1/2025

The CoESPU MAGAZINE

The online Quarterly of Stability Policing

2025

Center of Excellence for Stability Police Units - *Sub lure ad Pacem tuendam Milites paro*

CYBERSECURITY & STABILITY POLICING: NEW FRONTIERS FOR GLOBAL SECURITY

FOREWORD

Dear Readers,

Welcome to the latest edition of the CoESPU Magazine!

This year marks a major milestone for the Center of Excellence for Stability Police Units, as we celebrate our 20th anniversary. From our founding in 2005, CoESPU has grown into a global leader for training, doctrine development, and capacity building on Stability Policing around the world.

We will commemorate our remarkable journey with special events in Vicenza and Rome on June 26th and 27th—and invite you to join us. These celebrations will provide an opportunity to reflect on our journey, acknowledge our achievements, and reinforce our commitment to the future.

But, we are not resting on our laurels. CoESPU remains steadfast in our mission, and busier than ever—focused on equipping peacekeeping forces with the necessary skills, knowledge, and ethical foundations to operate effectively in diverse and challenging contexts.

The courses we conduct enrich the expertise of our participants and reinforce the importance of knowledge-sharing in tackling the complex challenges of modern peacekeeping and Stability Operations. Through engagement with international experts, instructors, and professionals, CoESPU continues to serve as a hub for innovation and excellence in training personnel dedicated to upholding peace and security in fragile environments.

But, CoESPU could not do any of this alone and I extend my gratitude to our partner institutions, instructors, and all those who contribute to our activities. Your dedication and expertise are the driving force behind CoESPU's success. Likewise, I commend the commitment and professionalism of the officers and personnel who have undertaken our training programs, bringing their valuable experiences and perspectives to our shared mission.

As you read this edition of the CoESPU Magazine, you will find the three speeches delivered by the respective Commandants/Directors of CoESPU, EUROGENDFOR, and NATO Stability Policing Centre of Excellence on the Stability Policing Day, held at the Vicenza's International SP Hub on June 27th, 2024. Moreover, I commend the thought-provoking article by Major General (US Army Reserve) John F. Hussey on the <<need for US Stability Policing>>. He strenuously advocates for the establishment of a US Military Police Stability Battalion to strengthen his nation's capacity to maintain peace in conflict and crisis areas. And I cannot help but supporting his viewpoint!

Above all, I invite you to explore all the insights, achievements, and initiatives contained in this edition of the CoESPU magazine. They represent the best of our collective efforts.

Enjoy your reading!

Giuseppe De Magistris
Brigadier General
CoESPU Commandant

PUBLISHER:
COESPU, VIA MEDICI, 87
ZIP: 36100, VICENZA (ITALY)
Telephone +39 0444 932190

The CoESPU Magazine is devoted to the publication of professional concepts and issues, research and doctrinal products developed by the Carabinieri Center of Excellence for Stability Police Units, in collaboration with other international research Centers. The Magazine addresses topics of professional, technical, operational and juridical nature in the field of Stability Policing within Peace Operations. Based on the core values of ethics, integrity, professionalism and respect for diversity, harmonically inflected and informed by the traditions of over two hundred years of Carabinieri history, the Magazine fosters Human Rights and gender mainstreaming, while seeking to enhance current police peacekeeping doctrine and promoting international police peacekeeping interoperability, cognizant of Lessons Learned and best practises. The CoESPU Magazine is constantly committed to upholding UN standards, norms, procedures and curricula, while endorsing self-sufficiency of the participating Police Contributing Countries. Consequently, its editorial policy promotes the principles of representativeness, responsiveness, and accountability, as well as effectiveness, efficiency, transparency, and accessibility, to provide the highest professional standards to build trust and legitimacy of beneficiary Law Enforcement Institutions.

TABLE OF CONTENTS

FEAUTURES SECTION

ALUMNI

"The CoESPU Magazine – the on line Quarterly of Stability Policing" is a stand-alone on line publication.
Printed copies are intended for internal use and shall not be distributed.

Published on www.coespu.org

https://www.instagram.com/coespu/
facebook.com/coespu
linkedin.com/school/coespu
*@_CoESPU_*
coespurivista@carabinieri.it
coespu.org

THE COESPU MAGAZINE
REGISTRY COURT NUMBER:
VICENZA N.3367/2018 U.G. R.S. 8/2018.
ISSN: 2611-9005
COESPU MAGAZINE [ONLINE]
PUBLISHED ONLINE ON THE COESPU WEBSITE WWW.COESPU.ORG - INTERNET SERVICE PROVIDER: AXERA SPA, VIA MADONNETTA N. 215 INT. 4 - 36075 MONTECCHIO MAGGIORE (VI) ITALY

- “FEATURES SECTION”

1 - STABILITY POLICING DAY 2024

Speech delivered by BG Giuseppe De Magistris, CoESPU's Commandant, on the occasion of the Stability Policing Day 2024

The concept of Cyber Security has taken on an increasing impact throughout history, having effects even on the function of Stability Policing in conflict and post-conflict contexts.

In recent years, *Cyber Security* has emerged as a widely-used term with increased adoption by the general public, practitioners and politicians alike. However, there is still very little understanding of what the term really entails. At the beginning of the century, terms regularly used in this context would be "Computer Security," "Information Technology Security," or "Information Security". Then, towards the end of the first decade, the term "Cyber Security" started to become increasingly popular[1].
Definitions of *Cyber Security* may vary depending on the context – government, academia or private sector – but, overall, Cyber Security has been defined as "the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and assets[2]."
According to a more succinct definition, "Cyber Security is the practice of protecting networks, programmes, devices, and data from malicious attacks and the practice of ensuring confidentiality, integrity, and availability of information[3]".

The importance of *Cyber Security* cannot be overstated. Our daily lives, both personal and professional, are intertwined with digital technology. From online banking and shopping to social networking and cloud storage, we rely on the internet and digital systems for convenience and efficiency. However, this reliance makes us vulnerable to cyber threats.
Cyberattacks can have devastating consequences. Data breaches can expose sensitive personal and financial information, leading to identity theft and financial loss. For businesses, the impacts can be even more severe: operational disruptions, loss of intellectual property, reputational damage, and significant financial costs. In critical sectors such as healthcare, energy, and transportation, cyberattacks can endanger public safety and national security. Most importantly, cyberattacks are fundamental tools of the wider *Hybrid Warfare* and, in particular, of *Cognitive Warfare*[4] and *Foreign Information Manipulation and Interference Threats (FIMI)*[5] insofar as they are used to alter how a target population thinks, and hence how it acts by *weaponising* public opinion.
Cyber threats are constantly evolving, becoming more sophisticated and pervasive, the most common and concerning being:

- Malware: malicious software, such as viruses, worms, trojans, spyware, and ransomware that can infiltrate and damage systems or steal data. Notably, almost every modern cyberattack involves some type of malware.
- Social Engineering and Phishing: frequently referred to as "human hacking," social engineering manipulates targets into taking actions that expose confidential information, threaten their own organization's financial well-being or otherwise compromise personal or organizational security.
- Phishing is the best-known and most pervasive form of social engineering. Phishing uses fraudulent emails, email attachments, text messages or phone calls to trick people into sharing personal data or login credentials, downloading malware, sending money to cybercriminals or taking other actions that might expose them to cybercrimes.
- Man-in-the-Middle Attacks (MITM): involves intercepting the communication between two endpoints, such as a user and an application. The attacker can eavesdrop on the communication, steal sensitive data, and impersonate each party participating in the communication (for example Wi-Fi eavesdropping, DNS or IP spoofing).
- Denial-of-Service (DoS) Attacks: overwhelming a system, server, or network with traffic, causing it to crash and become unavailable.
- Advanced Persistent Threats (APTs): prolonged and targeted cyberattacks aimed at stealing sensitive information over time.
- Insider Threats: risks posed by employees or other insiders who intentionally or unintentionally cause harm to an organization's information systems.
- Supply Chain Attacks: hacking an organization by compromising a third-party vendor in its supply chain.
- Zero-Day Exploits: a type of cyberattack that takes advantage of a zero-day vulnerability - an unknown or as-yet-unaddressed or unpatched security flaw in computer software, hardware, or firmware. "Zero day" refers to the fact that a software or device vendor has "zero days" - or no time - to fix the vulnerabilities because malicious actors can already use them to gain access to vulnerable systems.
- Internet of Things (IoT) attack: exploitation of vulnerabilities in IoT devices, like smart home devices and industrial control systems, to take over the device, steal data or use the device as a part of a botnet for other malicious ends.
- Data Manipulation: a form of cyber-attack that doesn't steal data but aims to change the data to make it harder for an organization to operate.
- Multi-vector, polymorphic attacks: surfacing in 2017, a new class of multi-vector, polymorphic cyber threats combine several types of attacks and change form to avoid cybersecurity controls as they spread. Firstly, they are a singular attack that involves multiple methods of attack. In this sense, they are "multi-vectored (i.e. the attack can use multiple means of propagation such as via the Web, email and applications." However, they are also multi-staged, meaning that "they can infiltrate networks and move laterally inside the network." The attacks can be polymorphic, meaning that the cyberattacks used such as viruses, worms or trojans constantly change making it nearly impossible to detect them using signature-based defences

In other terms, *Cognitive Warfare* is thus an unconventional form of warfare that aims at altering enemy's cognitive processes, exploiting its vulnerabilities and mental biases, and provoking thought distortions, influencing decision-making and hindering actions, with negative effects, both at the individual and collective levels.
Cognitive Warfare and FIMI threats are clearly linked to *Cyber Security* as they utilise, *inter alia*, the same cyber technological infrastructure, especially in the initial stages of content creation, amplification, and dissemination. In fact, specific cyberattacks could be considered a precursor to FIMI incidents and vice versa. For instance, cyberattacks could be used to obtain information that could later become the basis for fake content creation in information operations. Similarly, stealing voter registration data could support and develop specific

narratives, whereas obtaining personal email addresses could be used to disseminate content. Fake accounts could be created, existing accounts compromised to establish legitimacy, and websites hacked to display fake content.
To distort the narrative and shift the blame onto other actors through:

- develop image-based and video-based content;
- impersonate legitimate entities;
- degrade adversaries;
- use formal diplomatic channels

Observed incidents featured at least 30 languages, 16 of which were EU-based. Formal diplomatic channels were used to deliver content, distort facts by reframing the context of events, and degrade adversaries. Fabricated content was then amplified and distributed by cross-posting across multiple groups and platforms, which propagated it to new communities among the target audiences or to new target audiences.
According to the 1st EEAS Report on FIMI threats[6], *inter alia*, the war in Ukraine has provided evidence of alignment and support between Russia and the People's Republic of China (PRC), with some content (such as the alleged U.S. military biolabs in Ukraine) being amplified by PRC-controlled media and official social media channels.
It is also important to consider the effect that FIMI threats could have on the cyber security domain. As the emergence of *deepfakes* and "disinformation-for-hire" services could lead to novel, highly sophisticated and successful impersonation attacks and deception techniques, understanding FIMI adversarial behaviours would also help build our resilience against them and maintain our security posture.
It is therefore paramount adopting a robust *cyber security* posture to rapidly build-up capacity and resilience in the cognitive domain. In parallel, educating a multi-disciplinary workforce (and society as a whole) against combined scenarios of cognitive warfare and cyber-attacks would help to improve their resilience.
A very beneficial interdisciplinary collaboration within the FIMI defender community is the recent creation of the DISARM (DISinformation Analysis & Risk Management) framework, designed to represent a knowledge base and taxonomy of known FIMI adversarial behaviours, as well as defences against them[7].
The DISARM Red framework represents Tactics, Techniques and Procedures (TTPs) of incident creator FIMI behaviours, whereas DISARM Blue describes potential response options.
It marks an invaluable step towards facilitating the dialogue on, and understanding of, FIMI behaviours across the community, having the way for improved analytical maturity of FIMI threats and standardised threat intelligence information exchange.

