



# *NATO Stability Policing Centre of Excellence*



## The role of Stability Policing in countering hybrid threats 2<sup>nd</sup> Doctrine Forum Final Report 2022



At the NATO SP COE in Vicenza, Italy.

[www.nspcoe.org](http://www.nspcoe.org)

## TABLE OF CONTENTS

TOPICS	PAGE
<b>EXECUTIVE SUMMARY</b>	3
Background	3
Participants	4
Main Findings	4
<b>1. INTRODUCTION</b>	6
Aim	6
Purpose	6
Timeline of the event	6
<b>2. FINDINGS OF THE SYNDICATE</b>	7
Question 1	7
Question 2	7
Question 3	8
Question 4	9
Question 5	10
Question 6	10
Question 7	11
Additional Findings	12
<b>3. CONCLUSIONS</b>	14
SPCOE Viewpoint	14
<b>4. WAY AHEAD</b>	15
<b>REFERENCES</b>	16
Bibliography	16
<b>ACRONYM LIST</b>	17
<b>DISTRIBUTION LIST</b>	18

### DISCLAIMER

This document has been issued by NATO Stability Policing Centre of Excellence (SPCOE) and its contents do not reflect NATO policies or positions, nor represent NATO in any way, but only the NATO SPCOE or author(s) depending on the circumstances.

The report is classified as Non-Sensitive Information – Releasable to the Public.

## EXECUTIVE SUMMARY

### Background

In the current changing times, NATO faces new challenges. The Secretary General's 2019 and 2020 annual reports, as well as the "NATO 2030" report, indicate that hybrid threats are a challenge that NATO will be called upon to address. The ongoing conflict in Ukraine proves that this indication was spot on.

According to the Allied Joint Doctrine for Stability Policing (AJP-3.22), before, during and after a conflict, threats will arise that may affect the success of the mission. In addition to conventional threats that affect military forces, other threats to the population may arise<sup>1</sup> from the destabilisation efforts of hostile actors using hybrid attacks. As stated in the "NATO 2030" final report of the Reflection Group appointed by the NATO Secretary General, "Hybrid and cyber-attacks are not, themselves, threats; they are tools employed by hostile actors, state, and non-state actors alike, that are the threat"<sup>2</sup>. A hybrid threat is defined as "an action of state or non-state actors, whose goal is to harm or undermine a target by combining overt and covert military and non-military means"<sup>3</sup>.

In its search for strategies to counter hybrid threats, NATO should not overlook the potential role of Stability Policing (SP), whose possible contribution should be assessed and captured within the relevant doctrinal corpus. This prompted the Doctrine and Standardization Branch of the NATO SPCOE to organise the 2<sup>nd</sup> NATO SP Doctrine Forum under the theme "**The role of Stability Policing in countering hybrid threats**".

To help forum participants better understand hybrid threats, colleagues from the Hybrid CoE in Finland were invited to give a lecture and provide their insights as Subject Matter Experts (SMEs) during the workshop discussions.

In addition, a successful doctrine forum required a common understanding and a broad perspective on SP. To develop such an understanding, SPCOE considered it necessary to approach the issue by learning from previous SP operations. Thus, there was a need for the forum members to have a closer look on an operational level at what SP was, and what it is in 2022. This was attempted by first setting the scene by SPCOE Doctrine Branch who presented the current Doctrinal situation in NATO. Then through SP practitioners who were invited from different countries and various background of the civilian, police, and military mindsets, who had experience in different SP operations all over the world. Several SMEs who were already committed to the SP Book project were available. In that view, the project of the SP Book series was presented by the team management (Lt. Col. Marti Grashof and Dr Joanna

---

<sup>1</sup>AJP-3.22 Allied Joint Doctrine for Stability Policing, Edition A Version 1, dated July 2016, par. 0205, NATO UNCLASSIFIED

<sup>2</sup> NATO 2030: United for a new era. Analysis and recommendations of the Reflection Group appointed by the NATO Secretary General, Brussels, 25 November 2020, p. 45

<sup>3</sup> Definition issued by the European Centre of Excellence for Countering Hybrid Threats

Siekiera), where hybrid threats would take a crucial position, especially in the 2<sup>nd</sup> and 3<sup>rd</sup> volume.

## **Participants**

The total number of the participants was 46 from 12 countries (CZE, DEU, GRC, ESP, FRA, ITA, NDL, POL, POR, TUR, UK, USA), from Academia, CZE MP, EuroGendFor, FIN Hybrid CoE, ITA Carabinieri, FRA Gendarmerie, DEU MP, MP CoE, NATO Structure, NATO SP CoE, NLD Marechaussée, ESP Joint Defence Staff, ESP Guardia Civil, USMC University.

