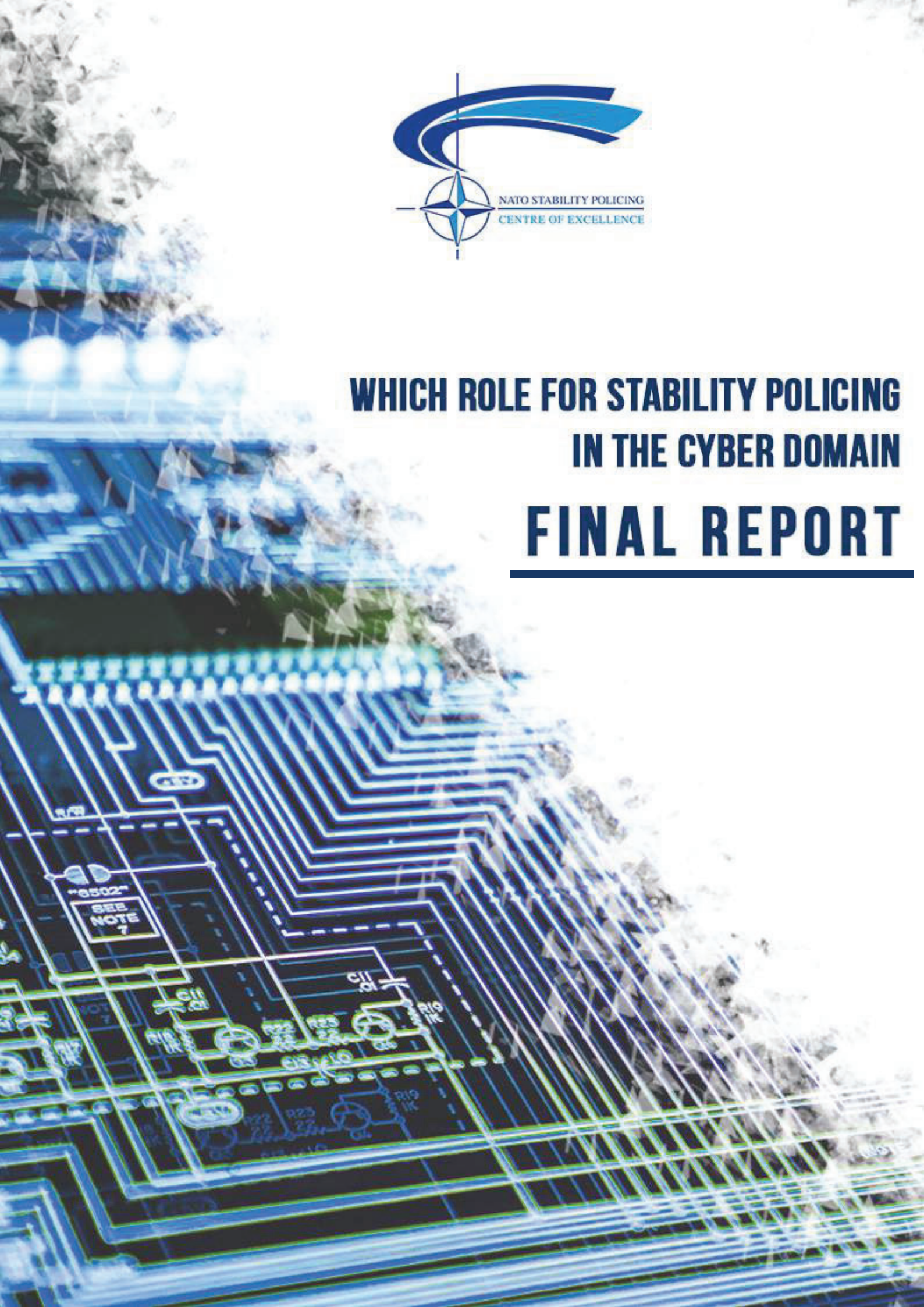
NATO STABILITY POLICING
CENTRE OF EXCELLENCE

WHICH ROLE FOR STABILITY POLICING IN THE CYBER DOMAIN

FINAL REPORT



F O R E W O R D

On October 10th, 2023, in Copenhagen, the Supreme Allied Commander for Transformation, General Philippe LAVIGNE, introduced the NATO Multi-Domain Operations Conference referring to the concept of an evolved world governed by “data dominance”, or “data centricity”. As an effect, NATO itself, he said, is evolving into a “data-centric organization”.

The key point of this perspective is that all information necessary to activate the decision-making process is all around us, well beyond the reach of the traditional collective defence sensors.

In a world centred around data, data themselves are the most valuable assets, that allow the best and the most time-effective decision-making.

But data are also the most vulnerable of the assets, whose loss or dispersion is hardly controllable or even detectable.

And data, all data, are shared (they already were) and collected (and this is the most relevant innovation of a data-centric world) through the cyber world.

Under this perspective, while official institutions are debating around the ways and rights to share data among themselves (during the MDO Conference someone mentioned a certain “data jealousy” of official institutions), malign actors simply “mine” data around the web, through malicious and sophisticated data-collection manoeuvres, free-riders in an apparently lawless melting pot that connects all domains.

It is in the cyber domain where most of the modern cognitive war takes place, and therefore where a strong vigilance must be established.

It is in the cyber domain where all relevant data are flowing, and therefore where to monitor and to catch the relevant and time-sensitive information.

In this way, cyber domain is the new frontier of the collective defence, where the Alliance needs to setup its own outposts, as key enablers of its advanced defence strategy, but also beacons of moral principles and ethical caveats.

On these regards, Stability Policing bears with itself the principles of legality that are the pillars of the most advance internal legal systems, that would complete the significance of these outposts in the quasi-lawless land of cyber.

And as a bridging factor between non-contiguous cognitive worlds, as an “intermediate force”, between the defence and internal security realms – that in the cyber world are inextricably intertwined – I believe that Stability Policing will be relevant, once again, in its capacity of “connecting the dots”, to gather the maximum advantage from such a new and complex environment: that’s the ability of the Stability Policing operator, to bear the lenses (the green and the blue, we used to say) of different cognitive worlds, that provide the Planner and the Commander of the capability to read the reality from different perspectives and with different sensitiveness, breaking (or, better, “bridging”) the boundaries of the military and civilian worlds.