Cyber threats come from numerous threat actors, including:

- Hostile Nation-States: National cyber warfare programmes provide emerging cyber threats ranging from propaganda, website defacement, espionage, and disruption of key infrastructure to loss of life. Government-sponsored programs are increasingly sophisticated and pose advanced threats when compared to other threat actors.
- Terrorist Groups: terrorists conduct cyber-attacks aimed at destroying or abusing critical infrastructure, threaten national security, disrupt economies, and cause bodily harm to citizens. They are less developed in cyber attacks and have a lower propensity to pursue cyber means than nation-states. However, it is likely that terrorist groups will present substantial cyber threats as more technically competent generations join their ranks.
- Corporate Spies and Organized Crime Organizations: Corporate spies and organized crime organizations pose a risk due to their ability to conduct industrial espionage to steal trade secrets or large-scale monetary theft. Generally, these parties are interested in profit-based activities, either making a profit or disrupting a business's ability to make a profit by attacking key infrastructure of competitors, stealing trade secrets, or gaining access and blackmail material.
- Hacktivists: Hacktivists' activities range across political ideals and issues. Most hacktivist groups are concerned with spreading propaganda rather than damaging infrastructure or disrupting services. Their goal is to support their political agenda rather than cause maximum damage to an organization.
- Disgruntled Insiders: Disgruntled insiders are a common source of cybercrime. Insiders often don't need a high degree of computer knowledge to expose sensitive data because they may be authorized to access the data. Insider threats also include third-party vendors and employees who may accidentally introduce malware into systems or may log into a secure S3 bucket, download its contents and share it online, resulting in a data breach. Check your S3 permissions or someone else will.
- Hackers: Malicious intruders could take advantage of a zero-day exploit to gain unauthorized access to data. Hackers may break into information systems for a challenge or bragging rights. In the past, this required a high level of skill. Today, automated attack scripts and protocols can be downloaded from the Internet, making sophisticated attacks simple.
- Natural Disasters: Natural disasters represent a cyber threat because they can disrupt your key infrastructure just like a cyber attack could.
- Accidental Actions of Authorized Users: An authorized user may forget to correctly configure security, causing a potential data leak. Some of the biggest data breaches have been caused by poor configuration rather than hackers or disgruntled insiders.

A successful cybersecurity architecture has multiple layers of protection spread across the computers, networks, programmes, or data to help defend against cybersecurity threats, as well as accidental damage, physical disasters, and other threats. Tipically, it entails:

- Application security: used to test software application vulnerabilities during development and testing, and protect applications running in production, from threats like network attacks, exploits of software vulnerabilities, and web application attacks.
- Information security: protects the integrity and privacy of data, both in storage and in transit.
- Operational security: includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.
- Network security: monitors network traffic, identifies potentially malicious traffic, and enables organizations to block, filter or mitigate threats.
- Cloud Security: implements security controls in public, private and hybrid cloud environments, detecting and fixing false security configurations and vulnerabilities.

- Endpoint security: deployed on endpoint devices such as servers and employee workstations, which can prevent threats like malware, unauthorized access, and exploitation of operating system and browser vulnerabilities.
- Internet of Things (IoT) security: connected devices are often used to store sensitive data, but are usually not protected by design. IoT security solutions help gain visibility and improve security for IoT devices.
- Disaster recovery and business continuity: define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.
- Threat intelligence: last, but not least, Threat intelligence combines multiple feeds containing data about attack signatures and threat actors, providing additional context for security events. Threat intelligence data can help security teams detect attacks, understand them, and design the most appropriate response.

Cyber Security does not typically fall within the purview of *Stability Policing*. As was detailed earlier, Cyber Security is about protecting systems, networks, and data from cyberattacks, ensuring the integrity, confidentiality, and availability of information. *Stability Policing*, on the other hand, refers to filling the policing gap in environments vulnerable to disruption and conflict, ensuring public order and safety through robust police forces. However, in today's interconnected world, the line between cyber threats and physical threats is increasingly blurred. Cyber Security is no longer just an IT issue; it is a fundamental component of national and community security. Cyber threats can undermine the stability of societies, disrupt critical infrastructure, and erode public trust in institutions. Most notably, in the case of peace support operations, they may scupper the peace process since the very beginning or create a hostile environment to the mission (think of what is happening in the Sahel region, for example) by *weaponising* public opinion and influencing host-State policies. Therefore, cybersecurity and Stability Policing are intrinsically linked in our efforts to safeguard both the digital and physical realms.

The nexus between cybersecurity and Stability Policing manifests in several key areas:

- protection of critical infrastructure: critical infrastructure such as power grids, water supply systems, transportation networks, and communication systems are essential for the functioning of society. Cyberattacks on these systems can cause widespread disruption and pose significant risks to public safety. Stability policing must therefore include measures to protect these infrastructures from cyber threats, ensuring their resilience and reliability;
- combatting cybercrime: cybercrime encompasses a wide range of illegal activities conducted through digital means, including identity theft, financial fraud, cyberstalking, and the distribution of illicit materials. Effective stability policing requires law enforcement agencies to develop capabilities to detect, investigate, and prosecute cybercriminals. This involves collaboration with cybersecurity experts, investment in advanced technologies, and international cooperation;
- counter-terrorism efforts: terrorist groups increasingly use digital platforms for recruitment, propaganda, and planning attacks. Stability policing must adapt to this reality by monitoring online activities, disrupting terrorist networks, and preventing the spread of extremist content. Cyber intelligence and digital forensics are crucial tools in this fight, enabling law enforcement to track and counteract terrorist operations;
- civil unrest and public safety: cyberattacks can be used to incite or exacerbate civil unrest, disrupt public services, and spread misinformation. Stability policing must include strategies to mitigate the impact of such cyber threats, ensuring that law enforcement can maintain order and protect citizens during times of crisis.

While the integration of cybersecurity and Stability Policing is essential, it also presents several challenges:

- resource constraints: law enforcement agencies often face limited resources and funding, which can hinder their ability to develop and maintain robust cybersecurity capabilities. Balancing traditional policing needs with the demands of cyber threats requires strategic allocation of resources and innovative solutions;
- skill gaps: the rapidly evolving nature of cyber threats necessitates a highly skilled workforce with expertise in cybersecurity. Training and retaining such personnel within law enforcement can be challenging. Partnerships with private sector organizations and academic institutions can help bridge these skill gaps;
- legal and regulatory frameworks: cybersecurity and cybercrime often involve complex legal and regulatory issues, particularly when it comes to cross-border activities. Harmonizing laws and regulations, ensuring respect for privacy and civil liberties, and establishing clear guidelines for law enforcement actions in cyberspace are critical components of an effective strategy;
- public trust and cooperation: maintaining public trust is essential for the success of both cybersecurity initiatives and stability policing. Transparency, accountability, and community engagement are key to fostering cooperation between law enforcement and the public. Educating citizens about cyber threats and encouraging proactive measures can enhance collective security.

Given the complexity of the challenges at the intersection of cybersecurity and Stability Policing, a collaborative approach is essential. Some strategies to consider can be:

- Multi-Agency Collaboration: effective cybersecurity and stability policing require coordination among various government agencies, including law enforcement, intelligence services, and cybersecurity agencies. Regular communication, joint training exercises, and shared intelligence can enhance overall preparedness and response capabilities.
- Public-Private Partnerships: the private sector plays a crucial role in cybersecurity, as many critical infrastructures and digital services are privately owned and operated. Building strong partnerships with private companies can facilitate information sharing, improve threat detection, and enhance incident response efforts.
- International Cooperation: cyber threats do not respect national borders. International cooperation is vital to addressing the global nature of cybercrime and terrorism. Sharing best practices, harmonizing legal frameworks, and participating in multinational initiatives can strengthen collective security.
- Community engagement: engaging with the public is essential for building resilience against cyber threats. Public awareness campaigns, educational programs, and community outreach initiatives can empower citizens to protect themselves online and support law enforcement efforts.

In conclusion, the nexus between cybersecurity and Stability Policing is a critical aspect of modern security strategies. As cyber threats continue to evolve and affect our societies, integrating cybersecurity into Stability Policing is essential for protecting both the digital and physical realms, as well as to ensure state-institution resilience. By addressing the challenges through collaboration, resource allocation, and public engagement, we can create a safer and more secure environment for all.

Note

1 It had been in use during previous years but its popularity gained considerably when U.S. President Barack Obama in 2009 proclaimed, "I call upon the people of the United States to recognize the importance of cybersecurity and to observe this month with appropriate activities, events, and trainings to enhance our national security and resilience" (The White House – 2009)
2 Schatz, Daniel; Bashroush, Rabih; Wall, Julie (2017), "Towards a More Representative Definition of Cyber Security". Journal of Digital Forensics, Security and Law 12 (2).
3 U.S. Cybersecurity and Infrastructure Security Agency (CISA).
4 https://www.act.nato.int/activities/cognitive-warfare/
5 https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape
6 https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en
7 https://www.disarm.foundation/

Giuseppe De Magistris
BG - Italian Carabinieri
CoESPU's Commandant

2 - STABILITY POLICING DAY 2024

Speech delivered by COL Hans Vroegh, Eurogendfor Permanent Headquarters' Commander, on the occasion of the Stability Policing Day 2024

Thank you for this great opportunity to gather here a mong a topic which connects us from our DNA,Stability Policing as a cutting-edge capability in order to contribute to peace and stability in area's of crisisor just after crisis. The world is on fire and I am convinced that we as Police forces can contribute to all the challenges we faces.

I will focus what we as EUROGENDFOR do, what ourcurrent activitiesare, ourway forward and how we contribute to Crisis Management Operations.

The European Gendarmerie Force, established in 2007 by the Treaty of Velsen, has proven itself as an indispensable tool in handling global crisis management operations. Serving various international organizations such as the European Union (EU), NATO, and the United Nations (UN), EUROGENDFOR plays a crucial role in substitution and strengthening capabilities in diverse crisis situations. As the world evolves, so EUROGENDFOR must too and needs to adapt.

The organization is currently consolidating its mechanisms to rapidly deploy forces, adapt its Standard Operating Procedures (SOPs) and Tactics, Techniques, and Procedures (TTPs) to the latest law enforcement practices, enhance communication strategies, and redefine its strategy for the next five years.
Additionally, it aims to increase member states' participation, integrate police forces into operations, bolster cooperation with the European External Action Service (EEAS), and support deployed forces throughout missions. While traditionally not focused on cyber security, EUROGENDFOR recognizes the growing importance of this domain for both collaborative efforts and internal security.

