with weak state structures.</p>	<ol style="list-style-type: none"> 1. Terrorism increases when these factors are combined together, the developing countries are an innate model for this. 2. Tensions and turmoil in the middle east, in States like syria, Irak and Yemen are good examples of the phenomena.
Social	<p>S.1. Social inequality is expressed by measures the extent to which countries provide for the social and environmental needs of their citizens.</p> <p>S.2. Level of citizen's education is the most effective factor in the formation of attitude, effects the attitudes and religious beliefs.</p> <p>S.3. Correlation between terrorist threat and unemployment is described and explained in many cases all over the world.</p> <p>S.4. A higher proportion of unmarried males increases the association with intra-societal violence and instability.</p> <p>S.5. Perceptions of deprivation and inequality.</p>	<ol style="list-style-type: none"> 1. Political and criminally motivated violence is largely or more likely the work by illiterate as well as by well educated youngsters and adults
Technological	<p>T.1. Terrorism in one country can spillover into neighbouring areas through the use of new forms and platforms of communications.</p> <p>T.2. Mass media can influence the patterns of terrorism by enhancing agenda setting, increasing lethality and expanding the transnational character</p> <p>T.3. Digital and technological tools use by terrorists.</p>	<ol style="list-style-type: none"> 1. Mass media can influence the patterns of terrorism by enhancing agenda setting, increasing lethality and expanding the transnational character.

Envi	EN.1. Weak and collapsed states that contribute to international terrorism.	1. Ongoing or past wars can have terrorism motivations rooted within. Armed conflicts also have facilitating influences on transnational terrorism.
	EN.2. Undergoing societal changes brought through modernisation.	2. Creating the conditions for terrorism through mobility, communication, widespread targets

3.2. SWOT ANALYSIS

Table 18. SWOT analysis | Terrorism

Internal factors	Strengths (S)	Weaknesses (W)
External factors		
Opportunities (O)	<ul style="list-style-type: none"> • Commitment of security forces to fight against the phenomenon. Local and international opinion are in support for eradicating terrorism. • Exchange of expertise between countries, unifying the efforts against this wave of violence that hampers the existence of democracy and the status quo in all countries. • International agencies, security and military forces with judicial authorities, are working under the umbrella of respecting the fundamental principles and basics of the international human rights. 	<ul style="list-style-type: none"> • These Islamic groups all over the countries need to be studied by immersing inside them as they grow. • Radicalists are creating new networks to attract more followers. • They develop their capacities in parallel to the existing measures.
Threats (T)	<ul style="list-style-type: none"> • Improve capacity building of our units in terms of training exchange of expertise with international partners. • Encourage experts in the field to conduct studies about the phenomenon of terrorism. 	<ul style="list-style-type: none"> • Raise budgets for counter terrorism departments/ increase their level of readiness in terms of equipping operational units.
	<ul style="list-style-type: none"> • Cooperate with other forces and agencies /on the international level. • Seek the best possible remedies for the issue taking into consideration the shared experiences. 	<ul style="list-style-type: none"> • Raise awareness about the impacts and the collateral damages of terrorism. • Increasing security measures and plans to combat this phenomenon.
	<ul style="list-style-type: none"> • As states started to invest in security solutions, law enforcement resources are being gradually increased and enhanced. • Raising public awareness and educate those who are attracted to their ideas. • Collaboration with international organizations can help to unify and aim the efforts. 	
	<ul style="list-style-type: none"> • The attacks are increasing because of political instability in some countries. • Coordinations between groups are transpassing borders • Despite efforts on the central levels. • Their objective is to establish an Islamic state in one country then expand their influence across nations and poison the world with their retro ideas. • Followers are both well • Educated and illiterate people. 	

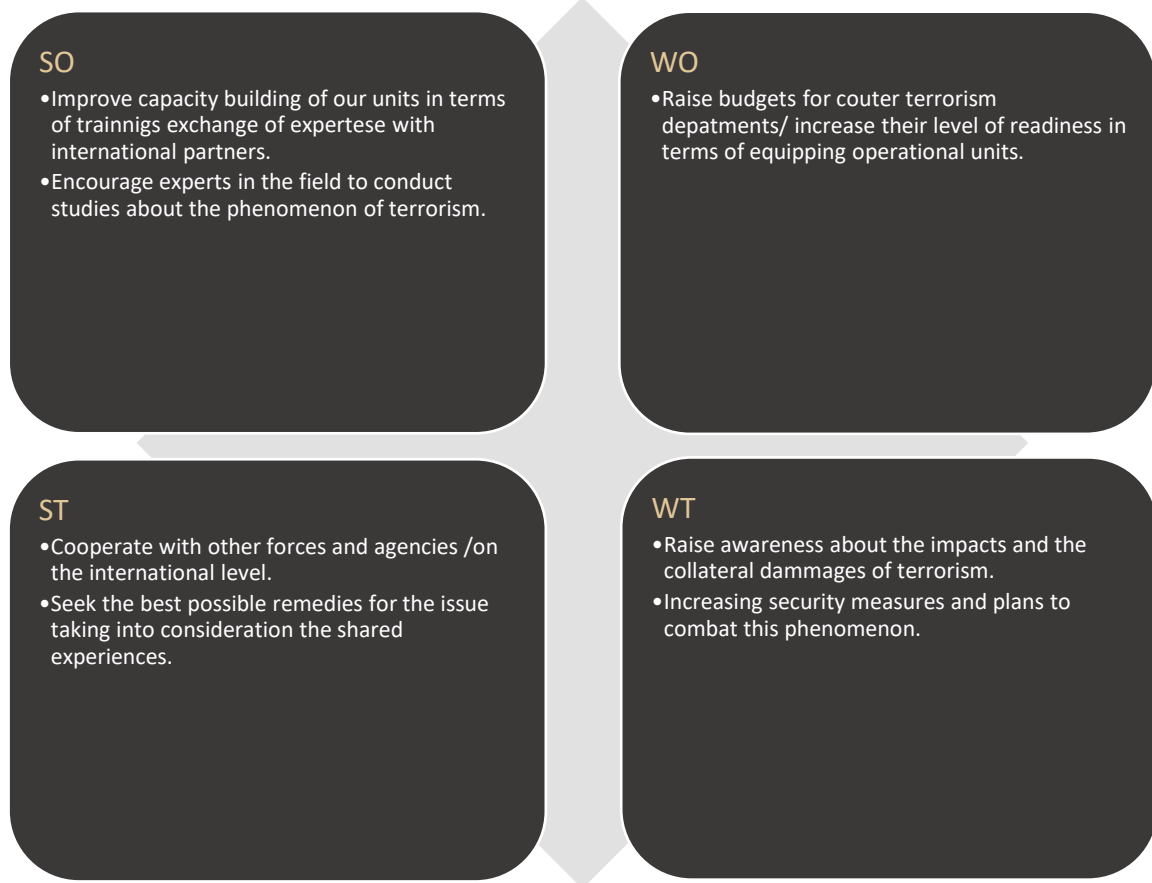


Figure 17. Key Strategies | Terrorism

4. DISCUSSION

We have adopted the following approach to address this phenomenon:

1. Contribute to the development of legal legislation to keep pace with terrorist crimes. The purpose was the issuance of the Terrorism and Money Laundering Law (Law No. 26 dated 2015 pertaining to combating terrorism and preventing money laundering), whereby the previous law was rendered obsolete and the current provision for new crimes (praise and glorification of terrorism on social networks & special investigation methods...).
2. Contribute to the design and implementation of the counter-terrorism strategy that is based on (response, prevention, protection and pursue).
3. Contribute to coordinating the efforts of the National Commission for Financial Analysis, which is entrusted with preventing terrorist financing by verifying and investigating all suspicious financial transactions related to individuals and entities that might be linked to terrorism.
4. Contribute to coordinating the efforts of the National Counter-terrorism Commission that is entrusted with the mission offighting against terrorism.

5. Creating units specialized in investigating terrorist crimes (the NG CT Investigation Unit within the CT Department) with greater human and financial capabilities to accommodate the significant volume of cases registered by the specialized units both centrally and regionally.
6. Developing officers' technical knowledge and capabilities to keep pace with the development of terrorist crimes (camouflage and concealment tradecraft), which have become chiefly dependent on media platforms, social networks and encrypted applications for communication.
7. Reinforcing the field units' first response capabilities and rapid reaction to a terrorist attack and updating the Modus Operandi by carrying out mock operations as well as testing and exercising to determine the units' operational readiness.
8. Banning all disruptive activities and manifestations through which takfiri organizations seek to extend their influence on the ground in sheer defiance of the law and the state. (Illegal marriage, controlling mosques, giving sermons and preaching without a license, creating schools and associations illegally and outside of any supervisory authority, distribution of publications espousing takfiri messages...).
9. Real-time monitoring of terrorist organizations' electronic platforms to track terrorists' movements and threats and analyze their trends through the messages that they transmit through their publications (narrative, implementation methods, goals, trends, methods and techniques ...) in order to be ahead of the curve in the process of combating the threat and unveiling the preparatory work that precedes implementation.
10. Real-time monitoring of movements of terrorist elements stationed in the mountains, setting up ambushes to eliminate or arrest them, uncovering logistical support networks and arresting them inside cities, exchanging data about them within a comprehensive framework of terrorism prevention.
11. Real-time monitoring of dangerous takfiri elements' movements, especially those released from prisons and returning from hotbeds of tension or those who have recently adopted radical ideology, in addition to uncovering all sleeper cells and thwarting their plans.
12. We have taken preventive measures to shield society from terrorism through various measures. We banned the promotion of books and publications with a takfiri-oriented approach, prevented the ideologues of extremism and terrorism from entering Tunisia, discharged extremist imams who were operating illegally and replaced them with moderate people who do not suffer from schizophrenia (works as an employee of the state and charges it with infidelity at the same time).
13. We contributed to the issuance of a law that prevents the travel of youngsters into hotbeds of tension without a parental authorization (under 30 years old).
14. Relying on special investigation methods (infiltration, covert and overt surveillance, communication interception, technical surveillance and signal intelligence...)
15. Developing methods of field work by relying on advanced technical means in the judicial and intelligence arenas.
16. Establishing regional CT departments nationwide which report to the central administration and work within an intelligence framework specifically linked to CT.
17. Immunizing individuals from the dangers of recruitment and decoying, detect infiltration of the security and military units, taking strict measures against all individuals proven to be involved or



sympathetic to terrorist elements and organizations, and following up on all subjects of interest in coordination across all the branches of the armed forces.

18. Reinforcing the intelligence cycle, sharing and exchanging data pertaining to threats between the various intertwined entities centrally and regionally, identifying the sources of terrorist threat, working on neutralizing them and circulating intelligence feeds regularly to update them and take the appropriate lines of action.
19. Evaluating and updating insurance systems periodically to identify and address weaknesses and vulnerabilities immediately.
20. Cooperating and coordinating with foreign agencies in the field of intelligence sharing, training and exchange of experiences to identify and benefit from different strategies and approaches in the CT field.

4.1. CHALLENGES:

Although we have been able to win the war of combatting terrorism and achieve a commendable level of anticipation, the level of terrorist threats to our country remain relatively high for the following reasons:

1. The concentration of terrorist elements in the western mountains.
2. The concentration of terrorist elements on the Algerian borders.
3. The deterioration of the security situation in Libya.
4. The shift of ISIS movement From Syria and Iraq to the African Sahel and Sahara (the preferred area for terrorist organizations currently).
5. The return of groups of terrorist elements who were arrested in hotbeds of tension, some of whom completed their prison sentences.

5. CONCLUSIONS & RECOMMENDATIONS:

We then assess that addressing the phenomenon of terrorism must be holistic in which all parties and interests intersect. Whilst the security solution has paved the way for the elimination of the phenomenon around specific places and times, it cannot eliminate the terrorist thought or ideology. We therefore suggest the following measures:

1. Adopting an electronic surveillance system (bracelets) for terrorist elements released from prisons, especially those returning from hotbeds of tension, subject to a complementary penalty that requires administrative monitoring aiming at tracking their movements and curbing their danger.
2. Establishing an effective system to monitor the cyberspace (in the form of electronic armies), which terrorist organizations exploit to devise new, more covert methods to plan and implement operations.
3. Isolate dangerous inmates from the newly radicalized elements in prisons and draw up a special program for their reintegration into society.
4. Rehabilitation of children and women returning from hotbeds of tension to reintegrate them into society and deracialize them.

5. Establishing electronic platforms to spread moderate religious narrative and banning the circulation of extremist books and publications, and preventing terrorist organizations from spreading their poisonous ideology on social networks.
6. Drawing best practices and inspiration from the strategy of restraining force, soft force, and smart force that adopts a mixture of the two methods, similar to the Western strategies adopted to combat terrorism.
7. Issuing a law regulating the state of emergency to ensure greater protection for those involved during crises, especially terrorist operations.
8. Seeking to create a national crisis management center, entrusted with the mission of training and crisis management and regulating interventions and interoperability. This should enable us to reach international standards and develop sufficient organizational flexibility and resilience.
9. Thinking about establishing joint platforms to combat terrorism at the regional and local levels, especially among countries that have common borders. These countries share the concern of monitoring terrorist threats due to the transnational nature of the phenomenon (a transnational crime), which requires concerted and coordinated efforts.



REFERENCES

<https://legislation-securite.tn/>

Website of the National Counter-Terrorism Committee: http://www.cnlct.tn/?page_id=1029

Legislative Guide to Global Conventions and Protocols to Combat Terrorism: https://www.unodc.org/pdf/crime/terrorism/Legislative_Guide_Arabic.pdf

A study on counter-terrorism legislation in the Arab Gulf states and Yemen: https://www.unodc.org/documents/terrorism/Publications/Study_CT_Legislation_Gulf_Yemen_Arabic.pdf

Arab Convention against Terrorism: [https://s3-eu-west-1.amazonaws.com/public.lidit.dcaf/lois/d%C3%A9cret%20n%C2%B099-1470%20du%2021%20Juin%201999%20\(en\).pdf](https://s3-eu-west-1.amazonaws.com/public.lidit.dcaf/lois/d%C3%A9cret%20n%C2%B099-1470%20du%2021%20Juin%201999%20(en).pdf)

The Arab Gulf Cooperation Council Agreement to Combat Terrorism <https://www.almeezan.qa/AgreementsPage.aspx?id=1231&language=ar>:

Handbook of International Cooperation in Criminal Matters to Combat Terrorism (Added) https://www.unodc.org/documents/terrorism/Publications/Manual_Int_Coop_Criminal_Matters/Manual_on_International_Cooperation_in_Criminal_Matters_related_to_Terrorism_-_Arabic.pdf

NATO Counter-Terrorism Reference Curriculum (Added) https://www.nato.int/nato_static_fl2014/assets/pdf/2020/12/pdf/2012-DEEP-CTRC-arabic.PDF

XI. PAPER | TRANSNATIONAL CRIMINAL NETWORKS

Citation:

Youssouf, A., Transnational criminal networks. Overcoming Security Threats arising from Globalization 4.0 – FIEP Association, 2022.

Published: October 2022

Publisher's Note: FIEP stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors.

Djibouti

National Gendarmerie

Abdoul-karim Ibrahim YOUSOUF



abdokibrah@gmail.com

Abstract: Transnational organized crime is a growing problem across the world and in Africa. This article has focused on organized crime observed in Africa. If international criminal organizations continue to target the African continent in particular, it is because of the significant illicit wealth that can be generated there. These are based on the enormous financial gains generated by these illegal trafficking, but also the various social and political vulnerabilities, the fragility and governance problems of States, as well as the limited police capacities and the corruption present on the continent to varying degrees. International criminal organizations and networks operate throughout Africa. These criminal groups maintain close ties with each other across borders and operate in a number of illicit trades, in particular drug trafficking, migrant smuggling, fraudulent drug trafficking, environmental damage, financial crime, counterfeiting of goods, cybercrime, trade in small arms and light weapons, maritime piracy and illicit trafficking in works of art and cultural property.

Keywords: Transnational organized crime, vulnerabilities, law enforcement, cooperation and coordination



1. INTRODUCTION

Transnational organized crime has experienced phenomenal growth in recent years. No nation in the world is spared, whether as a source, target or transit country. Transnational criminal organizations continue to illegally cross porous land borders for various forms of trafficking. These international illicit markets generate billions of dollars every year.

Indeed, the main objective of criminal groups involved in transnational organized crime is to generate maximum financial gain. Thus, there are significant inter-regional illicit financial flows as well as considerable transfers of illicit profits throughout the continent, often to foreign countries. Money laundering related to all criminal market activities takes place on a global scale.

The threat posed by organized crime in Africa is serious, yet the capacity of law enforcement security services to deal with this complex problem at the national, regional and continental levels is limited. It is necessary to fight in a strategic and coordinated way against this illicit trafficking by coordinating operations between national agencies but also by developing partnerships and cooperation agreements between agencies responsible for law enforcement throughout the African countries and the rest of the world.

To combat this protean crime, the common legal basis is the United Nations Convention against Transnational Organized Crime¹³, known as the Palermo Convention. This United Nations convention, signed in December 2000 in Palermo, in tribute to Judge Giovanni Falcone. The convention entered into force on September 29, 2003 and establishes a universal framework for the implementation of international police and judicial cooperation to improve the prevention and repression of organized crime phenomena. This convention is complemented by three additional protocols relating to trafficking in persons, the smuggling of migrants, money laundering and the illicit manufacturing and trafficking of firearms. 147 States are signatories to this convention. The Republic of Djibouti signed this United Nations convention on April 20, 2005.

According to the Palermo Convention, the definition of an "*Organized criminal group*" is: "*a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit*".¹⁴

2. MATERIALS AND METHODS

This study will focus on presenting, first, the vulnerabilities and the different forms of these transnational criminal phenomena that plague the economy and security on a global scale and in particular the development of the African continent. A PESTEL analysis where the factors that affect the political, economic, social, technological, environmental and legal aspects will be defined. Then, SWOT matrix analysis will be used to determine whether these factors strengthen or weaken countries in the fight against transnational organized crime, and which areas need to be strengthened. At the end of this reflection process, recommendations and strategies to better fight against these scourges will be proposed.

¹³ https://treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-12&chapter=18&clang=en

¹⁴ https://www.unodc.org/documents/middleeastandnorthafrica/organised-crime/UNITED_NATIONS_CONVENTION_AGAINST_TRANSNATIONAL_ORGANIZED_CRIME_AND_THE_PROTOCOLS_THERETO.pdf

3. RESULTS

3.1. ANALYSIS OF EXTERNAL ENVIRONMENT

3.1.1. VULNERABILITIES

Three major vulnerabilities are identified when analyzing organized crime on the African continent:

- *Conflicts;*
- *Poor governance of state structures;*
- *Prevalence of corruption.*

These local factors facilitate the expansion of criminal groups, which could be designated as “amplifiers”, in the sense that they aggravate the impact of organized crime and represent opportunities and incentives for criminal organizations. They also weaken State and community responses.¹⁵

The problem of state legitimacy arises when state organs and structures do not function properly. Poor governance leads to the absence of a coordinated strategy to deal with all these forms of organized crime.

The problem of state legitimacy arises when state organs and structures do not function properly. Poor governance leads to the absence of a coordinated strategy to deal with all these forms of organized crime.

On the other hand, the African continent has several conflict zones in which populations live in a situation of insecurity. Indeed, countries such as Libya, Mali, the Central African Republic, Somalia, Ethiopia and South Sudan are facing insecurity caused by rebel groups or Islamist terrorist organizations. Terrorist groups such as Alshabab in Somalia and Alqaida, the Islamic State or Boko Haram in West Africa, precisely in the Sahel region and in the Lake Chad basin, carry out terror operations and have created a context of insecurity. Criminal actors find opportunities to set up their illicit markets in these contexts of armed conflict. In these “fragile” countries in a situation of insecurity, security agencies and law enforcement agencies become weak and no longer receive the financial resources they need to fight against these criminal groups. These law enforcement agencies then become ineffective in the fight against organized crime. Criminal groups have more resources than the security agencies in these countries. In summary, these armed conflicts reduce the resilience of these governments to be able to respond to the challenge of fighting organized crime.

These traffickers of arms, narcotics, human beings can also resort to corruption to achieve their objective which is to increase their financial gains. Corruption within security agencies undermines efforts to combat cross-border organized crime and poses a risk to public safety. Any level of corruption is considered a direct threat to national and international security.

3.1.2. THE DIFFERENT FORMS OF ORGANIZED CRIME:

3.1.2.1. DRUG TRAFFICKING

In the early 2000s, the West African maritime coast experienced a rise in drug trafficking, particularly cocaine. Latin American drug traffickers have targeted fragile West African states on the face of the Atlantic Ocean as a transit zone for their illegal goods bound for Europe. The traffickers have chosen this region of the African continent because of the difficulties of direct

¹⁵ Webinar: “Understanding the Vulnerabilities to Transnational Organized Crime in Africa”: <https://www.youtube.com/watch?v=ASB9O6aTN3A> (Africa Center for Strategic Studies: December 10, 2020)



shipping to Europe and the increase in customs and police controls in the Caribbean which initially served as a transit zone. The example of the Republic of Guinea Bissau is a model to study because this country has turned into a "narco-state". The political and military authorities of this country have been particularly corrupt and the South American traffickers have succeeded in setting up governments which facilitate and protect their illegal activities.

East Africa, meanwhile, has become a transit region for heroin from Afghanistan and Pakistan. The port of Mombassa, the island of Zanzibar and Mozambique are identified as important transit points for this heroin, which is destined for South Africa, Europe and the United States.

Finally, the third category of illegally trafficked narcotics is methamphetamine. South Africa and Nigeria are two producing countries of this drug which is then sent to Asian countries.¹⁶

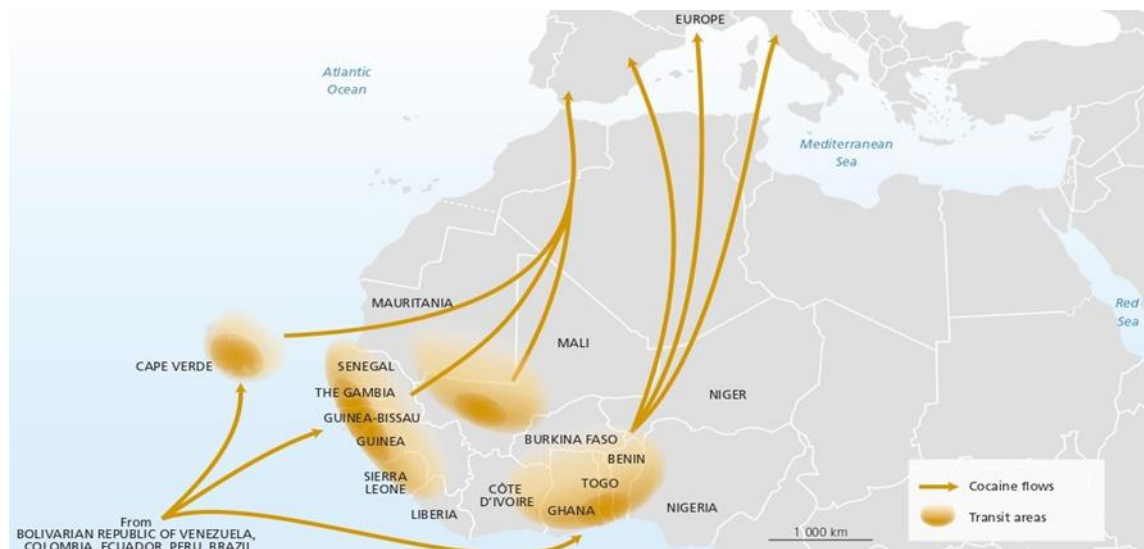


Figure 18. Cocaine flows and transit areas

3.1.2.2. MIGRANT SMUGGLING AND HUMAN TRAFFICKING

The aspiration for a better life or for social and economic success pushes, in particular, African youth to migrate to European countries or the Arabian Peninsula. Criminal networks have understood that exploiting this situation can offer them an opportunity for considerable financial gain. Migrant smugglers demand significant financial remuneration. They endanger this youth by making them cross desert regions and maritime areas such as the Mediterranean or the Red Sea, at the risk of dying of thirst or drowning. Some of these migrants are retained by these human traffickers and subject them to sexual or labor exploitation.¹⁷

¹⁶ Pages 09 to 24 of the following UN report: https://www.unodc.org/documents/data-and-analysis/tocta/West_Africa_TOCTA_2013_EN.pdf

¹⁷ Pages 25 to 31 of the following UN report: https://www.unodc.org/documents/data-and-analysis/tocta/West_Africa_TOCTA_2013_EN.pdf

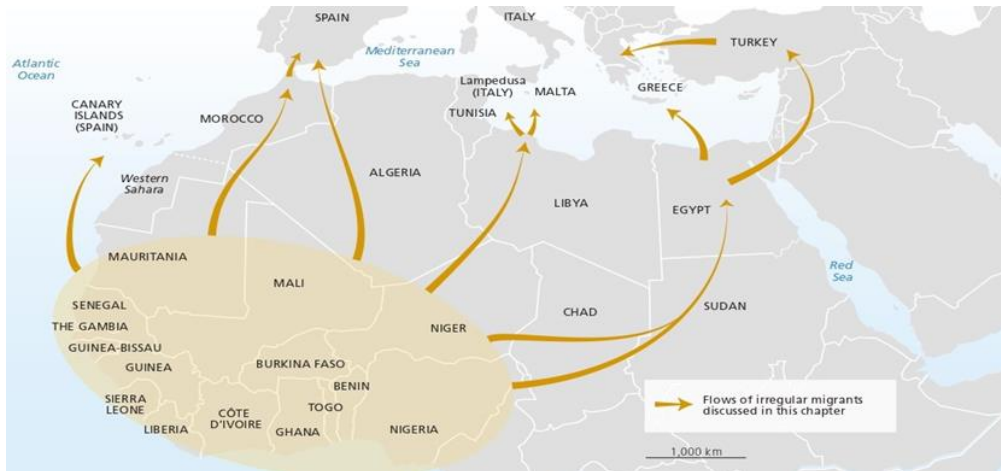


Figure 19. Flows of irregular migrants

3.1.2.3. POACHING OF RARE ANIMAL SPECIES AND ENVIRONMENTAL POLLUTION

The African continent has a great diversity of flora and fauna as well as valuable natural and mineral resources. Criminal networks realized the significant financial gain they could acquire by illegally exploiting these vast resources. Over the past 20 years, illegal poaching of rare animal species has steadily increased. This is due to the high financial value of these species, particularly on the Asian market. Rhinoceros horn, from poaching of the species in protected areas in southern Africa, can be cited as an example. Available statistics demonstrate the extent of trafficking in South Africa, where there has been a rapid increase in rhino poaching over a short period. The flora also undergoes rapid degradation. African forests, home to some of the most diverse and valuable timber species, are being plundered by illegal logging. Losses to Africa from illegal logging are estimated at US\$17 billion per year. In Madagascar, for example, rosewood and ebony are now highly sought after for the manufacture of musical instruments in Europe and North America or furniture in Asia. On the other hand, there is an increase in illegal and unregulated fishing caused by the presence of European and Asian fishing vessels in African maritime waters. Sub-Saharan Africa records losses estimated at one billion US dollars per year due to illegal fishing. Criminal networks, operating in countries with weak governance, also contribute to the pollution of African land by burying toxic waste from major industrial countries.

