NATO STANDARD

ATP-3.16.1

COUNTERING INSIDER THREATS (CIT)

Edition A Version 1
APRIL 2016

NORTH ATLANTIC TREATY ORGANIZATION
ALLIED TACTICAL PUBLICATION

Published by the
NATO STANDARDIZATION OFFICE (NSO)

INTENTIONALLY BLANK

NORTH ATLANTIC TREATY ORGANIZATION (NATO)

NATO STANDARDIZATION OFFICE (NSO)

NATO LETTER OF PROMULGATION

13 April 2016

1. The enclosed Allied Tactical Publication ATP-3.16.1, Edition A, Version 1, COUNTERING INSIDER THREATS (CIT), which has been approved by the nations in the Military Committee Joint Standardization Board, is promulgated herewith. The agreement of nations to use this publication is recorded in STANAG 6513.

2. ATP-3.16.1, Edition A, Version 1 is effective upon receipt.

3. No part of this publication may be reproduced, stored in a retrieval system, used commercially, adapted, or transmitted in any form or by any means, electronic, mechanical, photo-copying, recording or otherwise, without the prior permission of the publisher. With the exception of commercial sales, this does not apply to member or partner nations, or NATO commands and bodies.

4. This publication shall be handled in accordance with C-M(2002)60.

for
Dieter Schmaglowski
Deputy Director NSO
Branch Head P&C

Edvardas MAŽEIKIS
Major General, LTUAF
Director, NATO Standardization Office

INTENTIONALLY BLANK

RESERVED FOR NATIONAL LETTER OF PROMULGATION

INTENTIONALLY BLANK

RECORD OF RESERVATIONS

CHAPTER	RECORD OF RESERVATION BY NATIONS
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

RECORD OF SPECIFIC RESERVATIONS

[nation]	[detail of reservation]
DEU	DEU ratifies STANAG 6513, understanding that in conjunction with and for the purpose of clarification of para. 0209a, the authority of NATO commanders to collect data as part of an act of investigation on presumed internal threats has a legal basis, as well as understanding that all applicable restrictions of the aforementioned legal basis must be strictly observed. Thus, from DEU point of view, it has been made clear that investigatory powers may not be arbitrarily asserted. Depending on the particular operation, the legal basis for investigations in the context of internal threats may be rules under international law including potential agreements with the host nation and/or laws and regulations under the national legislation of the sending state. Legal restrictions regarding investigative acts of NATO commanders arise from international sources of law on the one hand and from provisions under the relevant national laws and regulations on the other hand.
TUR	The insider threat includes both actions by insurgents and host-nation security force members, whether a rogue soldier or individual of authority, It may cause a negative approach and biaa to HN security forces by NATO forces members. Moreover It may degrade the mutual thrust between partners. Writing HN's service personnel may be most proper instead of using host-nation security members.
USA	The US does not subscribe to the advising roles as described in the ATP. US doctrine shows that advisors have three primary roles: Advising, Support and Liaison. The US will lift this reservation when the roles described are harmonized with US doctrine roles (Advising, Support and Liaison)
Note: The reservations listed on this page include only those that were recorded at time of promulgation and may not be complete. Refer to the NATO Standardization Document Database for the complete list of existing reservations.	

INTENTIONALLY BLANK

TABLE OF CONTENT

	Page
PREFACE	IX
CHAPTER 1 – FUNDAMENTALS OF COUNTERING INSIDER THREATS	
Introduction	1-1
Definitions	1-1
Insider Threat Causations	1-2
Insider Threat Prevention	1-5
CHAPTER 2 – COUNTERING THE INSIDER THREAT WHILE CONDUCTING SECURITY FORCE ASSISTANCE OPERATIONS	
Understanding the problem	2-1
Conceptual Framework	2-1
Summary	2-11
ANNEX A – OBSERVATIONS, INDICATORS, AND BEHAVIOURS	A-1
LEXICON	
PART I – ACRONYMS AND ABBREVIATIONS	LEX-1
PART II – TERMS AND DEFINITIONS	LEX-2
REFERENCES	REF-1

INTENTIONALLY BLANK

PREFACE

0001. Purpose. The purpose of Allied Tactical Publication (ATP)-3.16.1, *Countering Insider Threats* is to provide a useful framework to understand, prevent, and counter insider threats and insider acts of violence during Allied joint operations. This publication is intended to guide operational and tactical commanders and staff.