To deep dive a little bit more further I am going to tell you something about our missions.

Our Current Missions and Projects of the European Gendarmerie Force

1. **International Missions**: EUROGENDFOR is actively involved in various EU civilian and military missions in the Balkans, the African continent, the Middle East as well as Eastern Europe. These missions envisage a large array of tasks and objectives to implement the Common Security and Defence Policy, described in detail by the specific mandate for each of these missions, issued by the Council of the European Union. With regards to EUROGENDFOR' contribution, through the participation of robust units, individual officers, specialized teams from our member states, we can speak about contributing, under EU led missions, with the purpose to the strengthening of the capabilities of local law enforcement agencies, like capacity building, security sector reform, support for the rule of law and with an overall focus on stabilization efforts in post-conflict areas.
2. **Regarding Training and Capacity Building**: EUROGENDFOR relies on the capabilities and expertise of our members states to provide general or specialized police training to local law enforcement agencies in countries where it operates. This includes providing training in areas such as crowd and riot control, forensic investigations, and counterterrorism, but also can be tailored to specific requirements from the missions as examples, Tactical Combat Casualty Care, International Humanitarian Law, Human Rights, Management of stress in a conflict, Explosive awareness, Gender, but also now related to the latest request of one of the EU candidate states, in delivering expertise in subversion and financial flows aimed at influencing elections. Our largest project for the moment is our efforts in Ukraine, where 'we contribute to the EUAM mission with an multinational specialised team in order to train the Ukrainian Law Enforcement Agencies in strengthening their capabilities for their tasks in the so called Liberated Adjacent Territories.
3. **Collaboration with EU agencies, UN and NATO**:
   - **EU**: EUROGENDFOR collaborates closely with EU bodies and agencies, such as the EEAS, to support the implementation of the EU's Common Security and Defence Policy through its civilian and military missions deployed across the globe. This includes rapid deployable forces, providing specific expertise (i. e. operational planning, maritime police, etc.).
   - But also with other parts within the EEAS, like the FSD and the Crisis Response Centre EGF is working close together on common projects like the EU Delegations CPTs, to provide a guaranteed security for missions in crisis and to establish and provide courses for their Regional Security officers.
   - Also we have a close collaboration with the ESDC which allowng us for the preparation and implementation of a pilot course which covers the "European gendarmerie forces in crisis management operations". This includes lessons in joint operations and intelligence sharing to combat organized crime and terrorism.
   - It is in mutual cooperation where we gets more interconnected with the EU academic environment and I where we contribute to each other efforts in trainings and courses.
   - **In the recent past** EUROGENDFOR deployed assets a number of times to support UN peacekeeping missions, through individual police officers, specialized teams and formed police units. At the PHQ level opportunities to identify projects and common commitments were discussed recently with the leadership of the UN Standing Police Capacity based in Brindisi, Italy.
   - **NATO**: the commitment of EUROGENDFOR was best illustrated by the longstanding effort to ISAF Afghanistan, IOT to strengthen the security sector capabilities and to support the security sector reform from 2014 to 2021. As EUROGENDFOR we still have work to remain in close contact with the relevant NATO planning capacities for contributing to NATO' s military missions.

We need to adapt to New Realities

EUROGENDFOR is enhancing its ability to generate rapidly deployable forces. This involves streamlining recruitment, contributing to the process of force generation, contributing and delivering PDTs and contributing to training processes to ensure that personnel can be quickly mobilized to respond to emerging crises. By continuously updating our SOPs and TTPs, EUROGENDFOR ensures that its methods remain aligned with the latest developments in law enforcement and crisis management practices where the PHQ will be the centre of gravity in order to support its members states in their international agenda's.

Supporting Deployed Forces

EUROGENDFOR is committed to supporting its forces throughout

the lifecycle of a mission. This involves providing the necessary real-life support to enhance the quality of their performance and ensure they can effectively accomplish their mandated tasks. Such support includes logistical assistance, ongoing training, and access to advanced equipment and technology, but also provide the necessary flexibility when a 'mandate of a mission is changed or extended.

Strategic Enhancements

To remain effective and relevant, EUROGENDFOR, under CIMIN leadership, is redefining its Strategy for the next five- years cycle from 2025-2029. This strategic re-evaluation involves exploring ways to contribute to crisis management operations, to improve the governance of EUROGENDFOR, to be more efficient, rapidly deployable, aligned with the evolving security environment and respecting and implementing the strategic guidance of our members states.

Enhanced Communication and Cooperation

Effective communication is vital for the success of any crisis management operation. EUROGENDFOR is enhancing its communication strategy to ensure that information flows smoothly between all levels of the organization and with the external partners. Strengthening cooperation with the EEAS is also a priority.

By working closely together with this key EU body, EUROGENDFOR can better align its operations in accordance with the broader EU security and defence policies.

Because strategic communication is of such great importance, a panel of experts from our member states worked on creating a new Strategic Communication Plan in the last week of May 2024 in our PHQ.

- **The latest EU strategic document** that gives direction to the European security and defense policy is the EU Strategic Compass f rom 2022 to 2030, which builds upon the CSDP.
- The Strategic Compass establishes a common strategic vision for the EU's security and defence. This vision is rooted in the EU's commitment to protecting its citizens, EUs values, and interests, while contributing to international peace and security.
- **Strategic Compass (2022-2030)**
  - Establishes a common strategic vision for the EU's security and defense.
  - It provides a shared assessment of the strategic environment and of the threats and challenges whichthe Union is facing.
  - It sets concrete and wide-ranging objectives to achieve these goals.
  - The SC gives directions to allow for faster deployment, in complex environments, specifically in current and future civilian CSDP missions.

The Strategic Compass identifies terrorism, violent radicalisation and the proliferation of weapons of mass destruction as the main threats to European security.

In a second section, it lists hybrid strategies, cyberattacks, disinformation campaigns, direct interference in our elections and political processes, economic coercion and the instrumentalization of irregular migration flows, and the use of disruptive technologies as an element of strategic advantage.

Vulnerability in the so-called "global common spaces" the so called third pillar, such as maritime, air and outer space, and cyberspace, while the fourth pilar includes climate change, environmental degradation, natural disasters and global health crises.

When we look at Cybersecurity, in a Stability Policing environment, can be analysed by itself, but also in the context of a broader hybrid threat context:

To exemplify - Russia's adept use of globalization and state-of-the-art technologies exemplifies how hybrid threats exploit vulnerabilities, destabilize adversaries, and impede decision-making processes.

The concept of the 'grey zone' encapsulates the ambiguity deliberately introduced by hybrid warfare, blurring the lines between peacetime and wartime, creating an environment characterized by asymmetry and unpredictablyunexpectedness.

Hybrid threats can take different forms and vary depending on the context.

Some examples of elements that can contribute to

hybrid threats includes a few, and I mention

Disinformation campaigns: Spreading false or misleading information to influence public opinion.

Cyberattacks: The use of digital means to disrupt, spy on, or sabotage systems.

Political subversion: Influencing or undermining the political process by means of manipulation, bribery or blackmail.

Economic pressure: The use of economic measures, such as sanctions or financial manipulation, to cause destabilization.

Unconventional military actions: Conducting military operations without a formal declaration of war. And..

Proxy Wars: Supporting armed groups or conflicts to advance one's own objectives without direct involvement.

Hybrid threats are dynamic and evolve with changing geopolitical conditions. It is important for countriess and organizations to develop flexible and coordinated approaches to deal with these complex challenges.

- **Juist about Cybersecurity Vulnerabilities**

  G **TFs** encounter the challenge of addressing and adapting to evolving cybersecurity threats. As hybrid threats increasingly exploit digital domains, GTFs must continuously enhance their cybersecurity measures to safeguard critical information and infrastructure from sophisticated cyberattacks. As we fortify our response to hybrid threats, GTFs acknowledge the challenge posed by evolving cybersecurity threats. The interconnected nature of the cyber domain **demands continuous enhancement of our cybersecurity measures**. By identifying and addressing vulnerabilities, we ensure the protection of critical information and infrastructure, fortifying our resilience against sophisticated cyberattacks within the hybrid warfare landscape.

The Growing Importance of Cyber Security

Although cyber security has not traditionally been a focus for EUROGENDFOR, its significance is rapidly increasing. The effective implementation of mandated tasks by international organizations often depends on secure and reliable communication and data management systems. Cyber threats pose a significant risk to these systems, potentially compromising mission success and personnel safety.

Way ahead:

EUROGENDFOR is analysing how to take steps to integrate cyber security into its operations. This includes:

1. **By Training**: Providing comprehensive cyber security training for all personnel to ensure they can recognize and respond to cyber threats and identify opportunities inenhancing the collaboration with EU cybersecurity agencies to protect critical infrastructure.
2. **Invest in Technology and** remaining informed about cutting edge cyber technologies to both, know what you could deploy yourselfand also know what your adversaries coulduse against you.
3. **By investing and establishing Partnerships**: Collaborating with cyber security centres and experts to develop robust security protocols and share best practices.
4. **Organisesufficient Cyber Response**: Establishing internal procedures for monitoring cyber activity and responding to cyber incidents swiftly while maintaining the operational and communication capabilities where possible.
5. **Organise and conduct regular audits**: to identify and address potential vulnerabilities that can be exploited in the ever-evolving cyber domain.

I come to a conclusion:

The European Gendarmerie Force is adapting to the complex and evolving landscape of global crisis management. By enhancing its rapid deployment capabilities, updating its strategies and practices, increasing member state participation, improving communication, and strengthening cooperation with the EEAS.

EUROGENDFOR is positioning itself to meet future challenges effectively. Integrating cyber security into its operations ensures that EUROGENDFOR can protect both its internal systems and also the collaborative missions it is undertaking. As EUROGENDFOR continues to evolve, it remains a crucial force for stability and security in an increasingly unpredictable world.

I thank you for your attention.

Hans Vroegh

COL - Dutch Royal Marechaussee

Eurogendfor Permanent Headquarters' Commander

3 - STABILITY POLICING DAY 2024

Speech delivered by COL Luigi Bramati, NATO SP COE's Director, on the occasion of the Stability Policing Day 2024

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.