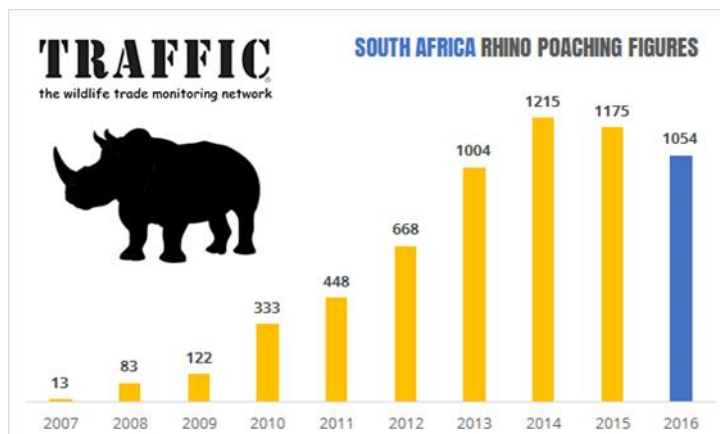


Figure 20. Rhino poaching statistics in South Africa from 2000 to 2016

Source: wildhood foundation: <https://www.wildhood.org/en/2017/02/27/rhino-poaching-numbers-decline-south-africa-2016-crisis-persists/>



3.1.2.4. TRAFFICKING OF FRAUDULENT DRUGS

Imports of counterfeit drugs in Africa have increased over the past two decades. China and India are also two of the most frequently identified sources of fraudulent drugs, as evidenced by incidents reported to the Pharmaceutical Security Institute. A recent forensic study of fraudulent medicines detected in Africa has confirmed the Asian origin of these products. This traffic constitutes a real danger to the public health of African populations given the absence or the low quantity of active substance of these drugs.¹⁸

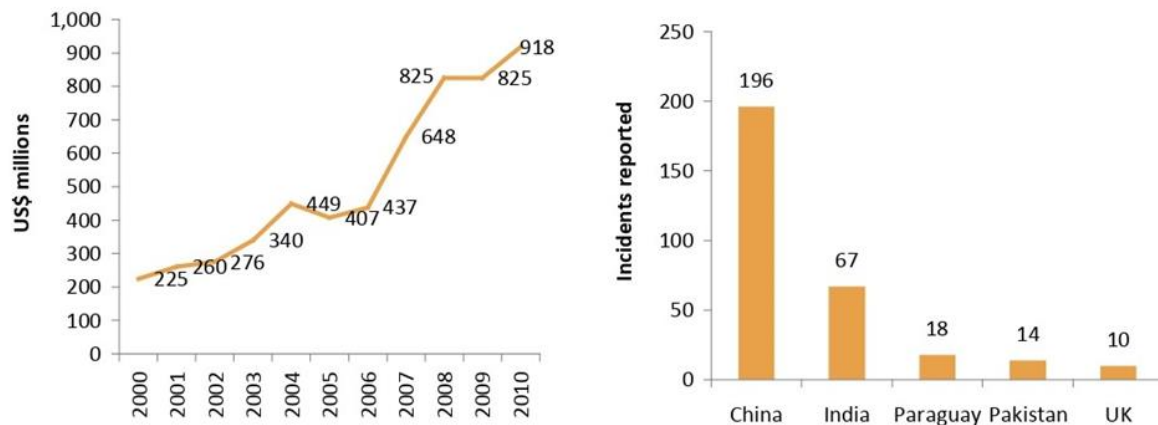


Figure 21. Pharmaceutical imports for eight West African countries, in millions of US\$

3.1.2.5. ARMS TRAFFICKING

Africa is a major destination for arms. Nearly 100 million small arms are said to be in circulation, stockpiled or in the possession of private individuals on the continent. Several situations have contributed to the proliferation of these weapons. The case of the collapse of the Libyan State which had a large arsenal of weapons of different categories could be cited as an example. Indeed, the collapse of the Libyan regime has allowed terrorist groups and criminal organizations in West Africa and the Sahel to recover Libya's stockpile of weapons. This has fueled the areas of insecurity that persist in this region of the African continent. Also, arms embargoes have been decreed by the United Nations for certain countries in situations of armed conflict, such as Somalia. To circumvent these embargoes, weapons are often imported using fake end-user certificates or transferred to secondary destinations that serve as transit countries.¹⁹

¹⁸ Top five origins of counterfeit medicines detected worldwide, by number of incidents reported to the Pharmaceutical Security Institute, 2010

¹⁹ Pages 33 to 37 of the following UN report: https://www.unodc.org/documents/data-and-analysis/tocta/West_Africa_TOCTA_2013_EN.pdf

3.2. PESTEL ANALYSIS

Table 19. PESTEL analysis | Transnational organized crime

Factors	Key Macro Trends	Implications for Security Forces
Political & Legal	<p>P.1. Countries tend to adopt a law on organized crime.</p> <p>P.2. Political authorities tend to demonstrate a real will to fight organized crime.</p>	<ol style="list-style-type: none"> 1. National organized crime laws will make it easier for security forces and the judiciary to better fight organized crime. 2. If the high political authorities commit to fighting organized crime, the security forces will be able to benefit from more resources.
Economic	<p>E.1. The “underground economy” generated by criminal trafficking weakens the financial resources of States and the growth of legal trade.</p> <p>E.2. The corruption of political authorities and law enforcement agencies facilitates the expansion of criminal activities.</p>	<ol style="list-style-type: none"> 1. Law enforcement agencies in different countries should build the capacity of financial investigators. 2. Within the various agencies, it would be necessary to strengthen the ethics and professionalism control services.
Social	<p>S.1. The poverty of the populations allows criminal and violent groups to recruit unemployed young people.</p> <p>S.2. The media raises public awareness of the problem of organized crime.</p>	<ol style="list-style-type: none"> 1. Put in place financial empowerment and entrepreneurship policies for the poorest social strata. 2. A better sensitization by the media, will allow the community to be a true partner of the security forces, in particular in the search for intelligence.
Technological	<p>T.1. Cybercrime is a growing form of organized crime.</p>	<ol style="list-style-type: none"> 1. Security forces must have units specialized in monitoring criminal activities on the Internet.
Environmental	<p>EN.1. Trafficking in animal species leads to the disappearance of certain rare species.</p> <p>EN.2. The traffic of toxic waste causes pollution of the waters of rivers, rivers and seas and agricultural areas.</p>	<ol style="list-style-type: none"> 1. Government authorities must strengthen the resources of forest rangers and coast guards in order to fight against toxic waste pollution and illegal poaching.



3.3. ANALYSIS OF INTERNAL ENVIRONMENT

3.3.1. STRUCTURAL ORGANIZATION OF SECURITY FORCES

The security forces of the countries of the African continent, such as the National Police, the National Gendarmerie, the Coast Guards, are institutions of a military or paramilitary nature. The personnel of these organizations are governed by disciplinary regulations. The chain of command is pyramidal in nature, with a Director General having a staff that gives directives at the strategic level. Then at the operational level, the missions to fight against crime are carried out by Groups and units.

3.3.2. JUDICIAL AND INTER-AGENCY COOPERATION

Judicial systems and security forces in different countries around the world must give priority to real cooperation between magistrates and operational collaboration in the field of intelligence and joint operations between forces. Geographic borders should no longer be constraints in dealing with organized crime. This cooperation between States is necessary, not only because the people involved in the different trafficking (accused, victims, witnesses, etc.) may be of different nationalities, or be in different countries. It is also fundamental because the evidence may be on the territory of a State other than that which initiated the proceedings.

3.3.3. SWOT ANALYSIS

Table 20. SWOT analysis | Transnational organized crime

Internal factors	Strengths (S)	Weaknesses (W)
	<ul style="list-style-type: none"> • Law enforcement agencies have a military culture and command is not dispersed. • The process of structural change and increased resources has already begun in several countries. 	<ul style="list-style-type: none"> • Law enforcement agencies in different African countries need more resources. • Coordination between the different national agencies is still weak. • Cooperation between countries at the judicial and operational level is also insufficient. • The operational units of law enforcement agencies are not yet sufficiently specialized in narcotics, cybercrime, financial crime.
External factors		
Opportunities (O)	<ul style="list-style-type: none"> • Increasing the material and human resources as well as the financial budgets allocated to the fight against transnational organized crime. • All African States should sign and ratify the UN Convention against Transnational Organized Crime. • At the national level, strengthening the existing legal frameworks in each country to ensure the sentencing of identified criminals. 	<ul style="list-style-type: none"> • Focus efforts on financial flows linked to drug trafficking and transnational organized crime to eliminate their sources of funding • Implementation of information exchange mechanisms between the different national agencies (establishment of an inter-agency working group: customs, police, gendarmerie, coast guard, national security). • Strengthening of cross-border operational cooperation between the securities forces of neighboring countries (intelligence exchange and joint operations).
Threats (T)	<ul style="list-style-type: none"> • Development of the code of conduct and anti-corruption guidelines as well as monitoring and evaluation. • International judicial cooperation (arrest, transfer of criminals from one State to another). 	<ul style="list-style-type: none"> • Raising awareness through the media on the fight against transnational organized crime. • Building trust and increasing partnership between border communities and security forces.



3.4. EMERGING STRATEGIES

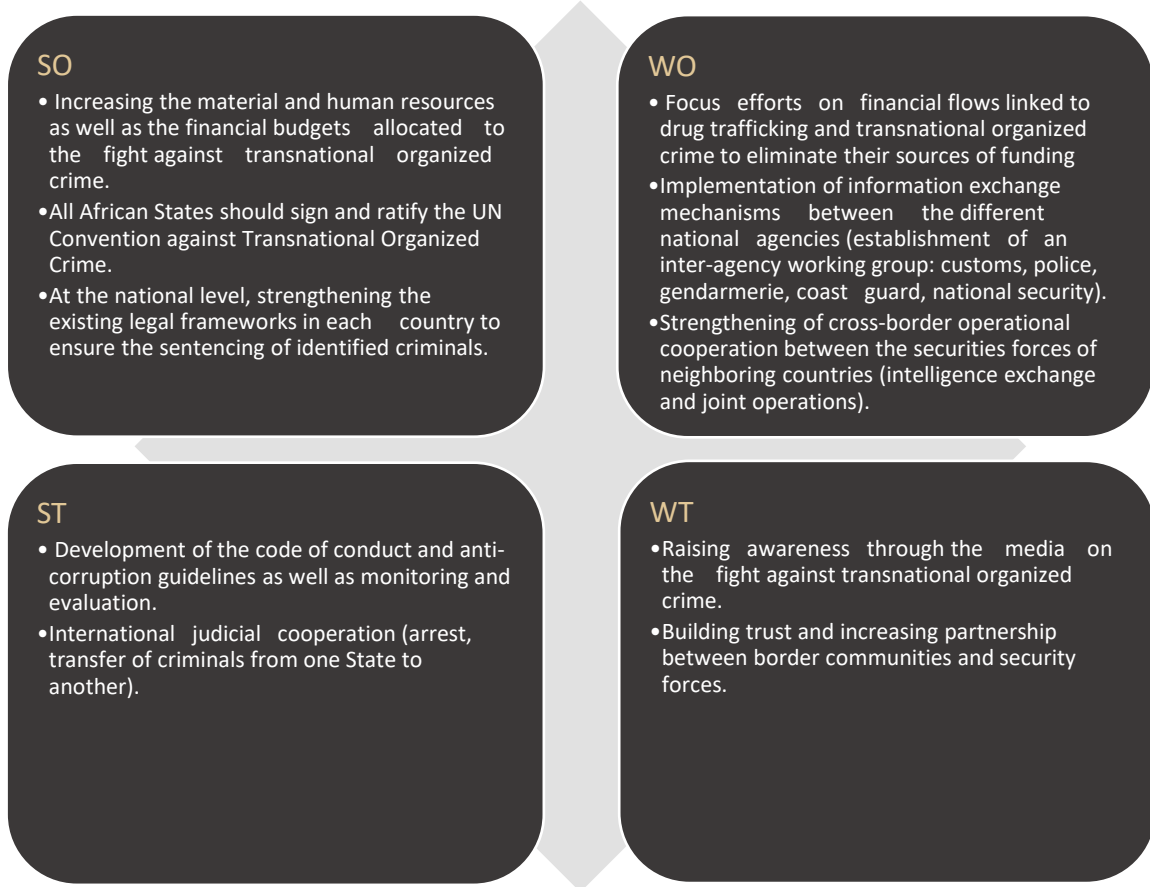


Figure 22. Key Strategies | Transnational organized crime

4. CONCLUSIONS AND RECOMMENDATIONS:

The objective of this analysis was to provide an overview of the context of threats, linked to organized crime, currently observed in Africa. This article has drawn attention to the various criminal networks as well as the various illicit markets likely to constitute a direct danger to the safety, security and development of the African continent. Cybercrime and illicit arms trafficking constitute trafficking that facilitates the development of other criminal trafficking. Finally, this article has addressed the issue of illicit flows of funds and assets by focusing on the main money laundering activities taking place in all African countries. Whether it is for the trafficking of narcotics, fraudulent medicines, works of art, wildlife, natural resources, or human trafficking, the criminal networks operating in Africa will continue to thrive and evolve according to the political, socio-economic and security context in which they operate. They will relentlessly strive to adapt and expand their illicit activities opportunistically to increase their profits.

The close link between organized crime, terrorism and armed conflict is crucial, and will probably continue in the short term to destabilize many parts of Africa. Therefore, it is urgent to put into action the control strategies, some of which have been presented in this publication.

Briefly, it is a question of strengthening the rule of law and good governance in the various States of the African continent, fighting against corrupt practices, raising public awareness, strengthening the coordination mechanisms of national law enforcement agencies the law and finally operational cooperation between the security forces of the various African countries. In addition, it is also more than necessary to put in place judicial cooperation agreements between all countries so that criminals cannot escape criminal prosecution, their arrest and their extradition.

In summary, without this international and coordinated fight, these criminal networks will continue to grow and their activities will undoubtedly have devastating effects on the development and stability of African States.



REFERENCES

- ENACT (2021). Africa Organised crime index 2021, Evolution of crime in Covid world. https://africa.ocindex.net/assets/downloads/enact_report_2021.pdf
- Interpol (2018). Overview of Serious and Organised Crime in Africa 2018. <https://enactafrica.org/research/analytical-reports/interpol-overview-of-serious-and-organised-crime-in-africa-2018>
- UNODC (2013), Transnational Organized Crime in West Africa: a threat assessment [https://www.unodc.org/documents/data-and-analysis/tocta/West Africa TOCTA 2013 EN.pdf](https://www.unodc.org/documents/data-and-analysis/tocta/West_Africa_TOCTA_2013_EN.pdf)
- UNODC (2013), Transnational Organized Crime in Eastern Africa: a threat assessment [https://www.unodc.org/documents/data-and-analysis/Studies/TOC East Africa 2013.pdf](https://www.unodc.org/documents/data-and-analysis/Studies/TOC_East_Africa_2013.pdf)
- UNODC (2011). estimating illicit financial flows resulting from drug trafficking and other transnational organized crimes (october 2011). [http://www.unodc.org/documents/data-and-analysis/Studies/Illicit financial flows 2011 web.pdf](http://www.unodc.org/documents/data-and-analysis/Studies/Illicit_financial_flows_2011_web.pdf)
- United Nations Treaty collection. https://treaties.un.org/pages/ViewDetails.aspx?src=IND&mtdsg_no=XVIII-12&chapter=18&clang=en
- United Nations Convention Against Transnational Organized Crime, G.A. Res. 25, annex I, U.N. GAOR, 55th Sess., Supp. No. 49, at 44, U.N. Doc. A/45/49 (Vol. I) (2001), entered into force Sept. 29, 2003.
- Webinar: “Understanding the Vulnerabilities to Transnational Organized Crime in Africa”: <https://www.youtube.com/watch?v=ASB9O6aTN3A> (Africa Center for Strategic Studies: December 10, 2020)

XII. PAPER | COUNTERFEITING

Citation:

Chaid, A., Counterfeiting (documents, pharmaceuticals, goods and products, digital contents). Overcoming Security Threats arising from Globalization 4.0 – FIEP Association, 2022.

Published: October 2022

Publisher's Note: FIEP stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors.

Morocco

Royal Gendarmerie

Abdessamad CHAHID



a.chahid@gr.ma

Abstract: The current article is devoted to unveil one of the very astonishing criminal phenomena for law enforcement around the globe, that is to say "Counterfeiting (documents, pharmaceuticals, goods and products, digital contents)". The main idea is to shed light on its origins or motivations, the benefits taken from the rise of the digital technology, the "Globalization 4.0", and its implications, chiefly, during the pandemic Covid-19 era. In this same vein, the focus will also be oriented to reckon the applied countermeasures by the Moroccan Authorities and the Royal Gendarmerie as a point in case, in view of mitigating its influence on the socio-economic spectrums.

This article unveils the most practical steps and countermeasures devoted to mitigate the seriousness of the counterfeiting phenomenon.

The article adopted the dynamic SWOT analysis to help in some manners to make a concrete dissection of the aforementioned criminal phenomena in view of finding rooms to disrupt its still relentless ramifications.

Keywords: counterfeiting; fake goods; legal corpus;



5. INTRODUCTION

Globalization is rendering access to technology more and more effortless and opportunuous for everybody around the globe. In parallel, criminal effervescence and vulnerabilities grasp more advantages to widen the range of their illicit activities.

For starters, Counterfeiting is a crime involving the theft of someone's trademark. Businesses – both small and large – use trademarks to help consumers like you identify their products. A trademark is most often a word, phrase or symbol that identifies the source or origin of a particular good or service sold in commerce.

A counterfeit is an item that uses someone else's trademark without their permission. By making or selling a counterfeit, criminals seek to profit unfairly from the trademark owner's reputation.

Unfortunately, counterfeiting is excruciating and happens to be global and everywhere. This criminal phenomenon can affect what we eat, what we watch, what medicines we take, what we drive and what we wear – and all too often the link between fake goods and transnational organized crime is overlooked in the search for knock-offs at bargain-basement prices. The perception of this kind of crimes by Law enforcement agencies around the world stems from the fact that it's not a mere criminal act, but it is seen as a confirmed easy source of money and lucrative business used in nourishing other serious crimes and illegal networks activities such as terrorism, piracy, illegal migration and so on.

In this vein, increased sales of and access to counterfeits pose serious threats to the economy and to public health and safety. As the Organization for Economic Co-operation and Development (OECD) noted in a 2007 study, the Internet was a significant factor in the distribution of counterfeits and was becoming an increasingly important vehicle for sales of all kinds of merchandise. The report also noted that public health and safety were put at grave risk by counterfeit goods, such as pharmaceuticals, airplane and automotive parts, and electronic goods that were made with substandard and/or toxic materials.

6. MATERIALS AND METHODS

The current study is going to connect dots over the applied countermeasures to disrupt the spiral rates regarding counterfeiting phenomena and how efforts are directed to sensitize stakeholders and consolidate strategies to lessen vulnerabilities.

In this vein, the study will have recourse to SWOT analysis to make a dissection of the counterfeithing phenomenon and identify best practices to be adopted to mitigate its impacts over vital realms, meanwhile, help consolidate the actions tackled by law enforcements in this same perspective.

The final results will be funnelled to provide a compilation of takeaways and recommendations that may help define appropriate startegies to counter this criminal phenomenon.

In this perspective, framing the extent of harm and danger's seriousness deemed very inflicting and astonishing. In truthful way, the costs are difficult to quantify in addition to the baffling non-monetary damage related to resulting illness and death. Counterfeiters continue to reap significant profits, while millions of consumers are at risk from unsafe and ineffective products. It is a truly transnational problem.

7. RESULTS²⁰

7.1. ANALYSIS OF EXTERNAL ENVIRONMENT

Table 21. PESTEL analysis | Counterfeiting

Factors	Key Macro Trends	Implications for Security Forces
Political & Legal	<p>P.3. Regularisation and rationalization of the internet space is becoming more and more on the A-list of strategies;</p> <p>P.4. Consoliation of actions devoted to preserve personal contents;</p> <p>P.5. The Widening access to technology is becoming crucial for all state structures (digitalization of Administration);</p> <p>P.6. Legal gray areas and shortages of legal corpus perseverance</p>	<ol style="list-style-type: none"> 1. Contraction of the area of actions regarding the fight against similar crimes; 2. Necessity to take into account the preservation of personal contents 3. Increased strategies to enhance the protection of real activities 4. Data gathering is becoming more delicate
Economic	<p>E.3. Significant effects on the job market through the displacement of legitimate economic activity by counterfeiting</p> <p>E.4. Flagrant fiscal losses for many markets</p> <p>E.5. Complicated fraudulent nature of counterfeiting, which relies on the activity being hidden from view</p> <p>E.6. Recourse to illicit jobs for easy money</p> <p>E.7. reputational damages counterfeit products can have on a business, in some cases, it can pose an even greater threat to customers' health and safety</p>	<ol style="list-style-type: none"> 3. Reinforcement of security plans to disrupt impacts on market normal activities 4. Consolidating communication and police of proximity to mitigate resulted ramifications 5. Enhance the actions devoted to control quality and disponibility of accurate goods 6. Sustaining interdepartments startegies to counter the spread of counterfeiting item 7. Cement border control and the exchange of data
Social	<p>S.3. Recourse to vulnerable activities to grant social privileges</p>	<ol style="list-style-type: none"> 3. Consolidation of police of proximity in view of anticipating and sensitizing against counterfeiting
Technological	<p>T.2. Increase of options offered by the internet to encourage the recourse to counterfeiting</p> <p>T.3. Preservation of anonymous counterfeiters to commit their criminal acts</p> <p>T.4. Enlarging the terrain for illicit activities that may grow neck and neck with counterfeitig</p> <p>T.5. Offering free platforms for counterfeiters to find new modus operdi and related options</p>	<ol style="list-style-type: none"> 2. Complex counteractions tackled throughout a wide space of activities 3. Continuous takeways to cumulated with the spiral growing illicit of technology for criminal purposes 4. Adapted trainings especially on technological arena and the permanent sensitization of the personnel of law enforcement are extremely necessary to follow up the spiral implications of this kind of crime 5. Enhacing cooperation as the crux of any action devoted to disrupt the counterfeiting phenomenon.
Environmental	<p>EN.3.Flagrant nuisance for health and environment in general.</p> <p>EN.4.Augment the vulernabilities regarding multiplication of pandemic risks.</p> <p>EN.5.Weaken the safety of many critical infructrures devoted to preserve environment because of fake raw materials.</p> <p>EN.6.Deceleration of the course of application green strategies.</p>	<ol style="list-style-type: none"> 2. Enhance the interdepartment joint actions against counterfeiting. 3. Consolidate the role of specilized environment Unit to anticipate action and define breaches regarding the implications of counterfeiting. 4. Procurement and use of counterfeit products and components in critical applications, whether knowingly or otherwise, will require replacement to prevent accident or critical malfunction.