0002. An insider threat is may exist during North Atlantic Treaty Organization (NATO) non-Article 5 crisis response operations (NA5CRO) such as counterinsurgency (COIN) operations, peace operations, military support to stabilization and reconstruction, and security force assistance activities but may be present during any NATO operation, even in peacetime.

0003. At a strategic level insider attacks erode the validity of the mission and may create increased friction between senior leaders of NATO and the host nation (HN). At the operational level they increase burden on intelligence and force protection assets. At the tactical level insider attacks ensure that the reestablishment of trust between the two forces will be near impossible.

0004. Trust among NATO forces and between NATO forces and HN security forces is essential for effective working relationships. Trust is the most essential basis for human interaction and comradeship and character of leadership with discernment. A commander who is sending signals to be perceived as mistrust may observe less effective working relationships and lack of loyalty.

0005. Within the hierarchy of NATO doctrine, ATP-3.16.1 is directly subordinate to AJP - 3.16, *Allied Joint Doctrine for Security Force Assistance*, which describes the fundamental aspects of security force assistance.

0006. ATP-3.16.1 provides the doctrinal underpinning for mitigating threats when conducting security force assistance with host-nation security forces. AJP-3.14, *Allied Joint Doctrine for Force Protection* forms the cornerstone of NATO force protection doctrine and should be referenced in conjunction with this ATP.

0007. Members conducting counter-insurgency operations (AJP-3.4.4, *Allied Joint Doctrine for Counterinsurgency*), host-nation support (AJP-4.5, *Allied Joint Doctrine for Host-Nation Support*), and stabilization and reconstruction (AJP-3.4.5, *Allied Joint Doctrine for Military Support to Stabilization and Reconstruction*) should ensure that they understand the tenets countering insider threats since it is likely that their personnel will have regular contact and interaction with host-nation security forces.

0008. Linkages. ATP-3.16.1 is linked with, and has references, to:

- AJP-01, Allied Joint Doctrine
- AJP-2, Allied Joint Intelligence Counter Intelligence and Security Doctrine
- AJP-3, Allied Joint Doctrine for the Conduct of Operations
- AJP-3.2, Allied Joint Doctrine for Land Operations
- AJP-3.4, Allied Joint Doctrine for Non-Article 5 Crisis Response Operations
- AJP-3.4.1, Allied Joint Doctrine for Peace Support Operations
- AJP-3.4.4, Allied Joint Doctrine for Counterinsurgency (COIN)
- AJP-3.14, Allied Joint Doctrine for Force Protection
- AJP-3.16, Allied Joint Doctrine for Security Force Assistance

Chapter 1 – FUNDAMENTALS OF COUNTERING INSIDER THREATS

Introduction

0101. NATO is likely to be faced with the challenge of stabilization and COIN in unstable states for the foreseeable future. Based on lessons learned by NATO's forces in Afghanistan, it is possible that cultural friction may arise when NATO partners and troop contributing nations (TCNs) conduct COIN and/or security force assistance (SFA) activities.

0102. While NATO conducts long-term operations within a host nation, the potential for insider attacks will exist. This threat exists during multinational operations with non-NATO nations, from HN security forces, and from HN and TCN contractors providing support to NATO forces.

0103. Cultural friction occurs when two or more entities, such as organisations, units, teams, groups, and individuals, from different countries culturally resist (think or act in opposition, shaped by implicit beliefs and tacit values) each other in real contact or interactions. Interactions sparking cultural friction are not limited to military operations and may occur on a personal level when advisors are eating and interacting with their supported HNSF members.