Luigi Bramati
COL - Italian Carabinieri
NATO SP COE's Director

THE NEED FOR U.S. STABILITY POLICING

Bulgarian military police train by detaining and searching U.S. military police forces from 508th Military Police Company during Saber Guardian in Slobozia, Romania, May 31, 2023 (U.S. Army/Samuel Hartley)

The Need for U.S. Stability Policing

by John F. Hussey

Published on Joint Force Quarterly Issue 115, 4th Quarter 2024

Military commanders must plan for, train, and resource an adequate number of military personnel to implement order, protect property, and maintain security to prevent lawlessness. Lawfulness is the foundation of stability. Operational

planners must anticipate that U.S. mili- tary forces will likely encounter chaos with a dysfunctional police force. The situation will likely require immediate attention to protect the indigenous people of the area, their property, and their economic livelihood. Successful planning and execution of a stability police force will enable the U.S. military to achieve or ensure stability during the immediate transition from combat operations to stability operations. Moreover, a stable environment during this transitional period will enable the United States to eventually achieve its strategic endstate.[1]

It is time for the U.S. military to recognize and accept the fact that it must establish a stability policing capability. For definitional purposes, stability policing is police-related activities intended to rein- force or temporarily replace indigenous police forces (IPF) to contribute to the restoration and/or upholding of public order and security, the rule of law, and the protection of human rights.[2]

Once major combat operations subside, a gap exists in which the host- nation's security establishment has disintegrated or simply does not exist, and some form of stability policing is re- quired to perform direct law enforcement roles and train IPF that can conduct com- munity policing.[3] Establishing security with the military and the police is vital for a variety of reasons, most importantly to consolidate gains by providing secu- rity. Conceptually, it will be difficult to achieve other objectives and rebuild the other pillars of society such as political and economic systems without a safe and secure environment. The cost of not fix- ing this gap will be significant because the population will not feel secure, and the host-nation's government will lose legiti- macy in the eyes of its citizens. Nefarious actors will also expand their trade and take full advantage of this gap and in some cases may become the de facto government. In addition, the operational deployment of U.S. military forces on the ground will be extended.

In many postconflict environments, extremist and criminal organizations present a variety of threats. The host- nation government, if present, is trying to establish itself and gain legitimacy in the eyes of the civilian population. Prior to the initiation of Operation Iraqi Freedom, RAND conducted a study on nation-building. The report noted that a gap often exists in which the host na- tion's security establishment is not up to par in the weeks following the arrival of foreign troops or police which are being used to create security and stability. During this time insurgents, organized criminal networks, or random criminals are unorganized and there may still be some form of order that must be ex- ploited to prevent chaos and lawlessness Military forces can prevent conflict, act as peacekeepers to separate combatants, and begin disarmament. However, they lack the mandate or the expertise to enforce the local rule of law by law enforcement– specific training

> "IT WILL BE DIFFICULT TO ACHIEVE OTHER OBJECTIVES AND REBUILD THE OTHER PILLARS OF SOCIETY SUCH AS POLITICAL AND ECONOMIC SYSTEMS WITHOUT A SAFE AND SECURE ENVIRONMENT"

Marines with Kilo Company, 3rd Battalion, 8th Marine Regiment, partnered with Afghan National Police, patrol Garmsir District, Helmand Province, Afghanistan, June 1, 2012 (U.S. Marine Corps/Kenneth Jasik)

or experience.[4]
While the military historically has provided the security in postconflict environments, recent U.S. experiences in Iraq and Afghanistan indicate that the
United States has a mixed track record in establishing security, partly because it is the policing component of this force. In Afghanistan, the military's approach to the police assistance mission was to repli- cate what it was doing to train the Afghan National Army, which has the potential to create a militarized police force.[5] Civilian police have more experience working with the civilian population than do mili- tary personnel. Additionally, those with the proper education and experience have the prerequisite police skills to conduct civilian law enforcement duties and to train an IPF.[6]

"THE UNITED STATES DID NOT CAPITALIZE ON THE LESSONS LEARNED FROM PREVIOUS EFFORTS IN HAITI, THE BALCANS, OR IRAQ, WHICH RESULTED IN A PATTERN OF FAILING TO DEAL WITH LARGE-SCALE BREAKDOWNS IN PUBLIC ORDER THAT OCCURED AFTER INTERNATIONAL INTERVENTIONS"

Change the Paradigm

The U.S. military did not achieve a decisive victory during the Iraq War for a variety of reasons. Perhaps the foremost reason was the inability to consolidate gains through activities to make enduring any temporary opera- tional success and set the conditions for a stable environment allowing for a transition of control to legitimate authorities.[7] Consolidating gains in the Iraq and Afghanistan wars required the killing or capturing of enemy forces, both regular and irregular. Simultane- ously, U.S. forces should be separating the enemy from the population, seizing control of weapons and munitions, and controlling the population in a way that maintains order and security without creating incentives for further resis- tance.[8] To achieve these goals, the U.S. military would have to provide security through a national police force that would focus on securing the population by reducing the criminal elements.
General Tommy Franks, USA, U.S. Central Command commander when the wars in Afghanistan and Iraq began, was responsible for the planning and execu- tion of the war plans in both campaigns. The plans were seriously flawed and
incomplete because the planners ignored phase IV (stabilize) and phase V (enable civil authority). Invading another country with the intention of regime change without a serious strategy for providing security after major combat operations defies logic and falls short of proper professional military standards of compe- tence.[9] The U.S. military often does well at planning and executing major combat operations; conversely, it does poorly at consolidating gains. General Franks and his top commanders believed that upon completion of combat operations, the postwar phase, or phase IV stability operations, would be the responsibility of other U.S. Governmental agencies. While the military had one view, many of the civilians at the Pentagon were sure
that U.S. Central Command should have known that they were responsible for postconflict Iraq.[10]

General Franks believed that the United States had sufficient combat forces in Iraq but did not initially have enough civil affairs, military police, and other units that could execute phase IV stabilization operations. He noted that it was not the level of forces but rather
their composition. He believed that there were enough military personnel present as far as raw numbers were concerned but that the forces in theater did not have the background or experience necessary to interact with a civilian population and establish order after major combat was over.[11]

U.S. Military Training of Civilian Police During Conflict

During the Vietnam War, South Viet- namese police were expected to procure intelligence, maintain public order, and simultaneously fight the Viet Cong. The various roles of the police created con- fusion within the police agency itself, among the population, and with the Viet Cong. The primary mission of the South Vietnamese police was to fight conventional crime; however, they were simultaneously expected to perform a counterinsurgency and counterterror- ism role. As a result, they were often targeted by the Viet Cong and had to respond to attacks that many would describe as terrorist or insurgency-like attacks. Numerous South Vietnamese police officers were killed during this conflict.[12]
The U.S. Office of Public Safety provided more than 300 advisors and ap- proximately $300 million for the training of the South Vietnamese police force dur- ing the Vietnam War. During this time, the South Vietnamese police force grew from 16,000 to 122,000. Unfortunately, the U.S.-trained South Vietnamese police gained a reputation for commit- ting acts of brutality and torture—and for conducting sweeps that included the arrest of seemingly innocent individu- als. They became overly "militarized," and as drug abuse became rampant in Vietnam, anti-narcotics units began to form. Those involved in anti-narcotic law enforcement operations soon were ac- cused of corruption, which then grew to become prevalent within the ranks of the South Vietnamese police force. The force quickly lost credibility with the popula- tion and the U.S. advisors who trained them.[13]
Fast-forward to the U.S. role of developing police in Afghanistan. Shortly after the U.S. invasion of Afghanistan following the September 11 attacks, the international community assessed that the Afghan police were in a desperate state and required extensive international assistance. Initially, the United States did not capitalize on the lessons learned from previous efforts in Haiti, the Balkans, or Iraq, which resulted in a pattern of failing to deal with large-scale breakdowns in public order that occurred after interna- tional interventions. The inability to plan for the proper personnel and resources allowed for looting and civil disorder to occur. This created a climate of impunity and encouraged criminal violence and street crime. The lack of security created widespread civil unrest.[14]
The United States failed to conceptualize and plan to deploy the required international civilian police to Afghanistan. The initial internal analysis discovered that the Afghan police lacked the necessary training, uniforms, logistical resources, and infrastructure necessary to function. In essence, according to Ryan Crocker, then Deputy Assistant Secretary of State for Near Eastern Affairs, the Afghan police were at "ground zero." Consider the fact that trainers had to contend with a population that had an 80-percent illiteracy rate.[15]
The inter- national community rapidly recognized these deficiencies as well as a major fund- ing deficit. It quickly became apparent that the international community would have to provide training to the nascent Afghan police candidates.[16]

Massachusetts National Guardsman with 772nd Military Police Company fires M26 Modular Accessory Shotgun System during Justified Accord 2024 for less-lethal weapons tactics training at Counter Insurgency Terrorism and Stability Operations Training Centre, Nanyuki, Kenya, February 28, 2024 (DOD/Carter Acton)

Since the U.S. military responded quickly and with a "light footprint," the United States did not consider deploying any type of police assistance team.[17] In fairness, this was not an initial concern when one considers that the United States believed it was necessary for a hasty military response to the attacks of September 11. When the United States did respond and consider the necessary requirements to train, resource, and bolster the Afghan police, the U.S. military–led police assistants trained on "what they knew," which resulted in an overmilitarized approach to policing. Once again, similar to what occurred in Vietnam, the U.S. military placed more emphasis on training the Afghan police to engage in combat operations against the insurgency waged by the Taliban rather than policing the civilian popula- tion. In Iraq, the police were equipped with mortars and machine guns, not tools commonly associated with those trying to build rapport with the local community.[18]

Like what occurred in Vietnam, Afghan police commanders engaged in criminal activities, namely the torture of detainees, corruption, and even extrajudi- cial killings. Once again, the U.S. military and advisors encountered the quandary of how to balance the U.S. goals of combating the insurgency with the long- term objectives of creating a professional police force that respected human rights and the rule of law.

The Department of State and Department of Defense (DOD) must accept the fact that the military is not trained, resourced, or prepared to train foreign police forces. Organically, the mil- itary does not possess the organizational structure to deploy, on a large scale, trained law enforcement experts familiar with the concepts of community policing. As far as personnel and resources, senior leaders had limited alternatives and had to rely on deployed military personnel with no experience in policing to serve as police advisors. Nearly anyone could conclude that there are two correlating factors that one can observe between U.S. actions in Vietnam and those in Afghanistan and Iraq. In each situation, there was an actual conflict raging, and the training of the host-nation police focused more on the support of military operations, which entailed combating enemy insurgents, as opposed to protect- ing the civilian population.[19] Deploying military personnel to police a local com- munity should not be the primary option. Simply stated, most military forces are not trained to do civilian police work.[20]

Military Police Can Assist in Consolidating Gains

The 200th Military Police Command (MPC) is one of only two military police commands in the U.S. Army, and it provides the full range of mili- tary police (MP) support to large-scale combat operations globally. As the senior MP command of the U.S. Army Reserve, the 200th MPC has approxi- mately 14,000 Soldiers and civilians.

It conducts mission command for all assigned and attached units conduct- ing or supporting MP operations by integrating capabilities from all three military police disciplines: police opera- tions, detention operations, and security and mobility support.