²⁰ Main ressources used
www.iccwbo.org/publication
www.redpoints.com/blog
www.zurich.com.au



7.2. ANALYSIS OF INTERNAL ENVIRONMENT

Table 22. SWOT analysis | Counterfeiting

Internal factors	Strengths (S)	Weaknesses (W)
	<ul style="list-style-type: none"> • Need to consolidate mechanisms devoted to detect anticipatively the presence of counterfeiting item • Law enforcement agencies are permanently improving their responses to disrupt counterfeiters • Sharing of information help maintain a control over suspected areas of illicit activities • Consolidation of rapid and continuous exchange of information among all stakeholders including nn security entities 	<ul style="list-style-type: none"> • Need for implication for all stakeholders to promote global and participative strategies • Proximity of the internet space paves the way for illicit activities t transcend borders and widen the pace of targets • Absence of deterrent legislation that encourages counterfeiters, as they have less fear of being apprehended and prosecuted than they would for other crimes • Counterfeiters exploit border-control weaknesses and poor regulatory frameworks to widen their activities and gain more transnational avenues. They use false documents to obtain pharmaceutical ingredients, as well as manufacturing equipment to replicate genuine products
External factors		
Opportunities (O) <ul style="list-style-type: none"> • Need to consolidate mechanisms devoted to detect anticipatively the presence of counterfeiting item • Enhancement of specialized training and training of trainer as main option to update the reactivity • Continuous exchange of information help anticipate any successful strategy • Importance of RETEX regarding the fight against counterfeiting 	<ul style="list-style-type: none"> • Enhance the training and the training of trainers regarding the disruption of counterfeiting chiefly via the internet space • Diversify the resources in dealing with counterfeiting and providing adapted logistics 	<ul style="list-style-type: none"> • Intensify sensitization among stakeholders and community • Sustain combined mechanisms to counter this criminal phenomenon and reinforcing cooperation
Threats (T) <ul style="list-style-type: none"> • Detection of presence of counterfeit components can result in cost overruns and expensive project delays • Counterfeiting provides easy money for other illicit activities • Many fake and counterfeit products are so identical in look and feel to genuine parts that it is getting harder to distinguish them visually 	<ul style="list-style-type: none"> • Promote international judicial cooperation with financial and economic devoted entities • Keep up with the new modus operdi used throughout the courses of action 	<ul style="list-style-type: none"> • Mitigate risks and encourage alternatives that may help anticipate, report and neutralize freshly any attempt regarding the occurrence of acts related counterfeiting

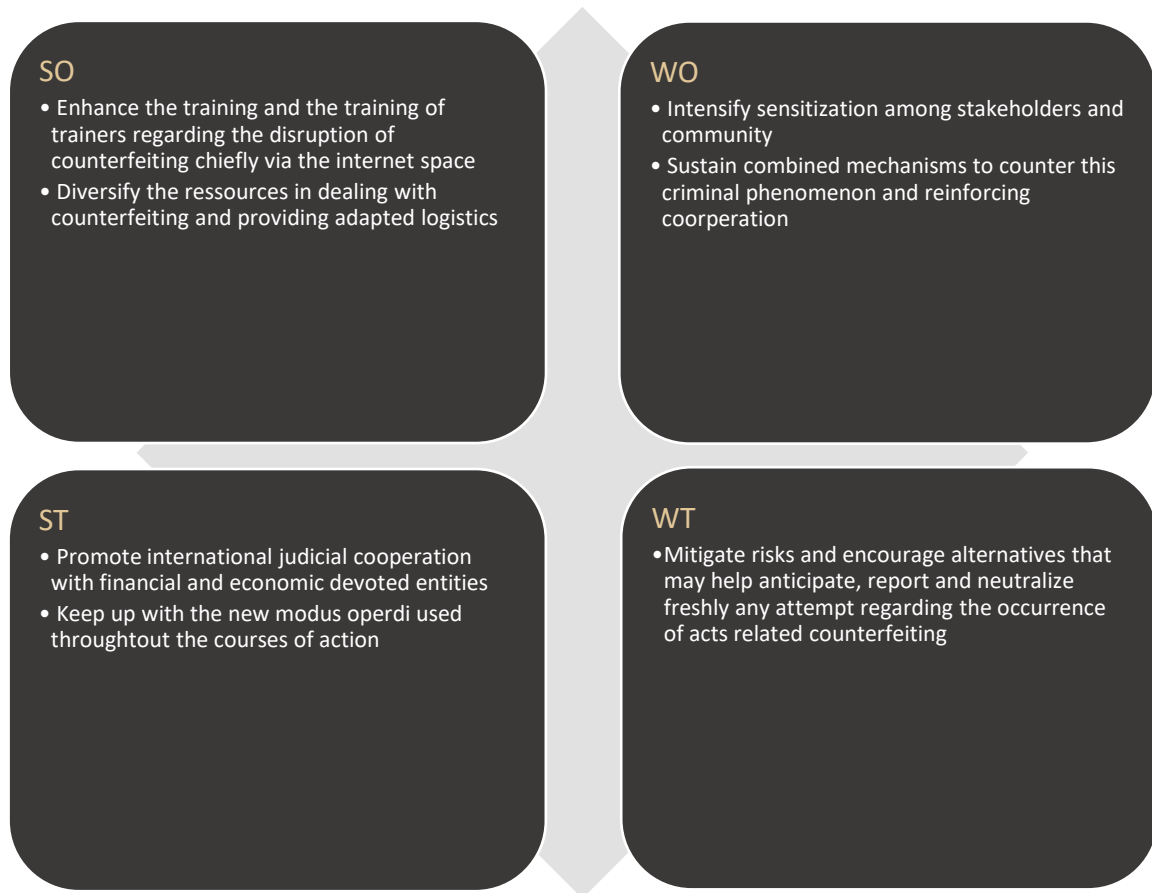


Figure 23. Key Strategies | Counterfeiting

7.3. JUXTAPOSITION OF THE MATRICE RESULT OF THE NATIONAL RESPONSE/DISCUSSION:

7.3.1. NATIONAL LEGAL CORPUS:

To fight against illegal practices infringing the trademark, trade and service mark, the Kingdom of Morocco has aligned itself with international standards in this area, enshrining in its legislation various administrative and judicial actions capable of ensuring better defense of the rights of trademark owners and to disrupt any criminal attempt.

To this end, our country has subscribed to the commitments resulting from the main international instruments applicable to trademarks, in particular the Paris Convention for the Protection of Industrial Property of 1883, the Madrid Agreement concerning the International Registration of Trademarks of 1891, the Protocol of 1989 relating to this Agreement, the Nice Agreement Concerning the International Classification of Goods and Services for the Purposes of the Registration of Marks of 1957, the Trademark Law Treaty of 1994 and the Convention of the Council of Europe on the counterfeiting of medical products and similar crimes involving threats to public health of 2011.

It has also concluded several commercial and free trade agreements guaranteeing an obligation to protect industrial property, including trademarks, in particular the Morocco-Tunisia free trade agreement of 1996 (art. 20), the Morocco -Jordan of 1998 (art. 14), the Morocco-Egypt free trade agreement of 1998 (art. 14), the Agadir agreement creating a Euro-Mediterranean free trade area of 2001 (art. 22), the Morocco-United States of America free trade agreement of 2004 (art. 15.2), the



agreement creating a free trade area between Morocco and the United Arab Emirates of 2001 (art. 17), the agreement Morocco-Turkiye Free Trade Agreement of 2004 (art. 27).

Thus, the defense of the brand, which is the common denominator of all these agreements, treaties and conventions ratified by Morocco, is governed in Moroccan legislation by Law No. 17-97 of February 15, 2000 relating to the protection of property. Industrial property, which was supplemented and modified initially by Law No. 31-05 of February 14, 2006 which introduced the opposition procedure and border measures in the field of industrial property, then by Law No. 23 -13 of November 21, 2014, has reinforced the repressive actions of counterfeiting.

Through these laws, the Moroccan legislator has sought to meet two essential requirements, which are to protect trademarks against any form of counterfeiting (i.e. any form of use by counterfeiters of an identical or confusingly similar), and to regulate any trademark use so that it cannot mislead or cause confusion.

The defense of the brand is of particular importance; and in this sense, its effective implementation helps to strengthen the economic fabric and attract foreign direct investment.

7.3.2. ACTIONS TACKLED BY THE MOROCCAN ROYAL GENDARMERIE:

For the purpose to counter this economic crime, the Royal Gendarmerie mobilized investigators in the field to dismantle criminal networks as well as a team of experts whose main mission is to produce proof of any infringement of industrial property rights.

7.3.3. TRAINING OF SPECIALIZED TECHNICIANS:

To support judicial investigations in this area, the Royal Gendarmerie Criminalistics Institute (ICGR) has contributed, since 2010 to the training of specialized technicians "Referents in Environment and Public Health (RESP)" whose main missions are the fight against counterfeiting and smuggling, the protection of the environment, the prevention of major risks, and the protection of endangered spaces and species... They are included within the Environment Brigades of the various Regions of the Kingdom and equipped with rolling means and equipment necessary for the sampling, collection, packaging and delivery of samples intended for expertise. The seizure of articles suspected of counterfeiting can be carried out directly by the elements of the judicial brigades or by the RESPs when these articles present a threat or an imminent danger to the health of consumers. Similarly, they may act on the order of the public prosecutor's office following the filing of a complaint by the right holder or his legal representative and after designation by requisition of the authority responsible for accompanying the complainant to produce evidence of infringement.

7.3.4. SCIENTIFIC EXPERTISE:

The expertise of seized products and articles is provided by a counterfeiting expertise Unit, created within the ICGR. It consists first of all on verifying the registration of the mark at the Moroccan Office of Industrial and Commercial Property (OMPIC), and then proceeds to a technical and scientific comparison of the suspected counterfeit articles with their authentic equivalents of the same model and series.

Each time, the comparative expertise covers the examination of the packaging, labeling, printing, dimensions, weight and qualitative and quantitative analysis. Similarly, the Institute has developed guides for recognizing fakes in partnership with rights holders, making it possible to better distinguish between genuine and counterfeit products.

Generally speaking, the items seized correspond to cosmetic and sanitary products, clothing, leather goods and luxury shoes, vehicle spare parts, medicines and food supplements, toner for printers, detergents, alcoholic beverages, etc.

7.3.5. SUPPORT AND CAPACITY BUILDING:

Representatives of Justice, Royal Gendarmerie (ICGR), as well as other stakeholders, regularly participate in meetings and training and sensitization seminars organized by OMPIC, with manufacturers and the National Committee for Industrial Property and Anti-Counterfeiting (CONPIAC) chaired by the Ministry of Industry, Trade and New Technologies, bringing together ministerial structures and representatives of the private sector stakeholders. Thus, several workshops were organized with the Union of French Manufacturers (UNIFAB) and the National Institute of Industrial Property (INPI France) in collaboration with CONPIAC and the National Anti-Counterfeiting Committee (CNAC **France**).

8. CONCLUSIONS AND RECOMMENDATIONS:

In a nutshell, it is clearly obvious that counterfeiting is a global problem that is growing with expanding pace of globalization. It is also a deceptive representation of imitation or fake products as original or genuine products that unfortunately happens to be not a new problem and is not limited to just currency or branded consumer goods. It is now expanding into industrial, construction and even critical aviation and military applications with alarming potential consequences.

To counter this astonishing phenomenon, or at least to contain its spiral propagation, this current article unveiled both general takeaways and specific recommendations as follows:

1. The necessity to consolidate the international cooperation as a main platform for exchange and RETEX;
2. The fight against counterfeiting should be combined and collective, implicating all the stakeholders not only the coercitive actors;
3. The need to rationalize the access of Internet while performing online related activities (more data exigencies). Buying on the Internet or other alternate sources or importing directly increases your chance of becoming a victim of counterfeit product frauds;
4. Lessen anonymous access to regarding platforms;
5. Knowing source for procurement of critical products and components and buying from authorized distributors provides at least some assurance of product quality and integrity of authentic parts;
6. Reporting suspected counterfeit products and distribution channels to law enforcement authorities and brand manufacturers help stakeholders anticipate and generate efficient reactive strategies. Ignoring knowledge about specific counterfeit products and sources of distribution can perpetuate this risk with potential for tragic consequences.



REFERENCES

Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) - of January 1, 1995.

Anti-counterfeiting trade agreement of October 1, 2011.

Law n° 31-05 amending and supplementing law n° 17-97 relating to the protection of industrial property (promulgated by Dahir n° 1-05-190 of February 14, 2006). Law No. 34-05 amending and supplementing Law No. 2-00 relating to copyright and related rights (promulgated by Dahir No. 1-05-192 of February 14, 2006).

Law No. 9-94 on the protection of plant varieties (promulgated by Dahir No. 1-96-255 of (January 21, 1997).

Dahir No. 1-11-03 of 14 Rabii I 1432 (February 18, 2011) promulgating Law No. 31-08 enacting consumer protection measures.

Law No. 17-97, promulgated by Dahir No. 1-00-91, of 9 kaada 1420 (February 15) relating to industrial property as amended by Law No. 31-05 in Article 201.

Ministerial Order No. 3486-13 of 27 Safar 1435 (December 31, 2013) setting the technical specifications for liquid and solid detergents and disinfectants.

NM 09.0.000 relating to the labeling of textile and clothing products.

Law No. 52-17 (promulgated by Dahir No. 1.19.06 of Joumada 18, 1440 - January 25, 2019) repealing Law No. 17-88 relating to the indication of the period of validity on cans of assimilated products and packaged drinks.

Ministerial Order No. 3486-13 of 27 Safar 1435 (December 31, 2013) setting the technical specifications for liquid and solid detergents and disinfectants.

www.zurich.com.au

XIII. PAPER | TRAFFICKING OF ARMS

Citation:

Valenzuela, N & Cortés, F, Illicit Traffic of firearms. Overcoming Security Threats arising from Globalization 4.0 – FIEP Association, 2022.

Publication date: October 2022

Note by editor: FIEP kept neutral in relation to the jurisdictional complaints in maps published and institutional affiliations.

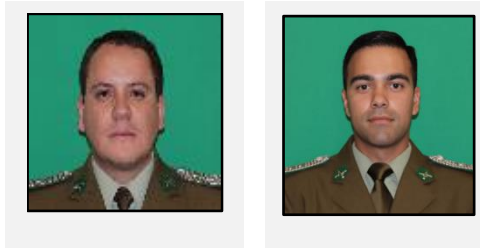


Copyright :© 2022 by the authors.

Chile

Carabineros de Chile

Nicolás Valenzuela Urzúa/ Felipe Cortés Aburto



nicolas.valenzuela@carabineros.cl

Abstract: The present article analyzes the process used in the internment and legal export as the illegal arms in the country, and the different mechanisms used to fight against the illicit traffic of firearms.

To determine these mechanisms, it was necessary the collection of information from the different departments of Carabineros de Chile related to forfeiture, expertise or entries in the intelligence technological systems. These are major divisions such as: the Department of Arms and Explosives Control O.S.11, the Criminal Analysis Department and the Criminalistic Department LABOCAR, by receiving quantitative records set in the Excel database. With this, it was possible to verify the evolution of traceability of firearms.

Finally, a strategic diagnosis of the exogenous and internal were carried out, that identify the strengths and weaknesses, opportunities and threats linked to the traffic of illicit in Chile, for establishing strategies and to reinforce the strengths and minimize threats, creating ways to increase the efficiency to fight against the crime under investigation.

Keywords: Firearms, traceability of firearms, IBIS Systems I.B.I.S



1. INTRODUCTION

Currently, the progress of the neoliberal political rationality has resulted in a transition from a clear disciplined society to a control society, in which the individual is enhanced to decide his/her destiny. This control society acquires a notorious relevance as soon as it is executed under a “danger culture”, in which this control and risk are closely related each other. It can be explained by the behaviors that some individuals adopted such as the drugs traffic, terrorism or crimes of social connotation and the use of excessive violence in the moment of using firearms.

In this sense, the collective violence translated and shown in the use of arms in certain sector of the world should be understood by means of the local history, which determine certain parameters to understand this phenomenon. Then, “the local history is vital to create the identity of a territory, its appropriation and physical dominion by means of its important milestones and the daily life that also are building, in their inhabitants, collective meaning and values”. (Cruz, G. De la Jara, A. 2007)

That is reason why the impact of using firearms led to create subjective and objective associations in its manage. Therefore, “one of the most evident and real consequences of the unduly use of firearms, is the number of injured and deaths related to arms. In addition, how it affects is higher. (The United Nations Office against Drugs and Crimes) 2020). This implies the need to find ways to mitigate the indiscriminate use of firearms by the criminal organizations, avoiding by this way its legal and illegal acquisitions. To face it, Chile has created a governmental campaign headed by the Ministry of the Interior, whose objective is to deliver anonymously the firearms and ammunitions to Carabineros de Chile, without giving, his/her name nor present any identifying document, no matter the arms type, caliber or condition such as: inherited, non-registered or modified arms. This obstructs to get firearms by illicit means.

Other way of mitigation is to know the traceability of the registered firearms, by using several marking methods that identify an arm at international level, such as: The mitigation mechanism that Chile presents is to know the traceability of firearms registered by using the several methods of marking that identifies an arm at international level, such as: serial number on the stamp in the test bench. Sometimes these methods are avoided by the criminal organizations, who alter or erase those identification points, which jeopardize to obtain the identity of its owner and its traceability.

In relation to the previous, there is a method by which it is possible to determine the traceability scientifically of the firearms or blank arms adapted to fire, that have been involved in criminal acts. It is possible to reach what it is mentioned above by using one of the most advanced tools in forensic science and in criminal investigation within our country, we are referring to the Identification Automated System of Ballistic Sings (IBIS), equipment operated by Carabineros de Chile, by means of the Criminalistics Department LABOCAR, by the Ballistic Laboratory and IBIS. This system allows to capture, share and compare great deal of amount of information and images of samples in networks of acquisition of ballistic images, as well as to identify projectiles or magazines that coincide automated (Ultra Electronics Forensic Technology, s.f)

2. MATERIALS AND METHODS

This study analyzed the process used in the legal and illegal import and exportation of firearms and the different methods of mitigation used to counteract the crime of the firearms traffic. The method to be used is based on in the hypothotetic – deductive reasoning, supported by the documented analyzed and the source of triangulation.

Firstly, the strategically endogenous and exogenous surroundings will be analyzed using the same method of other articles of this publication. By starting with factors definition that affect political, economic, social, technological, environmental and legal of the ciber-threats.

Later, the SWOT matrix analysis will be used to determine if these factors are reinforcing or weakening countries in the fight against the firearms traffic, and what are the areas or mechanisms that must be reinforced or be untreated for now. Later, this matrix will be transformed in a SWOT dynamic matrix, to help to define the strategies to be adopted.

Finally, the collected information processed in the previous stages will be used to define the best strategies to follow to counteract the threats of illicit traffic of firearms according to the current situation.

3. RESULTS

3.1. EXTERNAL ANALYSIS OF THE SURROUNDINGS

Table 23. PESTEL analysis | Trafficking of arms

Factors	Key Framework Trends	Implications in the Security Forces
Political & Legal	P.1. Reductions in the legal restrictions for the possession or carrying firearms per American countries.	1. The shortage of legal restrictions in the neighbor countries, cause the illegal sale of firearms to countries where the arms possession is limited.
	P.2. Increase in firearms possession in the United States.	2. The United States have been turned into one of the main exporters of illegal firearms, providing with them to the criminal organizations of the country.
	P.3. Shortage of legislation that limits new tools and methods to create firearms 3D.	3. Higher complexity in pursuant of firearms 3D, due to a gap in legislation.
	P.4. Reinforcements of policies for protection in the entry and exportation of species in the frontier paths.	4. Complexity to obtain the traceability of firearms from abroad.
	P.5. The need of a database at world level for the owners of firearms.	5. The communication networks among countries are more important to fight against the transnational organized crime.
	P.6. Methods of firearms traceability at world level.	6. It must be implemented more human and logistic resources in the frontier paths.
	P.7. Integration of countries at worldwide level in the Permanent International Commission (CIP) for the portable firearms tests.	7. Increase of threats related to the new type of firearms.
Economic	E.1. Economic instability in the Latin American countries.	1. Exceptional increase in postal packages that transfer accessories for firearms, using terrestrial via or using dissuasive methods as the aluminum paper, to be detected for technologic means, as X rays.
	E.2. The conflict in Ukraine affects the rise of basic products.	2. The virtual currency complicates to obtain the traceability of the sales of illegal items bought by the internet users or the dark web, being necessary to invest in new technological methods.
	E.3. The crypto currency will be turn more relevant and more people will star to use it and accept it.	3. The public funds for security forces are reduced.
	E.4. Other financing world crisis is to affect at least the western countries.	
	E.5. Increase of the electronic commerce.	



Social	<p>S.1. More accessibility in the transfer to foreign countries, by means of terrestrial, air or se transport.</p> <p>S.2. Increase in the international migration.</p> <p>S.3. Increase of social demonstrations by the people, in which any surge of a different opinion with the government is replied by an act against it.</p> <p>S.4. Increase of youth violence at international level.</p> <p>S.5. Increase of intercultural members of different international criminal organizations.</p> <p>S.6. Conflict for the indigenous territories</p>	<ol style="list-style-type: none"> 1. The easiness for travelling of people without any restriction, complicate to make a good enforcement of each one of the passengers, especially by terrestrial transportation. 2. Migration carries new modus operandi in committing crimes, which carries higher violence records and new nexus with other countries that increase the traffic of firearms between criminal organizations. 3. It is necessary to create and implement new methods of protection and mitigation by the police forces. 4. New techniques and occupation means to control the public order by the police forces. 5. The need for acquisition of illegal wide-caliper arms to be used by the communications against the police personnel.
Technological	<p>T.1. Creation of the printing machine 3D</p> <p>T.2. Advanced technological mechanisms to modify firearms.</p> <p>T.3. Investigation of new tools used in firearms that can leave the mitigation and detection obsolete.</p> <p>T.4. System of identification of the ballistic for firearms.</p> <p>T.5. The criminals always are more advanced than the state in the new technology fields.</p>	<ol style="list-style-type: none"> 1. Complexity to detect firearms 3D 2. Difficulty to make the traceability of firearms. 3. The need to spend money for the unification of an IBIS System, which is integrated with all those police forces or agencies dedicated to the neutralization of crimes at national and international levels. 4. The need to create mechanisms for the detection of the latest modus operandi used for the transnational transfer of firearms.
Environmental	<p>EN.1. Chile is presented as a country with several frontier multiple entries, by air, sea and land.</p>	<ol style="list-style-type: none"> 1. The criminals and the actors at national level will have an easy entry by the illegal paths. 2. The shortage of the human resources to enforce the law and control each of the illegal paths.

3.2. ANALYSIS OF THE INTERNAL SURROUNDINGS

After analyzing the external factors that affect the threats in the illicit traffic of firearms. It is necessary to analyze which is the current estate of the import process of firearms in Chile, the legal framework and the traceability as methods of mitigation of this crime.

3.2.1. LEGAL FRAMEWORK

In Chile, the natural and judicial person that wishes to import, or export armament, should request the duly authorization from the “*Dirección General de Movilización Nacional*²¹(D.G.M.N)”, or by means of the control authorities, in accordance with the several documents detailed in the articles 61 and 62, of the Complementary Rules and Regulations for the Law of Arms Control. Later, the testing bench of Chile will be in charge to the firearms certification making the quality, stability and danger control, indicating the exact data of each of them (type, trademark, model, caliber, and the serial number, etc). Subjecting these items to control is mandatory for importers and manufacturers in the event of being rejected will be reported to the origin country or destroy them. It is the Company responsibility.

²¹ Organismo asesor del Ministerio de Defensa de Chile, que satisface los requerimientos del potencial humano, material e industrial requeridos por las instituciones de las Fuerzas Armadas para la movilización nacional.

Then, the DGMN proceed to the samples taking of the shoot effect in projectiles and magazines of bullets and cartridges, then to incorporate the information in the Automated Ballistic Identification System IBIS of all the firearms and ammunitions manufactured in the country or imported.

After of executing the process for identification, certification and ballistic fingerprint, it will continue with the registration of the armament in the “*Registro Nacional de Inscripciones de Armas,*” (The National Record for Arms Registration) will be done by the controlling authority, entering in the database of the DGMN, assigning a unique identification number (ID). The present registration will be performed by a natural person, who is his/her owner or carrier. In the event of juridical persons by its legal representative; in this moment, the user indicates the use of the firearm (personal defense, security and protection, hunt, sport, collection or other authorized by the D.G.M.N).

In order to reduce the effect of blank arms to be adapted or turned into real firearms that shoot ammunitions, the legislator modifies the Law of Arms Control, stating the blank arm as an object subjected to the control, which requires the respective authorization or registration for its use, just for objectives duly stated that are: professional dog training, control of damaging fauna, public events, movie filiation and performing arts or other similar determined by the Complementary Rules and Regulations.

In this sense and according to the several studies performed in this matter, by means of the Resolution Exempt 433 dated on the February 23, 2022, of the Ministry of National Defense. It is forbidden to trade blanks arms of 10 trademarks: Bruni, Ekol, Zoraki, Blow, Leo, Kusey, Carrera, Ceonic, ISSC y Kimar, because they are arms of easy adaptability or transformation for shooting ammunitions, its functioning and easy parts and pieces modifications that have better precisions as a result of the shoot, mainly in the magazines and cannon. (Official Journal, 2022).

3.2.2. PRESENT REALITY IN CHILE

According to the statistical data of the D.G.M.N, along the history, in the National Record of Arms Registration, a total of 845.663 firearms have been registered until 2021, keeping an annual registration rate of 41,5 firearms per 100.000 inhabitants, it is a decrease in the registration from the 1995 to 2021, with an average of 10.755 firearms registered annually.

In relation to the import of firearms in Chile, from 2011 to 2021, it keeps an average of 7.528 firearms registered in the country during this period, prevailing the pistol type firearms, which includes 47, 6% of the total, followed by the shotgun with a 35,1%, while the rest 17,4%, corresponds to rifle, revolver, carbine and other arms.

Between 2018 and 2021, Carabineros de Chile has a total of 13.803 cases²², at national level, linked with transgressions against the Law of Arms Control, such as: illegal possession, unjustified shooting, explosives devices, among others: of the total cases, 2.007 are detentions, in which 10.417 firearms were seized (revolver, pistol, rifle, sub-rifle, gun machine, sub gun machine, carbine, hand crafter arms, blank arm adapted).

Then the proportion of the seized firearms, considered the years under study in relation to the detainees are: one to five, where each detention is linked to transgression against the law of arms control, there is a probability to find five firearms. In relation to the reports, it keeps 11.796, which have been

²² Hechos o sucesos que revisten características de “delito”. Estos casos delictuales, se informan a través de un parte policial al Ministerio Público y estamentos jurisdiccionales.



addressed to the Public Ministry by means of the police reports without finding the criminals nor the evidence.