Stability Policing is therefore the ideal candidate to bring to the Alliance a broader analysis spectrum of the reality picture carried by the cyber domain and will significantly contribute to a more effective and time-relevant detection capability, particularly where the boundaries between the collective defence and internal security realms are thin and often blurred.

This workshop marks a significant step ahead for Stability Policing evolution towards its 21st century challenges, and I am sure that the observations and deduction carried on by this very highly qualified panel will often resonate in the upcoming revision process of the relevant NATO doctrine.

Luigi BRAMATI
Colonel, ITA Carabinieri
NATO Stability Policing CoE Director

REPORT OF THE WORKSHOP:
WHICH ROLE FOR STABILITY POLICING IN THE CYBER DOMAIN

This report was produced by:

Captain (ITA CC) Marco CODISPOTI, NATO SP CoE Analysis/Evaluation & Experimentation Section Staff Officer and OPR of the event.
Ms. Matilde MASOTTI (Padua University), Workshop Intern.

This report was coordinated and reviewed by:

Colonel (ITA CC) Luigi BRAMATI, NATO SP CoE Director
Lieutenant Colonel (NLD KMAR) Marti GRASHOF, NATO SP CoE Chief of Staff
Colonel (ROM JAND) Dorin LUTA, NATO SP CoE Lessons Learned Branch Head
Major (ROM JAND) Alin Mihai CHELARESCU, NATO SP CoE Analysis/Evaluation &Experimentation Section Chief.

Acknowledgements to:

Workshop moderator: Ms. Giulia TEMPO (NATO HQ – Joint Intelligence & Security Division – Strategy and Policy Unit – Data, Cyber & Systems Team) and

Workshop facilitator: Ms. Carola FREY (Euro-Atlantic Resilience Centre – Strategic Analysis and Cooperation Department).

Special contributions:

Lieutenant Colonel Alessandro DE VICO (ITA CC), NATO Allied Command Operations – SHAPE Deputy Provost Marshall)
Major Mathieu JOHANN (FRA GEND), NATO SP CoE Doctrine and Standardisation Branch Head
Lieutenant Colonel (ITA CC) Michele APOLLO, NATO SP COE Validation & Dissemination Section Chief
Chief WO Tedy Alexandru ROTARU (ROM JAND), NATO SP COE Education & Cooperation Staff Assistant.

At the NATO SP CoE in Vicenza, Italy, from October to December 2023.

TABLE OF CONTENTS

EXECUTIVE SUMMARY 5

INTRODUCTION: THE KEY QUESTION **7**

THE ORGANISATION AND THE CONDUCT OF THE WORKSHOP 9

TREND ANALYSIS 11

PRESENTATIONS 12

1. CYBERSPACE DOMAIN & THE ROLE OF NSPCOE .....
2. SHAPE'S PERSPECTIVE ON WHICH ROLE FOR SP IN THE CYBER DOMAIN .....
3. LINKS BETWEEN CYBER RESILIENCE, NATO'S CYBER DOMAIN AND SP .....
4. WHICH ROLE FOR SP IN THE CYBER DOMAIN .....

LINES OF EFFORTS 19

CONCLUSION: THE ANSWER 22

ANNEX A PARTICIPATING ORGANISATIONS 26

ANNEX B GLOSSARY OF ACRONYMS 27

ANNEX C DOCTRINAL REFERENCES 28

EXECUTIVE SUMMARY

The NATO Stability Policing Centre of Excellence (NSPCoE), through the Lessons Learned analytical approach, has identified the need to expand the perspective on how Stability Policing can effectively contribute to the Military Operations.

Between 11 – 13 October 2023, NSPCoE organised a dedicated workshop (WS) inviting stakeholders, Subject Matter Experts and practitioners from the NATO Cyber Community, the Intelligence Community and the Stability Policing Community, to identify how Stability Policing should evolve within the Cyber domain.

NATO defines Stability Policing (SP) as "*police-related activities intended to reinforce or temporarily replace the indigenous police in order to contribute to the restoration and/or upholding of the public order and security, rule of law, and the protection of human rights*"[1].

As reported in the NATO 2022 Strategic Concept, "*Cyberspace is contested at all times. Malign actors seek to degrade our critical infrastructure, interfere with our government services, extract intelligence, steal intellectual property and impede our military activities*"[2].

Focusing on the last quotation and transferring its significance into practice, the Cyber domain is likely to assume an increasingly central role in the human dimension, influencing diverse sectors including economics, politics, information, and education. This transformation is expected to induce significant alterations in geopolitical dimensions and perspectives which will no longer be solely shaped by those who control maritime, terrestrial, or aerial domains, but rather by those who, through cyberspace, manipulate public perceptions. This new battleground is characterized by strategic weapons, exemplified by the misuse of social media, and encompasses various dimensions such as information manipulation, activist deception, disinformation, and online threats. Simultaneously, within an increasingly "militarized" internet, cyber warfare is gaining prominence in prospective conflicts, necessitating new solutions to assist governments in safeguarding their assets. Cyberspace has emerged as the preferred domain for destabilization campaigns and hostile activities, moving on from the feasibility of conventional domains. Within the above-mentioned scenario, terrorist groups and violent extremists have exploited the Internet and social media to cause harm in both the digital and physical worlds. Cyberattacks and disinformation campaigns targeting election infrastructure, political parties and politicians are undermining political participation, as well as the legitimacy of essential institutions, while sowing discontent and mistrust. States and non-State actors are

[1] NATO Allied Joint Doctrine for Stability Policing (AJP 3.22)
[2] NATO Strategic Concept 2022

rapidly increasing their cyber capabilities and developing increasingly sophisticated cyber arsenal[3].