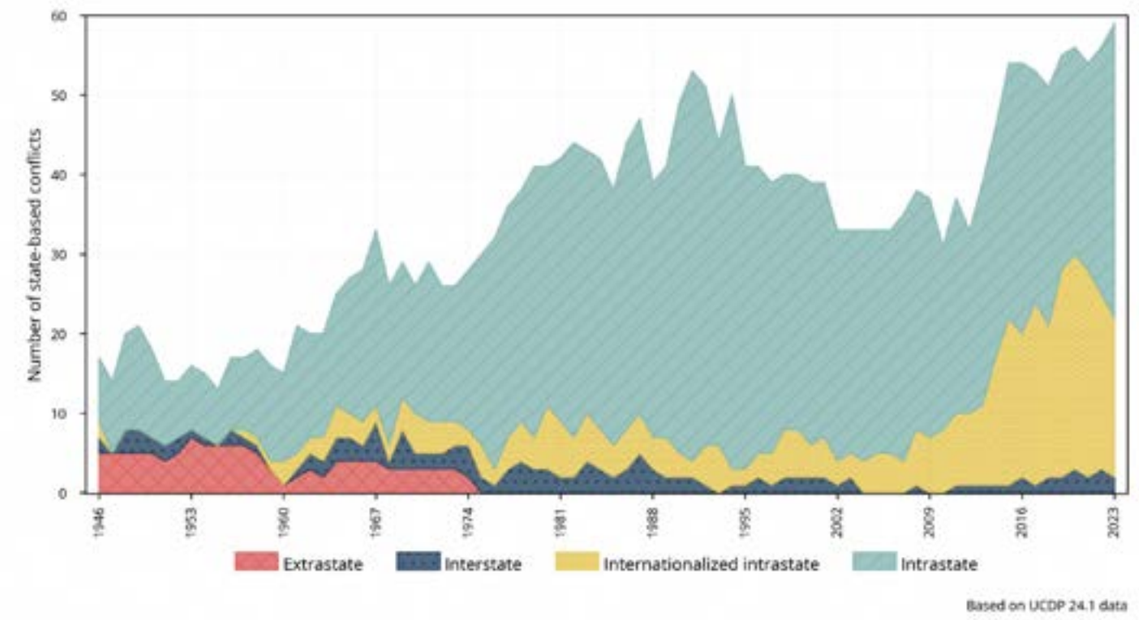
During a quarterly training brief, with an audience consisting of the deputy commanding general officers, command sergeant major, key members of staff, and the command teams from 4 brigades and 25 battalions, it seemed evident that this command was unique not only as an MPC, but also many of the Soldiers held key positions within our nation's criminal justice system. Present in the audience were a judge, a Federal Bureau of Investigation agent, several chiefs of police, senior-ranking police officers, members of the Department of Homeland Security, court administrators, and practicing attorneys. These Soldiers were unique to this unit in that their civilian skills and military skills were in alignment, and they were all assigned to an MPC. The knowledge, skills, and abili- ties, both military and civilian, had the potential to augment military command- ers and military operations in support of the Army and the joint force.[21]

The 200th MPC has already or is coordinating with each of the geographic combatant commands and Army Service component commands to initiate and build

Table. U.S. Military Police vs. NATO Stability Police

U.S. Military Police	NATO Stability Police
Designated military forces with the responsibility and authorization for the enforcement of the law and maintaining order, as well as the provision of operational assistance through assigned doctrinal functions.	NATO stability policing activities are intended to reinforce or temporarily replace indigenous police in order to contribute to the restoration and/or upholding of public order and security, rule of law, and the protection of human rights.

Figure 1. State-Based Conflicts by Type of Conflict (1946–2023)



Source: Shawn Davies et al., "Organized Violence 1989–2023, and the Prevalence of Organized Crime Groups," Journal of Peace Research 61, no. 4 (2024), https://ucdp.uu.se/downloads/charts/.

lasting relationships. The purpose is to provide a strategic vision by geographi- cally aligning the four brigades, building partner relations, and integrating into regional training events while enhancing detention operations into contingency plans and operational plans. Perhaps the most important alignment at the time of writing is the European theater based on a resurgent Russia and the fact that Russian forces were engaged in the inva- sion of Ukraine.

As part of this strategic concept, key leaders from the 200th MPC conducted site visits in the European theater to meet with various commands to synchronize capabilities and planning. It was also important to meet key North Atlantic Treaty Organization (NATO) Allies to understand their mission and capabilities and see how the MPC could work to- ward common goals and unity of effort.

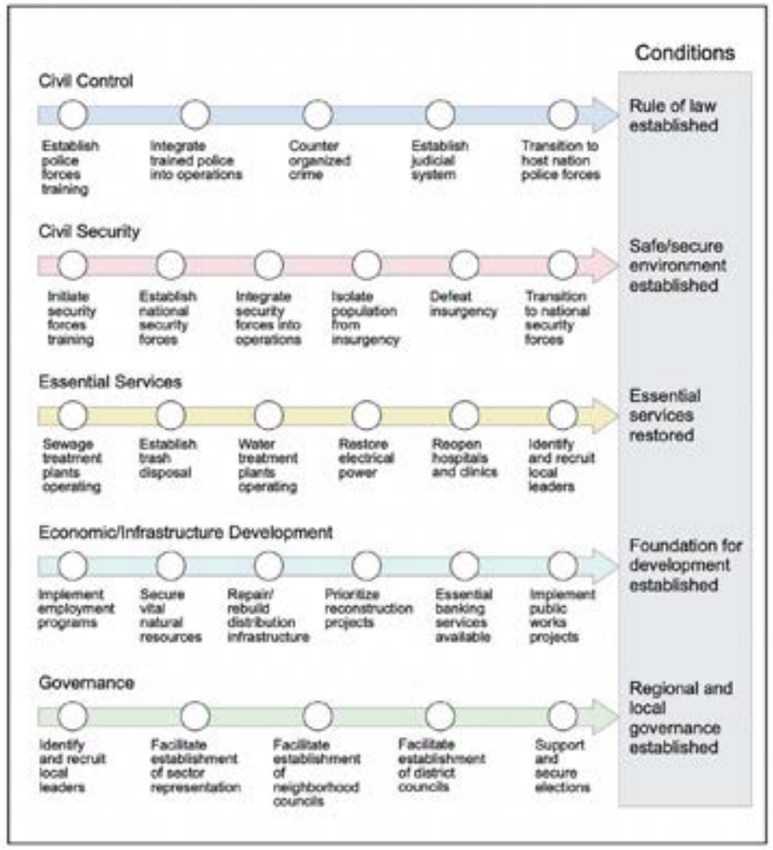
The trip included a visit to the NATO Stability Policing Centre of Excellence in Vicenza, Italy, and a meeting with various leaders from this institution. Members of the 200th MPC came to learn the mission of the NATO Stability Police and how that capability could assist U.S. MPs on the battlefield. This meeting was key for a variety of reasons, perhaps most important to differentiate the capabilities and mission set of the U.S. Military Police and that of the NATO Stability Police.

As the meeting with NATO Allies concluded, the leadership of both com- mands gained an understanding of each organization's capabilities and how the various MPs with different missions can support each other on the battlefields of the future. More important than un-derstanding each other's capabilities was the fact that the senior leadership quickly appreciated there were deficiencies and were able to identify gaps. One of the key aspects that is often overlooked that inev- itably will affect consolidated gains is that military forces will encounter civilians on the battlefield who will require assistance and, if not dealt with, can potentially disrupt military operations. Military plan- ners also know there will be nefarious actors seeking to take advantage of the absence of the rule of law and proactively applying their criminal trade against a dysfunctional or struggling government and an absent or emerging police force.

What Does the Future Battlefield Really Look Like?

Senior leaders in the U.S. military have a responsibility to monitor the inter- national threat environment, which is becoming increasingly complex. To reduce the anxiety that confronts senior military leaders, the new National Defense Strategy (NDS) has repri- oritized the threats facing the United States to a "1 + 1 + 3" construct. According to the Joe Biden administra- tion, the greatest threat comes from China, which the NDS describes as the "most consequential strategic competi- tor," followed by "acute threats" from Russia, and then persistent threats from other potential adversaries such as North Korea, Iran, and violent extrem- ist organizations.[22] Regardless of the threat forecast of the NDS, the fact remains that "Politicians, like generals, have a tendency to fight the last war."[23] Is the NDS correct? Are the challenges that the United States might encounter likely to come from nation-states, or could they come from elsewhere? Some contend that the very institution of warfare is declining and, in some cases, becoming obsolete.[24] Historians and noted scholars posit that we have witnessed a change in warfare since the post–World War II era.[25] There is no question that warfare is ubiquitous and can be documented in virtually every corner of the globe. However, most of those conflicts have not been large-scale combat operations, but rather what many would describe as civil war. These internal struggles are often interlaced with social problems, with conflicts stemming from age-old ethnic and religious hostilities, territorial autonomy, political ideologies, reduced resources, limited opportunities, and wealth distribution.[26]

Figure 2. Sample Lines of Effort



Source: Joint Publication 5-0, Joint Planning (Washington, DC: The Joint Staff, December 2020), IV-31.

These modern conflicts differ signifi- cantly from past interstate conflicts. In previous conflicts, we often saw nations and their militaries engage in traditional warfare to achieve national objectives.[27] Modern conflicts frequently do not consist of a sovereign nation-state in an interstate conflict with a traditional military chain of command. This may result in these con- flicts being waged without traditional laws of warfare; thus, they can be more brutal and chaotic. Often, those in charge are more focused on the control of the popu- lation. Therefore, civilians are targeted and sometimes preyed on by nefarious actors.[28] These conflicts are typically the result of globalization; populations with limited resources seek greater opportunities and thus erode the sovereignty and capacity of many states.[29] In many areas of the globe this may result in failed or fragile states or even brown zones, specific neighborhoods or geographic areas where state govern- ments are reluctant to intervene. These areas can be considered "no-man's-land," and leaders must anticipate that personnel operating within these areas will likely encounter a failed, broken, destroyed, or simply nonexistent justice apparatus (that is, a lack of effective police, judiciary, and detention operations).[30]

According to Sean McFate, since 1939, only 6 percent of armed conflict has been conventional, while 94 percent has been unconventional. He further contends that conventional warfare no longer wins wars.[31] Regardless, military planners must contend with and plan for the worst-case scenario, which would be conventional war with a nation-state such as China or Russia. Irrespective of the conflict—conventional, unconventional, or hybrid—the U.S. military will encoun- ter a civilian population on the battlefield that must be part of the operational plan, and resources must be dedicated to them.