From the variables of firearms seized at national level by Carabineros de Chile. They are three types: 76,7% of the total seizure, the non-lethal firearms of pistol type are (27,9%), revolver (25,9%) and shotgun (22,9%). However, it is been observed a constant search for increasing the possession of firearms by the criminal organization in order to defend their territory and commit crimes, creating a new criminal phenomenon, that is the acquisition of blanks arms (currently they are forbidden in the country), which are modified and adapted for shooting that cause the same damage of a non-lethal arm. Precisely, between 2018 and 2021, the seizure of arms adapted for shooting has increased in 182%, reflected in the 130 arms adapted and seized in 2018 versus the 367 that were seized in 2021.

In relation to the ammunition seized during 2014 by Carabineros de Chile at national level, it was possible to seize of 43.811 ballistic cartridges of unique projectile, multiple projectiles and those of handcraft made, including the ballistic cartridges of 9mm caliber, the 25,6% of the total. It corresponds to the first place of the total number of seizures, followed by the cartridges of 22 caliber (19,6%) and the 12 caliber (16,6%), here it is observed two calibers that in spite of being for war use, keep an important percentage within the total of the 7,62 mm caliber (4,1%) and 5,56 mm (2,5%), represented with 1.798 and 1.104 ammunitions seized respectively. This situation is relevant to visualize the existing illegal ammunitions of gross caliber import in Chile. War arms such as usually use this: rifle, its use by civilian is forbidden. From it, we can realize about the existence of illicit traffic of arms in our country.

The firearms that are seized in police incidents by Carabineros de Chile are taken to the Criminalistics Department of the Institution, LABOCAR where the ballistic experts analyze the evidence and ballistic nature such as: conventional firearms, blank arms non-modified and blank arms adapted for shooting, by photographic examination, descriptive analysis, estate of conservation, mechanical functioning and shooting capacity if appropriate. Then an expertise ballistic report of the examined item is sent.

In this sense, during 2019 to 2021, 9422 were examined by the Criminalistics Department of Carabineros de Chile, where the 42,4% were blank arms, equivalent to 3994, distributed in 2945 non-modified blank arms and 1049 modified blank arms and adapted for shooting. The criminal organization members have altered the last ones for criminal purposes, or just for causing damage and fear in the citizens. This grants firepower to different criminal gangs of the national territory.

Concerning the different types of the firearms examined by LABOCAR; the pistol of all kinds such as: conventional, non-modified blank arms and blank arms adapted to shooting, including the 55,5% of the total number examined from 2019 to 2021. By this way it is possible to see a trend to reduction in the conventional pistol, that has been reduced in a 49,9% since 2019, from 728 to 365. This situation is in contrast with the examinations performed to the blank pistol arms modified and adapted to shooting, that are increased in 27,7%, from 271 to 346, in the same period. This is based on the above mentioned in relation to the increase in the acquisition of blank arms by the criminal organizations in order to modify and adapt them for shooting, being use in criminal actions and for protection of their territory.

Besides, another relevant phenomenon is observed, that is the handcrafted manufactured ammunition, that corresponds to the 1,3% of the total, equivalent to 564 cartridges, aspect that is linked with the searching by the criminal organizations for increasing their power by creating centers of operations dedicated to modify and alter firearms and ammunitions in order to transform into independent bodies for armament acquisition to be used in criminal actions and protection for their territory.

3.2.3. THE TRACEABILITY AS MITIGATION METHOD OF THE FIREARMS TRAFFIC CRIME

Our country presents several processes that are a great contribution to obtain the traceability of firearms at national and international level whose fulfillment is the responsibility of the manufacturers or importers. One of them is the certification performed by test bench of Chile, which is inserted in the Permanent International Commission (C.I.P) for the test to the portable firearms. Here rules are established to ensure the reciprocal recognition of the marks that are stamped in all the firearms and ammunitions in Chile, just like the other 13 states of the commission perform, where each one has unique mark to identify the original country.

Within the same context, each firearm at national level, keep a unique serial number related to the place of manufacture, type of arm and sequence number of the manufacture year. Besides, it indicates trademark and country of manufacture. The numeral inserted in the firearm are of vital importance for its identification worldwide level. In Chile the serial number of the firearm is entered to the database of the “*Dirección General de Movilización Nacional*” giving a unique firearm identification number (ID), which is transformed in other tool for the country to identify the armament.

As in turn, in Chile, it is possible to determine the traceability of firearms and blank arms adapted for shooting scientifically that are been part of a criminal incident. By means of the use of one of the most advanced technological forensic matter and criminal investigation in our country, we are referring to the Automated System for Identification of Ballistic signs (I.B.I.S), equipment operated by Carabineros de Chile by means of its Criminalistics Department LABOCAR, in its ballistic laboratory and I.B.I.S.

3.2.4. AUTOMATED IDENTIFICATION OF BALLISTIC SIGNS (I.B.I.S) IN CHILE

In our country, the IBIS System is implemented in both police forces, they are: Carabineros de Chile and Investigations Police, the first one corresponds to the Chilean Uniformed Police Force of the country, which performs scientific work, by means of Criminalistics Department of Carabineros de Chile LABOCAR, being the responsible for executing the ballistics examinations of the evidence lifted by the 443 police units at national level. These are entered by certified experts, who are the main actors of the system, since they must verify each one of the HIT23 delivered by the software. After the verification, these must be expressed in the respective ballistic expert report, being informed about the results that go directly to the Public Ministry or agency that requires the backgrounds according to the legislation of our national territory.

Between 2014 to the 2021, the Criminalistics Department of Carabineros de Chile has entered to the database of the IBIS System; a total of 8285 ballistic evidences, cases and projectiles, 2018 was the highest entry 1498. According to the entered elements, a total of 668 HIT along the country was obtained, that enable to relate the several criminal cases with a firearm. This is the vital element for the criminal procedure and traceability of the ballistic evidence.

From the point of view of the police operations and with the intention of achieving a more effective management, Carabineros de Chile has innovated and integrated new applications and technological tools for this purpose.

Since its creation, at the early 90’s from the AUPOL system that enable to register and manage report of police cases, the current criminal analysis system that contemplate geo-referring, satellite images and predicting models as well as the incorporation of the technological systems that make the work on field more efficient. (Carabineros de Chile, 2021). One of the institution platforms is the Territorial

²³ HIT: Coincidencias que permiten asociar evidencia entre sí, ejemplo: 01 HIT se puede relacionar con X evidencias balísticas.



Information Analysis System of Carabineros de Chile S.A.I.T 2.0; consist in a territorial information system that guides the analysis and the knowledge on space distribution of crime. It is aimed at supporting the operative and strategic management of Carabineros de Chile (Ministry of the Interior and the Public Security, 2010).

In this sense, the amount of ballistic evidence entered and analyzed by the IBIS system, the criminalistics Department of Carabineros de Chile LABOCAR has realized that, in spite of the contribution made by this software to the investigations tended to the relation between criminal facts. This special agency together with Criminal Analysis Department were in charge of performing space positioning of the whole evidences entered in the I.B.I.S, by means of the S.A.I.T 2.0, geo- referencing all the original ballistic elements (cases and projectiles) lifted by personnel in charge of the occurrence spot, by this way it was possible to envisage the cases, and detail the number of HIT, the number of the police report, crime and type of evidence.

According to the study made by the Criminalistics Department LABOCAR, revising the ballistic historical evidence entered to the I.B.I.S System of Carabineros de Chile, it was possible to observe 30 entries at national level related to ammunition of 5,56 mm caliber. Here 19 HIT were obtained, 19 firearms 5,56 mm caliber that have participated in different police events and currently they are of civilian possession. It is relevant to say that the present ammunition of 5,56 mm caliber of firearms of war use, such as: assault rifle and gun machines, situation that brings the illegal and clandestine acquisition of this type of armament by the criminal organizations, translated into illegal traffic of firearms and used in criminal actions. The Chilean laws establishes that the only authorized agencies to use arms are the Chilean Armed Forces and Order Forces Carabineros de Chile, basing this hypothesis on the illegal possession by the criminal organizations, which brings different modus operandi for the import of illegal arms of wide caliber to our country.

4. DISCUSSION

Because of the strategic diagnosis mentioned in the previous chapter that characterized the internal and external environment, it was possible to number the strengths and weakness that enabled to identify the opportunities and threats, which the future action must concentrate on, from an individual or collective perspective, in order to create and use the existing capacities. It was also possible to identify threats, where efforts of mitigation should be made, given the weaknesses identified, taking the opportunity with the same objective, the possible strength. All this information is present in the following table, in Power. For systematization of the information effects, the emerging strategies of the Power SWOT analysis is represented in terms of: Increase (SO), Diversification (ST), Targeting or Focus (WO) and Defense (WT).

Table 24. SWOT analysis | Trafficking of arms

Internal factors	Strengths (S)	Weaknesses (W)
	<ul style="list-style-type: none"> • The human being trained and specialist, allow a work according to the needs presented, by this way to perform a scientific work at following the traceability of arms in the country. • The automated system of ballistic signs. (I.B.I.S) proportionate a solid work of the investigations linked to follow up in the use of firearms. • Modification of the Law of Arms and Explosives in updated to the social reality. 	<ul style="list-style-type: none"> • Geographical aspects as long and expense frontier, which have legal paths as well as the large zones where there are illegal paths that do not have personnel to control the entrance and way out of people. • The creation of firearms by means of the 3D printing, which do not keep mechanisms of traceability just like the serial number or other mark that can help to identify the owner, jeopardizing as it turns the ballistic micro signs that are detected by the IBIS System due to percussion mechanism or bore scratched of the arm 3D. • The perimeter of the arm 3d, do not activate the detectors of metals, which affects the detection of items by the agencies responsible to execute the control of legal paths.
<p>External factors</p> <p>Opportunities (O)</p> <ul style="list-style-type: none"> • The technological advance grants an added value of the preventive, investigative and control work. It allows carrying out efficient process in matter of fighting against the arms traffic. In this sense, the use of the technology is useful as support granting concrete evidence. • Composition of Work teams and tables in order to generate a test bench with those proposals and local practices with a positive impact. • To unify a test bench that determine the origin at external level of the illegal entrance of arms 	<ul style="list-style-type: none"> • The creation of synergies and the implementation of information exchange platforms, at the international level. • Unification of the best practices (work tables) taking advantages of the technology used by the I.B.I.S system, creating by this way, a unique ballistic finger print bench, between the police institutions and estate agencies dedicated to the control and proofs of the firearms at word level geo-referencing its use in the criminal act. • Modification of the Law of arms, as to the new modus operandi for shooting and firearms 3D. 	<ul style="list-style-type: none"> • The application of logistics equipment, mainly technological systems, are of great help in the control and prosecution of the crime of firearms, taking into account the entry by authorized and non-authorized steps, considering the extensive national territory maintained by the Republic of Chile. • The evolution of the new modus operandis by the criminal organizations have complicated the detection of these illicit items, such as it is the case of firearms in 3D, that do not present elements of traceability and composed of polimeters, that jeopardize its discover by the metal detectors. • Equipment such as x-rays are of vital importance for the agencies in charge of the control of the species that enter or leave the country.
<p>Threats (T)</p> <ul style="list-style-type: none"> • Arms trafficking affects everyone in a transversal way, increasing its use, being reinforced by aspects implicit in modernity. • The advance of societies consolidated by new technologies and especially globalization, which entails the opening of borders, creating criminal organizations links around the world. (3) The ease of access of firearms by citizens of foreign countries, such as the United States, increases the possibility of arms trafficking to various countries. • The increase in violence by criminals brings with it the acquisition of firearms, for their protection against other organizations or in their effect for the execution of the crime. 	<ul style="list-style-type: none"> • Trained and specialized officers on the different control points will be of vital importance for the detection of these illicit acts, who will be responsible for preventing the entry of firearms into the country, thus avoiding the position of these elements in criminal organizations, cutting the criminal chain before their execution, preventing the commission of crimes against people or property. • The modifications performed in 2022 to the law of arms control, such as: the prohibition of the specific blank arms, more instructive measures in the investigation, higher penalty for sale of ammunitions and the creation of the AND registration; this last idea contribute to the traceability of firearms forcing to improve and specialize the police personnel in the manage of the I.B.I.S system. 	<ul style="list-style-type: none"> • The extensive territorial strip of Chile, allows the Access of illicit elements by different illegal paths, such as sea, land and air, which is uses by the criminal organizations to increase its firepower and be used for the defense or commission of crimes against people and property. It is very relevant to reinforce the control of the species entered or departure of the country. • The constant review of the internal proceedings related to the agencies in charge of control and armament protection. Its storage and shooting mechanism proof are of vital relevance to see the weaknesses that keep those institutions surrounded by activities using firearms, ensuring the correct handling of those items.



4.1. STRATEGIES

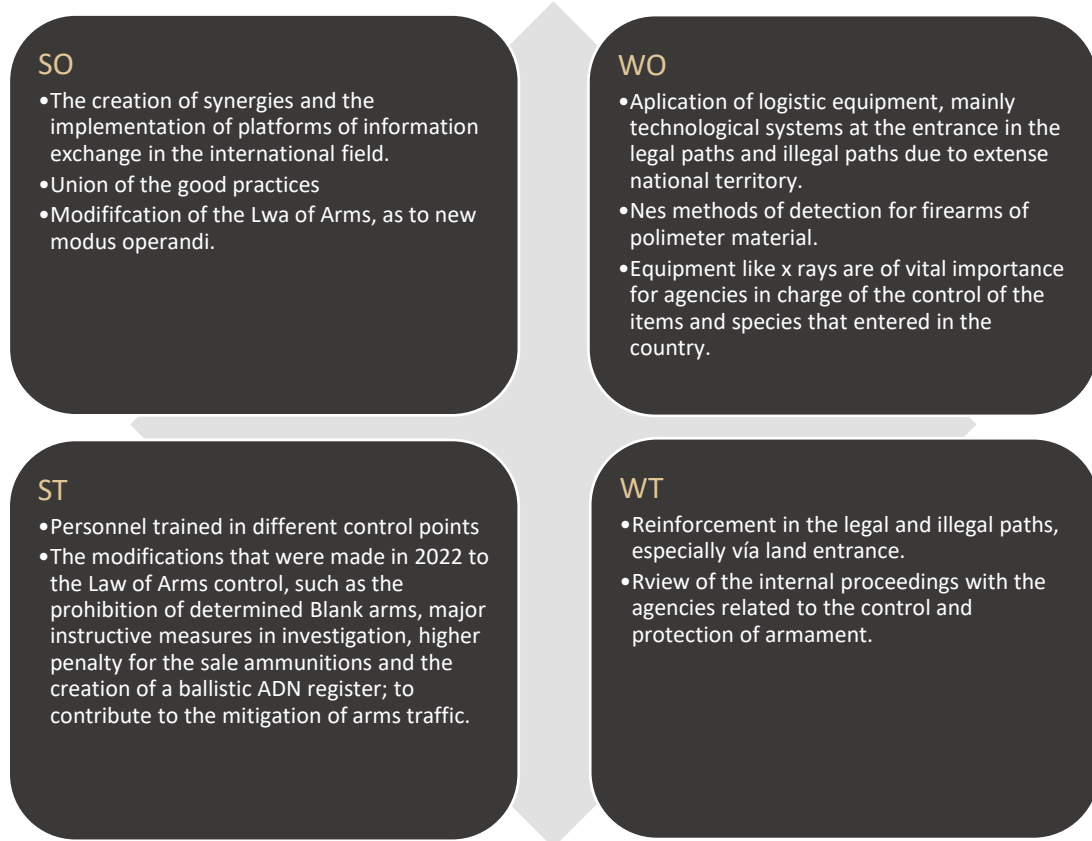


Figure 24. Key strategies | Trafficking of arms

5. CONCLUSIONS & RECOMMENDATIONS

As the results of the strategic analysis explained, there are many ways to increase the efficiency to fight against the illicit traffic of firearms.

The strategies proposed in the dynamic SWOT matrix are as follows:

1. Create international information mechanisms regarding the traceability mechanisms of a firearm (manufacturing serial number, unique identification number of the country's weapon, stamp of the Test Bench, ballistic fingerprint delivered by System I.B.I.S)
2. Creation of an international ballistic fingerprint bank, in relation to the incriminated evidence and entered into the Ballistic Identification System used by police institutions and state agencies dedicated to the control and testing of firearms worldwide, managing to geo-reference the use of the different weapons in criminal acts.
3. Modification in the Arms Control Law, referring to the control element of 3D printers in the creation of firearms and the prohibition of blank weapons that maintain characteristics necessary to be adapted for shooting.
4. Strengthening in the authorized passages, mainly in the terrestrial ones, in order to control the species that cross the borders, increasing the use of technological elements, such as X-rays, which facilitate the detection of prohibited elements.
5. International Judicial Cooperation take the advantage the relations between agencies in charge of enforce the law and judicial agencies.
6. Review and constant control of the agencies in charge of storage and handling of the firearms registered in the country.
7. The creation of specialized equipment in cybercrime that achieve methods of traceability with the purchases of firearms by internet, mainly by means of payment by virtual currency.



REFERENCES

- Aduanas (2021), “Contrabando de armas en Iquique: Aduanas intercepta piezas para armas 30 fusiles”, Chile Aduana Customs, obtenido de <https://www.aduana.cl/contrabando-de-armas-en-iquique-aduanas-intercepta-piezas-para-armar-30/aduana/2021-08-02/122030.html>
- Aduanas (2021), “Importación desde Estados Unidos ocultaba pistola, rifle, municiones, miras, accesorios para armas, radios e incluso medicamentos”, Chile Aduana Customs, obtenido de <https://www.aduana.cl/importacion-desde-estados-unidos-ocultaba-pistola-rifle-municiones/aduana/2021-08-11/173513.html>
- Carabineros de Chile (2021) Plan Estratégico de Desarrollo Policial 2021- 2028, Carabineros del Centenario.
- Cruz, G. De la Jara, A. (2007) Diagnóstico Psicosocial del Territorio: Fuentes y Metodologías para la Intervención a Nivel Local en Materias de Seguridad.
- Gobierno de Chile, “Nuestro país”, obtenido de <https://www.gob.cl/nuestro-pais/>
- Ministerio del Interior y Seguridad Pública (2010), “Gobierno conoce herramientas tecnológicas utilizadas por Carabineros”, obtenido de http://dsp.gob.cl/sitio-2010-2014/n5570_20-07-2010.html
- Oficina de las Naciones Unidas Contra la Droga y el Delito. (2020) Introducción a las Armas de Fuego: Disponibilidad, Tráfico Ilícito y uso Delictivo.
- República de Chile Ministerio de Defensa Nacional Subsecretaria de Guerra (2007) Reglamento Complementario de la Ley N 17.798 sobre Control de Armas y Elementos Similares.
- República de Chile Ministerio de Defensa Nacional Subsecretaria de Guerra (2007) Reglamento Complementario de la Ley N 17.798 sobre Control de Armas y Elementos Similares.
- Ultra Electronics Forensic Technology (2019), IBIS, obtenido de https://www.ultra-forensictechnology.com/wp-content/uploads/2019/05/IBIS_Brochure_2019_SPA_Web.pdf

XIV. PAPER | ENVIRONMENTAL CRIME

Transnational Environmental Crime. The European Framework: A Focus on Italy

Citation:

Bizzotto, M.; Colamedici, J. Overcoming Security Threats arising from Globalization 4.0 – FIEP Association, 2022.

Published: October 2022

Publisher's Note: FIEP stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

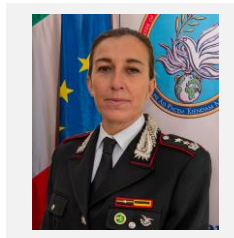


Copyright: © 2022 by the authors.

Italy

Arma dei Carabinieri

Marina Bizzotto¹



Julian Colamedici



¹ marina.bizzotto@carabinieri.it

This study aims to analyse the European relevant C-TEC policies and legal framework, with a brief focus on Italy, and point out some possible emerging strategies and best practices by means of a Dynamic SWOT Analysis.

Abstract: In a world that appears ever more chaotic, unpredictable, and difficult to comprehend, tackling transnational environmental crime (TEC) has become a real challenge for international organizations, governments, and law enforcement institutions all around the globe. Among the others, the European Union and its Member States have developed through the years particularly far-reaching and effective prevention and contrast instruments – even if not always nor everywhere equally successful, due to several political, economic, social, technological, and legal differences. Moving from this consideration, the aim of this paper is to briefly analyse the European relevant policies and legal framework, with a concise focus on the Italian system, in combating environmental crime and provide some possible emerging strategies that may be considered for the future. To this end, the analysis will start with a quick overview of the present international and European context, characterized by a new wave of globalization, currently shrunk by the ongoing pandemic and the resurgence of stark geopolitical strains. A short account of the mentioned prevention and contrast capabilities, grounded on the available related figures and data will follow. The outcomes will conclusively serve as a basis to try to point out some potential strategies and best practices.

Keywords: Environment; Environmental Crime; EMPACT; EU Law; EUROPOL; INTERPOL; ITA Carabinieri.



1. INTRODUCTION

Environmental protection has become one of the founding pillars of a wide range of international actors. The UN SDGs, above all, strongly address the issue. But also, the COP 26, co-chaired by the UK and Italy, and the Next Generation EU, which focuses its objectives towards the so called “ecologic transition”. The European Union, in particular, seems to be one of the most advanced organizations in climatic action, aiming to reach the net-zero carbon emissions level by 2050, and even realize a complete shift to “green power”. Italy, on its part, as a fully-fledged member both of the UN and the EU, is currently implementing an ambitious program of reforms through the National Plan for Recovery and Resilience (*Piano Nazionale di Ripresa e Resilienza - PNRR*, 2021) to spur the development of a more sustainable and environmentally reliable social and economic system. The Green New Deal – as well as the PNRR – has dedicated attention not only to the system but also to biodiversity, wildlife preservation and the fight against any type of illegal trade (log, timber, waste, and endangered species). This social and economic system indeed presents increasing security challenges: one of these, partly exacerbated by the still ongoing globalization process, is the enlargement of environmental transnational crime worldwide. It is a threat that affects all Countries and peoples, with little or no distinction to nationality or political system. Therefore, building a robust and effective framework to uphold environmental protection and help tackle environmental crime, while fully implementing the ambitious UN goals – preservation, mitigation and sustainable development above all – is fundamental. This includes: strengthening judicial systems, enhancing international cooperation for investigation, inflicting effective domestic sanctions, etc. It is also key to consider, while assessing such challenges, not only the main threats and possible solutions, but also the internal and external context in which they occur. To this end, the present work aims to provide a brief and clear-cut overview of the extant institutional and international environment regarding this research sector. In particular, before looking into the European and Italian frameworks, it is worth mentioning the successful experience gained by some members of the FIEP association in this specific field. For example, France, Italy, Spain, and Portugal, have constituted within their own governmental organizations highly specialized environmental units: i.e., the French OCLAESP, the Italian Carabinieri CUFAA; the Spanish SEPRONA and the Portuguese SEPNA – which have so far proved to be a particularly effective way to unite and strengthen national efforts in combating environmental crime – a path that may be hopefully followed also at the international, multilateral level.

2. MATERIALS AND METHODS

This work explains the conceptual framework, presents the recurring data in a strategic diagnosis and discusses the results. Because of the complexity of the subject, the analysis will move from a picture of the current international situation, supported by relevant data, moving then to Italian example and trying to formulate an answer to the central research question. On this regard, it is necessary to acknowledge from the very beginning that the available data and figures cover only a specific period of time and are limited to the visible/estimable or already discovered crimes, while still too large a part of it remains non-estimable or simply unaccountable, and therefore difficult to study and combat.

The present work, being embedded into the 2022 FIEP Publication initiative “*Overcoming Security Threats arising from globalization 4.0*”, is drafted in accordance to the “Strategic Diagnosis” methodology, pointed out as common “research design” by the Association, currently chaired by Portugal (FIEP Portuguese Presidency, Research Paper’s Guidelines – International Affairs Commission, 2022, p. 9). This means, briefly, that the analysis on which the paper grounds its results has been conducted as follows (*Ibid.*, p. 6):

- the “external environment” (grounded on a PESTEL analysis framework), which takes into account “exogenous environmental trends”, with a particular focus on the international perspective – mainly from a European point of view;
- the “internal environment”, related to “the institutions’ intrinsic characteristics and capabilities”, focusing on Gendarmeries and police forces with military status – in this case, the Italian Carabinieri;
- a “combination of the outcomes achieved” by such studies, also with the help of a dynamic “SWOT” matrix;
- a subsequent drawing of the potential “strategies to be adopted” in order to overcome challenges and enhance strengths – inferred on through the aforementioned analysis model;
- a conclusive, comprehensive “list” of those strategies, eventually integrated by possible implementing recommendations and relevant best practices.

3. RESULTS

3.1. ENVIRONMENTAL CRIME - BRIEF EPISTEMOLOGICAL FRAMEWORK: THE EUROPEAN CONTEXT

As emerges from the data, environmental crime is still growing: indeed a 5% to 7% yearly growth in number of offenses has turned it into the fourth largest criminal activity in the world (L. Colantoni, M. Bianchi, *“Fighting Environmental crime in Europe. Preliminary report”*, 2020, p. 5). Though environmental crime is often considered to be a low risk-high profit crime, what is often overlooked is the fact that the money earned through such crimes can finance other violent criminal activities, terrorism, and insurgent groups, as well as undermining the overall wellbeing of communities (Interpol, *“Pollution crime: a decade of changing mindsets”*, 2020b).