Not to mention the recent COVID-19 pandemic, which exposed the collective vulnerability to disruption and abuse. According to UN[4], in one week in April 2020, there were over 18 million daily malware and phishing emails related to the disease reported by a single email provider, in addition to more than 240 million COVID-19-related daily spam messages. Global data breaches have cost countries and companies trillions of dollars, while malware attacks have caused billions of dollars in lasting damage to computer systems necessary for key economic and societal functions. Meanwhile, health-care facilities have been targets of serious cyberattacks during the COVID-19 crisis, with the International Criminal Police Organization reporting a rise in global ransomware attacks. In a nutshell, the whole World Health Organization was under cyberattacks with civilian hospitals and critical health-care infrastructure facing huge criticalities. Health structures must be inviolable, not only in times of armed conflict, but always.

Moving from a robust Lessons Learned (LL) perspective, the intent of the WS was to explore the subject matter across the entire DOTMLPF-I[5] spectrum, with to final goal of defining the SP role within the Cyber domain. A robust analytical approach has been required to properly put in context the topic in a coherent perspective within the current NATO doctrinal framework and taking into consideration all NATO actors already having a role in the Cyber Domain.

The key takeaway from the workshop was the acknowledgement that Cyber is not just about computers and that it is already part of every operation. Since it constitutes an always-challenged domain, it is imperative to have a mindset shift to a more “proactive approach” and, as strategic end state of the WS, to set the conditions to extend the SP capabilities also to the Cyber domain.

People fear Cyber because they don’t understand it. There are many advantages, *cyber shouldn’t be only seen as a threat but also as an opportunity*. To counter this cyber fear, it is necessary to have education, skills, and cyber hygiene practices to remove the stigma and stereotypes from it. *Cyber has to be law enforced*.

---

[3] Roadmap_for_Digital_Cooperation_EN.pdf (un.org)
[4] Report of the Secretary-General Roadmap for Digital Cooperation June 2020
[5] Doctrine, Organisation, Training, Materiel, Leadership, Personnel, Facilities, Interoperability

INTRODUCTION: THE KEY QUESTION

In a dynamic security environment, affected by a large variety of threats from multiple origins, the Alliance faces more challenges today than ever before. In this regard, to support its qualified and specialised contribution to the Alliance and to its Sponsoring Nations, the NSPCoE is constantly committed to evolve and adapt the SP capability to the wider NATO threat landscape.

Considering the challenges depicted by the NATO 2022 Strategic Concept and to support the Alliance's "360° approach", the NSPCoE Lessons Learned Branch has identified the existence of a gap related to the absence of any specific doctrinal references concerning the evolution of SP within the Cyber domain. More specifically, SP is so far by definition mainly a "Land Centric" capability; however, from a Multi Domain Operations (MDO) point of view, it has been identified the need to expand the perspective on how SP can effectively contribute to the Military Operations.

"Which role for the Stability Policing in the Cyber domain?"

Moving from the Key Question "*Which role for the Stability Policing in the Cyber domain*?", the NSPCoE promoted a dedicated WS aimed to gather stakeholders, Subject Matter Experts, and practitioners from the NATO Cyber Community, the Intelligence Community, and the Stability Policing Community, to find a common ground of discussion regarding the opportunity to identify how Stability Policing should evolve within the Cyber domain.

From the Cyber WS clearly emerged the conclusion that Cyberspace is not only computers: it is a full environment, including networks, technology, data, and the human factor that operates behind them. Cyber is a cross-cutting domain, introduced officially since 2016, that affects every aspect of societies. A key factor is represented by the absence of physical boundaries, meaning not having a clear distinction between what is the "military" part of the threat and the "civilian" portion of it. This elevates the Cyber threat[6] to the role of one of the most relevant ingredients of the Hybrid threats.

---

[6] There does not exist a NATO agreed definition of Cyber threat; however, one of the most common definitions is *any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. (US National Institute of Standard and Technology (NIST) – Computer Security Resource Centre (CSRC)*

The evolving threat landscape, recognising that Cyberspace is constantly subject to ongoing disputes, requires a constant analysis of Cyber threats, a close collaboration between teams and the exchange of good practices concerning the cyber aspects and implications of crisis management. Cyberspace is already integrated into the coordinated, cross-domain approach of the alliance.

While SP may not hold a primary role in direct cyber operations, its strengths, methodologies, and core principles allow to play a complementary role in the wider cyber landscape. Indeed, the definition of SP does not exclude at all any different approach required to include the Cyber domain as part of the SP Battlespace and the existing NATO doctrinal framework does not close the door to cyber in Stability Policing. Some of the basic ingredients of the Cyber threat perfectly fit the SP environment and are rapidly emerging as a reality that cannot be further ignored or under-estimated as part of the evolution of its vision and the related capabilities.

During the Vilnius Summit was highlighted the need to adopt a better integrated civilian-military approach: it is not solely about cyber, but it was made clear that cyber needs to become better at supporting the "*deter and defence*" and this can be done by working closely with all networks and stakeholders that are not necessarily part of the enterprise, but that operate and whose work can be relevant. This is where SP might have room as one of the tools to effectively operate in a Joint, Inter-agency, Inter-governmental and Multinational response to the resolution of the complex challenges of a crisis, offering innovative and scalable options by expanding the reach of the military instrument.

As main results of the workshop, several Lines of Efforts (LoE) have emerged, divided for the three branches constituting the NSPCoE:

- For the Lesson Learned Branch: to acknowledge that Cyber, already part of every operation, is not just about computers, and that it is necessary to have a mindset shift towards a "*proactive approach*"; moreover, the acknowledgement of SP playing a bigger role within NATO as a bridging factor between Domains.
- For the Doctrine and Standardisation Branch: to define how SP should be framed, update NATO doctrine on SP and on cyber, reflecting the shift of mindset towards cyber patrolling, provide training on standardization, and develop a dedicated professional figure/ mainstream cyber into SP curricula.

- For the Education, Training and Exercises Branch: to train and exercise SP in cyber through the blue lens approach, having a Law Enforcement role in IT, participate in relevant courses and trainings, identify training gaps, develop relevant courses and, finally, participate in relevant exercises (NATO, COEs, etc.)