## **Main Findings**

The main outcomes of the fruitful discussions carried out during the entire event are the following:

- Hybrid threats are not new but are currently being used with different tools and involve new domains such as cyber, thus requiring new and adapted responses.
- SP can help address and mitigate hybrid activities in various remits, notably Law Enforcement, infrastructure, cyber, military/defence, culture, social, legal, intelligence, political, information and diplomacy.
- Criminal investigations including technical tools remain a priority for the prevention and the detection of crimes with hybrid nature.
- SP ability to counter hybrid threats should be incorporated into the relevant doctrinal corpus of the Alliance.
- A clear mandate is a necessary pre-requisite for the deployment of SP assets, regardless of the scenario (conflict/sub threshold, art.5, NA5CRO<sup>4</sup>, etc.).
- SP assets should be integrated in planning and training from the early stages of the crisis response planning process and should be part of the Joint Task Force Command Structure as well.
- SP is scalable and should involve a model of deployment tailored to the permissiveness and requirements of the environment.
- SP is expected to work closely with the local population, aiming to maintain the domestic cohesion but also to better understand the civilian environment.

---

<sup>4</sup> Non-Art. 5 Crisis Response Operations

NON-SENSITIVE INFORMATION  
Releasable to the Public

- SP can play a role in strategic communication, using several methods in order to influence perceptions, attitudes and behaviour, contributing to the achievement of political and military objectives.
- SP is suitable to deal with covert threats also within domestic environments, such as irregular armed groups.
- SP can face riots and demonstrations as means of destabilization, provide security of critical infrastructures, or investigate on a potential sabotage.
- SP contributes to countering other covert threats, such as disinformation aimed at misleading public opinion, and supports as long as SP gains the civilian population's trust, thereby helping to win the battle of narrative.
- SP can bridge not only the public security gap, but also operate within the grey zone.
- SP Units (SPU) are very suitable to implement Intermediate Force Capability (IFC) under the threshold of war and thus to avoid/minimize collateral damages.

## 1. INTRODUCTION

### **Aim**

The event aimed at bringing together stakeholders, experts and practitioners from NATO, NATO countries, Law Enforcement Agencies, Academia, and the wider International Community, to provide opportunities for discussions and exchange of ideas and information about SP and hybrid threats. During the event, the role of SP in countering hybrid threats in fragile and/or unstable/destabilised contexts was explored.

### **Purpose**

The purpose of the 2<sup>nd</sup> Doctrine Forum was:

- a. The description of the SP role in countering hybrid threats.
- b. The promotion of SP as an effective tool to prevent and mitigate hybrid threats.
- c. The identification of legal framework implications in countering hybrid threats.
- d. The identification of possible improvements of the Allied doctrinal corpus with regards to the role of SP in countering hybrid threats.
- e. The enlargement of the SP network.

### **Timeline of the event**

The event lasted three days, from September 20 to 22, 2022. During the first day of the event, several lectures were delivered by SMEs in the fields of SP and hybrid threats to familiarise the audience with both the subject matters. Specifically, presentations on SP were delivered from both a doctrinal and an operational perspective, while at the end of the day a wargame scenario in hybrid threats was presented, in which all participants were involved during the plenary session. The second day was dedicated to the work of the syndicates, during which several questions stimulated discussion among the members of each of the three syndicates, aiming at attaining the five objectives listed above. Results were presented to the plenary during the third and last day of the Doctrine Forum.

## 2. FINDINGS OF THE SYNDICATES

### Question 1

#### **How can NATO SP contribute to countering hybrid threats?**

SP can contribute to countering hybrid threats in several ways. SP, by its nature, is expected to work closely with the local population. This can lead to a better understanding of the environment and the potential covert hybrid threats. The local population is, on many occasions, more sympathetic to the SP's mandate, hence SPUs are in an advantageous position to obtain useful information. Moreover, SP can provide such information to the commander through intelligence obtained by linking several actors, including the Joint Task Force (JTF), Host Nation (HN) and international law-enforcement agencies.

SP can play a significant role in supporting Strategic Communication (STRATCOM) operations, using several methods to influence perceptions, attitudes, behaviour, and thus contributing to the achievement of political and military objectives. For instance, it can deal with disinformation aimed at misleading public opinion and help win the battle of narrative by regaining the trust of the civilian population.

SP is well designed to address both domestic and external threats, also if covert; specifically, to face riots and demonstrations, ensure the security of critical infrastructures, investigate potential sabotage and financial crimes, carry out crowd control and Law Enforcement activities.