0104. Cultural friction while conducting SFA activities led to an increase in insider attacks as more and more NATO forces were in contact with the host nation security forces (HNSF). Insider attacks degrade the fragile trust that is built between partners and can impact activities at the strategic, operational, and tactical level. Whilst preventing these attacks from ever occurring should be the goal, it is realistic to assume that there will be some attacks regardless of preventive measures therefore NATO forces should be familiar with steps to counter any potential insider threats.

Definitions

0105. An insider is a person who has a position of trust within an organization or access to personnel, facilities, and equipment. Insiders could be fellow non-NATO coalition personnel, TCN personnel, host-nation security force personnel, trusted host nation civil government personnel or anyone granted access to NATO personnel, facilities, and equipment.

0106. An insider threat is a threat from within with the potential for an attack by, or facilitated by, an insider. Whilst it may seem that this could be anyone, and it could, this publication will attempt to reduce the number of potential threats by providing screening and recognition tools.

0107. An insider attack occurs when an insider initiates an act of violence against NATO forces. Perpetrators of an insider attack possess motive, intent, and capability, and need opportunity in order to attack. Insider attacks are often characterized by surprise.

Insider Threat Causations

0108. The insider threat includes both actions by insurgents and host-nation security force members, whether a rogue soldier or individual of authority, and can be generally categorized as one of five categories; personality-based, event-based, crime-based, insurgent-based, or a general.

0109. Personality-based insider attacks may arise out of disputes over character, culture, or as a result of mental illness. Some examples are,

- A personal altercation occurs when the insider becomes belligerent from a disagreement with/or a perceived socio-cultural transgression committed by NATO forces.
- The insider may not like something about the NATO forces of a personal nature (e.g., jealousy, finds certain individuals objectionable).
- When an insider has undergone radicalisation he is motivated to attack for perceived religious, political, or other ideological reasons. The individual may exhibit intense hatred for those who do not ascribe to his beliefs and is seen as adhering to the more extremist aspects of that theology. The individual may exhibit a desire to become a martyr if that is an aspect of his beliefs.
- The insider believes that current security situation favours insurgent and/or anti-government forces and switches sides for self-interest.
- If the insider has had a family member or friend killed or arrested by NATO forces he may feel personally slighted by NATO members and target them.
- Use and abuse of drugs, both legal and illicit, may influence an insider to violent action.
- A mentally ill attacker exhibits symptoms of mental illness. These can include the gamut of psycho-social pathologies including severe stress and anxiety. Some of the most dangerous symptoms include angry outbursts for no apparent reason, sudden dramatic changes in behaviour, and talking to oneself.

0110. Event-based attacks occur when an insider construes NATO members' actions as valid reasons to conduct an attack. Some examples are,

- Burning or desecration of religious texts and sites
- Insult to religious leaders broadcasted within media channels
- Host-nation president (or some other well-known leader) denunciation of NATO action or an incident that occurred out of theatre
- Civilian casualty event attributed to (correctly or not) NATO forces

0111. Crime-based insider attacks may occur when an insider is at risk of being caught in the planning of a crime, commission of a crime, or following actual criminal misdeeds. Some examples are,

- An insider can be motivated to attack in order to protect his criminal enterprise from perceived threats by NATO forces.
- An insider attack may occur if the individual is caught stealing from NATO (either supplies of personal property).