THE ORGANISATION AND THE CONDUCT OF THE WORKSHOP

In preparation for the WS, an initial stakeholder analysis has been conducted by the NSPCoE, to identify a set of key contributors having the ability to design an initial framework and including representatives at Strategic, Operational and Tactical levels.

A full list of the participating organizations is provided in Annex A.

The working level session was introduced by four presentations, with the aim to provide a common initial background to all participants and to offer some additional information, useful to sustain the following conversations within the panel discussion:

- Ms. Giulia TEMPO (Moderator - NATO HQ – Joint Intelligence & Security Division – Strategy and Policy Unit – Data, Cyber & Systems Team), offered a quick overview on the Cyberspace Domain & the role of SP;
- Lieutenant Colonel Alessandro DE VICO (ITA CC) - NATO Allied Command Operations – SHAPE Deputy Provost Marshall, provided, through a Webex VTC, a presentation on SHAPE's perspective about the role for SP in the Cyber domain;
- Ms. Carola FREY (Facilitator - Euro-Atlantic Resilience Centre – Strategic Analysis and Cooperation Department) briefed on the links between Resilience, Cyber and Stability Policing;
- Colonel Dorin LUTA (ROU JAND) delivered a presentation on Stability Policing, the NSPCoE and the possible common ground of SP and the Cyber domain.

The participants went through the four presentations, each dealing with different aspects of Cyber and the potential role of SP within this domain. These presentations were then followed by a panel discussion, conducted by the moderator and by the facilitator. During the discussion among participants (coming from diverse backgrounds), a trend analysis, related to several issues considered as relevant to Cyber as to SP, emerged. Based on the identified cross-cutting trends, the alliance and its partners should assess adapting their posture.

TREND ANALYSIS[7]

The vast and intricate aspects of the cyber world constantly change how our institutions, society and organizations connect, operate, and maintain their security. This trend analysis predicts upcoming changes in the cybersecurity space and provides insights into current dynamics. By doing so, it will be possible to identify the opportunities and challenges that lie ahead and to clearly define the role that cyber resilience plays.

	TREND	OBSERVATION	PROJECTION
1	Cyber domain expansion	The digital landscape has widened with cyber incidents rising. Human cognition is a target, leading to manipulations of perception.	As our reliance on technology increases, cyber issues affect everyone from individuals to entire nations
2	Stability Policing evolution	The existing NATO framework could accommodate a cyber aspect to Stability Policing.	The future role of Stability Policing might incorporate "digital aspects" (e.g. cyber forensics), and rapid response to cyber-induced civil disruptions. They will serve as a bridge between the physical and digital realms, ensuring societal stability
3	Multi-domain threats	Threats are multi-faceted. A cyber incident can incite civil unrest with cascading effects	Cyber incidents will have palpable ramifications in the real world, causing disruptions in vital services.
4	Cyber-physical convergence	The line between physical threats and cyber threats is diminishing, with hybrid campaigns becoming more prevalent.	Defence strategies will approach threats in a comprehensive manner, encompassing both digital and physical effects.
5	Technological vulnerability expansion	New technologies introduce new vulnerabilities. Devices interconnect, AI evolves, and cyber threats will in turn evolve accordingly.	There's an imminent need to enhance cyber resilience.
6	Resilience strategy evolution	A shift towards incorporating cybersecurity in resilience strategies is evident.	Cyber threats tend to be at the forefront of future resilience planning.
7	Engaging communities	As cyber threats escalate, trust in the digital domain becomes	Trust restoration post cyber incidents has to be properly planned, and SP could have a role both with the Alliance and outside.

[7] From "Pillars of Cyber Resilience: Fundamental Elements", Carola Frey, Euro-Atlantic Resilience Centre

		precarious and “fear” might take its place.	
8	The imperative of digital literacy	Recognizing the importance of understanding cyber threats across societal strata is key to any resilience strategy.	Comprehensive cyber literacy will become essential, necessitating investments at various levels: awareness, basic, advanced, expert. Understanding personal implications – “What does digital literacy mean to me?”. Recognizing its role in daily tasks – “How does it affect my work?”. Being able to communicate its significance to others and addressing obvious issues – “How can I convey its importance? What immediate actions can I take?”. Leveraging the digital domain for benefits and handling complex threats – “How can we harness the digital domain for our benefit? How do we tackle intricate cyber threats?”.
9	Dynamic adaptation	A dynamic feedback mechanism to address the ever-evolving threat landscape is needed.	Real-time intelligence can be critical to developing agile and adaptive strategies.
10	Public-Private Partnerships (PPP)	The private sector’s role is indispensable in multi-domain operations, bringing both benefits and challenges.	(Effective) collaboration between public and private sectors will be key, especially during crises
11	Experience sharing	Rapid technological progression demands swifter and broader sharing of best practices and intelligence	Cooperation and diplomacy in cyber will be pivotal for a secure digital landscape.

PRESENTATIONS

1. Cyberspace domain & the role of NSPCoE – Ms. Giulia Tempo

The first presentation, proposed by Ms. Giulia TEMPO, touched upon the Cyberspace domain and the Role of NATO Stability Policing Centre of Excellence, giving an introduction from the NATO HQ perspective.

Firstly, she presented the strategic environment in the Cyberspace domain, underlining that since Cyberspace was declared a domain of operations in 2016. Ever since, it has been constantly targeted by malicious activities and, therefore, it is vital to acquire a more proactive posture. A brief overview of the Cyber Threat Landascape was presented, composed of a matrix of four elements including:

- Adversaries: Cyber Threat Actors (supported by Russia, China, Iran, and others potentially emerging).
- Targets: such as NATO Networks, NATO-affiliated Entities (e.g. COEs), Allies & Partners, Supply Chain Entities.
- Objectives: System destruction/disruption, Intelligence collection, Influence Projection;
- Capabilities: it was underlined how each adversary has specific tactics, techniques, and procedures (TTPs), that intrusions create analysable artifacts and finally that determining responsibility is time intensive, but possible.