Additionally, SP is an appropriate capability to address inter/intra-state irregular actors such as criminals, terrorists, and insurgents, while building capacity through the missions of Replacement or Reinforcement in a destabilised/unstable context and by providing Defense & Deterrence through a robust presence and intelligent investigation procedures, thus contributing to the resilience of the HN.

### Question 2

#### **What is the added value of an SP contribution to countering hybrid threats as opposed to a heavily military focused approach?**

The main added value of an SP contribution to countering hybrid threats, as opposed to a heavily military focused approach, derives from its capability to work closely with civilians. Not only are SPUs trained on how to consider the surrounding environment, but also in the traditions and customs that can affect the outcome of SP activities. They have developed capabilities to identify the influencers in society and how the latter expects security and police forces to interact with citizens. In this way, SP aims to retain social harmony, while the main target of a hybrid combination of military and non-military tools is to harm civil society and private sector in order to undermine domestic cohesion and the unity of the Alliance.

Moreover, SP brings the policing aspect within military employment/Baseline Activities and Current Operations (BACO), and normal military activities up to the highest level of a conflict. It should be noted that the use of policing assets creates effects that are included in NATO plans, while the rest of the Allied force does not necessarily have the capabilities to address them. Some of such effects are contributing to a functioning society, trusted government, reduced finances and basing for malign activity, free assembly, safeguarding of property, creation, restoration or maintenance of trust in democratic systems and reduction of harm and the threat thereof.

Another added value of SP is its de-escalation nature when we refer to facing riots and demonstrations caused and exploited by hostile actors whose aim is to cause unrest within a society. The SP presence can be adapted to the current level of conflict through the gradual use of non-kinetic means and methods as part of deterrence or assurance measures (Article 5 and NA5CRO). SP can also serve as a transitional capability in both pre-, during and in post-conflict scenarios. Moreover, keeping the use of force at low levels helps avoid or minimise collateral damage, which directly improves NATO's image from the perspective of the HN, of NATO Allies and the wider international community.

### Question 3

#### **Is there scope for different approaches above and below the threshold of conflict / war?**

There is scope for different approaches above and below the threshold of conflict/war, especially in the context of hybrid threats. SP is well-suited to address both scenarios for its flexible vertical and horizontal escalation capabilities across all instruments of power. The police forces are established, trained, and resourced to constantly adapt to the threats they face.

In the scenario below the conflict/war threshold, SP may be used under Article 3<sup>5</sup> to assist nations in building their resilience and resistance to attacks. In the case of Article 4<sup>6</sup>, SP officers can provide NATO with specific expertise. In the scenario beyond the conflict/war threshold, when Article 5<sup>7</sup> is invoked, SP can directly address part of the problem, for instance by posting its officers at the border.

---

<sup>5</sup> Article 3 (Resilience): In order to more effectively achieve the objectives of this Treaty, the Parties, separately and jointly, by means of continuous and effective self-help and mutual aid, will maintain, and develop their **individual and collective capacity to resist armed attack**.

<sup>6</sup> Article 4: The Parties will **consult** together whenever, in the opinion of any of them, the territorial integrity, political independence or security of any of the Parties is threatened.

<sup>7</sup> Article 5: The Parties agree that an armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the United Nations, will **assist the Party or Parties so attacked** by taking forthwith, individually and in concert with the other Parties, such action as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area.

However, in order for SP forces to be deployable in both scenarios, it is necessary to update the NATO doctrine and create a model of deployment tailored to the permissiveness and to the requirements of the environment.

#### **Question 4**

##### **What are the specific hybrid threats SP is more suitable to address and why?**

Based on the main added value of SP and its abovementioned capability to work closely with the populace, SP can justify its suitability to successfully counter the covert threat of disinformation aimed at misleading public opinion and investigate illicit actors targeting the Alliance and its populations. As long as SP maintains the trust of the civilian population, it will be able to contribute to winning the battle of narrative.

SP is suitable to deal with other (c)overt threats, such as irregular armed groups in the domestic environment and can also provide security in critical infrastructures or investigate a potential sabotage thereof.

In the face of this kind of threats, intelligence plays a significant role. SP is able to obtain critical information also through undercover police operations and investigation procedures and participate in the intelligence process benefitting the whole force.

To this end, the deployment of forensics assets in general and digital forensics in particular plays a critical role. These tools, which SPUs have in their arsenal, serve *inter alia* to also prosecute digital crimes as well as other illicit attacks such as (potential) sabotage of critical infrastructures conducted or supported by hostile actions in the cyber domain. The control of the cyber domain is crucial when facing hybrid threats in fragile and/or unstable/destabilised contexts, with the focus on disrupting economic transactions. For this reason, SP is also a suitable tool since it can deal with cyber economic crimes. The development of new technical tools to counter cybercrime and emerging disruptive technologies remains priority for SP for the prevention and the detection of crimes with hybrid nature.