0112. Insurgent-based insider attacks may occur when an insider has in some way been influenced by members of, or is actually a member of, an insurgency. Some examples are,

- Co-option occurs when an existing HNSF member is recruited to assist or act on behalf of an insurgency. A member can be recruited through multiple means, to include ideological pressures, financial incentives, intimidation, or familial and tribal ties. Co-option allows the insurgency to access the security forces, but as opposed to infiltration, co-opting an existing member circumvents whatever existing initial screening and vetting processes new recruits undergo. Co-option can take a grander form as well, where, for example, accommodation or cooperation exists between whole groups of HNSF and insurgents. However, this is beyond the scope of singular insider attacks.
- Infiltration transpires when an existing insurgent member clandestinely joins the host-nation's security forces through the standard recruitment process to support the insurgency. Gauging the level of possible infiltration in partnered security forces is difficult as infiltrators will likely attempt to remain undetected. Additionally, the process of infiltration removes a fighter from the insurgent ranks and puts the fighter at risk if he is exposed during the recruiting and training process. Thus, a successful infiltrator is more likely competent and experienced and may be used in a more tactically effective manner, such as facilitating insurgent efforts by providing intelligence on NATO and host-nation tactics or movement or by targeting high-profile host nation leadership. Thus,

he is less likely to abandon his cover to conduct a onetime attack on a few NATO individuals. Still, such onetime attacks are significant and sow distrust between NATO embedded advisors and HNSF, as well as undermine international perceptions of NATO efforts.[1]

- Impersonation occurs when an insurgent poses as a HNSF member to conduct attacks. With counterfeit uniforms and identifications (IDs) available, impersonation is often easier to accomplish than co-option or infiltration. Within more sophisticated cases of impersonation, there is likely some level of facilitation, complicity, or awareness by HNSF members, whether it be providing an ID, escorting the individual onto base, or simply knowing of the attacker's intentions to target NATO members. Thus, a case of impersonation likely includes possible co-option through such facilitation or complicity of HNSF members.

0113. An insider attack may occur due to other, general reasons that don't belong in the aforementioned categories. Some examples are,

- Organizational culture includes the social dynamics, tensions and activities reflecting the daily life for both the internal organization within the particular host-nation unit, as well as the general relations between NATO forces and host-nation security force units. In many under-developed nations, the relations between rank and file soldiers and police are often very fraught; there are factions at work, predatory leadership practices (such as stealing pay and/or siphoning money from food funds; and potentially, sexual abuse of young recruits/soldiers), tribal, political and criminal network factions that make it difficult for soldiers to get their salaries, do their jobs without interference, support their family, and even survive. Similarly, unit morale may play a role in insider attacks. The second and third order effects of these factors may lead to increased risk for an insider attack. Additionally, the inter-service relations between NATO advisors and the host nation unit may serve as a catalyst for an insider attack, particularly if they have already occurred before or nearly occurred before (it is vital to learn the history of local unit relations).

- It is likely that internecine insider attacks may preclude increased risks for an attack on NATO forces. If NATO members learn of an insider attack occurring within the host-nation's security forces, they should consider that information when setting their force protection posture and when conducting risk management and mitigation procedures.

[1] While this is a threat to NATO forces, it is beyond the scope of this publication to explain counter-intelligence methods to prevent infiltration. However, the CIT framework is applicable to threats by infiltrators.

0114. The aforementioned factors are not an exhaustive list of potential causes and there may be other potential catalysts which prompt an insider attack. Since often the attacker does not survive the attack, it may prove difficult or even impossible for NATO to determine an attacker's reason for the attack."

Insider Threat Prevention

The Importance of Good Advisors

0115. Evidence from recent operations indicates that a large number of insider attacks are a result of cultural friction between NATO forces and the HNSF they are advising. Therefore the first step in prevention is to overcome these cultural frictions which can be accomplished by picking the right personnel to be embedded advisors. While this publication is not meant as a primer for security force assistance activities, it is important to have a baseline understanding of what an embedded advisor does before addressing insider threats and attacks. Additionally, it is important to note that how embedded advisors act when conducting their duties can provide the motive and/or opportunity for the targeted violence of an insider attack. Targeted violence refers to situations in which an identifiable perpetrator poses a threat of violence to a specific individual or group.[2]