Ukraine was introduced as a Lesson Learned in Cyberspace: cyber is used as an enabler for kinetic attacks and data, information and intelligence sharing (DI2S) enables deterrence messaging and ensures the development of response options. In the presentation it was highlighted that international cooperation is key to ensure that the Alliance is resilient and able to deter and defend in cyberspace and that data, info and intel sharing is key to maintain 360º cyber threat awareness. To be able to defend NATO networks, there must be continuous multi-perspective activities and management of cyber risk at the enterprise level. Additionally, the necessity to have threat-informed/driven, mission-aware and business-aware cybersecurity.

Subsequently, during the presentation, the Strategic Concept 2022 was reminded to all participants, with highlights on the Alliance's multi-domain operations, the digital transformation necessarily happening and the cyber adaptation roadmap, providing in the 12 Annexes a variety of lines of efforts and specific actions to undertake to realize such adaptation.

In the third part of the presentation, the three levels (POLITICAL, MILITARY and TECHNICAL) of cyberspace were displayed.

At the political level, the main functions are Deterrence, Messaging & Coordinating Collective action, platform for situational awareness and the promotion of a free, open, and secure cyberspace. To these, other were subsequently added, such as the support to decision-making, the political contribution to Deterrence & Defence posture, the imposition of costs & promotion of a Norms-Based Approach to cyber, the partnership and capability development and finally the promotion of NATO as a platform for Info-Sharing, Situational Awareness, and political decision-making.

A small paragraph was dedicated to the NATO's Comprehensive Cyber Defence Policy, that reaffirmed cyber defence as part of collective defence, acknowledged that cyber space is contested at all times, recognized the significance of cumulative effects of malicious cyber activities and campaigns, clarified that NATO will actively address cyber threats at all times, outlined NATO's comprehensive approach to cyber defence, underlined the importance of resilience for NATO and Allies and, lastly, highlighted the benefit of leveraging innovation and partnerships.

At the military level, the guiding principles are the Persistent Level of Readiness and the Centralized Coordination. These principles, through the duties of protecting and defending, strengthening Deterrence and Defence, and integrating into multi-domain operations, lead to the general military vision of being able to defend in Cyberspace as effectively as in Air, Land, Sea and Space and that Cyberspace is integrated into the coordinated, multi-domain approach of the alliance.

Cyberspace operations carried out by the alliance are divided into three major categories: CIS enabling operations (e.g., Employment, Security, Use and Maintenance), Defensive Cyberspace Operations (e.g., Internal Defence Measures, External Defence Measures) and Cyberspace Intelligence, Surveillance and Reconnaissance (e.g., Permissive Collection, Non-permissive Collection).

At the technical level, the governance of Cyber Defence aims at setting the rules for the CIS security for NATO through directives and policies, following doctrinal efforts (AJP 3.20) and providing advice on security trends associated with technological developments. This is followed through IOT secure NATO information in the public cloud, security for the Interconnection of CIS, supply chain security for CIS, quantum threat to cryptography and classified cyber defence information sharing.

Lastly, a part of the presentation was dedicated to the way forward for Cyberspace Cooperation. From the Vilnius Summit came out that the alliance needs to adopt a better integrated civilian-military approach: it is not about cyberspace exclusively, it was made clear

that cyber must necessarily become better at supporting the "*deter and defence*" and this must be done by including grey cyberspace as well and by working closely with all networks and stakeholders that are not necessarily part of the enterprise, but are operating and can be relevant, considering the possibility of creating a dedicated Deterrence and Defence task force and potential structural reforms.

The cooperation with the NATO COEs is of extreme importance and must be engaged in all four pillars (Education, Training, Exercise & Evaluation / Analysis & Lessons Learned / Doctrine Development & Standardization / Concept Development & Experimentation). The concrete engagements proposed were yearly conferences and ad hoc engagements, RfS mechanism and the NATO Intelligence Academy. The key role of the NSPCoE is delivering annual briefings to the JISD-led Community of Interest, to NATO Intelligence Academy courses and workshops.

2. NATO SHAPE's perspective on which role for SP in the Cyber domain – Lieutenant Colonel Alessandro DE VICO

The presentation was opened with the description of the functions of the Provost Marshal Office.

The central part of the presentation regarded NATO and the Cyber domain, underlining the steps undertaken since the cyberattacks against Estonia's public and private institutions in 2007, and the consequent Policy on Cyber Defence of 2008, the recognition of Cyber Defence as an essential component of the Collective Defence in 2014, the Warsaw Summit of 2016, where cyberspace was conceptualized as "domain" of operations and a Cyber Defence Pledge, the 2016 NATO-EU Technical Arrangement on Cyber Defence, the 2019 PO(2019)0084 - NATO Guide for Strategic Response Options to Significant Malicious Cyber Activities and the 2021 "New" PO(2021)0199 - NATO's Comprehensive Cyber Defence Policy.

The final part of the lecture dealt with SP in this new domain, highlighting five reasons why, traditionally considered as part of the Land Domain and conducted by land-oriented forces, SP can play a role within the Cyber environment:

1. Thinking only in terms of "computers" could be a critical error;
2. Cyber is at the same time a substantial ingredient of the Hybrid Threat;
3. Establishing and maintaining a Safe and Secure Environment (SASE) and Freedom of Movement (FOM) is a paramount in a SP mission;
4. Law Enforcement has an important role to play in support of the Host Nation;
5. Among the MP forces, especially the GTFs are used to policing in the civilian sphere in their counties - they can use the existing huge amount of LL and info and they have the necessary know-how to absolve police tasks in Cyber.

3. Links between Cyber Resilience, NATO's Cyber Domain and Stability Policing – Ms. Carola FREY

The presentation started with the definition of Cyber resilience as "*the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources*"[8] and its links with Cybersecurity. Cyber resilience continues operating during and after the cyber event, taking into consideration how the event impacts on the society, and it goes together with cybersecurity, focusing not just on prevention but on the ability to bounce forward and adapt after cyber incidents (and continue working). As a broader meaning, Cyber resilience is a comprehensive strategy to protect an institution's digital assets, ensuring continuity of services, robust information security, and adaptability. Beyond mere technical defences, it emphasizes the importance of culture and proper training in responding to cyber threats.