The scalability of SP offers flexibility and the ability of a deployment model that can easily be tailored to the permissiveness and requirements of the operating environment. The capability of de-escalation is very important when facing riots and demonstrations as a means of destabilisation. In such a case, the implementation of IFC is critical, and SP is particularly well suited to apply them.

Regarding the aforementioned situations combined with the hybrid domains recognised in the Conceptual Model of Hybrid Threats<sup>8</sup>, SP is more suitable to address

---

<sup>8</sup> According to the conceptual model, hybrid threats are conducted by applying combination of tools within 13 domains, namely infrastructure, cyber, space, economy, military/defence, culture, social/societal, public administration, legal, intelligence, political, diplomacy and information. Giannopoulos, G., Smith, H., Theodoridou, M., The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305.

its capability in the information, intelligence, military/defence, infrastructure, public administration, social/societal, culture, legal, and cyber domains.

### **Question 5**

#### **What means/tools do SP assets need to cope with these tasks?**

SP employment or deployment must be specific and credible. SP should be part of the planning from the very beginning including the horizon scanning looking for indicators and warnings. SPUs must be trained to be quickly deployable wherever necessary, particularly within NATO Nations to achieve a deterring effect. SP needs support of operating, training and outreach capacity and Communications and Information Systems (CIS) infrastructure.

A successful operation requires a clearly defined yet flexible mandate and legal framework, that is understandable and acceptable to both the sending and receiving nations and their authorities. Additionally, SP tasks and powers should be well specified.

The mandate can be taken over by a standing Very High Readiness Joint Task Force/NATO Response Force (VJTF/NRF)-style SP force. The force needs to be rapidly deployable, i.e., within a few days in order not to lose the deterring effect. The SP force and cadre of experts should be properly trained in cultural awareness and informed on the cultural aspect of the given HN.

SP resources and capabilities should be shared in a diverse and “open club” manner, ideally within a Smart Defence approach. Furthermore, for SP to be an active component of NATO, it needs to be established in JTF Command Structure.

Specialised SP Teams could be deployed beyond NATO borders as part of Crisis Response Planning (CRP), or an Operational Liaison and Reconnaissance Team (OLRT) could obtain an SP element. They will help to gain information and awareness of the situation on the ground, and in the event of a NATO deployment, the action will be better tailored to the problem and context.

### **Question 6**

#### **What are the specific considerations about prevention, deterrence, identification, and assessment? (and others?)**

The measures taken should always be proactive, and initially preventative and only then deterring. Prevention is improved by SP through Indigenous Police Force’s (IPF) capacity building to identify potential hybrid threats, mitigate their impact, and build or enhance resilience. Threat identification can be achieved with a continuous horizon-scanning and measurement of indicators to reveal the risk of a particular hybrid threat.

Deterrence is also part of a proactive pre-conflict approach and is especially important in the context of hybrid threats, as these usually operate below the threshold of conflict. It is necessary once threats have arisen and have been identified; in that case SP can

contribute to deter by a quick deployment of a robust presence and conducting intelligence-led investigations to counter these threats.

Hybrid warfare brings an increased need for attribution, i.e., the ability to counter the principle of anonymity that is typically exploited by hybrid actors. SP can also contribute to detection of a threat as opposed to normal criminal activity or a public safety issue.

Responsibilities within a NAC mandate should be clearly articulated, specifying if the HN retains its primacy, while SP takes on a reinforcement role, or if required, temporary replaces the indigenous police forces is required. Handover-takeover should be done preferably with a follow-on force and only if not otherwise practicable with the IPF, seeking to save Allied resources.

### **Question 7**

#### **What contributions/solutions/concepts/doctrinal inputs stemming from your field of expertise could SP use to improve its performance in countering hybrid threats?**

Doctrine and capabilities of SP should be made flexible, as the situation may be subject to rapid changes. At the same time, they should be tailored not based on expectations, but according to actual needs. It is advisable to articulate an SP Capability Matrix, that will assess the different SP capabilities of NATO member countries. The Matrix will clearly demonstrate countries' readiness to be deployed and facilitate a quick response when needed. IFC should be considered, as between the presence and the use of lethal force, there is a large range within which SP mostly operates, using kinetic and non-kinetic means, negotiation, mediation, and de-escalation.