0116. Advisors have three primary roles. First and foremost, advisors are typically members of an organization with a well-defined chain of command and familiar responsibilities. Second, advisors embed themselves with their counterparts. Third, advisors through the use of interpreters are communicators between their respective forces and their host nation counterparts.

a. As members of formal organizations (military, police, governmental, etc.), advisors receive and execute the orders of superiors. These orders may conflict with the orders their counterparts receive. Among other duties, advisors should act unobtrusively, but nonetheless positively, often observing, evaluating, and reporting on the performance of counterparts and their assigned unit.

b. Secondly, advisors live, eat, and work with the officers and men of their host units. Often, advisors soon regard themselves as one of them. Sharing common hardships and dangers forges potent emotional ties. The success and good name of their units become matters of personal importance to the advisor.

c. Finally, advisors are conduits between their superiors and foreign

[2] Fein, R.A., Vossekuil, B., and Holden, G.A. (1995). Threat Assessment: An Approach to Prevent Targeted Violence. *National Institute of Justice: Research in Action*. 1. Retrieved from https://www.ncjrs.gov/pdffiles/threat.pdf

counterparts. Advisors should introduce and explain one to the other; they help resolve the myriad of problems, misunderstandings, and suspicions which arise in any human organization, particularly when people of starkly different cultures approach difficult tasks together. Advisors with quick and easy access to influential counterparts can sometimes be the best possible means of communicating.

0117. As an advisor, understanding the host-nation population is a crucial element of pre-mission planning and the development of host nation forces. This is also the first step in preventing the cultural friction that can lead to insider attacks. Prior knowledge of socio-cultural differences aids in building effective relationships and prevents embarrassment, loss of rapport, and compromise of the mission.

a. Operating according to the priorities of the host-nation's citizens and timelines may involve periods of relative inactivity. Relationships are incredibly valuable. Active participation in indigenous social activities, such as actively engaging in "small talk" prior to an important meeting, isn't a distraction or an unproductive use of time; advisors should view it as the time where they arrive at a mutual understanding of where they and the forces they are advising are going and how they are collectively going to get there. Advisors engaging in "small talk" should avoid topics HNSF may view as sensitive or become defensive as (e.g., religion, family, the role of women, social issues).

b. Advisors should not template assistance based on their background or prejudice. Advisors need to approach every problem from the perspective of a resident of the nation they are attempting to help. Their counterparts will always take a culturally appropriate approach or seek a more traditional solution. Advisors should observe and understand the cultural norms, their systems and processes before offering advice. Sustainable solutions will be ones that host nation citizens can embrace as their own.

c. Advisors need to accurately report their supported HNSF unit's deficiencies, HNSF leaders' strengths and weakness, detainee abuse, corruption, drug use, etc. to their chain-of-command and answer requests for information from their intelligence section. Accurate reporting will ensure that commanders have a more complete understanding of the HNSF units they are working with.

The Insider Threat Prevention Model[3]

0118. The insider threat prevention model is based on the combination of mastering force protection tactics, techniques, and procedures (TTP) and the use of attribution, a concept in social psychology addressing the processes by which individuals explain the cause of behaviour and events. This conceptual model consists of a set of six elements as depicted in Figure 1-1 and outlined the following paragraphs:

Figure 1-1 Insider Threat Prevention Model

[3] Keijzer, R. (2012). Insider Threat Prevention Model (IPTM) Principles. *COIN Common Sense, Volume 3 Issue 4*. 4. Retrieved from https://combinedarmscenter.army.mil/orgs/call/CI/ops/L2I2/L2I%20Documents/COIN%20Common%20Sense%20-%20Insider%20Threat,%20Dec%202012.pdf

a. Insider threats disrupt the bond between NATO forces and the host nation; one should understand and prepare for it. The first element and foundation focuses on mastering the TTP and the objective of understanding the host-nation's culture necessary for countering the insider threat security problem.

b. Patience, Listening and Respect. This element is key to insider threat prevention and is squarely based on common principles of human interaction centred on kindness, understanding and empathy.

c. Reliability and Professionalism. Reliability is a pre-cursor of trust and a leading indicator of professionalism.

d. Communication. Surveillance detection and information gained from interacting with host nation partners will ultimately enhance insider threat prevention.

e. Partnership. The feeling of a partnership is the result of practicing the first four elements where partners see each other as fellow team members.

f. Trust. Gain and maintain trust through mutual understanding.