At the State level Cyber Resilience deals with national security concerns, the protection of critical infrastructure, the continuity of services, the protection of data, the upholding the rule of law, the technological progress and innovation and the public confidence and trust. At the NATO level, it regards collective defence obligations, hybrid warfare, the protection of critical infrastructure, the operational integrity, the evolving threat landscape, the layered resilience, and the alliance credibility.

In the last part of the presentation, a link between Cyber resilience and Stability Policing was created, also through a subsequent discussion among the stakeholders. What resulted from the discussion is that Stability Policing might not hold a primary role in direct cyber operations, however its strengths, methodologies, and core principles allow it to play a complementary role in the wider cyber landscape.

[8] Cited from: Petrenko, 2019

4. "Which role for Stability Policing in the Cyber Domain" – Col. Dorin LUTA

The final presentation was redacted by the SP COE Lessons Learned Branch Head, Col Dorin Luta, who presented the NATO Stability Policing Centre of Excellence, its doctrine, missions, and tasks, concluding the presentation with the key question "*Cyber – a new domain for SP*?"

The common ground between SP and Cyber proposed at the end of the presentation, laid the foundation for the following panel discussion among stakeholders and experts. In these conclusions, the main statement that can be found is that Cyber can't be approached only in terms of "computers". To help with the construction of the following discussion, some questions and statements were put forward.

Firstly, that Cyber is no longer an activity for "practitioners". Law Enforcement has an important role to play in supporting a Host Nation in domestic cyber operations, to help developing cyber capability and awareness. In addition to this, it should be considered the risk to have "Stone Age commanders" in a new highly sophisticated operating environment.

The existing NATO doctrinal framework doesn't close the door to Cyber in SP. From these, some questions were proposed as an input to the conversation:

- *In Cyber & Hybrid threats – Is there room for SP as one tool to operate in the response to the resolution of the complex challenges of a crisis*?
- *Is there room for Cyber in ensuring a Safe and Secure Environment (SASE) and Freedom of Movement (FOM)*?

Indeed, SP and Cyber have a common ground given that Cyber can't be approached only in terms of "computers". On the contrary, a new approach to military operations is required since, in a virtual world, the absence of any physical boundaries is not supporting an easy distinction between what is the military part of the threat and what is the civilian portion of it. SP is surely one tool to operate in the response to the resolution of the complex challenges of a crisis, especially in a Cyber & Hybrid threat scenario, introducing the relevant key question whether a Safe and Secure Environment and the Freedom of Movement of population must be seen also under a cyber perspective. The answer cannot be but positive, given that in the latter scenario SP is surely a stakeholder, while Law Enforcement has always a recognized important role to play in supporting HN in domestic cyber operations. Being no longer Cyber considered an activity for "practitioners", on the contrary Commanders at any level should start thinking in terms of possibly conducting SP activities also in the Cyber Domain and they should be properly educated to do so by having Cyber as part of their basic set of skills. Consequently,

more steps are required on training the LE leadership to avoid the risk of having “Stone Age commanders” in a highly sophisticated operating environment.

Finally, from a doctrinal perspective, starting from the definition of SP in NATO as “Police-related activities intended to reinforce or temporarily replace the indigenous police in order to contribute to the restoration and/or upholding of the public order and security, rule of law, and the protection of human rights”[9], we conclude that the above definition does not exclude at all any different approach required to include the Cyber Domain as part of the SP Battlespace and the existing NATO doctrinal framework does not close the door to cyber in Stability Policing.

[9] *AAP-06 NATO Glossary of terms and definitions (ed. 2021)*

LINES OF EFFORTS

To be able to have a concrete improvement in terms of developing a doctrine and consequently a cyber capability of SP within the domain, several lines of effort (LoEs), divided for the three branches constituting the NSPCoE, have been identified. The LoEs aim to assist the development of the concept and provide a roadmap to be followed in the aftermath of the Workshop.

A) LESSON LEARNED

Cyberspace was declared a domain of operation in 2016, and according to AAP-06 NATO glossary of terms and definitions 2021, cyber is not only computers, but it is "*The global domain consisting of all interconnected communication, information technology and other electronic systems, networks and their data, including those which are separated or independent, which process, store or transmit data*."

1) Digital aspect to be incorporated in SP role.

It is no longer possible to see Cyber as an isolated event, but it is part of a wider threat landscape and already part of every operation. The future role of SP should incorporate the "*digital aspect*", because threats are not isolated to one domain.

Cyberspace is already integrated into the coordinated, cross-domain approach of the Alliance.

2) Moving towards SP in Multi-Domain Operations concept

The aim of Stability Policing is to move towards the Multi-Domain Operations (MDO) concept (not just lad-centric). Consequently, it is essential to evolve to MDO: it is no longer possible to see Cyber as something that does not concern everyone. Erosion of distance, speed of interaction, low cost and difficulty of attribution are characteristics making the Cyber domain unique and constant subject to malign activities under the threshold of Article 5, some of which could trigger it. There is the need to assume a more proactive and inward posture: not only be reactive and deal with this kind of situation also within the Alliance territory.

B) DOCTRINE

1. Update both NATO doctrines on SP and on Cyber, reflecting mindset shift towards cyber patrolling.

Building a solid doctrinal reference point is key for the matter as it influences every following step. The doctrinal issue has been identified as a priority by all the participants and is commonly recognised as the default starting point for the concept initiation.

During this process of building a robust doctrinal reference, firstly is essential to keep always in mind the duty to be coherent with the current doctrinal corpus related to AJP 3.20 and AJP 3.22 as a starting point.

AJP 3.22 - Stability Policing will be soon under revision. It is important to redefine Stability Policing so it can also build on Cyber capabilities and react and adapt to new threats and the wider Alliance landscape.

AJP 3.20 - Cyber operations is currently under revision. It would be interesting, once defined Stability Policing in Cyber operations, to insert a paragraph and have a reference to SP and its function within the Cyber Domain.