Until now, the SP component has always been an afterthought when a problem with civilians arose after the army had been deployed. This can be addressed by including SP in operational planning for missions, activities, and tasks from the beginning of a potential crisis within the CRP, Operation Plan and Operation Order (OPLAN/OPORD).

To further promote SP, considerations should be made embedding its content in the Allied doctrinal corpus and attaching SP publications as references. Currently SPCOE contributes to the publications such as AJP-3.10.1 Psychological Operations (PSYOPS), AJP-3.15 C-IED, AJP-3.20 Cyberspace Operation, by responding to request for feedback. Other doctrines relevant to hybrid threats are AJP-3.10 Allied Doctrine for Information Operations, ACIEDP-02 NATO Weapons Intelligence Team (WIT) Capabilities, AIntP-15 Countering Threat Anonymity: Biometrics in Support of NATO Operations and Intelligence, APP-13 NATO Handbook for Coalition Operations; and SP context should be considered within them.

Moreover, SP should be included in Education and Training (E&T) of all military personnel/units to familiarise them with the concepts of SP from the very beginning. It would be particularly useful to point out (military) implications for acquiring knowledge about SP at different levels.

### **Additional findings**

- **Stability Policing can be used both outside and inside NATO territory.**

The debate over whether SP missions should be deployed outside or within the borders of NATO countries led to a consensus that limiting NATO activities to territory would only hinder flexibility. In its present state, AJP-3.22 sets SP actions for unstable states that are fragile, failing, or failed. It could be argued that member countries of NATO are not fragile, failing, nor failed, and therefore SP is of no use to them. However, hybrid threats target countries that are normally considered stable, so from a hybrid perspective, every country is on the verge of instability. Certainly, countries may ask for help at different levels of instability.

Although there may not be an imminent need, we must consider the possibility that NATO's adversaries will look to dismantle the social cohesion of Member Countries and to break apart nation-states to disrupt the Alliance's synergistic effect. In the case of a hybrid attack, Member Countries may ask for support to benefit from the same synergetic effect, especially in the case of border control or weaponised migration management.

- **Need for legal framework adjustments.**

In a hybrid environment, SP works at the speed of legal adjustments. As we have seen, the enemy uses the grey zone below the threshold of conflict to achieve its effects without NATO being able to deploy. Legal framing is problematic because once a solution is applied, it simultaneously becomes a problem as the adversary takes advantage to find new gaps. There is no definitive answer to the legislative ground if the adversary uses law warfare or lawfare. Conversely, SP constitutes a significant and proactive tool for NATO to conduct "legal operations"<sup>9</sup>. Legal Operations represent the use of law as an instrument of power. The term may encompass any category of actions in the legal environment by state or non-state actors aimed at, among others, gaining/undermining legitimacy, advancing/undermining interests, or enhancing/denying capabilities, whether at the tactical, operational and/or strategic/political levels. They may occur across the entire spectrum of peacetime, crisis, and conflict either alone or in conjunction with any other Diplomatic, Information, Military, Economic, Financial, Intelligence or Legal (DIMEFIL) instruments of power to create the same or similar effects as those traditionally sought from conventional military action or in the context of strategic competition or as part of a hybrid strategy<sup>10</sup>.

---

<sup>9</sup> See ACO Directive 080-119, ACO Legal Operations, 5 May 2022, par. 1.2 b

<sup>10</sup> Ibid.

The more specific the framework is, the more it is immobile and easy to target. The legislative framework thus needs to be constantly responsive, as shown by the example of Finnish legislation adaptable to a dynamic hybrid environment.

Transitions back and forth between military-led and civilian-led can also be important to tackle. Adversaries will exploit constant changes of situations to make it appear as military, civil-military or civilian to cause confusion for the authorities. Hence not only the legal framework must be adaptable, but also the act of transitioning from one level of the framework to another.

- **Possible ways to operate Stability Policing within NATO structure.**

Once the SP doctrine is developed, it must be endorsed in operating practice. Ideally, an SP concept would be introduced to JTF Headquarters (HQ) and Higher Headquarters (HHQ). Other possibilities of putting SP into practice are as follows:

- Continue with the traditional concept since the deployment in Bosnia and Herzegovina and the one in Kosovo, in which the commander of the Multinational Specialised Unit (MSU) has the role of the SP advisor.
- Ensure advocating for SP presence within the NATO Response Force (NRF), at Supreme Headquarters Allied Powers Europe (SHAPE) at the Military Committee and at political level, shaping construction of a long-term commitment plan.
- Make a group of experts, such as Provost Marshal with a policing background, SP advisor, advisor on detention operations and others to advise the commander and be part of the planning process to incorporate SP into the plans during all the phases.
- Appoint a separate SP advisor at the same level of the Provost Marshal.
- Create an additional Policing Component Command to the Land, Air, and Maritime.
- Introduce an additional SP branch, or put SP personnel across and throughout the staff, taking care of intelligence, operations, planning, training, etc. from an SP perspective.
- Establish permanent SP representatives under JFC and places SP SMEs with intelligence expertise in J2, operational expertise in J3, and planning expertise in J5.
- Establish an ad-hoc section providing SP education and training to create an expertise ready for specific needs. Make use of the “train the trainers” approach or apply the capacity building approach from the missions into NATO Member Countries, for instance by designating a HN Gendarmerie Type Force as trainers on a rotation basis.