0119. Insider attacks can be caused by personal confrontations that involve cultural insensitivities. Instruction on conflict de-escalation and conflict resolution techniques should be a core part of pre-deployment training. It is important to remember that a voiced threat may be nothing more than "venting" on the part of the aggrieved individual. Various cross-cultural conflict escalation scenarios should be utilized for role playing exercises. Effective integration of insider threat intelligence indicators into mission planning and execution reinforces NATO force protection, limits casualties, and helps set conditions for future success. Similarly, security and small arms TTP should be developed and routinely practiced for confronting an insider attack.

0120. Even if the forces and advisors do everything "right" an insider attack still remains within the realm of the possible. An insider attack can be premeditated or opportunistic when a situation arises that facilitates or permits the violence or does not prevent it from occurring. When conducting an assessment of the events that led up to the attack, what transpired during the attack and post-incident actions will provide vital lessons learned that can be utilized to restore relations, continue development, and regain combat effectiveness.

CHAPTER 2 – COUNTERING THE INSIDER THREAT WHILE CONDUCTING SECURITY FORCE ASSISTANCE OPERATIONS

Understanding the Problem

Context

0201. The concept of insider threats and attacks dates back many centuries. Insider threats are not limited by location; they exist both on a relatively secure outpost whilst conducting security force assistance activities and while conducting patrols in a far less secure environment. The inherent or perceived abuse of trust, as well as mistrust, is an emotive issue that is easily sensationalized and manipulated. The motivations for insider attacks are various, often complex, and likely to evolve during a campaign.

0202. As noted in Chapter 1, NATO operations in Afghanistan revealed that insider attacks have a broad range of causes that span from the ideological to the criminal.

0203. Whatever factor, or combination of factors, caused an inside attack, opposing forces will likely seek to claim and exploit its consequences. The response of the NATO forces, TCN, and the HN should be cohesive, synchronized and resolute.

Conceptual Framework

0204. The countering insider threats framework has six functions: prepare, deter, detect, respond, recover and exploit.

0205. The model at Figure 2-1 shows the prepare, deter, and detect functions as components of a prevention strategy that comes before an attack and respond, recover, and exploit as reactions that come after an attack. In truth, the model is more complex. Prepare, deter, and detect are continuous and enduring. Respond is limited to the time it takes to neutralize the threat and make the local environment safe and secure again. Recover is a transitional action that sets the conditions for exploit and so is grouped with it as a single function. Exploit can either be linear, as in pursuit operations, or cyclical, in the case of lessons that enable development of the prevention strategy.