Such occurrence implies the need to better understand at the outset the phenomena we are studying, therefore it is necessary to define what “environmental crime” is. To start with, we may take the definition provided by the draft of the European “Environmental Crime Guidance”, which describes it as: *“unlawful conduct that breaches environmental legislation and causes significant harm or risk to the environment and human health”* (European Commission, *“Combating environmental crimes and related infringements: environmental compliance assurance: guidance document”*, 2021, p. 18). Which types of unlawful conduct can then be sanctioned under criminal law and/or administrative law, ultimately depends on the constitutional setting, specifics of criminal law concepts and the wider legal framework chosen by each different Country. Therefore, in order to better point out the different types of crime affecting environment at a transnational level, it could be useful to refer to the Interpol categories to explain their activities and analyse the collected data (Interpol, *“Environmental crime”*). Pollution crime, fisheries crimes, wildlife, and forestry crimes are the four main areas that may need further exploration to better comprehend the wider picture, in which them all are in fact embedded as a part of environmental crime *tout court*.

For the Interpol, it is thus strategically important to:

- identify links connecting pollution crime with other serious violations – such as fraud, corruption, tax evasion, and money laundering;
- coordinate multinational law enforcement operations at a global level to collect intelligence;
- identify relevant trends and risk indicators, to trigger worldwide intelligence led investigations.

Indeed, environmental crime is not that different from more “traditional” forms of organized crime. As reported on Interpol website, the same routes used to smuggle environmentally sensitive commodities across countries and continents are also used to traffic people, weapons, and drugs, frequently hand in hand



with passport fraud, corruption, money laundering and murder (Interpol, “INTERPOL marks a decade of tackling serious organized environmental crime”, 2020a). Tackling illicit financial flows is therefore crucial in tracking corruption networks that facilitate the trade.

In compliance with the EU law and its political priorities, also EUROPOL is widely engaged in combating environmental crime. The agency addresses the issue on its official website, presenting relevant data, its main activities tackling the phenomenon, and highlighting the different impacts that it produces on the environment and human health (Europol, “Environmental Crime”). It could be a different, but still interesting, perspective to comprehend this complex emergency.

Focusing on the negative impacts is a good way to understand that environmental crime is not victimless, but represents serious threats for the long-term humankind survival, such as an increased level of air pollution and pollution of soil, which is the premise to a consistent loss of biodiversity, and ecosystem alteration where common goods are hard to restore once lost. These impacts could become a source of diseases, alteration, and contamination of the food chain, ultimately leading to more disruptive climate change effects. Using the same categories adopted by the aforementioned “Fighting Environmental crime in Europe” report, environmental crime could be subdivided in four main areas, thus allowing an easier and clearer understanding of the phenomenon here addressed (L. Colantoni, M. Bianchi, 2020, p. 10):

- *“illicit waste management”;*
- *“hazardous substances management”;*
- *“illicit wildlife trade”;*
- *“production and use of ozone-depleting substances”.*

In order to tackle and contrast such threats, the European Union has launched the European Multidisciplinary Platform Against Criminal Threats (EMPACT), which regards the environmental crime as one of its chief priorities (Europol, “EU Policy Cycle – EMPACT”, 2022). Recalling the definition provided by the Europol website, quoted above, the EMPACT:

“[...] introduces an integrated approach to EU internal security, involving measures that range from external border controls, police, customs and judicial cooperation to information management, innovation, training, prevention and the external dimension of internal security, as well as public-private partnerships where appropriate”.

The EMPACT has also been recently revised, and the new programme will cover the 2022-2025 period; in particular, on the environmental part, the chief aim is:

“to disrupt criminal networks involved in all forms of environmental crime, with a specific focus on waste and wildlife trafficking, as well as on criminal networks and individual criminal entrepreneurs with a capability to infiltrate legal business structures at high level or to set up own companies in order to facilitate their crimes.”

3.2. ENVIRONMENTAL CRIME - BRIEF EPISTEMOLOGICAL FRAMEWORK: THE ITALIAN CONTEXT

In Italy the apparent trend is similar, as emerges from the collected data available online on the website “Noecomafia” – connected to *Legambiente*, an Italian NGO that advocates for environmental protection and related issues (*Legambiente*, *Noecomafia* website). They elaborate relevant figures on a regular basis – using relevant data from Italian Police Forces and Coast Guard – and publish a yearly account of the Italian environmental crime situation, which they divide in three main categories: “crimes against wildlife and animal welfare” (*Id.*, “*I numeri del racket degli animali*”, 2020), “crimes against health, agricultural and agri-food connected” (*Id.*, “*I numeri dell’agromafia*”, 2020), and “waste trafficking” (*Id.*, “*I numeri dell’illegalità*”).

nel ciclo dei rifiuti”, 2020). Considering the most recent ones, as available on the said website, as exposed in the below figure (Figure 1), we may try to advance some quick, further considerations. The current pandemic has even strengthened such problems: COVID-19 medical waste is indeed generating an overwhelming global demand for medical disposal – a waste crisis that organized crime has been quick to exploit (*Ibid.*).

The aforementioned figure, moving from the data elaborated by *Legambiente*, aims to focus on the current situation and present a first brief comparison between the 2019 and 2020 environmental crime figures in Italy, making thus possible to extract from it some more general considerations.

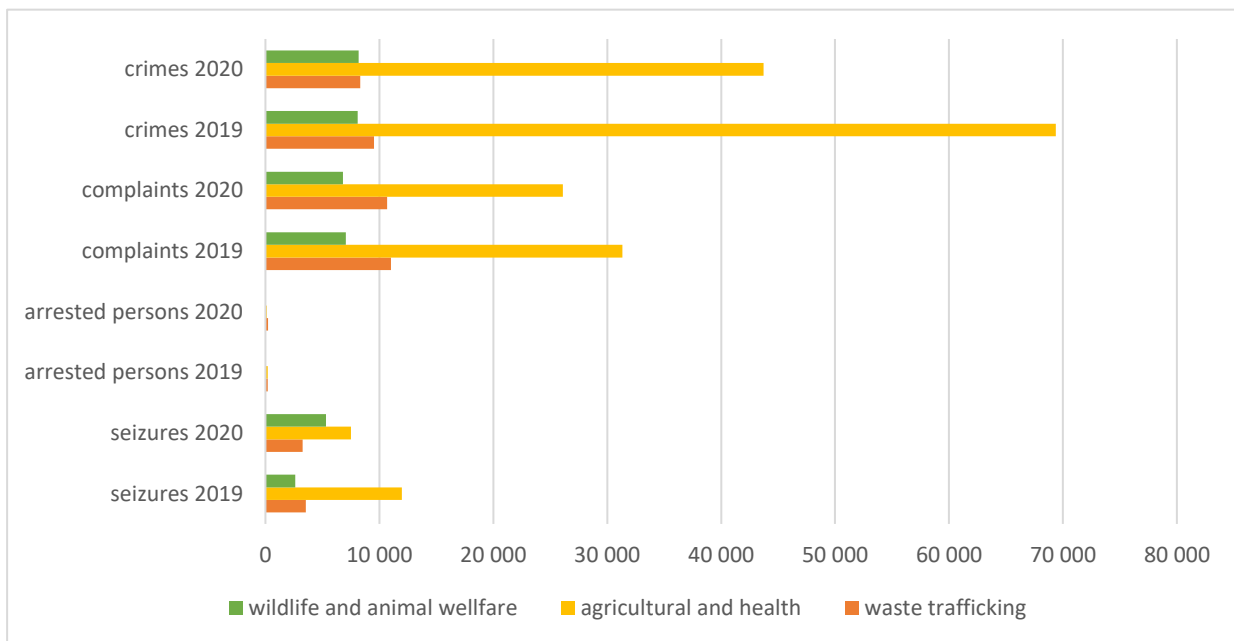


Figure 25. Combating environmental crime - Italian activity 2019-2020²⁴

Looking at the figures above it appears at a first glance clear that the pandemic has somehow hindered the contrast activities, but it is also interesting to underline that the numbers of successful operations remained nonetheless remarkably high and the overall trend seems therefore to proceed in the same positive direction. Environmental crimes ever more frequently – even if not always – have a transnational scope and, as stated before, it has been made also evident that they are usually linked with other different, serious crimes and criminal organizations, sometimes capable of operating all over the world, in several different Countries, in the cyber dimension as well as in more “traditional” ways, at the same time. That is precisely why to further develop, a common ground of contrast strategies and information sharing is of paramount importance for the International Community as a whole.

4. DISCUSSION

As emerges from the analysis conducted above, the complex interrelation between threats, opportunities, strengths and weaknesses allows us to point out several potential strategies and relevant best practices that may be taken into consideration to improve the current prevention and contrast instruments and policies regarding the tackling of environmental crime, which are concisely reported in the below dynamic SWOT analysis (Table 1) and emerging strategies (Figure 2) matrixes (on this point, see also L. Colantoni, M. Bianchi, 2020, pp. 35-36).

²⁴ Drafted by M. Bizzotto. Figure data sources: *Noecomafia* website, as elaborated by *Legambiente* on the basis of Italian Police Forces and Coast Guard data, available online: <https://www.noecomafia.it>, last access: 26/04/2022.



Table 25. SWOT analysis | Environmental Crime

Internal factors	Strengths (S)	Weaknesses (W)
	<ul style="list-style-type: none"> • International, European, and national advanced legal framework regarding TEC • INTERPOL, which regards as strategically important to: identify links connecting pollution crime with other serious violations; coordinate multinational law enforcement operations at a global level to collect intelligence; identify relevant trends and risk indicators • EMPACT, which considers the environmental crime as one of its chief priorities • EUROPOL, which is widely and strongly engaged in combating environmental crime in all its forms • National Law Enforcement Agencies, which are ever more capable to intervene throughout all the national territory and abroad with high skilled personnel thanks to specialised environmental branches (for Italy, the Carabinieri CUFAA) 	<ul style="list-style-type: none"> • Fragmentation of legislation, policies and contrast activities at the international level • Inconsistency of individual contrast strategies and lack of harmonization/homogeneity between states • Different levels of implementation from state to state • Lack of resources • Not fully effective cooperation, coordination, and collaboration among all the actors involved in combating TEC • Still many legal/jurisdictional/operational boundaries among nations
External factors		
Opportunities (O) <ul style="list-style-type: none"> • Brand-new instruments offered by the ongoing development of Information Technologies (IT) and digital services applicable to investigations, prevention strategies and contrast activities • Increasing role of NGOs and civil society in the advocacy for environmental protection, education, and management • Growing sensitivity of the wider public opinion to environment-related issues • Higher political attention to climate change, sustainable economy, and protection of the environment and biodiversity • Occasions posed by global challenges and major crises to better and strengthen current environmental policies 	<ul style="list-style-type: none"> • Strengthen and enhance the common institutional, strategical and legal framework against TEC at the international level, thus diminishing inconsistency and fragmentation • Intensify information sharing among partners and institutions involved in tackling TEC • Involve also non-governmental stakeholders and civil society in the fight against TEC, especially in prevention plans and educational programmes 	<ul style="list-style-type: none"> • Reduce operational differences and normative boundaries between States • Improve and strengthen multilateral international cooperation against criminal threats in a multidisciplinary perspective, following the example of the EMPACT • Simplify even more the procedures for international judicial cooperation
Threats (T) <ul style="list-style-type: none"> • Climate change and loss of biodiversity • Criminal organizations/non-state-actors involved in environmental crime and connected offences 	<ul style="list-style-type: none"> • Sensitize police agents and operators on TEC and systematically develop threats-adapting procedures within Law Enforcement Agencies and relevant institutions, ensuring effectiveness and efficiency also in a complex and rapidly changing environment • Consider the successful experience of the specialized units established by some States (e.g., the French OCLAESF; the Spanish SEPRONA; the Italian CUFAA; the Portuguese SEPNA): a path that may prove effective also at an international level, i.e., considering the opportunity of creating a specific coordinating agency/authority • Enhance public environmental awareness and mainstreaming 	<ul style="list-style-type: none"> • Bring international cooperation, coordination, and communication at a higher level, increasing information sharing and institutional dialogue on the specific issue • Increase systemic resilience and capacity to adapt and mitigate environmental crime's negative impacts • Avoid stereotyping/modelling on fixed parameters when dealing with TEC

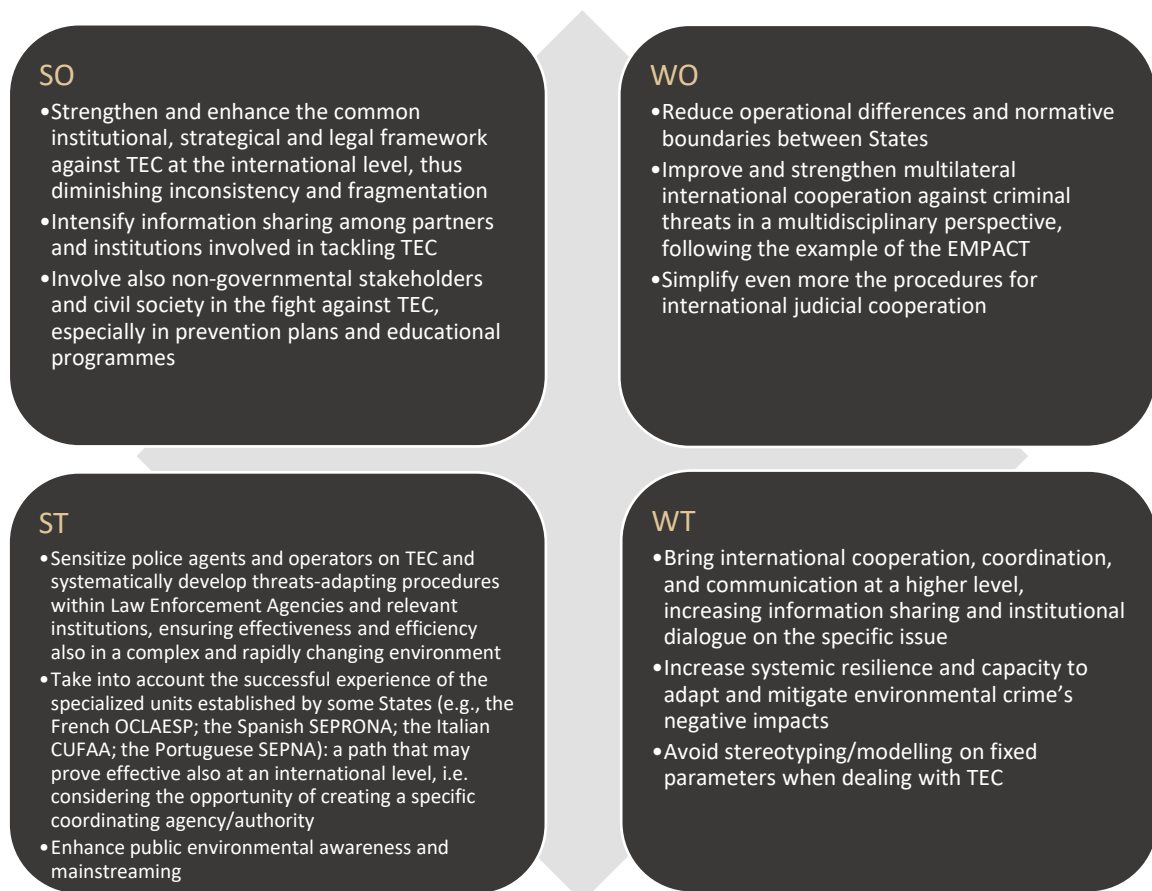


Figure 26. Key strategies | Environmental Crime

5. CONCLUSIONS & RECOMMENDATIONS

Environmental crime is a serious challenge both for national law and order agencies and international organizations, posing a dangerous threat to human health and security, as well as of the flora and fauna with which we share this ever more fragile planet. And it is also deeply pervasive: in recent years, transnational cooperation, information sharing and the implementation of common contrast strategies and best practices – grounded upon a growingly effective international law framework, with some regional and national excellences – has proved to be the most successful course of action to tackle such phenomena. Some instruments, e.g., the EMPACT, could actually show the right way to pursue, even if there is still much work to do: in this respect, also the European Council acknowledged that EMPACT is proving to be effective, increasingly efficient, and consistent with the aims and level of ambition of the EU. The Council, therefore, agreed to implement the EMPACT as a permanent instrument for cooperation to fight organised and serious international crime, driven by member states and supported by EU institutions, bodies, and agencies (Council of the EU and European Council, “The EU fight against organised crime”, 2021). From this point of view, the European Union appears particularly well positioned to foster international cooperation on fighting organised and serious crime, in close collaboration with its partners, allies, and other relevant international organizations, but also with the International Community as a whole, since to truly hope to defeat environmental crime – and thus contribute to preventing climate change and world pollution – a common effort will undoubtedly be required.



Therefore, in order to effectively tackle environmental crime, the better strategy seems to be to further develop the current instruments both at the national and at the international level, ensuring coordination and cooperation among states, organizations, and also the private sector. It is indeed paramount for the ultimate effectiveness of the overall contrast action against such a transnational threat to be closely coordinated with the other involved Countries that may in fact work with different legislations and in different scenarios. Nonetheless, the final aim of such efforts is generally the same: prevent environmental crime, combat it, and protect the environment and the populations from the unrecoverable damages it may cause to them. In pursue of this end, sharing any possible information is key to create a tactical advantage for the international and national actors at any level bestowed with the responsibility to fight this crime. In this respect, Italy could play an even more significant role, presently being particularly well-positioned to spur the countering of transnational environmental crime due to the unique competences developed by its Carabinieri, within which the CUFAA (*Comando Unità Forestale Ambientale e Agroalimentare*) represents the pillar of an articulated environmental protection system that involves several institutional actors, agencies and ministries. Moreover, Italy has developed an advanced and consistent legal framework to deal with environmental crime and more generally protect the environment from damages and abuses. In particular, it is also worth mentioning the “*Testo Unico in Materia Ambientale*”, first adopted in 2006 and last reviewed in 2018 (D. Lgs. n. 152/2006, “*Testo Unico in Materia Ambientale*”).

With this in mind, it is possible to identify some potential emerging strategies and point out a few relevant best practices to further improve the current prevention and contrast architecture both at an international, European and national level. Namely:

1. Involve non-governmental stakeholders and civil society in the fight against TEC, especially in prevention plans and educational programmes, enhancing public environmental awareness and mainstreaming;
2. Bring international cooperation, coordination, and communication at a higher level, increasing information sharing and institutional dialogue on the specific issue;
3. Simplify even more the current procedures for the international judicial cooperation;
4. Improve and strengthen multilateral international cooperation against criminal threats in a multidisciplinary perspective, following the example of the EMPACT;
5. Increase systemic resilience and capacity to adapt and mitigate environmental crime’s negative impacts, avoiding stereotyping/modelling on fixed parameters when dealing with TEC;
6. Strengthen and enhance the common institutional, strategical and legal framework against TEC at the international level, thus reducing inconsistency and fragmentation and diminishing operational differences and normative boundaries between states;
7. Sensitize police agents and operators on TEC and systematically develop threats-adapting procedures within Law Enforcement Agencies and relevant institutions in order to ensure effectiveness, resiliency, and efficiency also in a complex and rapidly changing environment. In this regard, it may be useful to take into account the successful experience of the national specialized units established by some States (e.g., the aforementioned French OCLAESP, Spanish SEPRONA, Italian CUFAA, and Portuguese SEPNA) – a path that may prove effective also at the international level, for instance considering the opportunity of creating a specific intergovernmental coordination agency/authority.

REFERENCES

- Council of the EU and European Council, “The EU fight against organised crime”, official website of the Council of the EU and the European Council, last update: 08/06/2021 (<https://www.consilium.europa.eu/en/policies/eu-fight-against-organised-crime-2018-2021/>), last access: 26.04.2022.
- D. Lgs. n. 152/2006, “*Testo Unico in Materia Ambientale*”, 03/04/2006, as modified by the D. Lgs. n. 21/2018, “*Disposizioni di attuazione del principio di delega della riserva di Codice nella materia penale a norma dell’art. 1 c. 85 l. q della L. 23 giugno 2017 n. 103*”, 01/03/2018.
- European Commission - Directorate-General for Environment, “Combating environmental crimes and related infringements: environmental compliance assurance: guidance document”, Publications Office, 2021, (<https://data.europa.eu/doi/10.2779/035969>), last access: 26.04.2022.
- Europol, “Environmental Crime”, Europol official website (<https://www.europol.europa.eu/crime-areas-and-statistics/crime-areas/environmental-crime>), last access: 26.04.2022.
- Id.*, “EU Policy Cycle – EMPACT”, Europol official website, last update date: 20/01/2022 (<https://www.europol.europa.eu/crime-areas-and-trends/eu-policy-cycle-empact>), last access: 26.04.2022.
- FIEP22 Portuguese Presidency, Research Paper’s Guidelines – International Affairs Commission – 2022 FIEP Publication entitled “*Overcoming Security Threats arising from Globalization 4.0*”.
- Interpol, “Environmental crime”, Interpol official website (<https://www.interpol.int/en/Crimes/Environmental-crime>), last access: 26.04.2022.
- Id.*, “INTERPOL marks a decade of tackling serious organized environmental crime”, Interpol official website, 23/11/2020 (<https://www.interpol.int/en/News-and-Events/News/2020/INTERPOL-marks-a-decade-of-tackling-serious-organized-environmental-crime>), last access: 26.04.2022.
- Id.*, “Pollution crime: a decade of changing mindsets”, Interpol official website, 30/11/2020 (<https://www.interpol.int/en/News-and-Events/News/2020/Pollution-crime-a-decade-of-changing-mindsets>), last access: 26.04.2022.
- L. Colantoni, M. Bianchi, “Fighting Environmental crime in Europe. Preliminary report”, *AMBITUS*, Istituto Affari Internazionali (IAI), 22/10/2020 (https://www.iai.it/sites/default/files/ambitus_pr.pdf), last access: 26.04.2022.
- Legambiente*, *Noecomafia* website (www.noecomafia.it), last access: 26.04.2022.
- Id.*, “*I numeri del racket degli animali (2020)*” (<https://www.noecomafia.it/2021/italia/animali/numeri/i-numeri-del-racket-degli-animali-2020/>), last access: 26.04.2022.
- Id.*, “*I numeri dell’agromafia (2020)*” (<https://www.noecomafia.it/2021/italia/agroalimentare/numeri/i-numeri-dellagromafia-2020/>), last access: 26.04.2022.
- Id.*, “*I numeri dell’illegalità nel ciclo dei rifiuti (2020)*” (<https://www.noecomafia.it/2021/italia/rifiuti/numeri/i-numeri-dellillegalita-nel-ciclo-dei-rifiuti-2020/>), last access: 26.04.2022.
- Piano Nazionale di Ripresa e Resilienza*, 27/04/2021 (<https://www.governo.it/sites/governo.it/files/PNRR.pdf>), last access: 26.04.2022.



Page intentionally left blank

XV. PAPER | HEALTH (PANDEMIC)

Citation:

Cassoré, S.; Health (Pandemic). Overcoming Security Threats arising from Globalization 4.0 – FIEP Association, 2022.

Published: October 2022

Publisher's Note: FIEP stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

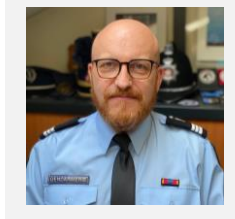


Copyright: © 2022 by the author.

France

Gendarmerie Nationale

Sébastien Cassoré



sebastien.cassore@gendarmerie.interieur.gouv.fr

This study aims to analyse the processes related to the protection of critical infrastructures in a national context in light of the legislative and the European security framework by means of a Dynamic SWOT Analysis.

Abstract: The research theme raises the issue of the ineffectiveness of anti-trafficking measures. Although many efforts are being made by States and the international community to tackle medicine trafficking, this type of crime is still growing. The objective of this study is to draw up an inventory of the current situation and assess the effectiveness of the response provided by States in the fight against medicine trafficking, in order to make it more efficient. The methodology followed in the framework of this study is essentially based on a collection of documents and the analysis of threat assessment. The study shows that this traffic is not sufficiently recognized as a real threat for our modern society, but is considered by the Organized Crime as a real opportunity, considering the risk/benefit balance. Moreover, in the case of transnational trafficking, it is almost impossible to compile the necessary evidence in the countries of origin, transit and destination in the absence of judicial cooperation. It is therefore crucial to advocate for a common legislation at both the national and international levels to effectively combat medicine trafficking.

Keywords: Falsified Medicines, Substandard Medicines, Unregistered Medicines, Counterfeit Medicines, Production and Traffic of Counterfeit/Illegal Medicines



1. INTRODUCTION

The Constitution of the World Health Organisation adopted by the International Health Conference held in New York from 19 June to 22 July 1946²⁵, states, inter alia, that the enjoyment of the highest attainable standard of health is one of the fundamental rights of every human being without distinction of race, religion, political belief, economic or social condition, that the health of all peoples is a fundamental requirement for world peace and security; that it depends upon the closest co-operation of individuals and States, and that the results achieved by each State in the improvement and protection of health are of value to all. The inequality of various countries in improving health and combating diseases, especially communicable diseases, is a peril to all.

Globalisation and the widespread movement of people now create ideal conditions for the emergence of highly contagious infectious diseases. The Covid-19 pandemic was a reminder to the world's population of its vulnerability and the limits of modern science in the face of an unknown and highly contagious virus. Although scientific advances have made it possible to counter the most harmful consequences of this disease with unprecedented speed, our societies have been profoundly transformed, creating a shock felt by all of humanity. This crisis has dramatically highlighted the risk posed by the trafficking of substandard, unregistered or falsified medicines, a recurring public health problem that had previously been met with almost general indifference.