- **To adapt to the new environment, break old paradigms.**

The traditional paradigms that NATO reflects in its planning and operations are not sufficient to today's security environment. The opposite of the VUCA (Volatility, Uncertainty, Complexity and Ambiguity) world is not the stable world, but the dynamic world, where stability is adaptable to the situation. This view diverges from the traditional idea of entering a crisis and then returning to peace. NATO needs to break some old paradigms, as it has started by breaking the difference between the internal and external security. Another paradigm to break is to transform the doctrines and capabilities and apply them in practice. For instance, SP personnel can be employed in a J5 section as a full planner and develop an SP-oriented hybrid response to a hybrid environment.

It is necessary to use creativity and flexibility when rethinking old paradigms. Therefore, wargaming and training should be adapted to different scenarios and allow officers to lose and thus create alternatives and original solutions.

### 3. CONCLUSIONS

#### **SPCOE viewpoint**

The 2<sup>nd</sup> Doctrine Forum met its main objectives, namely the expansion of the Stability Policing network and the recognition of the important role that SP can play in countering hybrid threats, especially in fragile and/or unstable/destabilised contexts.

SP focuses to retain social unity, while the main target of a hybrid combination of military and non-military tools is to harm civil society and private sector in order to undermine domestic cohesion and the unity of the Alliance. The possibility for a successful performance on this task derives from the SP capability to work closely and effectively with the populace thus, to be able to deal with covert (hybrid) threats such as, but not limited to, disinformation. Additionally, SP is well designed to address both domestic and external covert threats; specifically, to face riots and demonstrations, ensure the security of critical infrastructures, investigate potential sabotage and financial crimes, carry out crowd and riot control and law enforcement, disrupt irregular armed groups.

Overall, SP can help address and mitigate hybrid threats in various remits. SP activities are well designed to address all three Core Tasks, namely Deterrence and Defence, Crisis Prevention and Management and Cooperative Security. Yet, to address them effectively, SP doctrine and tasks must be reviewed in the broad Multi-Domain Operations context and within the new conception of 13 hybrid domains<sup>11</sup>.

In hybrid context, the border between internal and external security is blurred and even a country normally perceived as stable is subject to constant threat of hybrid attack, and thus is at the verge of instability. Moreover, adversary exploits the set of activities below the threshold of conflict, limiting NATO's ability to respond.

---

<sup>11</sup> See footnote 8. Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305.

In order to enable effective deployment, a NATO Member Countries' SP Capability Matrix should be articulated. SP contributions should be equally identified within different VJTF/NRF/ARF commitments and in other deployments, for instance in specialised teams.

Doctrinal development needs to be accompanied by a promotion of SP. To do so, SP doctrine should be incorporated as reference to broader doctrinal corpus; included from the beginning in E&T of all military personnel/units; present in planning of the operations, namely in OPLAN/OPORD; and represented at the higher senior levels, such as JTF HQ and HHQ.

#### **4. WAY AHEAD**

In order to enhance the Alliance's capability to perform its tasks against hybrid threats, SP should be taken more into account as an effective tool to counter these threats in various domains. To this end, SP contents shall be included in doctrinal corpus related to hybrid threats and hybrid warfare. As already mentioned, SPCOE currently contributes to a number of publications by responding to request for feedback. SP context should further be considered in other doctrines that are relevant to hybrid threats.

Besides, within the project of the SP Potential three-book series, hybrid threats should be assigned particular attention, especially in the second and third volume.