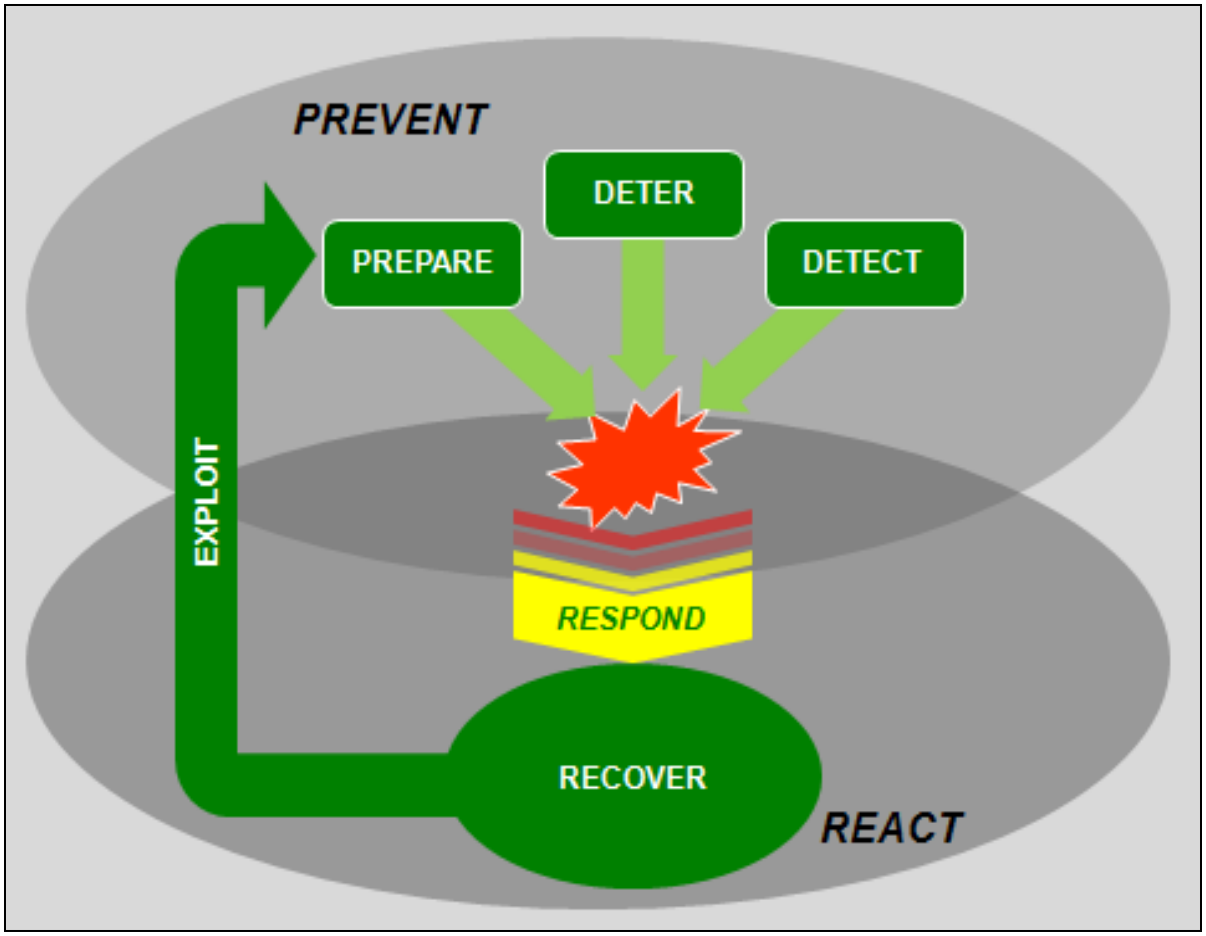

Figure 2-1 Countering Insider Threats Conceptual Framework

Prepare

0206. Preparation is a continuous process that starts prior to deployment and continues throughout operations. At the tactical level, tasks within this function are:

a. Pre-deployment

(1) Select for Aptitude. Not all NATO personnel may have the aptitude for working alongside partners of different cultures; such personnel are ineffective in advisory roles and can introduce risk to themselves and others. Commanders at all levels should ensure that personnel who are in key advisory and mentoring roles have the appropriate aptitude and motivation.

(2) Conduct Cultural Training. Cultural misunderstandings can result in grievances that may, particularly if combined with other influences, lead to insider attacks. To counter this, personnel should be culturally adaptive. The key characteristics of good cultural adaptability are

cultural awareness, interaction, skilful rapport-building, respectfulness, self-reflection, and self-control.

(3) Conduct Threat Awareness Training. Personnel typically dismiss the risk of an insider attack happening to them or their unit. This can lead to complacency. All personnel should understand the nature of the threat. Threat awareness training should be provided regularly.