The WHO considers in its guidance summary on its Global Monitoring and Surveillance System for these medicines that "Although millions of people still lack access to the basic medicines they need, the global trade in medicines has grown very rapidly in recent years. Unfortunately, this growth has paved the way for the introduction not only of good, effective and safe medicines, but also of medicines, vaccines and other products that do not meet quality standards and are sometimes toxic. In the worst cases, medicines containing the wrong ingredients can kill or cause serious harm... Increasingly, substandard and adulterated products do not prevent or cure disease... In the case of infectious diseases, this can have particularly pernicious consequences, as incompletely dosed antimicrobials ... kill only the most vulnerable pathogens, contributing to antimicrobial resistance by promoting drug-resistant mutations in the pathogen and its subsequent transmission. When people suspect that certain drugs are unsafe or ineffective, they begin to lose confidence in the drugs and the health system in general. Confidence in an intervention such as childhood immunisation, which is cost-effective and saves lives, can be undermined on a global scale if sub-standard vaccines are found anywhere. The economic impact is also significant. Medicines that neither protect nor cure patients strain household budgets and health systems, attacking the very fabric of society. Criminal falsification affects the financial position and reputation of legitimate generic and innovative pharmaceutical manufacturers." ²⁶

The consequences of the proliferation of substandard or falsified medicines are therefore very wide-ranging and our societies did not seem until now to be very concerned about an issue that was too often seen through the narrow prism of intellectual property and, consequently, as a matter of money that only affected very rich industries that only think about their profits.

Taking into consideration the impact of the pandemic on the trafficking of substandard or falsified medicines, it is therefore interesting to take stock of this type of trafficking with regard to the reactivity of the Organised Criminal Groups (OCGs) specialised in this type of trafficking and to determine the reasons that prevent States from tackling it more effectively:

25 https://www.who.int/governance/eb/who_constitution_en.pdf

26 WHO Global Surveillance and Monitoring System for substandard and falsified medical products : executive summary Geneva – WHO ; 2018 (WHO/EMP/RHT/SAV/2017.01) – Licence : CC BY-NC-SA 3.0 IGO

- What actions have been put in place to combat this traffic?
- How effective are they and what are the possible improvements?

This traffic cannot be reduced to a purely national problem, even if its most dramatic effects are often only visible on this scale. However, this would be to forget that the medicines market is entirely globalised, with production sites far removed from the countries where these products are consumed.

The general objective of this study is thus to evaluate the quality of the response brought by the States in the fight against the traffic of substandard, unregistered or falsified medicines by articulating three objectives which can be declined as follows

- To determine the difficulties encountered by the States to fight effectively against the traffic of counterfeit or falsified medicines;
- To take stock of the actions and mechanisms recommended by the international organisations specialised in the fight against this traffic;
- To formulate recommendations to improve the results obtained by the States and the international community in the fight against this traffic.

The work will be articulated in three parts. The first part will describe the theoretical and conceptual framework of the study, the second part will deal with the methodology used, and the last part will be devoted to the presentation and analysis of the research results.

2. MATERIALS AND METHODS

The first step will be to focus on the theories already developed on the theme in order to have a better perception of the concepts. Then, an answer will be given to the central research question as well as to the sub-questions.

2.1. LITERATURE REVIEW

The World Health Organisation has conducted a number of studies to quantify the problem and understand its impact. In its Global Surveillance and Monitoring System (GMSS) executive summary, it states that "media coverage of fake medicines, particularly those purchased over the Internet, has focused mainly on so-called 'comfort' medicines, such as slimming pills and impotence treatments. Over the past four years, however, the WHO has received reports of substandard and falsified medical products in all major therapeutic categories, from cancer drugs to contraception, antibiotics and vaccines. These reports are not limited to the most sophisticated medicines or the best-known brands: for example, antimalarials and antibiotics are the two medicines that appear most frequently in the database, and reports are almost equally divided between generic and innovator products."²⁷ The organisation estimates that one in ten medicines is falsified worldwide. This figure rises to one in four if only developing countries are considered, according to the organisation's latest report in 2018. For medicines sold on the Internet alone, one in two medicines is a fake, according to the WHO.

The World Customs Organization, in the Illicit Trade Report 2019, examines the global illicit trade in counterfeit and medical goods in 2019. As such, "Medical Products, looks at all illicitly traded and smuggled medical goods, such as medicines, pharmaceutical products and medical technologies, as well as products

27 WHO Global Surveillance and Monitoring System for substandard and falsified medical products: executive summary Geneva – WHO; 2018 (WHO/EMP/RHT/SAV/2017.01) – Licence: CC BY-NC-SA 3.0 IGO



that are counterfeit, genuine products that lack appropriate authorization or licenses and undeclared products. Reported cases and seizures of medical products trafficking increased from 2018 to 2019. “²⁸

For INTERPOL, “pharmaceutical crime is a major global public health concern, with the trade of counterfeit and illicit medical products a truly global criminal phenomenon affecting all countries through source, transit or destination points. Patients across the world put their health and even their lives at risk by unknowingly consuming fake and unregulated medical products, or products that have been altered, diverted, badly stored or have passed their expiry date. Growing consumer demand, the COVID-19 pandemic and widespread use of the Internet has meant that the advertisement, sale and supply of illicit medical products from unauthorized and unregulated websites has become a growing problem in recent years.”²⁹

Concerning EUROPOL, “The trade in counterfeit pharmaceutical products in the EU has been increasing over recent years, ... with medicines appearing as the seventh most-seized products at the EU’s external border. China, India and Singapore were the countries of origin most commonly detected in 2019, while in 2020 Singapore and India were replaced by Turkiye and, to a lesser extent, Vietnam. Criminals rely primarily on post and parcel services to ship counterfeit pharmaceutical products, which are mainly traded online. Weak links in global supply chains are exploited by counterfeiters of pharmaceuticals. This is particularly so when imports involve different countries, importers, retailers and distributors. Free trade zones are also misused in the trade in counterfeits products due to their lighter regulations and limited customs control.”³⁰

The European Union Intellectual Property Office estimates that “the total value of counterfeit pharmaceuticals traded worldwide is estimated to be up to EUR 4.03 billion (USD 4.4 billion). Customs seizure data analysed in the study “Trends in Trade in Counterfeited and Pirated Goods (2019), which covers the period 2014-2016, shows that counterfeit antibiotics, lifestyle drugs and painkillers were the most frequently encountered. This counterfeit trade is facilitated by the growth in small package shipments by parcel post or letter packets, which are more difficult for customs officers to detect. Between 2014-2016, 96% of all customs seizures of counterfeit pharmaceuticals were of postal or express courier deliveries. India and China are identified as the largest producers of counterfeit pharmaceuticals at global level, with Singapore and Hong Kong appearing as the most important transit points in the counterfeit pharmaceutical supply chain.”³¹

The Institute for Research on Counterfeit Medicines (IRACM), created in 2010 to combat this scourge, estimates in a 2015 publication that “more than 40% of medicines tested worldwide do not meet the required standards. Up to 70% of medicines used in Africa are fake. In France, counterfeit medicines account for 1% of medicines purchased. In poor countries, illicit medicines are mainly antibiotics, anti-malarials and anti-retrovirals. In rich countries, stimulants (amphetamine) and anti-cancer drugs are more affected. In 2011, counterfeit medicines accounted for 24% of customs seizures in Europe, ahead of cigarettes.”

28 www.wcoomd.org - COMP: 2020/2

29 <https://www.interpol.int/fr/content/download/17130/file/IGGH-pharmaceutical%20crime-Factsheet.PDF?inLanguage=eng-GB>

30 Intellectual Property Crime Threat Assessment 2022 – EUROPOL – EUIPO - ISBN 978-92-9156-310-4 doi: 10.2814/830719 TB-08-22-009-EN-N

31 https://euipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/Trade_in_Counterfeit_Pharmaceutical_Products/Trade_in_Counterfeit_Pharmaceutical_Products_en.pdf

2.2. CONCEPTUAL FRAMEWORK

A number of concepts are important to master concerning medicine trafficking. Indeed, it is important to make a clear distinction between counterfeiting, which is mainly related to Intellectual Property issues, and falsification. Moreover, the risks linked to medicine trafficking are intimately linked to the principles of Availability, Accessibility and Affordability, concepts which can be considered as one of the root causes of the existence of this type of trafficking.

2.2.1. DIFFERENCES BETWEEN COUNTERFEITED MEDICINE, SUBSTANDARD MEDICINE AND FALSIFIED MEDICINE

The World Health Organization adopted in May 2017, during the World Health Assembly, precise working definitions to qualify falsified medicines.

For each falsified medical product (medicine, vaccine and medical device), the WHO thus distinguishes three categories of situations, which we will explain below: "substandard products", "unregistered products" and "falsified products" :

- **Substandard products:** these are products that have not been manufactured in accordance with good manufacturing practices and do not meet quality standards. The causes can vary: storage in poor conditions (e.g. paracetamol that has become damp and the tablets blackened) or the use of the wrong active ingredient by mistake.
- **Unregistered products:** these are products that have either not been assessed according to the procedures laid down, or have not been approved, or neither.
- **Falsified products:** unlike substandard products, these are products that have been knowingly falsified by the manufacturer. While the packaging perfectly imitates that of the real medicine, the medicine contains too little or too much active ingredient or no active ingredient at all (often replaced by cornstarch, potato starch, chalk or saline), or even substances that are toxic to human health (e.g. antifreeze has been found in falsified medicines).

In some countries, even a genuine product is considered falsified if it has been fraudulently removed from the legal chain.

On the contrary, other administration can talk about counterfeit products:

- **Counterfeit medicine:** A medicine made by someone other than the genuine manufacturer, by copying or imitating an original product without authority or rights. Counterfeit medicines infringe trademark law.

The Directive 2011/62/EU of the European Parliament of the Council of 8 June 2011 define exactly the falsified medicinal product as any medicinal product with a false representation of:

- its identity, including its packaging and labelling, its name or its composition as regards any of the ingredients including excipients and the strength of those ingredients;
- its source, including its manufacturer, its country of manufacturing, its country of origin or its marketing authorisation holder;
- its history, including the records and documents relating to the distribution channels used.



2.2.2. THE 3 A'S PRINCIPLE

Access to medicine can be considered according to the three criteria of Availability, Accessibility and Affordability. These criteria can also be scrutinised as they may provide clues as to the risks of trafficking that may take place:

- **Availability:** Make sure new medicines are present in countries. **Shortages or other problems with the availability of medicines create challenges for the medicine supply chain, with a potentially serious impact on human and animal health.**
- **Accessibility:** Make sure people can get hold of the medicines. The issue of access to medicines is a fundamental component of the full realization of the right to health. Medical care in the event of sickness and the prevention, and treatment and control of diseases, depends largely on timely and appropriate access to quality medicines.
- **Affordability:** Make sure people have enough money to buy the medicines. Equitable access to essential medicines and other medical technologies depends on affordable pricing and effective financing. Promoting fair prices and cost-effective interventions is central to the achievement of universal health coverage.

3. RESULTS

In a first part, endogenous and exogenous strategic environments are going to be analysed using a PESTEL analysis where the factors that affect the Political, Economic, Social, Technological, Environmental and Legal aspects of the health system are going to be considered.

After that, the results of the documentary research will be presented in a SWOT table and then analyzed to bring an answer to the aforementioned research questions.

Then, the best strategies to tackle medicine trafficking will be listed according to the actual state of play.

3.1. EXTERNAL ENVIRONMENT ANALYSIS

Table 26. PESTEL analysis | Health (Pandemic)

Factors	Key Macro Trends	Implications for Security Forces
Political & Legal	<p>P.1. Legislation is not globally homogeneous</p> <p>P.2. Definitions of the different type of medicines are not globally shared</p> <p>P.3. Police and judicial cooperation between countries is often made difficult</p> <p>P.4. The fight against fake medicines is not always a priority in the societies in which they circulate the most</p> <p>P.5. The health systems and the access to medicines is quite different between each country</p>	<ol style="list-style-type: none"> 1. Need for effective international cooperation systems 2. Need for training and specialisation of each organisation 3. Increasing concerns for the Protection of the Civilians 4. Need for harmonising the legal framework throughout the world concerning this kind of crime 5. Need for alerting the population concerning the risks represented by this type of crime 6. Raising political awareness of the risks associated with this type of crime
Economic	<p>E.1. Countries that are producing the medicines are oftenly not the one which are consuming them</p> <p>E.2. Shortages or other problems with the availability of medicines create challenges for the medicine supply chain</p> <p>E.3. Medicines are high value products</p> <p>E.4. The health of local and national economies greatly influences people's access to health</p> <p>E.5. Private sector collects a lot of information about their products, including counterfeiting and theft</p>	<ol style="list-style-type: none"> 1. Need for the effectiveness of the cooperation between police and judicial authorities 2. Determine precisely the countries where false medicines is produced 3. The increase in economic inequalities increases phenomena related to crime 4. Increase role of private sectors in the security field 5. Secure and monitor the distribution chain to avoid diversion and theft
Social	<p>S.1. Massive demand for treatment</p> <p>S.2. Globalisation and the widespread movement of people now create ideal conditions for the emergence of highly contagious infectious diseases</p> <p>S.3. Widespread mistrust of institutions and politicians</p> <p>S.4. Massive misinformation through social networks</p>	<ol style="list-style-type: none"> 1. Anticipate the risks linked to the availability of products and to loop-holes generated by the administrative and legal framework 2. Improving illicit shipments and interception capabilities 3. Monitor networks and detect trends in new miracle treatments that may create opportunities for criminals
Technological	<p>T.1. The technology needed to produce medicines is accessible and inexpensive</p> <p>T.2. The globalisation of markets leads to a circulation of goods that is difficult to control</p> <p>T.3. Use of cyberspace and social network to order medicines that are not available</p> <p>T.4. Use of cryptocurrencies and webbanks</p>	<ol style="list-style-type: none"> 1. Involves the understanding and establishment of intelligence led policing 2. A need to introduce and apply tools that enable the processing of huge amounts of information 3. Need to create specific units in the security forces in order to deal with criminal phenomena perpetuated through the use of technological tools 4. Monitor the cyberspace to detect criminal activities 5. Increased demand of training in this area
Environmental	<p>EN.1. Falsified medicine endangers health and prolong illness, promote antimicrobial resistance and the spread of drug-resistant infections</p> <p>EN.2. Massive deforestation is encouraging the emergence of new diseases</p> <p>EN.3. Falsified medicines waste resources</p> <p>EN.4. Falsified medicines can pollute the environment during the manufacturing process</p> <p>EN.5. Falsified medicines can pollute the environment when discarded and used</p>	<ol style="list-style-type: none"> 1. Deforestation has a strong potential to create the conditions for new diseases to emerge and spread, creating though new needs 2. Increase the effort to tackle falsified medicines trafficking is a necessity to avoid infections resistance 3. Improve access to health system 4. Improve access to affordable medicines to avoid the use of illegal networks



3.2. INTERNAL ENVIRONMENT ANALYSIS

Following the external analysis concerning the factors affecting health, the McKinsey 7S Model is used to analyse the current situation of law enforcement in order to address them. This model identifies Structure, Strategy, Systems, Skills, Style, Staff and Shared Values.

3.2.1. STRUCTURE

As we saw before, this topic is merely specific and somehow very different from the common topics faced by law enforcement agencies in their day-to-day work. Thus, security forces often find themselves unarmed when confronted with this type of crime. This kind of infringement needs to be addressed properly and it is quite impossible if there is no specialized units. In France, for instance, the Central Office against Environmental and Public Health Crime is a specific judicial unit that is designed to investigate organised crime groups, but more importantly to support investigators and provide trainings to law enforcement agencies. This is in line with the recommendations made by the leading international bodies on this subject. This specialisation must as well be extended to the judicial system, insofar as magistrates must be able to fully understand the offences identified by investigators and thus prosecute the perpetrators in the best conditions.

3.2.2. STRATEGY AND SYSTEMS

ONUDC consider in this specific matter that despite the growing nature of the problem, legal systems around the world are facing numerous challenges in effectively combating these crimes. Such challenges include weak or inconsistent legal frameworks and ineffective criminal laws that often fail to criminalize attempt, participation by accessories and the possession and sale of illegally obtained products. Online and distance selling of medical products are also growing concerns but are often still inadequately addressed. Many medical product sector specific laws are inadequate and not harmonized with other laws and international standards. Some laws lack definitions, provide for insufficient penalties and fail to designate offences as predicate offences in anti-money laundering. National and international strategies must therefore be put in place, building on existing initiatives in this field, such as that of the WHO, UNODC or the Council of Europe's MEDICRIME Convention. There is a critical need to combat the global threat posed by the counterfeiting of medical products and similar crimes.

3.2.3. SKILLS

Law enforcements agencies should take the necessary measures to provide training and technical assistance necessary to enhance their ability to prevent, combat and eradicate counterfeiting of medical products

3.2.4. STYLE

In the security forces, the standard operating procedure is based on a well-defined hierarchy. Military status emphasizes this, even if it is less rigid than it was in the past. The hierarchy is still central, but the relationship between the different levels of command and the subordinates is more often than not based on flexibility and increased trust.

3.2.5. STAFF

There are few specialists in public health crime within the security forces. However, real effort have been made to provide quality training, partly online and partly face-to-face. Rewarded by the recognition of this speciality, which is subject to regular refresher courses, this qualifying training enables staff in the field and managers to rely on a contact level and to obtain very quickly adapted advice on this specific problem.

3.2.6. SHARED VALUES

Security forces in all countries share similar values. This is even more true for police forces with military status, which rely on strong values, such as honour, sacrifice, loyalty, austerity, discipline, abnegation, beneficent spirit:

- *Honour: is the idea of a bond between an individual and a society as a quality of a person that is both of social teaching and of personal ethos, that manifests itself as a code of conduct, and has various elements such as valour, chivalry, honesty and compassion.*
- *Sacrifice: Danger or serious work to which a person is subjected, an act of self sacrifice inspired by a sense of duty. It means subordinating one's own life or well-being for the sake of others.*
- *Loyalty: Compliance with the demands of fidelity and honour.*
- *Austerity: Moderation of the senses and passions in the face of higher goals such as the performance of duty.*
- *Discipline: Doctrine, instruction of a person. The meaning implies the observance of principles of obedience that only knows the moral limit of honour and the material limit of the Law.*
- *Abnegation: Sacrifice of one's will, affectations or interests, usually for professional reasons or altruism.*
- *Beneficent spirit: Benefactor, doing good for the others. Considering the needs of others above one's own.*



3.3. DYNAMIC SWOT ANALYSIS

Table 27. SWOT analysis | Health (Pandemic)

Internal factors	Strengths (S)	Weaknesses (W)
	<ul style="list-style-type: none"> • Drug delivery circuit • Establishment of links between the public and private sectors • Existence of specialised police and justice services • Existence of international bodies involved in the issue 	<ul style="list-style-type: none"> • Communication between police services • OCG detection capabilities • Cyber capabilities • International legislation related to drug trafficking / MEDICRIME Convention
External factors		
Opportunities (O)	<ul style="list-style-type: none"> • Securing the medicine distribution system • Anticipating risks of harm to the medicine distribution chain • Anticipating medicine and medical device shortages to anticipate products targeted by OCGs 	<ul style="list-style-type: none"> • Improving the transmission of police and customs information and promoting cooperation in order to hinder the action of OCGs • Raise awareness of this type of crime in international bodies and promote harmonisation of international legislation • Facilitate access to care and medicines
Threats (T)	<ul style="list-style-type: none"> • Communicating widely on the risks to consumers when buying outside the distribution chain • Establish partnerships with the private sector to increase capacity for analysis and control and detection of new modus operandi • Advising production and distribution companies on securing their facilities 	<ul style="list-style-type: none"> • Strengthen cyber capacity and provide training on the subject • Standardize international legislation based on the Medicrime Convention and UNODC recommendations • Strengthen and facilitate international police and judicial cooperation • Map and integrate all actors in national and transnational judicial operations

3.4. EMERGING STRATEGIES

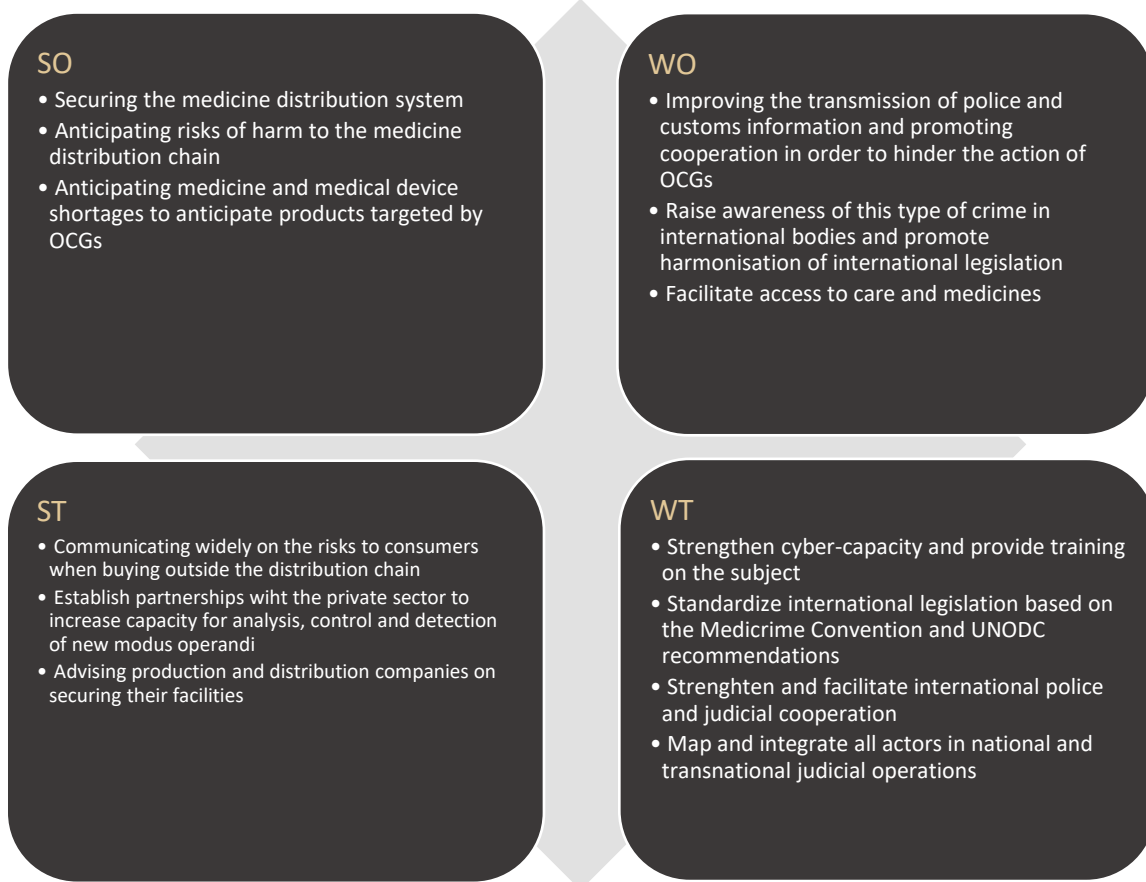


Figure 27. Key strategies | Health (Pandemic)

4. DISCUSSION

10 to 20 times more profitable than heroin trafficking according to Interpol, trafficking in health products has been developing very rapidly for several years and is now a real public health issue. A real scourge in the USA, causing nearly 115 deaths per day, the consumption of opiate derivatives became the leading cause of overdose in France in 2018 according to the annual report of the National Agency for the Safety of Medicines (ANSM).

In France, medicine trafficking has a strong impact on society by fuelling a constantly growing underground economy and causes major public safety problems (violence, aggravated theft, etc.). This type of crime causes, in particular, serious damage to fragile populations that have recently arrived on the territory as a result of illegal migratory flows: the case of unaccompanied minors (UAMs).

4.1. DIVERSIONS OF USE

Despite a particularly well-regulated medicine distribution system, France is affected by trafficking in falsified medicines. Diversion of medicines from their intended use is a major concern and is constantly increasing. This involves the use of substances intended to treat certain pathologies not for their therapeutic purpose (pain, sleep disorders, anxiety or drug dependence) but because of the side effects that accompany their consumption. While some of them cause hallucinations, others make it possible to endure fatigue, remove inhibitions or improve physical performance (Subutex, Artane, Tramadol, Tranxene, Rohypnol, Temgesic, etc.).



Fentanyl is a serious threat among medicines that are misused. A particularly powerful opiate intended to relieve pain in the treatment of serious pathologies, it is used as a narcotic. The risks associated with its use are reflected in the high number of overdoses in North America, where it is particularly popular. Also sought after in Europe, this medicine or its veterinary derivatives are sometimes combined with conventional drugs, thus multiplying their effects and, above all, the risks of overdose. Fentanyl and its derivatives require special attention.

The medicines classified as benzodiazepines¹ (Rivotril/Clonazepam and Lyrica and Pregabalin) have devastating effects. Their use is particularly popular with unaccompanied minors. The use of these psychotropic drugs gives rise to street violence (knife attacks, violent robberies), which contributes to a feeling of insecurity in certain areas of large cities, particularly around drug dealing points. Algeria and Morocco have been confronted with this phenomenon for more than a decade and have noted, for their part, the rise of trafficking from French territory, which is the main supplier of medicines that have left the legal chain.

Especially since 2019, the trends observed attest to an upsurge in the illegal procurement of high-value medicines (particularly anti-cancer or anti-hepatitis C) using false prescriptions. These medicines are collected illegally from pharmacies and are likely to be resold abroad by organised criminal networks. In addition to the risks to public health associated with the uncontrolled distribution of pharmaceutical specialities intended for serious diseases, these offences generate a very high level of damage to health insurance and can have an impact on the availability of treatments (risk of shortages).