In light of the AJP 3.20 currently undergoing revision and modification, and the impeding revision of the AJP 3.22, it is imperative to recognize that the present time frame presents a strategic opportunity for action and leverage, crucial for achieving a successful advancement in the sense of developing SP Cyber capabilities and functions, possibly with the involvement of CCDCOE, who is custodian of AJP 3.20.

2. Provide training on standardization.

Providing training on standardization refers to the need to support the development of a professional figure also through training related to the doctrinal and standardization processes of NATO. To this aim, a wide range of courses available can be consulted on through the NATO Standardization Office website.

3. Develop a dedicated professional figure/mainstream cyber into SP curricula.

In the Cyber domain there is the distinction between the actor behind the attack and the cyber persona:

- the actor behind the cyber event refers to real individuals in the physical world, human beings with their own unique identities;

- cyber personas, also known as online personas or digital personas, are representations of individuals in the digital realm, which may or may not accurately reflect their real-world identities. This distinction leads to the human security level.

Potentially consider a relevant professional curriculum is crucial to mainstream Cyber training and awareness throughout all the different levels of Stability Policing. Since in the Cyber realm it is impossible to have a single operator with both technical and investigative/intelligence skills, what Stability Policing could provide is a basic Cyber skill set for all LE personnel. Training people on Cyber hygiene and awareness would shrink the surface of attack and that would allow us to have more info about what is happening and in the end prosecution of someone.

Commanders too should be properly educated, having Cyber as part of their basic set of skills. They must enter a virtual dimension with no boundaries and having the ability to rapidly shift from the traditional land dimension to the virtual dimension of the Cyber domain.

C) EDUCATION & TRAINING

Education & Training aim is to train and exercise SP in Cyber by "*train as you fight*" principle. Indeed, under a strict Police perspective (blue lens approach) "*cyber-attack could happen every day and LE must be ready to contrast this threat, whereas the green lens train and prepare for a future attack when it happens*."

Moreover, this additional relevant suggestion emerged from the discussion.

1) Need to encourage the attendance on Trainings and Exercises on Cyber

In particular, it has been highlighted the importance of the participation to relevant courses on Cyber, managed by NATO, UE, UN or other organizations, included CoEs, IOT develop an adequate level of knowledge and skills for each LE personnel education and to facilitate the necessary shift of mindset towards cyber approach. At the same time, taking advantage of LL collection, there is the need to identify training gaps and develop relevant courses. For the above reasons, the participation of personnel in relevant exercises (NATO, COEs, etc.) is highly recommended, to fill potential gaps and to develop remedial actions.

CONCLUSION: THE ANSWER

Is it time to think in terms of Cyber-Stability Policing?

Nowadays it is necessary to move from the traditional concept of SP (*land concept*) towards a new concept of Multi-Domain Operations, which is transversal to the all the mentioned dimension and "*affects*" all of them: with the constantly increasing use of technology in daily life, cyber issues become more and more important both for individuals and for whole countries.

There are no clear and definite borders in the *cyber dominium* which today is largely contested, and all the developing technologies (*all of them are positive in their original meaning, but negative if misused*) could have important implications considering their effects that must be intended as not limited only to the single (*cyber*) attack, but that they can affect directly the decision-making processes of a country (*it is important to underline that cyber threats are no longer isolated to one domain but they directly interest/affect all of them; the Digital Literacy too recognizes the importance of understanding cyber threats at all levels of society)*.

Thus, the responsibility for security is to be considered in its "*collective*" meaning: an attack against any asset in any NATO country could have serious consequences also for the other Nations.

The "*dimension*" in which the allies are called to operate is a new, not physical and a hidden one, so it is necessary:

- to be very flexible, adapting constantly and quickly the countermeasures against this new "*invisible but very effective*" threat;
- to reach a common and better awareness of the *cyber domain*, in which any attack targets directly the human brain (*human factor*), easily reachable and influenceable through technological devices (*computers, smart phone, tablet…*);
- to enhance cyber resilience through a real awareness of individuals about the hidden risks of new technologies (*the increased global "interconnection" transformed all devices in potential "cyber threat entry points"*);
- to ensure that "*resilience-building"* measures are effective checking on the ground through a direct interaction with communities and gathering "*real-time*" feedback to redefine/improve strategies to better answer to societal needs.

1) CYBER AWAREENESS AND COMMUNITY ENGAGEMENT

Another role that SP could play is raising public awareness about cyber threats, to be able to take proactive measures to protect from cybercrimes.

Despite the impossibility of having a clear definition of a cyber conflict due to the always-contested environment, it is possible to refer to a cyber event in terms of "prevention" phase, "during the attack" phase and "post-attack" phase. SP could fit in all three in different ways, e.g. by rising awareness. What SP is missing is the technical ability to operate, so it may work as enabler for other entities, while relying on the technological capabilities of the nations.

Stability Policing should focus on the basics of cyber, to have a better awareness of the domain, and to make a common goal of a maturity level about it.

Since SP engages with communities, being a community-oriented policing, it might have a role of cyber educator in such environments. Firstly, when engaging with the community, it might be possible to understand how the information technology influences the perception of the local population towards the Law Enforcement/military and to gain information in order to have a real and complete knowledge of the operating environment (or more appropriately, the domain) , that together with the understanding of the threat are two essential elements of the Planning considerations in support of a SP mission.

Secondly, it might play a huge role in understanding the proper structures to counter cyber events and provide the right awareness on how to collect information and to preserve all devices related to data collection and cyberspace in general. SP could help the indigenous police to develop a cyber capability in order to be aware of the domain, the opportunity it offers, its threats, the possible attacks and the possibility of disinformation.

With increasing cyber threats, trust in the digital domain is fragile and engagement can be put to a test. Rebuilding and maintaining trust after cyber incidents will be a primary objective and SP could play a significant role in this matter.

2) CYBER RESILIENCE[10]

In the aftermath of the Cyber workshop held in October 2023, the report "*Pillars of cyber resilience: fundamental elements*" by Carola Frey was redacted, in which insights from the workshop itself are reported and conclusions regarding cyber threats, resilience building, and the role of Stability Policing were drawn. In this sense, it is possible to understand that SP

[10] From "Pillars of Cyber Resilience: Fundamental Elements", Carola Frey, Euro-Atlantic Resilience Centre

might play a role, despite being complementary, of extreme importance in terms of cyber resilience. Some of the conclusion regarding the function of SP are below reported.