This means that the U.S. military will not be able to consolidate gains and thus score a major combat victory in large- scale combat operations and simply pack up and redeploy. Planners must realize that the U.S. military and allied nations will be involved in some form of stability activities (SA) as the combat portion of the offensive and defensive operations wind down. One may define stability activities as the numerous military missions, tasks, and activities conducted outside of the continental United States and in coordination with other instruments of national power to maintain or reestablish a safe and secure environment and bolster host-nation legitimacy by facilitating essential governmental services, emer- gency infrastructure reconstruction, and humanitarian relief. SA will afford senior commanders the opportunity to consoli- date combat success into some form of a political victory and thus set the condi- tions for a stable environment, allowing for a transition of control to legitimate authorities.[32]

When planners consider lines of effort (LOEs), each operation or line is inde- pendent of others, although there may be crossover—thus, a relationship. Planners must consider a variety of factors, including culture, prewar level of

Army 2nd Lieutenant Madalynn Long, military police officer from 728th Military Police Battalion, issues orders to her platoon while conducting foot patrol as part of field exercise during multinational United Nations peacekeeping exercise Shanti Doot 4 in Bangladesh, March 1, 2018 (U.S. Marine Corps/Adam Montera)

Major General Marion Garcia, commanding general of 200th Military Police Command, talks to her staff in battle update brief during annual training exercise at Fort Knox, Kentucky, April 27, 2018 (U.S. Army Reserve/Elizabeth Taylor)

the gov- ernment, infrastructure, economy, and the postwar effects of each of these. While these are only some of the examples, there are obviously many more depending on the theater and nation involved. Planners will have to incorporate a method to evaluate success that can allow commanders and lead civilian agencies to determine when a transition occurs and the next phase can be initiated. Planners will use a tool known as the measurement of performance, which is an indicator used to measure a friendly action that is tied to measuring task accomplishment.[33]

As commanders continue to review their LOEs and apply their measurement of performance, their actual overall mea- surement of success will be determined by the measurement of effectiveness, which is an indicator used to measure a current system state, with change indi- cated by comparing multiple observations over time.[34]

As noted in Joint Publication 3-24, Counterinsurgency, for an insurgency (and let us add nefarious criminal actors) to flourish, there must be significant ca- pability gaps in the national government or local allies to provide security for its territory and population.[35] Legitimacy of the host-nation government will be achieved by its perceived ability to pro-vide basic services to the population, one of the most basic of which is to feel safe and secure. If the host-nation govern- ment cannot provide security for the population, it will not be able to gain their confidence, and governance will be difficult if not impossible to implement or conduct. Planners must realize that insurgents and nefarious criminal actors also understand this and will therefore target host-nation and allied military forces security personnel and security of the overall apparatus.[36]

When considering the overall operational plan, those responsible for the transition from combat to SA should consider Abraham Maslow's hierarchy of needs model. The model can help envision stability and the development of LOEs via the basics that any population will require in a war-ravaged environ- ment in which obtaining life's essentials (namely food, water, and safety) may prove difficult. In most situations, people who do not feel safe will move their families to seek safety and rely on the goodness of others by way of an international or nongovernmental orga- nization. This is why there are so many internally displaced civilians during a time of war. For civilians to return to an area they vacated, they must feel a sense of security and a sense of justice. This is a basic concept that military planners must recognize during any deliberate or crisis action planning. Without security, the conditions necessary to fulfill the other hierarchy of needs in Maslow's hierarchy will never be met.[37]

There are a variety of LOEs, but unless there is a safe and secure environ- ment, the others are simply concepts.

Based on that premise, the population does not focus on elections, construc- tion, and economic development until the basic rule of law and/or security are established. For example, on the International Day of Education, UNICEF reported that the war in Ukraine had jeopardized 5.3 million children who have encountered barriers preventing access to education, including 3.6 million children directly affected by school closures.[38] Leonard Rubenstein, a professor and director of the program on Human Rights and Conflict and Health at Johns Hopkins University's Bloomberg School of Public Health, noted that because travel is dangerous, people often "take their chances without medical care, which leads to more suffering and more death." Women giving birth are often afraid to go to hospitals and are more likely to receive a caesarean section if they do.[39] The civilian sector will not return to normalcy until the population feels secure from the dangers of war and from those nefarious actors often found in combat zones. With the rule of law and/or security absent, the population cannot focus on secondary and tertiary issues such as education, construction, and elections. Planners must ensure security is considered and provided for other LOEs to progress.

At the operational level, this focus may require a planner to consider the police, the judiciary, and corrections to resolve current criminal justice and civil law requirements and develop a more stable justice system under the control of the government and ultimately the population. The U.S. public and indig- enous population must understand that this is a long-term effort that may take

years to implement in war-torn nations or failed states. Planners must consider what personnel and resources are necessary and available at the tactical level of war to achieve the goals and move SA forward along the various LOEs.

U.S. Military and Stability Policing

At least 130 insurgent conflicts have occurred since World War II.[40] The 1990s were the first decade in nearly half a century in which the U.S. military was deployed on missions that involved the reconstruction of govern- ments, infrastructure, and economies after quelling the chaos of internecine conflicts.[41] Whether elected officials or senior military leaders like it, SA have become a main component of U.S. mili- tary operations. Commanders and mili- tary staffs must be versed in SA because they are simply part of the conundrum of conflict and failed/fragile states.

Conceptually, the State Department and DOD realize that host-nation stability is the goal. The ability of State and DOD to provide stabilization via the host nation and its security forces is a key component for U.S. forces to complete the mission and redeploy.[42]

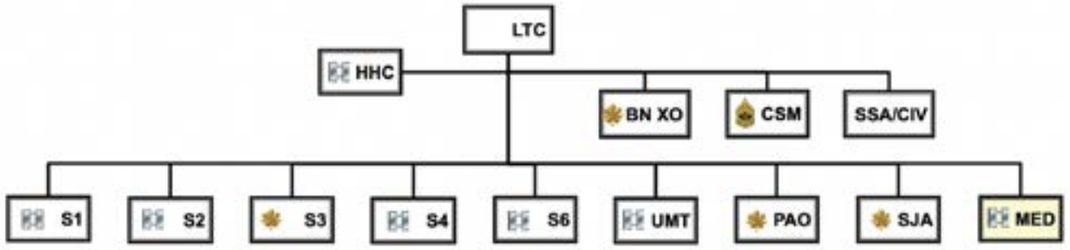
To achieve security during SA, the U.S. military and elements of the State Department have attempted to rebuild host-nation military and security forces, especially police forces and rule-of-law systems. Perhaps one of the most re- cently noted efforts was in Afghanistan.[43] Unfortunately, traditional MP and other military forces, except for the NATO Stability Police, did not have the techni- cal capability to train IPF. The training of police personnel requires experience as a civilian law enforcement officer, and military forces often lack the training, experience, and mindset for policing. Planners must understand that military forces are unfamiliar with the concepts of the rule of law and do not have the expertise to administer justice in a nonfunctioning justice system.

Additionally, those forces may not understand or appreciate the cultural sensitivity of the law in relation to the country or region in which they are deployed.[44] Deployed forces often bring with them an ethnocentric bias that could complicate SA.[45] Military forces do not have the expertise to conduct most law enforcement tasks. They do not routinely perform law enforcement missions and generally lack a law enforcement mind- set.[46] More generally, the military force lacks the experience and skills necessary to deal with civilians in a peacetime setting.

The most effective method to achieve operational goals in this area is to de- ploy individuals who have experience as civilian law enforcement personnel. NATO has

this capability in the form of its Stability Police. Stability policing consists of activities aimed at improving the capacity and capabilities of the law enforcement agencies within a host- nation and/or to police its population temporarily until they or a follow-on force can take over that responsibility.[47] Military planners must understand that the establishment of internal security in stabilization efforts is paramount dur- ing the "golden hour" after combat operations conclude to prevent additional unrest. Here the golden hour is the short time of several weeks to several months after combat operations when external intervention may enjoy both popular sup- port and legitimacy and the opposition has not had the time to organize.[48]

Figure 3. Military Police Battalion Command Structure



A Conceptual Change

RAND researchers concluded that an abuse of the civilian population, who will then lose confidence in both the military forces and the police within their nation.[50]

The Iraq Study Group, a group formed to conduct an independent, bipartisan assessment of the situation in Iraq and the implications for U.S. policy, provided several recommendations to improve Iraqi police. One was to suggest that police trainers "should be obtained from among experienced civilian police executives and supervisors from around the world. These officers would replace the military police personnel currently as- signed to training teams."[51]

A report from the Special Inspector General for Afghanistan Reconstruction, Police in Conflict: Lessons from the U.S. Experience in Afghanistan, noted in es- sence that the United States and the international community lack an expeditionary police assistance capability with the number of qualified police assistance personnel required for most stabilization missions in nations suffering from high levels of conflict. The report recommended that the Secretary of Defense develop a capability that can quickly identify and deploy military personnel who possess the necessary civilian police expertise.[52]

Members of the Army Reserve and Army National Guard often possess these unique civilian skills. The issue is that many of the individuals who possess police expertise serve in key leadership positions within Modified Table of Organization and Equipment units, and it would do more damage to remove a commander, key staff officer, or senior noncommissioned officer from a deploy- ing or deployed unit to conduct police assistance training. It is therefore neces- sary to create this capability in the Army Reserve or the Army National Guard by establishing a stability MP battalion. The personnel would have to demonstrate key law enforcement capabilities necessary to deploy to a combat zone and train an IPF. This could come from current members of the Reserve components;

however, the program must be expanded to capture the best that we have who are currently employed by civilian law en- forcement agencies.

Conceptually, U.S. Military Police could adopt the model being used by U.S. Army Civil Affairs and Psychological Operations Command (Airborne). In 2019, then–Secretary of Defense Mark Esper directed the Services to use a methodology frequently used by the Army Medical Department for physicians, Chaplain Corps for clergy, and Judge Advocate General for attorneys—namely, a direct commissioning route. The direct commissioning program was incorpo- rated into the existing 38G program, which provides unique civilian-sector expertise in the form of military govern- ment specialists.

Traditionally, 38G candidates specialize in one or more of the 18 skill identifiers from a variety of different occupations required to assist in the stabilization of a nation coming out of conflict. Specialties range from emer- gency management, water, and sanitation to the rule of law. Theoretically, this same program can be tailored to meet the needs of the MP corps. Candidates can be recruited from a variety of sources, in- cluding large metropolitan police forces. There are literally thousands of large, medium, and small urban and rural police agencies that have qualified personnel and trainers who would be eligible for this program. Candidates can come from the retired ranks as well as Federal, state, and local law enforcement academies lo-cated throughout the country. It should be noted that those who enter this pro- gram must meet the physical and medical requirements, and they would not be eligible to serve in a command or key staff capacity. Rather, their career would be spent in the career field that best uses their civilian police expertise.

This unit would be organically assigned under the 200th MPC and could be used as a global asset. While many of these law enforcement personnel could come from the Army Reserve or Army National Guard, each of the other Services would have an opportunity to contribute law enforcement specialists to this stability police battalion, thus making it a joint capability. The Naval Criminal Investigative Service is a civilian law en- forcement agency with a mission focus to investigate and defeat threats to the Navy and Marine Corps. Additionally, the Navy also has a master-at-arms program that is the naval law enforcement military occupational skill. The Coast Guard Police Department is a diverse force of Active- duty law enforcement personnel who would have capabilities that would greatly enhance stabilization operations. The Navy and the Coast Guard also share the unique ability to assist in both maritime and port security. The Marine Corps may be deactivating its three MP battalions, but presently they are still operational, and many Reserve personnel are civilian law enforcement officers.

Like the Navy, the Air Force has security forces whose mission it is to protect, defend, and fight. They are re- sponsible for maintaining missile security, defending air bases around the globe, performing law enforcement on those bases, and handling military working dogs. The Air Force also has an inves- tigative branch, the Air Force Office of Special Investigations, which provides professional investigative services to com- manders of all Air Force activities. The office identifies, investigates, and neutral- izes criminal, terrorist, and espionage threats to Air Force and DOD personnel and resources.