4.2. ONLINE SALES

The strict regulations governing certain substances (erectile dysfunction, anxiety or sleep treatments) are being circumvented by illegal structures trying to position themselves on a particularly profitable market. While French law applies to companies established on French territory, online pharmacies located abroad are multiplying without authorisation and without complying with the obligations specific to the customers' countries of origin. The lack of harmonisation of the law in this area facilitates this trade.

The result is the availability of falsified products on the world market, distributed without control. The risks to consumers, who are sometimes unaware of the illegal nature of online sales sites, are high. In addition, there is a significant loss for the laboratories affected by this illegal trade and a proven risk of selling counterfeit products.

At the same time, more and more dark web markets are offering such products. Sales concern both commercial products (falsified, counterfeit, stolen) and active ingredients, packaging (allowing the resale of fakes) or excipients. Anonymity is sought by darkweb users who are adept at encrypted communications, virtual currencies and other means that limit the risks of identification.

4.3. DOPING

Many medicines are used because of their effects on the performance of their users. The sports code provides for and punishes doping in the sports world, while the public health code deals with the behaviour of consumers who are not qualified as "sportsmen" under the law. Elite doping remains very discreet and is essentially aimed at professionals supported and supervised by a technical and medical team that benefits from the latest innovations in terms of concealing doping substances. At the same time, the consumption of such products is increasing, mainly in fitness and body-building centres or in prisons. The cult of the body, performance and physical beauty, amplified by social networks, encourages the search for ever more effective, faster or less effortful methods. The result is the increasing consumption of medicines that are not

used for their intended purpose, without any medical control.

This mass doping is mainly fed by the Internet. A number of online sales sites allow medicines and doping substances to be imported into France. Moreover, practices are widely documented on forums and other sites, allowing neophytes to start "treatment" protocols without prior knowledge. Criminal structures organise themselves and distribute the flows in different foreign countries. This makes logistical, financial and commercial activities more difficult to trace. Investigations have shown that these goods transit by sea or air from Asia. However, as the controls carried out are becoming more and more effective, a change in the flows has been noted. Eastern European countries (Slovakia, Bulgaria, Turkiye, Poland) are now among the shippers. This proximity leads to an increase in trade by road. Depending on the distance and value of the substances, hand delivery is becoming more common. The road transit points to France are identified as Switzerland, Belgium and Luxembourg. In addition to ports and airports, internal road flows and border crossings require increased vigilance.

There has been an increase in the trade in growth hormones, whether falsified or not. These very expensive products are prized for their effectiveness, arousing the interest of both consumers looking for guaranteed results and suppliers who see additional profits.

4.4. OPPORTUNISTIC TRAFFICKING

Following the COVID 19 health crisis, which France has been facing since February 2020, new types of trafficking have developed. Playing on people's fears and on the lack of supplies caused by the closure of borders, opportunistic traffickers have developed multiple illicit activities, mainly involving fraud, sales of protective devices outside the official markets (mask, hydroalcoholic gel), "miracle" medicines and solutions for treating waste from infectious activities. Law enforcement agencies have had to deal with nearly 200 cases of this type in the first six months of the crisis.

For several months now, illegal activities have focused on trafficking in false health passes. Here again, fraudsters have developed very elaborate hacking techniques, including of health professionals' websites to fraudulently generate vaccination certificates. Sales of these fraudulent passes are mainly made via social networks throughout the country and overseas. By the end of 2021, nearly 200,000 false certificates had been generated and nearly 400 investigations had been opened; some crooks were said to have made over €2 million in profits.

4.5. THE IMPACT

The consequences of trafficking in health products are significant:

- Population health (increase in addictions and overdoses)
- Public finances (imbalance of the social security system, hospitalizations, treatments)
- Everyday crime linked to the underground economy (burglaries, violence, etc)
- Economic damage to the pharmaceutical industry



4.6. OVERALL EVOLUTION OF OCG ACTIVITY:

Criminal organisations invest massively in this type of trafficking and implement measures designed to hinder the action of investigative services: financial flows are dissociated from logistics, which are in turn separate from the technical administration of the sales sites.

In the most complex cases, the structures set up are spread over several countries in order to take advantage of gaps in international cooperation. The increasing use of non-collaborative hosting services further complicates investigations.

In the context of mass diversions of substances used as psychotropic products, the structures commonly implemented are based on three hierarchical levels:

- collectors who are prescribed medicines by several doctors and then acquire them from several pharmacies (medical nomadism);
- wholesalers who centralise these medicines by employing several collectors, sometimes spread over a large geographical area
- exporters in charge of transporting the products to their destination abroad.

The lack of interconnection and traceability between the various prescription and delivery sites of the medicines makes it possible to multiply purchases while having them reimbursed by the social security system. In some cases, criminals use false documents or take advantage of the complacency or even the complicity of health professionals. They also use means typical of serious crime to conceal their actions: "disposable" telephones, encrypted messaging, scrambling devices, use of "nannies" and "mules". The dissociation of financial and logistical flows is facilitated by the massive use of the Internet.

5. CONCLUSIONS & RECOMMENDATIONS

Consumption of medicines out of a medical framework continue to be a social problem favouring illegal activities. The purposes of the misusing are various (psychotropic, recreational or performance enhancing), as well as the ways of consumption: absence or non-respect of a medical prescription, injection of non-injectable products (sublingual pills, patch contents, eye-drops...), and resale of medicines prescribed in the framework of a medical treatment. Moreover, COVID-19 pandemic emergency has significantly increased this threat, covering both medicines (including vaccines and supplements allegedly claiming curative/preventing effects) and other sectors like medical devices, biocides and sanitary products.

This abnormal consumption of medicines causes a growing demand that cannot be legally met and generates trafficking, mostly based on diversion from the legitimate supply chain. In addition, because of this growing demand, falsified medicines are inserted among those diverted from the legal chain. It even happens that some of these falsified medicines are re-introduced into the legal supply chain, through the parallel market.

Falsified medicines are manufactured in underground laboratories where criminals work in lack of any safety measures. This exposes the consumers to health risks by the consumption of these illegal products. In the best case, they will not produce the effect they are supposed to and the patient will not be treated.

Trafficking of medicines is a well-known and growing issue in the European Union and Third countries. Numerous cases highlighted large scale trafficking and confirmed that this criminal activity is as lucrative and even more than narcotics trafficking. This situation leads serious and organized crime to take over this business.

Beyond the tremendous benefits gained by the traffickers, this trafficking seriously harms the Public Finances and the Social Care System of some Member-States through the loss of millions of euros. It also alarmingly affects Public Health, especially because of the treatment of the addiction behaviours, overdoses as well as stock shortage.

The research results identified a series of obstacles that make state actions to combat medicine trafficking less effective. This is partly due to the lack of global and regional harmonisation on this issue, as it can only be considered by some states as a matter of intellectual property law. The risk for criminals is thus far too low. In addition, certain actors in the justice system, namely judges and police officers, are not sufficiently aware of this kind of traffic, that is perceived as less important from the point of view of law enforcement than drug trafficking.

Consequently, it becomes judicious to develop new strategies of struggle to improve the response brought by States to combat this unrecognized scourge. A global and inclusive approach at both national and international levels must be adopted, building on the many existing initiatives (UNODC, EU MediCrime Convention...). These strategies must imperatively include prevention measures and international cooperation mechanisms for prosecution and repression.

Based on the results of the study, the following strategies could be adopted:

In terms of growth, it would be interesting to adopt the following strategies:

1. Securing the medicine distribution system;
2. Anticipating risks of harm to the medicine distribution chain;
3. Anticipating medicine and medical device shortages to anticipate products targeted by OCGs;

In terms of targeting, the following strategies could be adopted:

1. Improving the transmission of police and customs information and promoting cooperation in order to hinder the action of OCGs;
2. Raise awareness on this type of crime in international bodies and promote harmonisation of international legislation;
3. Facilitate access to care and medicines.

Concerning diversification, the following strategies would be interesting to consider:

1. Communicating widely on the risks to consumers when buying outside the distribution chain;
2. Establish partnerships with the private sector to increase capacity for analysis and control and detection of new modus operandi;
3. Advising production and distribution companies on securing their facilities.

Finally, in terms of defense, these strategies could be followed:

1. Strengthen cyber-capacity and provide training on the subject;
2. Standardize international legislation based on the Medicrime Convention³² and UNODC;
3. Strengthen and facilitate international police and judicial cooperation;
4. Map and integrate all actors in national and transnational judicial operations.

³² Council of Europe Convention on the counterfeiting of medical products and similar crimes involving threats to public health (CETS No. 211) - <https://rm.coe.int/168008482f>



REFERENCES

- UNODC – United Nations Convention Against Transnational Organized Crime And The Protocols Thereto - <https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf>
- WHO Global Surveillance and Monitoring System for substandard and falsified medical products : executive summary Geneva – WHO ; 2018 (WHO/EMP/RHT/SAV/2017.01) – Licence : CC BY-NC-SA 3.0 IGO
- WHO - https://www.who.int/governance/eb/who_constitution_en.pdf
- WCO – Illicit Trade Report 2019 - www.wcoomd.org - COMP: 2020/2
- INTERPOL – IGGH-Pharmaceutical Crime Factsheet
<https://www.interpol.int/fr/content/download/17130/file/IGGH-pharmaceutical%20crime-Factsheet.PDF?inLanguage=eng-GB>
- EUROPOL - Intellectual Property Crime Threat Assessment 2022 – EUROPOL – EUIPO - ISBN 978-92-9156-310-4
doi: 10.2814/830719 TB-08-22-009-EN-N
- EUIPO – Trade in Counterfeit Pharmaceutical Products
https://euiipo.europa.eu/tunnel-web/secure/webdav/guest/document_library/observatory/documents/reports/Trade_in_Counterfeit_Pharmaceutical_Products/Trade_in_Counterfeit_Pharmaceutical_Products_en.pdf
- DIRECTIVE 2011/62/EU OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 8 June 2011 amending Directive 2001/83/EC on the Community code relating to medicinal products for human use, as regards the prevention of the entry into the legal supply chain of falsified medicinal products
<https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:174:0074:0087:EN:PDF>
- Council of Europe Convention on the counterfeiting of medical products and similar crimes involving threats to public health (CETS No. 211) - <https://rm.coe.int/168008482f>

XVI. PAPER | CBRN

Citation:

Anwar W., CBRN. Overcoming Security Threats arising from Globalization 4.0 – FIEP Association, 2022.

Published: October 2022

Publisher's Note: FIEP stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors

Kuwait

Kuwait National Guard (KNG)

Lt.Col. Waleed Anwar¹
Head of International
Relations Coordination (IRC)



Maj. Abdullah Nasser Aziz²
1st Staff Officer
International Organizations



KNG Address: Farwaniya Governorate \ Reggae - Sheikh Zayed Bin Sultan Al Nahyan Road (5th Ring Road) crossing Mohammed bin Al Qassem Street | Email: ¹waleed@kng.gov.kw | ²a.nasser@kng.gov.kw

Abstract: In the last three decades, the world has witnessed a significant increase in the consumption and usage of materials in a general sense. In an attempt by humanity to improve the quality of life and generate energy using various means, it became apparent that there is an increase in the chance of disastrous events.

In this article, the challenge is identifying the current system of defence against CBRN threats and conducting a strategic analysis regarding the overall capability and readiness of the general law protection/enforcement and paramilitary forces. Different types of strategic analysis are used here such as the SWOT Matrix along with PETSEL analysis, and the McKinsey 7s model.

After that, with the help of a dynamic SWOT matrix, various strategies for enhancing the abilities and readiness of security forces and first responders will be observable.

The finally selected strategies will be based on the need to amplify awareness on a national/international scale regarding CBRN, the duty of security forces to constantly improve in the area of life protection, and the obligation of CBRN responders to have an unceasing foundation of data.

Keywords: Chemical; Biological; Radiological; Nuclear, Environmental Hazards



1. INTRODUCTION

Significant progress in the area of CBRN as an energy resource and a form of armament as a result of globalization and international cohesion is apparent, and so are the dangers that come along with it. The majority of imperative threats related to CBRN shall be discussed, dissected, and analysed, to have a clearer vision of different sources of dangers and the repercussions they may impose.

With the beginning of globalization and the realization of the importance of using science to enhance the quality of life, different materials have emerged as candidates to be the next reliable source of energy. Materials that made their way to become crucial could be identified as chemical, biological, radiological, and nuclear substances. Forming them in certain ways could create a great amount of energy or destruction. Different nations not only looked at these new sources as a reliable source of energy but also as a means of armament and a form of protection against conflict.

In 1836, Samuel Colt invented his first revolving gun while the Industrial Revolution was underway. A race began between nations, companies, and rogue parties to develop the most advanced weapons. Such race had led to the invention of machine guns, various types of bombs and explosives, missiles, armoured vehicles, tanks, fighter aircraft and recently the weapons of mass destruction, which formed the shift that changed the face of modern wars and the probability of its occurrence.

The first use of the term “Weapon of Mass Destruction” on record is by Cosmo Gordon Lang, Archbishop of Canterbury, in 1937 in reference to the aerial bombardment of Guernica, Spain. He wrote in his appeal “Who can think without horror of what another widespread war would mean, waged as it would be with all the new weapons of mass destruction?”. The term “Weapons of Mass Destruction” was used to describe the unconventional weapons as a result of the usage of chemical, nuclear and biological agents along with the news spread about several countries’ interest in developing such weapons during that era. Based on the previous, weapons of mass destruction are defined as unconventional weapons which have a mass effect on both humans and the environment including chemical, biological, radiological and nuclear agents (CBRN). Ever since that era, the number of risks associated with CBRN has been on the rise.

Based on the depth and specifics, it is essential to form a detailed analysis of the threats that appear to be significant or imminent, and countermeasures to deal with them. In order to accomplish that, this publication will concentrate on forming the proper definitions for the threats, reviewing their significant dangers, and structuring the proficient countermeasures to eliminate them.

Emerging threats that have been increasing were matched with an emerging international framework to reach a common ground towards the defiance of threats. In the year of 1968, the Treaty on the Non-Proliferation of Nuclear Weapons (NPT) was opened for signature and officially entered into force in 1970 with more than (191) states parties to it by August 2016. The treaty states that "The NPT non-nuclear-weapon states agree never to acquire nuclear weapons and the NPT nuclear-weapon states in exchange agree to share the benefits of peaceful nuclear technology and to pursue nuclear disarmament aimed at the ultimate elimination of their nuclear arsenals.". Years later, many international conventions regarding this topic have been created in addition to the related UN Security Council resolutions, specifically, the resolution No. 1540 / 2004, which establishes "the obligations under Chapter VII of the United Nations Charter for all member states to develop and enforce appropriate legal and regulatory measures against the proliferation of chemical, biological, radiological, and nuclear weapons and their means of delivery, in particular, to prevent the spread of weapons of mass destruction to non-state actors."

Accordingly, there has been a general consensus on the importance of the following points as they simplify what is actually wanted by everyone.

Most of the existing international legal instruments against chemical, biological, radiological and nuclear (CBRN) terrorism identified above have common features. Generally, they:

- Establish particular acts as offences
- Require States parties to criminalize such acts under their domestic law
- Establish jurisdictional grounds for States parties to prosecute the described offences
- Include an obligation to “extradite or prosecute”, known under the Latin formula *aut dedere, aut judicare*
- Provide legal grounds for cooperation between States parties for extradition and mutual legal assistance purposes regarding the offences they establish

With the growing attention towards the importance of threats, a large number of experiments, studies, laws, and regulations have been developed focusing on this subject. Several organizations have been founded that have a significant influence in raising awareness on the status of CBRN threats such as the United Nations, the IAEA (International Atomic Energy Agency) and the OPCW (Organisation for the Prohibition of Chemical Weapons). The previous agencies are among the leading sources of research on the topic and also have some experience on the countermeasures that could be efficient in case of a CBRN disaster.

Most middle east region states have developed capabilities to elevate the readiness level which could be considered advanced and precise. Moreover, through international engagements with European agencies, security bodies, and private/governmental companies, many of these states managed to enhance the capabilities of classifying and anticipating CBRN threats.

“During 2015, Saab delivered the AWR (Automatic Warning and Reporting) system for the Kuwait National Guard. AWR is a flexible, modular and future-proof solution for the detection, identification, warning, monitoring and reporting of CBRN hazards. The system can be installed and operated from fixed locations such as camps and headquarters or mounted on vehicles, as well as, on soldier systems. It helps the operator to make fast and accurate decisions to limit the effects of a CBRN attack and it is a key part of the national CBRN centre.” More information about KNG AWR system provided by Saab on their official website.

From the perspective of the EU organization, the type of CBRN threat particularly addressed in recent studies varies according to the context of the drafting of the respective studies. Outlines either follow existing, well-known cases or discuss hypothetical threats. The focus is mostly placed on the (potential) malicious use of CBRN materials and agents, with natural occurrences, and accidental uses being addressed less frequently or only in very specific contexts, such as the Fukushima nuclear accident.

For one, the context is often set through references to examples of occurrences of CBRN threats, as well as to relevant recent policy developments. Recent studies from mid-2020 onwards, *i.e.* from during the COVID-19 pandemic, accordingly focus, particularly on biological threats (E.g. European Parliament, ‘How the COVID-19 crisis has affected security and defence-related aspects for the EU’, 2020). Other previous studies on CBRN make frequent reference to chemical threats based on the context of frequent chemical attacks of the past decade (*e.g.* European Parliament, ‘EU Civil Protection Responding to CBRN Incidents and Attacks, 2018). Nuclear threats are mentioned in the framework of developments of nuclear programmes, but also in terms of cross-border nuclear safety and liability and insurance concerns related to nuclear accidents (*e.g.* European Parliament, ‘Cross-border nuclear safety, liability and cooperation in the European Union’, 2019). Radiological threats are only considered to a very limited extent.



1.1. ACCORDING TO THE EU ORGANIZATION, MEASURES OF PREPARATION FOR AND COUNTERING CBRN THREATS:

- Availability of Medical and Protective Supplies.
- The ability to treat victims of chemical and biological attacks with the most appropriate countermeasures.
- Cross-border nuclear safety and related liability and insurance.
- Civil Protection Mechanism.
- Protection Mechanism
- Regulations targeting the types of CBRN threats.
- Strengthening of military capabilities relates to countering CBRN threats.
- EU Common Security and Defence Policy (CSDP) missions, (Stabilisation Unit UK 2014: Working in European Union Common Security and Defence Policy Missions).

CBRN threats could be either accidents or deliberate attacks by a known enemy or undefined terrorist groups. Classification of threat levels varies depending on many factors which differ from one country to another. Accordingly, each country develops its own response plans and strategies. CBRN can be categorized in accordance to the type of materials and delivery means used in the attack as follows:

- **CONTACT HAZARDS**

Created by chemical, biological or radiological agents that can be absorbed into the skin. These agents can be in solid, liquid or vapour form. Most biological agents do not pose contact hazards unless the skin is cut or abraded.

- **INHALATION HAZARDS**

Created by vapour, aerosols or contaminated dust that can be inhaled into the lungs.

- **INJECTION HAZARDS**

Result from chemical, biological or radiological agents being injected - either by the agent moving from the injection site into the bloodstream or being injected directly into a vein or artery.

- **INGESTION HAZARDS**

The result from chemical, biological or radiological agents being ingested into the digestive system.

- **RADIOLOGICAL HAZARDS**

Radiological agents present a significant additional hazard that results from the radiation they emit.

- **NUCLEAR HAZARDS**

In this context, will be those resulting from a nuclear explosion. These will include extensive blast and fire damage, direct radiation effects and widespread radiological contamination.

2. MATERIALS AND METHODS

This study is going to analyse how the CBRN threats can be countered. To do this, the method that is going to be used is based on hypothetical-deductive reasoning, supported by documental analysis and triangulation of sources.

In the first part, endogenous and exogenous strategic environments are going to be analysed using the same methods as other articles in this publication. Starting with a PESTEL analysis where the factors that affect the

Political, Economic, Social, Technological, Environmental and Legal Aspects of the CBRN threats are going to be defined.

After that, the SWOT matrix analysis is going to be used to determine whether these factors are strengthening or weakening the countries in the combat of CBRN threats, and what areas must be identified or is able for improvement in the time being... Later, that matrix will be transformed into a dynamic SWOT matrix, to help define the strategies to adopt.

In the end, the information gathered and processed in the earlier stages, will be used to define the best strategies to follow to successfully counter CBRN threats with relevance to the current situation.

3. RESULTS

3.1. EXTERNAL ENVIRONMENT ANALYSIS

Table 28. PESTEL analysis | CBRN

Factors	Key Macro Trends	Implications for Security Forces
Political & Legal	<p>P.1. International reliance on CBRN plants is increasing.</p> <p>P.2. The pace of technological development is increasing.</p> <p>P.3. Different nations are expanding the utilization of CBRN materials (weapon, energy, export, technology).</p> <p>P.4. The possession of CBRN plants becoming a strategic advantage (upper hand).</p> <p>P.5. Increase of rules and regulations towards the handling of CBRN materials.</p> <p>P.6. Regional instability increases the risk of threats and attacks on CBRN locations.</p> <p>P.7. Protection of critical infrastructure importance is growing, as the results of attacks may be catastrophic.</p>	<ol style="list-style-type: none"> 1. Growing reliance on CBRN plants adds energy source choices. 2. Modern tech may help pinpoint threats ahead of occurrence. 3. Improvement in the area of understanding the utilizations of CBRN material deemed unlawful. 4. Development of countermeasures and protocols to address anticipated incidents. 5. Applying gathered knowledge and lining up with international guidelines. 6. Developing capabilities to defend against sabotage efforts using CBRN or targeting CBRN locations. 7. Solving for maximal protection of critical infrastructure.
Economic	<p>E.1. Economies becoming more relative to energy production and CBRN plants.</p> <p>E.2. Oil production and the growing demand for raw materials.</p> <p>E.3. Privatization of governmental sectors shifts the economic balance of power.</p> <p>E.4. Price changes volatility create unsuspected shortages of materials.</p> <p>E.5. Trade regulations becoming more sophisticated.</p> <p>E.6. Conflict in Europe affecting contractual obligations and production/delivery time span.</p> <p>E.7. Existing a correlation between the need for nuclear energy and the price of oil.</p>	<ol style="list-style-type: none"> 1. Budget allocations constantly changing. 2. Increased attention on threats to oil plants. 3. Adaptability and flexibility in procurement. 4. Attention to supply/demand threats. 5. Ability to exceed bureaucratic barriers. 6. Adaptation to extension.



Social	<p>S.1. Increased reliance on technology.</p> <p>S.2. Transition of information becoming more diverse thus allowing for bias and inaccuracy.</p> <p>S.3. Chemical, nuclear plants and critical infrastructure creating more jobs.</p> <p>S.4. Growing population influences the demographics of urban vs rural.</p>	<ol style="list-style-type: none"> 1. The majority of technological devices contain materials classified under the chemical product category, also using technology as a threat is gaining more risk. 2. News that circulates after CBRN threats seem to deviate the public from original news sources. 3. CBRN locations becoming more accessible to the public do the requirement of manpower to operate critical infrastructure thus increasing the causality rate in case of accidents and the disclosure of confidential matters that may be used to cause harm. 4. Nuclear plants and oil refineries are generally located in remote zones far from heavily domesticated areas. The increase in demand to accommodate civilian expansion raises an important subject of discussion.
Technological	<p>S.1. Satellite visibility and navigation services.</p> <p>S.2. Assembling and manufacturing devices are now simpler given the tools available starting from delivery websites to online video tutorials.</p> <p>S.3. Emergence of new equipment, materials, hazardous chemicals,</p> <p>S.4. The surge of demand for lithium, batteries, oil, electricity</p>	<ol style="list-style-type: none"> 1. Critical infrastructure such as CBRN locations are viewable by GPS applications, which creates the need to place countermeasures. 2. Forming manuals and procedure lists that are in a pattern with creating devices that create threats and monitoring them. 3. Most equipment becomes obsolete after the introduction of a newer version. Therefore, it is imperative to be up to date with emerging productions. 4. Contingency plans to counter unexpected situations such as electricity shortages, which may cause danger to the integrity of CBRN plants.
Environmental	<p>EN.1. The existence of unrecycled waste from the industrial sector</p> <p>EN.2. Catastrophic events result from oil spills, natural disasters, and human/mechanical error.</p>	<ol style="list-style-type: none"> 1. Enforcement and support of environmental protection, maintaining close follow-up, fines. 2. Have a charted map of operations and response strategies in accordance with various categories of dangerous threats. Constant monitoring of events, and regular quality checks on equipment.

3.2. INTERNAL ENVIRONMENT ANALYSIS

After conducting the proper procedure of analysing CBRN threats from their external factors, we must also conduct an analysis to evaluate the current condition of law enforcement agencies and the current capabilities to defend against threats. The study conducted will be using McKinsey 7Smodel which focuses on determining structure, strategy, systems, skills, style, staff, and shared values.

3.2.1. STRUCTURE AND STRATEGY

Structure and Strategy will be studied simultaneously due to the correlation between them in the area of chemical defence, and they shall be analysed according to the standards followed internationally. For security reasons, only official publications released by governmental authorities will be mentioned and no law enforcement specific structures and strategies are going to be explained. For Example, US Joint Publicaton 3-41/2016 on Chemical, Biological, Radiological, and Nuclear Response, the European Commission, Brussels/ 2017 - Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks, and NATO Project on Minimum Standards and Non-Binding

Guidelines for First Responders Regarding Planning, Training, Procedure and Equipment for Chemical, Biological, Radiological and Nuclear (CBRN) Incidents).