## REFERENCES

### Bibliography

AJP-3.10.1 Allied Joint Doctrine for Psychological Operations (PSYOPS), Edition B Version 1, September 2014, NATO UNCLASSIFIED

AJP-3.15 Allied Joint Doctrine for Countering Improvised Explosive Devices (C-IED), Edition C Version 1, February 2018, NATO UNCLASSIFIED

AJP-3.20 Allied Joint Doctrine for Cyberspace Operations, Edition A Version 1, January 2020, NATO UNCLASSIFIED

AJP-3.22 Allied Joint Doctrine for Stability Policing, Edition A Version 1, July 2016, par. 0205, NATO UNCLASSIFIED

Giannopoulos, G., Smith, H., Theocharidou, M., The Landscape of Hybrid Threats: A conceptual model, EUR 30585 EN, Publications Office of the European Union, Luxembourg, 2021, ISBN 978-92-76-29819-9, doi:10.2760/44985, JRC123305

ACO Directive 080-119, ACO Legal Operations, 5 May 2022, par. 1.2 b, NATO UNCLASSIFIED

North Atlantic Treaty, Washington D.C. 4 April 1949, Articles 3,4,5

The Secretary General's Annual Report 2019, 19 March 2020, NATO UNCLASSIFIED

The Secretary General's Annual Report 2020, 16 March 2021, NATO UNCLASSIFIED

## ACRONYM LIST

ACRONYM	MEANING
ARF	Allied Reaction Force
BACO	Background Activities and Current Operations
CIS	Communications and Information Systems
CRP	Crisis Response Planning
CRP	Crisis Response Planning
DIMEFIL	Diplomatic, Information, Military, Economic, Financial, Intelligence or Legal
E&T	Education and Training
HHQ	Higher Headquarters
HN	Host Nation
HQ	Headquarters
IFC	Intermediate Force Capability
IPF	Indigenous Police Force
JFC	Allied Joint Force Command
JTF	Joint Task Force
NA5CRO	Non-Article 5 Crisis Response Operation
NAC	North Atlantic Council
NAC	North Atlantic Council
NATO	North Atlantic Treaty Organization
NRF	NATO Response Force
NRF	NATO Response Force
OLRT	Operational Liaison and Reconnaissance Team
OPLAN/OPORD	Operation Plan and Operation Order
SHAPE	Supreme Headquarters Allied Powers Europe
SME	Subject Matter Expert
SP	Stability Policing
SPCOE	Stability Policing Centre of Excellence
SPU	Stability Policing Unit
STRATCOM	Strategic Communications
VJTF	Very High Readiness Joint Task Force
VUCA	Volatility, Uncertainty, Complexity and Ambiguity

## DISTRIBUTION LIST

TO	
1	NATO ACT - CPD/JD&LL
2	NATO ACO
3	NATO ACT SP FOGO
4	NATO ACT SP SME
INFORMATION	
1	ITA Defence General Staff - Centre for Defence Innovation
2	Carabinieri General Headquarters
3	Centre of Excellence for Stability Police Units (COESPU)
4	ITA Permanent Delegation to NATO
5	KFOR – MSU Commander
6	Carabinieri ROS
7	Czech Military Police Main Headquarters - Chief of Czech Military Police
8	French Gendarmerie - Direction Générale de la Gendarmerie Nationale
9	French Gendarmerie – Commandement des Opérations Extérieures pour la Gendarmerie
10	French Armed Forces - Centre Interarmées de Concepts, Doctrines et Expérimentations (CICDE)
11	French Armed Forces – CMD/TN
12	Hellenic Army General Staff-MP Directorate
13	Royal Netherlands Maréchaussée - General Commander
14	Netherlands Defence Academy
15	Polish Military Gendarmerie Headquarters - Main Commander
16	Romanian Ministry of Internal Affairs - General Directorate for Operational Management - General Director
17	Romanian Ministry of Internal Affairs - General Directorate for European Affairs, Schengen and International Relations – General Director
18	Romanian Gendarmerie General Headquarters - General Inspector
19	Guardia Civil General Headquarters - International Cooperation Secretariat
20	MOD Spain - Joint Centre for Concept Development
21	General HQs of the Turkish Gendarmerie - Strategy Dev. & External Relations
22	NATO Supreme Headquarters Allied Powers Europe (SHAPE) - J2/J3/J5/J7/J9/PMO
23	NATO ACT - CAP DEV/SP SME/MP SME
24	NATO Allied Joint Force Command Brunssum (JFC-BS) - PM/J2/J3/J5/J7/J9
25	NATO Allied Joint Force Command Naples (JFC-NP) - PM/J2/J3/J5/J7/J9
26	NATO Land Command -PM/J2/J3/J5
27	NATO ARRC-PM/G2/G3/G5
28	1st (GE/NL) CORPS - PM/J2/J3/J5
29	NATO Multinational Corps North East - SP SME/G3/G5
30	NATO Rapid Deployable Corps-GR (NRDC-GR)-PM/G2/G3/G5
31	NATO Rapid Deployable Corps-ITA (NRDC-ITA) - SP SME/G2/G3/G5
32	NATO Rapid Deployable Corps-SP (NRDC-SP) - PM/G2/G3/G5
33	NATO Rapid Deployable Corps-TUR (NRDC-TUR)-PM/G2/G3/G5