In addition to a joint concept, the United States must consider its allies and the interagency community, both of which will play prominent roles in this venture. NATO has for many years been engaged in this task through its Stability Policing Centre of Excellence, which is a multinational collaborative effort to write doctrine, train, and execute stability police functions. The United States must also be prepared to use the interagency assets at its disposal. In the past, the United States has used a variety of inter- agency law enforcement assets, including the Department of Justice, the State Department's Bureau of International Narcotics and Law Enforcement Affairs, and the Federal Law Enforcement Training

Center. These interagency assets must be considered in conjunction with the military. The Military Police Stability Battalion would have the ability to rap- idly deploy; however, these missions can extend for many years and will require additional personnel and expertise to be successful.

Naturally, this can be tailored based on the need of the operation and the geographic area in which the military operation is occurring. For example, some locations may require more police personnel who are familiar with drugs, while other areas may have issues with human trafficking or weapons traffick- ing. This concept would allow police personnel with expertise in burglaries, rapes, latent fingerprints, DNA evidence collection, crime mapping analysis, and police intelligence, to outline just a few. The stability police force would not be involved in training police in military, counterinsurgency, or counterterrorism. Their force protection and resources will have to be provided by the U.S. military if this concept is to be effective.

> "LEGITIMACY OF THE HOST-NATION GOVERNMENT WILL BE ACHIEVED BY ITS PERCEIVED ABILITY TO PROVIDE BASIC SERVICES TO THE POPULATION, ONE OF THE MOST BASIC OF WHICH IS TO FEEL SAFE AND SECURE"

ternational police organizations. The issue thus becomes how expeditionary and deployable these agencies are. Regardless of which agency is in the lead, or where these capabilities are located, it is a require- ment that is necessary since the United States will absolutely be involved in these types of operations in the future. The United States should not depend on allies to supply these capabilities because each nation has its own inter- ests, some of which might not align with those of the United States. Addi- tionally, if the United States must act in a region where allies may not deploy or acts unilaterally in its own interests, having this capability will provide greater

> "THE POPULATION DOES NOT FOCUS ON ELECTIONS, CONSTRUCTION AND ECONOMIC DEVELOPMENT UNTIL THE BASIC RULE OF LAW AND/OR SECURITY ARE ESTABLISHED"

The Strategic Significance of a U.S. Stability MP Battalion

Police training programs normally fall under the purview of law enforce- ment organizations, such as the U.S. Department of Justice and United Nations–mandated options for commanders. Based on those factors, the United States must build this organic capability. Additionally, any geographic combat- ant command would benefit from having this type of capability to use in a noncom- bat environment to enhance the security plan. If the United States can train IPF who then gain the confidence of their population, there might be a reduction of failed or fragile states and transnational crime. A small investment during peace- time will be much more cost-effective than a major expenditure during combat operations or those SA that will inevitably occur postcombat.

The U.S. military has the personnel and capability to create a stability force battalion and should make the investment before it is faced with this dilemma. This is a realistic, strategic vision that is necessary and obtainable if there is a will to do so.

The policing capabilities that are present in the Army Reserve and Army National Guard are ubiquitous. These individuals also have a network in the civilian law enforcement community throughout the country, and the structure noted above can be operational within 3 to 5 years.

The annual training for this element can include a stability police battalion deploy- ing to parts of Africa and South America for a month at a time—and even longer, if necessary—to work with local police and conduct police training.

Notes

1 John F. Hussey, "Seizing the Initiative by Establishing the Rule of Law During Combat Operations," with Larry W. Dotson, Military Review, January–February 2013, 30–37.
2 Jorge Juan Perez Rodriguez, "Stability Policing Concept: A Must for the Alliance, an Opportunity for the Spanish Armed Forces," Cuadernos de la Guardia Civil: Revista de seguridad pública, no. 64 (2021), 55–72.
3 James F. Dobbins, "America's Role in Nation-Building: From Germany to Iraq," Survival 45, no. 4 (2003), 87–110.
4 Terrence K. Kelly et al., A Stability Police Force for the United States: Justification and Options for Creating U.S. Capabilities (Santa Monica, CA: RAND, 2009).
5 Special Inspector General for Afghanistan Reconstruction (SIGAR), Police in Conflict: Lessons From the U.S. Experience in Afghanistan (Arlington, VA: SIGAR, June 2022), https://www.sigar.mil/pdf/lessonslearned/SIGAR-22-23-LL.pdf.
6 Kelly et al., A Stability Police Force for the United States.
7 Field Manual (FM) 3-0, Operations (Washington, DC: Headquarters Department of the Army, October 6, 2017, Incorporating Change 1, December 6, 2017).
8 Mike Lundy et al., "Three Perspectives on Consolidating Gains," Military Review, September–October 2019, 16–30.
9 Michael E. O'Hanlon, "Iraq Without a Plan," Hoover Institution, December 1, 2004, https://www.hoover.org/research/iraq-with- out-plan.
10 Donald P. Wright and Timothy R. Reese, On Point II: Transition to the New Campaign; The United States Army in Operation Iraqi Freedom, May 2003–January 2005 (Fort Leavenworth, KS: Combat Studies Institute Press, 2008), https://history.army.mil/html/bookshelves/resmat/gwot/OnPointII.pdf.
11 Michael R. Gordon, "The Conflict in Iraq: Road to War; The Strategy to Secure Iraq Did Not Foresee a 2nd War," New York Times, October 19, 2004.
12 Jennifer C. Gibbs, ed., U.S. Foreign Police Advising: The Case of Vietnam (Carlisle, PA: Peacekeeping and Stability Operations Institute, 2020).

13 Gibbs, ed., U.S. Foreign Police Advising.
14 Robert M. Perito, U.S. Police in Peace and Stability Operations, Special Report (Washington, DC: United States Institute of Peace, 2017), https://www.usip.org/sites/default/files/sr191.pdf.
15 SIGAR, Police in Conflict.
16 SIGAR.
17 SIGAR.
18 Joint Center for International Security Force Assistance (JCISFA), Iraqi Federal Police: Advisor Guide (Washington, DC: JCISFA, May 2010), https://info.publicintelligence.net/ JCISFA-IraqiPolice.pdf.
19 Gibbs, ed., U.S. Foreign Police Advising; SIGAR, Police in Conflict.
20 Perito, U.S. Police in Peace and Stability Operations.
21 Author's observations while attending the quarterly training brief.
22 2022 National Defense Strategy of the United States of America (Washington, DC: Department of Defense, 2022).
23 Edward P. Warner, "Present Conditions Under the N.R.A.," American Marketing Jour- nal 1, no. 1 (January 1934), 6–14.
24 John Mueller, "War Has Almost Ceased to Exist: An Assessment," Political Science Quarterly 124, no. 2 (Summer 2009), 297–321.
25 Nils Petter Gleditsch, Peter Wallen- steen, and Håvard Strand, "Armed Conflict 1946–2001: A New Dataset," Journal of Peace Research 39, no. 5 (September 2002), 615–637, https://doi.org/10.1177/0022343302039005007.
26 Siniša Malešević´, "Is War Becoming Obsolete? A Sociological Analysis," The Sociological Review 62, no. 2, suppl. (December 2014), 65–86.
27 Malešević´.
28 Mary Kaldor, New and Old Wars: Organised Violence in a Global Era (Cambridge, UK: Polity Press, 2007).
29 Malešević´, "Is War Becoming Obsolete?"
30 John F. Hussey, "Recruiting, Vetting, and Training Police Forces in Postconflict Environments," Military Review, March–April 2019, 64–83.
31 Sean McFate, "The Sneaky War: Russia, China, and the U.S. and the Emerging Strategic Paradigm," National Defense University Foundation, video, 59:07, September 28, 2022, 11:55 mark, https://www.youtube.com/watch?v=DAhuNIg-iLE.
32 FM 3-0, Operations, chap. 8.
33 Joint Publication (JP) 5-0, Joint Planning (Washington, DC: The Joint Staff, December 2020), https://irp.fas.org/doddir/dod/jp5_0.pdf.
34 JP 5-0.
35 JP 3-24, Counterinsurgency (Washington, DC: The Joint Staff, April 2018), https://irp.fas.org/doddir/dod/jp3_24.pdf.
36 JP 3-24.

37 Saul McLeod, "Maslow's Hierarchy of Needs," Simply Psychology, January 24, 2024, https://www.simplypsychology.org/maslow.html.
38 UNICEF, "War Has Hampered Educa- tion for 5.3 Million Children in Ukraine, Warns UNICEF," January 24, 2023, https://www.unicef.org/ukraine/en/press-releases/war-has-hampered-education.
39 "Attacks on Ukraine's Hospitals Will Cause Long-Term Harm to Health," Relief Web, May 22, 2022, https://reliefweb.int/ report/ukraine/attacks-ukraine-s-hospitals-will- cause-long-term-harm-health.
40 JP 3-24, Counterinsurgency.
41 Nina M. Serafino, Peacekeeping and Related Stability Operations: Issues of U.S. Military Involvement, IB94040 (Washington, DC: Congressional Research Service, January 24, 2007), https://www.everycrsreport.com/ files/20070124_RL33557_b72fe14e4a4bc6456d1a4d3386c74ac96d52092b.pdf.
42 JP 3-07, Joint Stabilization Activities (Washington, DC: The Joint Staff, February 2022).
43 Patrick J. Reinert and John F. Hussey, "The Military's Role in Rule of Law Develop- ment," Joint Force Quarterly 77 (2nd Quarter 2015), 120.
44 SIGAR, Police in Conflict.
45 Hussey, "Seizing the Initiative by Establishing the Rule of Law During Combat Operations."
46 Kelly et al., A Stability Police Force for the United States.
47 Nicola Bonomi and Stefano Bergonzini, "What Role Can Stability Policing Play in Total Defence and Building Resilience?" Security: Theory and Practice 47, no. 3 (2022),
48 Hussey, "Seizing the Initiative by Establishing the Rule of Law During Combat Operations."
49 Kelly et al., A Stability Police Force for the United States.
50 Kelly et al.
51 James A. Baker III and Lee H. Hamilton, co-chairs, The Iraq Study Group Report: The Way Forward—A New Approach (New York: Vintage Books, 2006).
52 SIGAR, Police in Conflict.

John F. Hussey
MG - US Army (ret.)
former Commanding General of the 200th MP Command

ARMY RESERVE

ALUMNI

DEPUTY DIRECTOR'S CORNER

Dear Readers,

CoESPU makes a global impact for Stability Policing and remains indispensable to a diverse network—committed to advancing peace and security for the most vulnerable around the world.

Last year, CoESPU trained more than 952 professionals from 62 countries—who returned home to share the lessons learned in Vicenza. We partnered with the Office of Security Cooperation in Europe (OSCE)—strengthening a regional approach to combatting human trafficking around the Mediterranean. We joined hands with the United States Army to support essential programs for Women, Peace, and Security (WPS)—empowering those with the greatest stake in Africa's security. And, we produced ground-breaking research on topics as diverse the role of artificial intelligence in human security, the use of misinformation in violent extremist campaigns, and how cultural heritage protection is essential to combatting trans-national organized crime. And, so much more!

Few organizations in the world can boast such a broad and diverse impact as CoESPU!