The defence mechanism against CBRN threats is generally handled by chemical defence units. In the realm of CBRN, threats are considered as acts that may cause disastrous or catastrophic situations with the influence of chemical, biological, radiological, and nuclear factors. In order to form a shield of defence against CBRN threats, we will have four strategies structured above four types of specialities.

The first strategy is **Prevention**: it involves a great deal of preparation, strengthening, and development of strategies along with enforcing the appropriate tools using a strong foundation and a clear code of conduct. Collective development of the procedure, rules and regulations, systems, instrument quality, and equipment. Establishing structures to designate roles and responsibilities, monitoring changing variables, the development and training of unit members, and the continuous assessment of approaches and tactics. The main objective of this strategy is to decrease the amount of risk and to be well prepared for any circumstances that may arrive.

The second strategy is **Detection**: It is the review and analysis of all the variables that may influence the operating process of the designated unit and evaluation of the organization's overall security position and speciality capabilities. It is essential to maintain an up to date knowledge of the regional changes, and how unforeseeable events such as natural disasters, conflict, or misuse of hazardous materials impact the integrity of the defence in place. To achieve this, a collaborative effort is required especially with using the knowledge acquired to operate and develop instruments and equipment in possession while following up with the recognized standard procedure of operations and the progress made by a specialist in that area.

The third strategy is a **Response**: which is designated to identify the path of approach to a circumstance which involves the preparation for an imminent threat, operating while/through hazardous surroundings, or managing through the aftermath of a CBRN incident. The objective of this strategy is to classify the procedure of approach to a given incident and limit the damages that may occur while also having a sense of knowledge of the current situation and the process that must take place. The procedure is generally conducted by trained specialist teams equipped with appropriate gear and equipment frequently part of a unit universally termed Chemical Defence Unit usually part of a law enforcement organization.

The fourth strategy is **Recovery**: it is a process designed to assess, develop, and improve the situation that comes after a significant attack or threat. It is essential to maintain a high level of adaptation and rebuild capability while also taking into account areas of improvement and effective methodology against a CBRN incident. CBRN experts are the driving force and the tip of the spear in evaluating and progressing the required elements towards the secure management of a CBRN threat/attack/accident.

3.2.2. SYSTEM

It the importance of putting in place a suitable system to establish and organize the structure within the organization and apply the authority distribution according to necessity. Roles and responsibilities could be clearly identified. Data and information could be stored, tracked, and assessed according to essentiality or importance. Early detection is a key part of the process; therefore, it is generally regarded as standard to link different instruments to different control centre locations with minimal interference or performance error. CBRN detection centres rely on various systems to maintain an advantage over the threat, many centres use handheld or vehicle-mounted systems such as THALES, PROENGINE, BRUKER, FLIR –NBCRV¹, and SAAb which is used by Kuwait National Guard.



3.2.3. SKILLS

There are various layers of technicalities and levels of importance, it is up to the organization to select and categorize CBRN threats based on the implications associated. Therefore, there is a fast response to CBRN incidents that are seen to cause a high level of threat such as the dispersion of biological viruses or the accidental spills or emissions from oil/gas facilities that create hazardous environments. Moreover, incidents that are categorized as less threatening such as eradicating toxic waste or a periodic requirement of facility disinfection from chemical/biological materials.

3.2.4. STYLE

The style generally followed by security forces is the commitment to structure and hierarchy. Usually, it is clear to look at the hierarchical pyramid in which accountability and directions can be followed up by the command. The standard operating style is also in accordance with policies, legislation, and laws that support the security force accomplish its designated tasks.

3.2.5. STAFF

The number of specialists in the area of CBRN is limited within security forces due to the scarcity of this profession which requires a great amount of experience, knowledge, and understanding. Also, within security forces, specialists are supported by a league of experts who are capable of conducting complex assessments and interacting with CBRN incidents while also having the ability to minimize damages and recover efficiently.

Personnel who may be considered experts and specialists are generally recognized as essential which intensifies the need to constantly train and development to reach further levels of qualification.

3.2.6. SHARED VALUES

Kuwait National Guard forces usually have a common framework and a shared code of conduct, a list of important values that define the attitude of the force including:

- HONOUR
- LOYALTY
- INTEGRITY
- PROFESSIONALISM
- DEDICATION
- DISCIPLINE
- SACRIFICE

3.3. SWOT ANALYSIS

Table 29. SWOT analysis | CBRN

Internal factors	Strengths (S)	Weaknesses (W)
	<ul style="list-style-type: none"> Well trained and well-equipped staff always maintain a high level of readiness. Adaptation rate to given situations and scenarios is considerably proficient and the expertise of specialists in the area of CBRN protection and threat response is a foundation upon which the plans and protocols are designed and enforced. The constant convention of law enforcement bodies significantly solidates and improves the communication aspect required for a smooth and operational flow of delegations and responsibilities. 	<ul style="list-style-type: none"> Not being able to raise the desired awareness of the importance of regarding CBRN reports and moving variables and how they can affect the livelihood of an area. As globalization influences the rate at which CBRN materials increase in the number of purposes they serve. Having outdated information, training, and data could disable decision-makers from having the ability to conduct a reliable decision process.
External factors		
Opportunities (O)	<ul style="list-style-type: none"> More attention towards the establishment of research and development facilities related to studying CBRN along with the emerging innovations. Further involvement of CBRN experts and specialists in cohesive and immersive courses, conventions, and forums and reinforce procurement projections. 	<ul style="list-style-type: none"> Enlarge the scope of multimedia associations especially with international affiliates to have the latest information and safety criteria in the area of CBRN. Establishing interlinked database systems with multimedia outlets to facilitate and expand the reach of the public audience.
<ul style="list-style-type: none"> Different nations are gradually accepting the importance of investing in the development of clean reliable energy using power plants and distributing permits and licenses for the private sector to enlarge the scope of opportunities. Also, the amount of awareness has been raised more and transparency between nations has been on the improvement side as more information and technology are being shared to improve the protection level against threats and to improve the methods used to handle, manage, and interact with CBRN material/incidents. The involvement of corporate sectors in the business of CBRN general improvement could be having a significant influence on the progress of protection and interaction. 		
Threats (T)	<ul style="list-style-type: none"> The continuous development of personnel capabilities and developing on the existing knowledge by participating in the attendance of new developed technologies and methods. Presence in the international forums and platforms to strengthen and expand capabilities and general know-how, and utilizing the gained experiences to improve the readiness levels of associated units. 	<ul style="list-style-type: none"> Use of new approach methods to identify global trends and threats associated with the globalization rate of technological progress. Recognition of supplementary reconnaissance centres to increase data collection quantity.
<ul style="list-style-type: none"> The dynamic of CBRN threats is expanding and continuously changing form, with the emergence of new technology associated with the exploitation of energy sources to the procedures involved with uranium enrichment and the excavation of essential materials create a void difficult to comprehend. Different nations have different approaches to the procedure of containment. 		



3.4. STRATEGIES

Once the SWOT matrix is done, to establish strategies to be followed to enhance strengths and minimise threats, it is interesting to transform this matrix into a dynamic SWOT matrix, where strengths and weaknesses are combined with opportunities and threats.

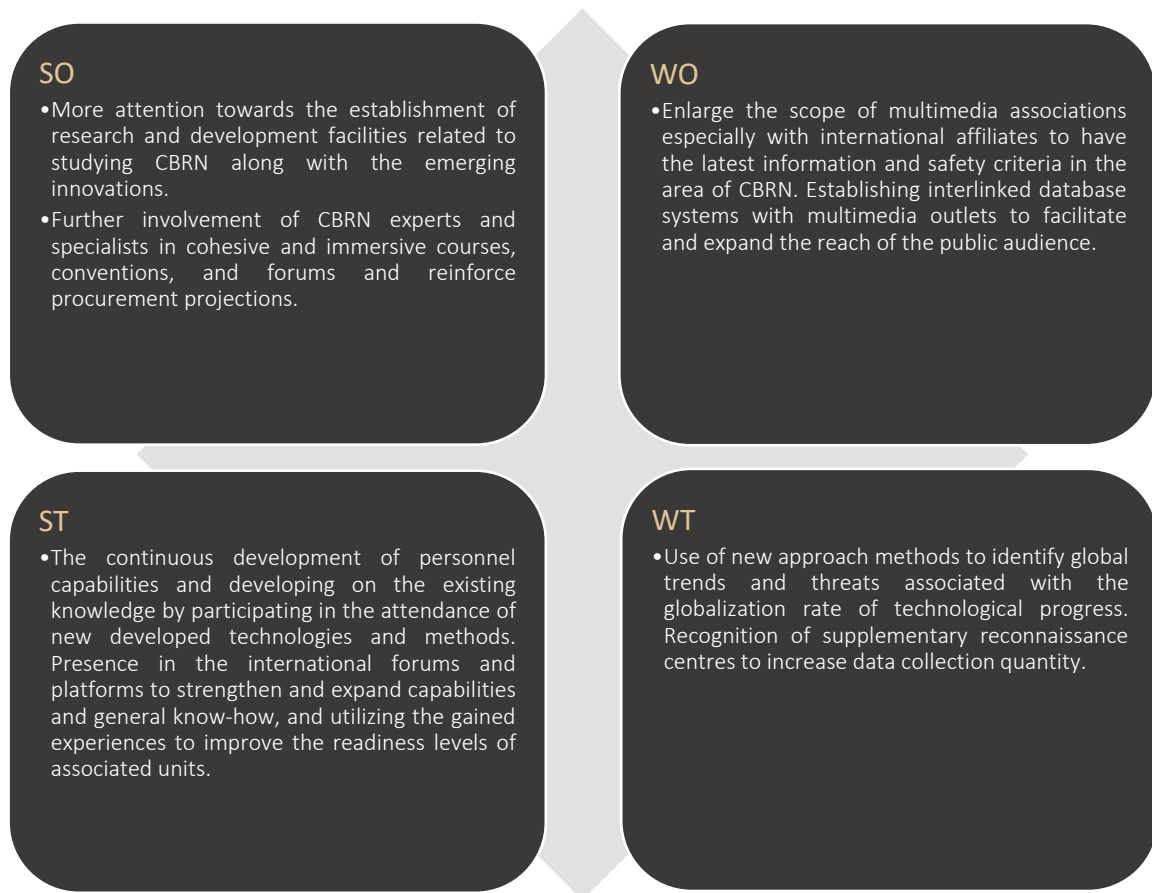


Figure 28. Key strategies | CBRN

4. CONCLUSIONS & RECOMMENDATIONS

It is apparent that there several approaches which have the power to positively influence the overall performance of CBRN threat associated units. There are several areas of improvement which should be further considered.

Due to the fact that many of the methods and tactics available to apply are various, there is still a necessity for the general subject of CBRN threats and sources to be studied, analysed, and verified to attain a clearer vision of the pathway of countering the threats of CBRN.

Therefore, it is imperatively essential to follow on with being more involved in the gathering and analysis of newly received data and information. It is evident that the data and new technology, have strengthened the stance against rising CBRN threats, more threats may arise each day and the stance always has room for improvement.

As the results of the strategic analysis show, there are many methods to raise competence in the fight against CBRN threats.

The strategies proposed in the dynamic SWOT matrix are as follows:

- Create more awareness about the possible threats of CBRN and ways to identify and counter a threat.
- Being up to date with the latest instruments and equipment developed to increase the capability rates of designated counter CBRN units.
- Utilize international relations and associations to strengthen the knowledge base and improve tactics and strategies to face threats arising from CBRN.
- Annual upgrade of facilities, procedures, plans, and systems.
- Unify communications between associated defence, policing, and radiation monitoring centres.
- Emphasis on the providence of the appropriate budget allocations based on need and necessity and with the ultimate goal of improving overall readiness.
- Combat smuggling of CBRN materials through improving border and customs controls to prevent and detect illicit trafficking of CBRN weapons and materials.
- Ensure that advances in biotechnology are not used for terrorist purposes by maintaining continuous pressure against terrorists and denying their access to such materials and equipment.
- Globalize the Counter-WMD terrorism fight through improving international coordination in planning a unified response strategy to terrorist attacks using CBRN weapons or materials.
- Detect and defeat Terrorist WMD plots by establishing an international effort that includes:
 - A. Improve coordination on related intelligence and information.
 - B. Destroy and degrade terrorists' WMD technical capabilities.
 - C. Deter support that such groups may have from rogue persons, bodies, or nations.
- Strengthen the national and international defences against CBRN Terrorism through enhancing military, intelligence, surveillance, interdiction, technical, and law enforcement capabilities.
- Enhance national and international infrastructure preparedness to deal with CBRN terrorism/accidents including health, military, civil community, medical industrial sector.... Etc.
- Require new methods of deterrence against CBRN terrorism through:
 - A. Effective military forces.
 - B. Strong declaratory policy.
 - C. Strong political tools to persuade potential adversaries not to seek or use WMD.
 - D. Overwhelming force if needed to isolate terrorists' CBRN capabilities.
- Improve interoperability among related local and international agencies and organizations whether governmental or nongovernmental concerning CBRN incidents prediction, detection, defence and mitigation.
- Acquire permanent and advanced training courses for specialized staff, civilians or military, using potential scenarios of CBRN incidents in cooperation with international partners.
- Consider the establishment of a joint procurement strategy and capability to guarantee the provision of medical supplies, protective tools, and basic needs in case of a CBRN attack or incident.



REFERENCES

United Nations

The International Legal Framework against Chemical, Biological, Radiological and Nuclear Terrorism

https://www.unodc.org/documents/terrorism/for%20web%20stories/1-WS%20CBRN%206%20modules/CBRN_module_-_E.pdf

International Atomic Energy Agency (IAEA)

Treaty on the Non-Proliferation of Nuclear Weapons (NPT)

<https://www.iaea.org/topics/non-proliferation-treaty>

United Nations

Security Council Resolution 1540.

https://www.un.org/en/sc/1540/documents/Yokohama_statement_final.pdf

EU Parliament

Directorate-General For External Policies Policy Department

EU preparedness and responses to Chemical, Biological, Radiological and Nuclear (CBRN) threats.

[https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653645/EXPO_STU\(2021\)653645_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2021/653645/EXPO_STU(2021)653645_EN.pdf)

UK Home office

The Release of Chemical, Biological, Radiological or Nuclear (CBRN) Substances or Material.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/62229/localauthority-cbrn-guidance.pdf

European Parliament

How the COVID-19 crisis has affected security and defence-related aspects for the EU', 2020.

[https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/603510/EXPO_BRI\(2020\)603510_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/603510/EXPO_BRI(2020)603510_EN.pdf)

European Parliament

EU Civil Protection Responding to CBRN Incidents and Attacks', (2018).

[https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/604964/IPOL_IDA\(2018\)604964_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/IDAN/2018/604964/IPOL_IDA(2018)604964_EN.pdf)

European Parliament

Cross-border nuclear safety, liability and cooperation in the European Union', 2019

[https://www.europarl.europa.eu/RegData/etudes/STUD/2019/608860/IPOL_STU\(2019\)608860_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2019/608860/IPOL_STU(2019)608860_EN.pdf)

Stabilisation Unit UK 2014

Working in European Union Common Security and Defence Policy Missions.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/765510/deployee-guide-series-eucsdp.pdf

US Joint Publicaton 3-41/2016

Chemical, Biological, Radiological, and Nuclear Response

https://www.jcs.mil/Portals/36/Documents/Doctrine/pubs/jp3_41.pdf

European Commission

Action Plan to enhance preparedness against chemical, biological, radiological and nuclear security risks, Brussels/ 2017.

https://ec.europa.eu/home-affairs/system/files/2020-09/20171018_action_plan_to_enhance_preparedness_against_chemical_biological_radiological_and_nuclear_security_risks_en.pdf

NATO Organization

Project on Minimum Standards and Non-Binding Guidelines for First Responders Regarding Planning, Training, Procedure and Equipment for Chemical, Biological, Radiological and Nuclear (CBRN) Incidents.

https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_08/20160802_140801-cep-first-responders-CBRN-eng.pdf

Saab Official Website

KNG AWR (Automatic Warning and Reporting) system provided by Saab.

<https://www.saab.com/newsroom/press-releases/2017/first-integrated-national-cbrn-centre-now-operational-in-kuwait>



Page intentionally left blank

KEY TAKEAWAYS AND RECOMMENDED STRATEGIES

Globalization 4.0, besides opening new opportunities in the most varied sectors of society, has also brought more complex and interrelated threats to the security arena.

In the context of these new threats, the proliferation of cybercrime stands out, from the outset, largely potentiated in the pandemic period, as a result of the mobilization of several activities, personal and professional, to the cyberspace, a domain that has also been the stage for actions of propaganda and disinformation, directed either to the population in general, or directly to States, putting into question the individual sovereignty itself.

In terms of environmental security, the world has been ravaged by significant climate change and natural disasters that act as threat multipliers, indirectly provoking regional disputes over natural resources, which are increasingly precious to the development and support of various States, with special incidence and repercussions for the more fragile, over which we also share responsibilities for protection and support.

Recent conflicts have further intensified the energy security problem, leading us to rethink our role in the planning and execution of security plans for critical infrastructures.

In the area of human security, the last decade has seen unprecedented migratory movements, which have strengthened our focus on combating human trafficking and intrinsically related crimes, such as document counterfeiting and sexual exploitation.

The latent threats of organised crime and terrorism also prevail, phenomena that have become part of the security lexicon of our societies, with dedicated space at the level of security strategies and public policies, which, besides putting lives at risk, may bring about significant economic impacts.

Faced with such a security framework, it is important to know in depth the strategic environment in which the gendarmerie forces operate, enhancing the knowledge of threats so that it is possible to act in an increasingly preventive way.

By correlating the analysis developed and the main findings achieved by the different authors, it becomes possible to highlight the key takeaways and cross-cutting strategies to be recommended.



KEY TAKEAWAYS

CRITICAL ISSUES

- Fight against cyberthreats and cybercrime still needs to be enhanced and emphasised, improving training, public awareness, materials and international judicial coordination.
- Mis/disinformation has a major social impact and poses a fundamental risk to democratic governance, leading to a need for social media platform and independent researchers to develop more efficient technological tools for early warning and stop disinformation, as well as the improvement of every public body's transparency to address disinformation by offering official answers.
- Climate change, in addition to severe meteorological events such as increased floods, storms, droughts, earthquakes, forest fires, and heatwaves, has serious consequences for our living spaces' critical infrastructures such as transportation networks, energy, water, and sewerage transmission lines, and food distribution systems, posing multiple risks to national security, which can lead to various crises. Law enforcement agencies shall be prepared to deal with the effects of climate change and strengthening climate resilience.
- The subsistence of the strategic resource will depend on regional cooperation, since unilateral efforts would be inefficient to manage a shared resource that does not recognize political divisions. Therefore, the commitment and action of all the actors involved is indispensable, along with advance planning and adoption of measures are essential to successfully meet emerging demands.

PROMISING POTENTIAL

- Considering the structure, territorial deployment and training of the Gendarmerie personnel, as a Security Force of Military nature with the characteristics of an Intermediate Force, it is the most appropriate institution to intervene in environmental and social emergency situations that require the assistance of the State.
- Gendarmeries are better placed to boost synergies among security actors and military capabilities.
- International cooperation among gendarmeries might lead to the creation of innovative international coordination agencies/authorities in areas of high expertise (*e.g.* transnational environmental crime)

GROWTH STRATEGIES | SO

- Foster synergies and the implementation of platforms of information exchange in the international field.
- Actively share good practices with stakeholders.
- Make better use of data provided by technological border tools to feed into operational intelligence.
- Enhance investment in R&D in order to prepare for future operations.
- Use intelligence as the foundation for more effective operational planning and deployments.
- Work on sharing operational information, using relevant channels such as Interpol, Europol and similar stakeholders.
- Proactively advise policy departments on (practical/operational aspects of) EU legislation.
- Create more specialists in cybercrime field to investigate the simplest crimes.
- Provide law enforcement with more equipment so that 100% of available personnel capacities can be utilised.
- Initiate and run communication campaigns for raising public awareness about propaganda and mis/disinformation.
- Strengthening the Public Relations department, in order to be able to monitor the public messages regarding public order forces and to provide an instant and strong answer to mis-disinformation.
- Implementing environmentally friendly practices.
- Increasing preventive observation (patrol) activities for environmental and wildlife protection.
- Establish and/or update cooperation and reciprocal assistance agreements with similar Forces in neighboring countries.
- Promote the joint implementation of preventive action activities, coordinated with other security stakeholders.
- Foster the use of alternative sources of energy.
- Creation of synergies and the implementation of information-sharing platforms, within the scope of Critical Infrastructures resilience.
- Anticipating risks of harm to sensitive distribution chains and promote their protection.
- Raise awareness of criminal phenomena among judicial actors, while organizing information and awareness campaigns in partnership with all stakeholders, notably by strengthening partnerships with relevant stakeholders (e.g. NGOs, civil society, media).
- Enhance the training and the training of trainers.
- Diversify the resources in dealing with counterfeiting and providing adapted logistics.



DIVERSIFICATION STRATEGIES | ST

- Move towards fully information-driven and risk-based operations, supported by the necessary technological tools.
- Promote international judicial cooperation by building on relations between law enforcement agencies and judges.
- Dedicate resources to raising public awareness.
- Establish partnerships with the private sector to increase capacity for analysis, control and detection of new modus operandi.
- Develop new partnerships with NGOs, professional association of journalists, universities and influencers, to raise public awareness and critical thinking.
- Protecting critical infrastructure to mitigate major crisis and ensure social stability.
- Strengthen the exchange of information and technological resources with similar forces to prevent and/or mitigate existing risks.
- Maintain updated information regarding the harmonization of regulations and promote their standardization in the areas of direct participation.
- Develop programmes to raise awareness and prevent cyber attacks among the general population.
- Develop and consolidate internal processes for resilience and protection against cyber attacks.
- Rely on international organizations to increase both the capacity and awareness of the law enforcement to better respond to international criminality.
- To foster judicial cooperation between countries of origin and destination to gather as much evidence as possible that can lead to the conviction of transnational criminals.

TARGETING STRATEGIES | WO

- Improve our array of technical resources: hardware, software and the ability of gendarmes to use these in daily operations.
- Work on sharing operational information, using relevant channels such as Interpol and Europol, to counter limited national resources.
- Use the increased budget to cover 24 hours a day in the fields where it is required and to improve the training of law enforcement agencies.
- Improving rewards in cybercrime research stations.
- Develop new means and use the latest technologies for early warning of campaigns that aim credibility and trust in public order forces.
- Promote more transparency and use all communication tools to have a better dialog with citizens and to maintain and raise their trust in gendarmerie forces.
- Developing a climate change strategy and releasing a road map.
- Formulate warning and mass dissemination mechanisms to immediately communicate risks and prevention measures to the potentially affected population.
- Based on the analysis of the information and data provided by specific environmental agencies, design contingency plans for each foreseen eventuality, framed in a Regional Program.
- Based on existing resources and in order to take advantage of territorial implementation, create structures dedicated to the prevention and investigation of computer-related crimes.
- Commitment to interoperability between systems and agents.
- Establish / enhance joint platforms to combat criminal activities at the regional level, especially among countries that have common borders.
- Develop certification processes, at the quality level, in what concerns the articulation between the Safety Plans and the Protection and Intervention Plans, increasing the levels of trust with the CI Operator.
- Develop resource sharing process, with particular focus on the cross-border area.
- Sustain combined mechanisms to counter criminal phenomena and reinforce cooperation with stakeholders.
- Reduce operational differences and normative boundaries between States, while fostering the simplification of procedures for international judiciary cooperation.



DEFENCE STRATEGIES | WT

- Find innovative ways to share and exchange scarce specialized knowledge where it is most needed, such as short-term expert training, study visits among experts, or plugging expertise short-term into multinational missions.
- Increase public awareness efforts.
- Raise awareness among the rest of the administration of the importance of the fight against cybercrime and the increase of the budget dedicated to it.
- Design communication strategies for own personnel.
- Create integrated answers to disinformation campaigns, together with other public institutions.
- Decreasing pressure on scarce resources while increasing the efficiency of scarce resource use.
- Decreasing natural resource scarcity and disaster-induced migration mobility.
- Identify and analyze the risks present in the affected areas, to implement actions to strengthen operational activities.
- Design a human resources management system for emergency situations that will enable the available personnel to be used more efficiently.
- Implement internal training processes to develop skills and institutional culture related to Critical Infrastructures protection.
- Optimise available resources using technological tools.
- Strengthen cyber-capacity and provide training on the subject.
- Use of new approach to identify global trends and threats associated with the globalization rate of technological progress.
- Bring international cooperation, coordination, and communication at a higher level, increasing information sharing and institutional dialogue.
- Strengthen and facilitate international police and judicial cooperation.
- Increase systemic resilience and capacity to adapt and mitigate environmental crime's negative impacts.



www.fiep.org

@fiep_association

@fiep.org



FIEP
FOUNDING
MEMBERS



FRANCE
Gendarmerie Nationale

ITALY
Arma dei Carabinieri

SPAIN
Guardia Civil

PORTUGAL
Guarda Nacional Republicana

TÜRKIYE
Jandarma

THE NETHERLANDS
Koninklijke Marechaussee

MOROCCO
Gendarmerie Royale

ROMANIA
Jandarmeria

CHILE
Carabineros de Chile

ARGENTINA
Gendarmeria Nacional

JORDAN
Darak Forces

QATAR
Lekhwiya

TUNISIA
National Guard

PALESTINE
National Security Forces

UKRAINE
National Guard

BRAZIL
Conselho Nacional de
Comandantes Gerais PM

DJIBOUTI
National Gendarmerie

KUWAIT
National Guard

SENEGAL
Gendarmerie Nationale



GUARDA NACIONAL REPUBLICANA
PORTUGAL