NON-SENSITIVE INFORMATION  
Releasable to the Public

34	NATO Rapid Reaction Corps - FR (NRDF-FR) - PM/G2/G3/G5
35	NATO Defence College
36	NATO School Oberammergau (DEU)
37	Joint Force Training Centre (JFTC) Bydgoszcz (PL)
38	George Marshall Centre for European Security Studies – Garmish (DEU)
39	NATO C-IED Centre of Excellence (CIED COE)
40	NATO CIMIC Centre of Excellence (CIMIC COE)
41	NATO CMDR Centre of Excellence (CMDR COE)
42	NATO Centre of Excellence Defence Against Terrorism (DAT COE)
43	NATO HUMINT Centre of Excellence (HUMINT COE)
44	NATO Military Police Centre of Excellence (MP COE)
45	NATO Security Force Assistance Centre of Excellence (SFA COE)
46	NATO Strategic Communication Centre of excellence (NATO STRATCOM COE)
47	NATO Counter-Intelligence Centre of excellence (CI CoE)
48	NATO Joint Chemical Biological Radiological Nuclear Centre of excellence (JCBRN CoE)
49	NATO Cooperative Cyber Defence Centre of Excellence (CCD CoE)
50	NATO Explosive Ordnance Disposal Centre of Excellence (EOD COE)
51	NATO Energy Security Centre of Excellence (ENSEC CoE)
52	Canadian Army Doctrine and Training Centre
53	RCMP – Royal Canadian Mounted Police
54	Bundeswehr - German Army Command (Land Operations/Military Police)
55	Mol – Public Security Services (Head of International cooperation & Information support direction)
56	National Republican Guard Headquarters of Portugal
57	UK Development, Concepts and Doctrine Centre
58	PhD candidate at Old Dominion University, Hampton Road, Virginia +Senior Strategic, Plans, and Policy Officer at US Army TRADOC
59	Director of Operations at Marine Corps University, Quantico, Virginia United States Marine Corps
60	US Army Training and Doctrine Command
61	US Peace Keeping and Stability Operations Institute (PKSOI)
62	US European Command - Police Liaison Advisor
63	US Special Inspector General for Afghanistan Reconstruction (SIGAR)
64	US ARMY – Africa/Southern European Task Force Unit
65	200th MP HQ
66	United States Institute of Peace (USIP)
67	Austrian Study Centre for Peace and Conflict Resolution (ASPR)
68	Austrian MP
69	Finnish Defence Forces International Centre (FINCENT)
70	Finnish Ministry of Defence
71	Civilian Planning and Conduct Capability (CPCC)-EU
72	Military Planning and Conduct Capability (MPCC)-EU
73	European Gendarmerie Force - Permanent Headquarters (ITA)
74	European Security and Defence College (ESDC)
75	The European Centre of Excellence for Countering Hybrid threats (Hybrid COE)

NON-SENSITIVE INFORMATION  
Releasable to the Public

76	FRONTEX
77	Peace Support Operations Division of the African Union
78	International Committee of the Red Cross (ICRC)
79	Organization for Security and Co-operation in Europe (OSCE)
80	EU Institute for Security Studies (ISS)
81	Pax for Peace
82	Centre for International Studies of Rome
83	Istituto per gli Studi di Politica Internazionale (ISPI)
84	Geneva Centre for Security Sector Governance (DCAF)
85	Egmont Group
86	University of Bergen
87	SME in Counter-Terrorism
88	Dr. Michiel de Weger
89	LTC. Paulo M. L. de Barros
90	LTC. Matteo Salvatori
91	LT. Israel Lazaro
92	LT. Rafael Obrero
93	LTC. Kurtis Kjobech
94	LTC. Joao Duque Martino (Eurogenfor HQ)
95	MAJ GNR Helder Manuel Gonçalves Garção
96	LTC. Christophe NIED
97	CAPT. Menno Bakker
98	CAPT. Magdalena Kruczek
99	JWC Andrew Eden (civ)
100	MNCIMIC GRP South Col. Mattia Zuzzi Multinational CIMIC Group
101	Dr. Michiel de Weger (also author)
102	Dr. Vasileios Syros The Medici Archive Project (MAP)&University of Basel (CH)
103	Dr. Sönke Marahrens Director of COI Strategy and Defence



## ***NATO SPCOE Doctrine Forum***

***“The role of Stability Policing in countering hybrid threats”***