But, none of what this talented team accomplishes is done alone. Operating under the guidance of the Carabinieri Headquarters and in partnership with the United States Global Peace Operations Initiative (GPOI), the United Nations, 17 different international organizations, and 19 universities—CoESPU is strengthened by a truly world-class network of likeminded leaders and organizations. We are incredibly grateful for their teamwork and support.

Few of these partnerships are more important than our relationship with the more than 15,000 CoESPU alumni from 128 countries. They are the ones with boots on the ground—making a difference in every corner of the world today.

So, I'm calling on all 15,000 of our alumni to stay engaged—with CoESPU and with each other. If you are a CoESPU alumni, sign up for our Alumni Database at www.coespu.org/user/register. Follow us on social media. And, most importantly, share stories of how CoESPU's training impacted you, or lessons learned from recent experience. We'd love to learn about the work you're doing today—and this magazine is a great venue to share ideas!

There is no doubt CoESPU's work remains more vital than ever and I remain confident that—with such a powerful network of partners and alumni that spans the globe—there's not a problem related to Stability Policing that CoESPU can't help solve.

So, stay in touch—and stay committed!

Joseph Bruhl
Col. - US Army
CoESPU Deputy Director

OPENING OF THE ACADEMIC YEAR

FEBRUARY 17th, 2024

CoESPU TRAINING

OSCE

OCTOBER 2ND – OCTOBER 11TH, 2024

7th Live simulation-training exercise anti Human Trafficking, organized by OSCE and carried out at CoESPU.

CPTM19, CPTM20, STM10, GP17, CP06 AND FPU CS (PDT21)

OCTOBER 23RD – NOVEMBER 19TH, 2024

19th and 20th UN Core Pre-Deployment Training Material course, 10th Special Training Material course, 17th Gender Protection course, 6th Child Protection course and FPU Command Staff (21st Pre-Deployment Training) course.

CPTM21, FPU CS (PDT22) AND TOT (PDT22)

OCTOBER 23RD – NOVEMBER 19TH, 2024

21st UN Core Pre-Deployment Training Material course, FPU Command Staff (22nd Pre-Deployment Training) course and Training of Trainers (22nd Pre-Deployment Training) course.

SA CB

NOVEMBER 6TH – NOVEMBER 19TH, 2024

Capacity Building - Strategic Advising course, sponsored by FIEP.

CENTURION EXERCISE 2024

NOVEMBER 11TH – NOVEMBER 22ND, 2024

Centurion Exercise 2024, organized by the Carabinieri in collaboration with the African Union.

AT18

DECEMBER 4TH – DECEMBER 17TH, 2024

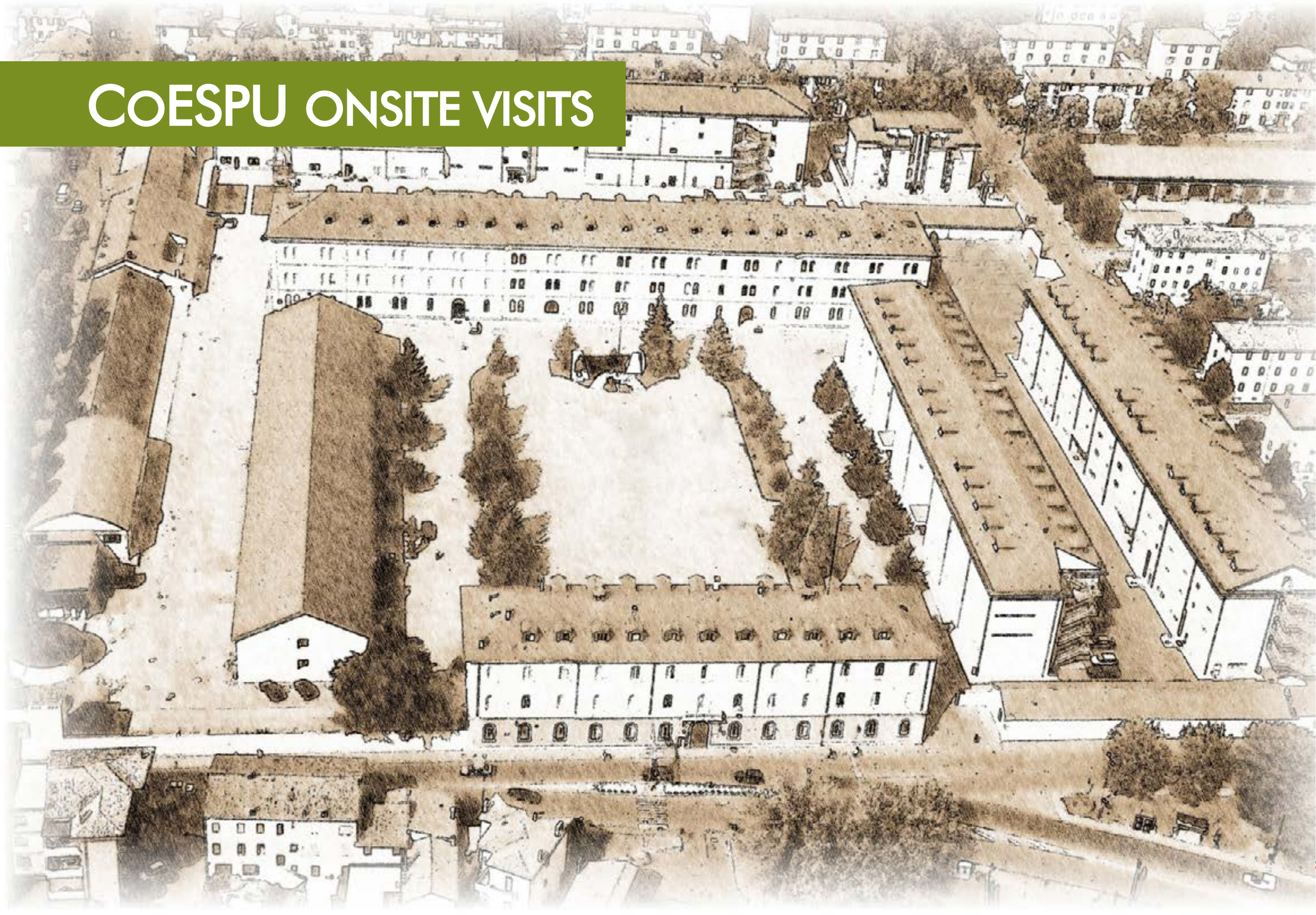
18th Asymmetric Threat course.

IMSISS - UNIVERSITY OF TRENTO

FEBRUARY 11TH – FEBRUARY 13TH, 2025

International Master on Security, Intelligence and Strategic Studies by University of Trento for 20 students from Glasgow, Dublin City and Prague Charles Universities.

CoESPU onsite visits



MG STÈPHANE BRAS, DEPUTY DIRECTOR OF OPERATIONS & DEPLOYMENT, FRENCH GENDARMERIE NATIONALE'S GENERAL DIRECTORATE

OCTOBER 1st, 2024

HONORABLE MARIA CRISTINA CARETTA FROM THE ITALIAN HOUSE OF REPRESENTATIVES

OCTOBER 7th, 2024

LTG. SALVATORE LUONGO, CARABINIERI DEPUTY COMMANDING GENERAL (NOW COMMANDING GENERAL)

OCTOBER 10th, 2024

EUROPEAN UNION COUNCIL'S COMMITTEE FOR CIVILIAN ASPECTS OF CRISIS MANAGEMENTS

OCTOBER 17th, 2024

MS ADINA LOVIN, GENERAL CONSUL OF ROMANIA IN TRIESTE

OCTOBER 28th, 2024

LTG MARIO CINQUE, CARABINIERI DEPUTY COMMANDING GENERAL

DECEMBER 19th, 2024

DR VINCENZO RIBONI, PRESIDENT OF THE VICENZA'S LIONS CLUB PALLADIO

JANUARY 15th, 2025

HIS EXCELLENCY DR FILIPPO ROMANO, NEWLY APPOINTED PREFECT OF VICENZA

FEBRUARY 5th, 2025

DR FRANCESCO ZERILLI, NEWLY APPOINTED QUESTORE OF VICENZA

FEBRUARY 7th, 2025

BG NAWAF MAJED GHANIM AL-ALI, CG ASSISTANT FOR OPERATIONS OF THE QATAR LEKHWIYAE

FEBRUARY 19th, 2025

AROUND THE WORLD

LJUBLJANA (SLOVENIA)

NOVEMBER 2024

The CoESPU's Gender Advisor opened a 10-day training, sponsored by the Centre for European Perspective - CEP and the European Commission, for the Mongolian Armed Forces.

KENYA

JANUARY 2025

A CoESPU's team assessed the capabilities of the Kenya Police in order to co-design a UNPOL-style Formed Police Unit Pre-Deployment Training under US State Department / GPOI's auspices.

PEOPLE COME PEOPLE GO

FAREWELL TO MAJ. SCIRÈ

OCTOBER 2024

Farewell to MAJ Daniela Scirè, CoESPU's Healthcare Section Head.

FAREWELL TO LGT LA NOTTE

OCTOBER 2024

Farewell to LGT Vittorio LA NOTTE, CoESPU's Real-Life Support Head.

FAREWELL TO LTC ISTRALI AND LGT BAVA

NOVEMBER 2024

Farewell to LTC Giorgio ISTRALI, CoESPU's Logistics and Infrastructure Section Head, and LGT Roberto BAVA, Budfin Service Officer, retired.

FAREWELL TO LGT. MAIORANA

NOVEMBER 2024

Farewell to Lgt. Giovanni MAIORANA, from CoESPU's Training Department, retired.

FAREWELL TO LGT OGGIANI, LGT FOCHESATO AND SERG MENEGHINI

JANUARY 2025

Farewell to retiring Lgt. Guido OGGIANI and Serg. Graziano MENEGHINI, from CoESPU's HQ Support Group, and Lgt. Giuseppe FOCHESATO, Library Head.

WELCOME TO MS. KAMOUN

JANUARY 2025

Welcome to Ms. Sara Lina Kamoun, from Padova University, here to attend a 3-month internship for a deep dive in the field of Stability Policing.

FAREWELL TO MS. MILANI

JANUARY 2025

Farewell to Ms. Maddalena Milani, from Padua University, following a 4-month internship in the fields of Stability Policing, Effective Communication, Content Creation, Community Management, and Data Analytics.

CoESPU THROUGH THE EYES OF CHILDREN

MARCH 2025

Vicenza's 2nd-grade kids bring our 20th Anniversary to life with colorful drawings, depicting Carabinieri as Peace, Courage, Protection and Hope archytipes!

follow us on social media

coespu.org

coespurivista@carabinieri.it

linkedin.com/school/coespu

facebook.com/coespu

https://www.instagram.com/coespu/

*@_CoESPU_*

Visit: www.coespu.org

We welcome your contributions!

Should you wish to collaborate with our Magazine, please send your articles, tales or pictures from the field to coespurivista@carabinieri.it

Center of Excellence for Stability Police Units

Caserma "Gen.A. Chinotto"
via Giacomo Medici, 87
36100 - Vicenza Italy
coespu.info@carabinieri.it - www.coespu.org