The emphasis on resilience building has been at the core of cyber security as a founding strategy in response to rapid technological developments. Building a strong digital infrastructure that can both repel and withstands cyber threats is an important task in cyberspace. Institutions, as well as individuals, can be better equipped to fight back sophisticated cyber-attacks through the anticipation of possible vulnerabilities and regular updates of security measures.

Cyber resilience acknowledges that technology on its own, regardless its level of advancement, cannot serve as the sole line of defense. Human actors, often perceived as the weakest element in the cyber chain, become of paramount importance in this strategy and are at the heart of every cyber incident. By placing focus on the human factor, cyber resilience seeks to convert potential vulnerabilities into assets. This is where the relevance of digital literacy is underlined.

Digital literacy encompasses a depth of understanding beyond basic knowledge of online tools. It's about cultivating a mindset where individuals become active participants in their own cyber safety. They earn the understanding and skills to navigate in the digital domain confidently and safely. Starting with the application of basic, still fundamental cyber hygiene practices, such as regularly updating software and exercising caution with phishing emails, and progressing to the acquisition of advanced skills, including the ability to identify and counter potential threats, digital literacy ensures that everyone is equipped to take part in the larger sector of cyber defence.

With no clear borders in cyber, the responsibility for security is to a certain extent collective and SP serves as a bridge, translating traditional practices to the digital environment.

SP's established frameworks and guidelines are adaptable to the multifaceted nature of contemporary threats. Its significance in sharing experience, proactive involvement, and swift response can be pivotal, particularly in instances where cyber incidents have tangible consequences, such as civil disruptions. In such scenarios, SP's expertise in understanding human motivations, behaviors, and societal interactions can offer insights into deciphering the intent behind cyber activities, helping in proactive immediate threat detection and targeted interventions. SP can work in parallel with cyber specialists by providing operational support to ensure a smooth transition between digital investigations and on-ground enforcement, and consequently the return to societal stability.

In addition, SP can provide a bridge between technical cyber experts and the public by drawing up sophisticated cyber terminology and threats in an easy-to-understand manner. Direct interactions with communities allow at the same time to gather real-time feedback on the effectiveness of cyber policies, ensuring strategies are continually updated, adaptive, and responsive to the changing threat landscapes, and facilitate grassroots cyber awareness, transitioning civilians from mere recipients of “cyber protection” to active participants in community-level resilience, ensuring that resilience-building measures are effective and aligned with on-ground realities.

3) CYBER PREVENTION AND CYBER PATROLLING

Stability Policing in the Cyber domain can focus on preventing cybercrimes from occurring in the first place, implementing security measures, conducting risk assessments, best practices for online safety.

It might be possible to talk about cyber patrolling, working on crime investigation but also intended as a complete digitalization of SP to rebuild and assure a cyber-SASE (Safe and Secure Environment) in a preventive way. It is important to remember that despite having a physical dimension of the attack, such as the physical device used to perpetrate it, there might be a hidden dimension to it: effects visible in the physical world might been caused by hybrid/cyber campaign for instance.

A cyber-attack can lead to unrest and have ripple effects. Attacks in the cyber realm will have direct, tangible impacts on the physical world, such as disruption in utilities, transportation, and other essential services. Stability can contribute by taking all these threats, trying to prosecute the outcomes and to mitigate consequences these have on the nations. SP assets can conduct a LE activity in Cyber Domain as part of the Temporary Replacement mission within fragile states.

SP could offer a contribution also to deter the development of cyber-sanctuaries having the ability to harm the security of the Alliance and its member states.

ANNEX A

PARTICIPATING ORGANISATIONS:

- NATO HQ, Bruxelles (Belgium)
- SHAPE (Supreme Headquarters Allied Powers Europe), Mons (Belgium)
- NATO RAPID DEPLOYMENT COMMAND (NRDC-ITA), Solbiate Olona (Italy)
- NATO STABILITY POLICING COE (NSPCoE), Vicenza (Italy)
- NATO COUNTERINTELLIGENCE COE, Krakow (Poland)
- EURO-ATLANTIC RESILIENCE CENTRE (E-ARC), Bucharest (Romania)
- EUROGENDFOR HQ, Vicenza (Italy)
- SPANISH JOINT CYBER COMMAND (MCCE)
- POLISH MILITARY GENDARMERIE
- ROMANIAN JANDARMERIA
- ROYAL NETHERLANDS MARECHAUSSEE

ANNEX B

GLOSSARY OF ACRONYMS

CCDCoE: The NATO Cooperative Cyber Defence Centre of Excellence

CICoE: The NATO Counter-Intelligence Centre of Excellence

CO: Cyberspace Operation

COEs: Centres of Excellence

DOTMLPFI: Doctrine, Organisation, Training, Materiel, Leadership Personnel, Facilities, Interoperability

FOM: Freedom of movement

HN: Host Nation

JISD: Joint Intelligence and Security Division

LE: Law Enforcement

LL: Lessons Learned

LLB: Lesson Learned Branch

LoE: Lines of effort

MDO: Multi-Domain Operation

NSPCoE: the NATO Stability Policing Centre of Excellence

RfS: Request for Support

SASE: Safe and Secure Environment

SHAPE: Supreme Headquarters Allied Powers Europe

SP: Stability Policing

TTPs: Techniques, tactics and procedures

ANNEX C

DOCTRINAL REFERENCES

List of doctrinal references (limited to Unclassified doctrine) in support of the Cyber Workshop:

NATO 2022 Strategic Concept

NATO AJP- 01 Allied Joint Doctrine

NATO AJP- 3 Allied Joint Doctrine for the Conduct of Operations

NATO AJP- 3.20 Allied Joint Doctrine for Cyberspace Operations

NATO AJP- 3.22 Allied Joint Doctrine for Stability Policing

NATO AJP- 5 Allied Joint Doctrine for the Planning of Operations

DISCLAIMER

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