(4) Develop and Practice TTP. Posture, presence, and profile are critical to countering insider attacks. Guardian angels are designated armed individuals, pairs, or small groups of NATO personnel whose sole purpose is to protect other NATO personnel who are in close proximity to HN personnel in a position of trust. If not deterred, attacks can develop quickly, giving little chance to those involved to react and defeat them. Guardian angel drills are essential for developing rapid response, recovery, and exploitation capabilities and should feature prominently in training. It should be remembered that they are only one part of the physical defence and that physical defence is only one part of defeating insider threats.

(5) Conduct Advanced Weapon Training. Normal weapons proficiency is insufficient to respond to insider attacks, which often occur in close quarters and crowded spaces and develop rapidly. Advanced weapons training is required to enhance speed of response, controlled weapons handling, and accurate shooting as an ultimate response. This is particularly vital for guardian angels.

b. While Deployed

(1) Plan each Operation. Plans, orders, and rehearsals for every interaction between partners should take account of insider threat and force protection. The planning of operations should consider risks, the importance and the cultural implications associated with specific dates or events – for example religious holidays, anniversaries, or following significant incidents. The uncertainties, opportunities, and distractions in transitional operations such as base transfers may lead to an increase in risk. Insider attacks have occurred on NATO forces when personnel have been socially interacting, e.g., playing sports. NATO base security operations should be planned and rehearsed.

(2) Assess Threat, Vulnerability, and Risk. The attacker possesses motive, intent, and capability and needs opportunity in order to carry out an insider attack. Motive, intent, and capability are identified through threat assessments; opportunity is identified through vulnerability assessments. Risk assessment examines threat and vulnerability in

order to gauge probability and impact. Commanders should carry out these assessments both in fixed locations and while on operations in order to mitigate the identified risk. In shared locations attention should be given to any divisions between NATO forces and host-nation security forces locations. When visiting host-nation security forces bases, secure areas and rally points should be identified. Moving personnel to secure, defensible areas in the event of an insider attack allows for a more secure approach for dealing with an active insider attack and supports recovery and exploitation.

(3) Implement Risk Mitigation Measures. Once a risk assessment has been completed, commanders should mitigate the risks. Implementation of appropriate force posture and disposition as well as dress state and arming status are the foundation of tactical insider threat risk mitigation. This applies not just to the posture of NATO forces but to HNSF forces and whether or not they should have easy access to weapons while on NATO bases. This implementation process should cover day-to-day internal operations of NATO bases. Bases within NATO's control should be modified to enhance physical security. Some risks may be mitigated through engagements with partner chains of command.

(4) Develop Messaging. An insurgent narrative may seek to portray the NATO forces and the supported host-nation security forces as divided and unsuccessful. NATO should counter that through proactive messaging. When an insider attack occurs, an insurgency will seek to capitalize on it to attack cohesion. The responsive messaging should be coherent, convey the facts of an incident, and reinforce resolve. Talking points should be prepared in advance to allow the dissemination of information to start quickly, with talking points increasing in scope as and when facts become clear.

(5) Rehearse. Counter insider threat plans, TTP, and standard operating procedures (SOP) should be rehearsed to ensure successful implementation.

(6) Adapt. All aspects of preparation should be dynamically informed by lessons identified from operations, including after insider attacks. As part of an agile and responsive lessons process, risk assessments, force posture, TTP, and SOP should all be reviewed and, where necessary, amended and rehearsed.

Deter

0207. Deterrence is conducted simultaneously and continually at every level. It ranges from strategic communications to continuous rapport-building between NATO and partnered host-nation security forces to the rigorous application of visible force protection measures. Based on the assumption that NATO personnel are being observed at all times, following these steps demonstrates our preparedness to defeat insider attacks. At the tactical level, tasks within this function are:

a. Build and Maintain Rapport. Establishing rapport provides protection at multiple levels. Many cultures provide for the protection of friends. Politeness is usually an important part of the HN's culture; HN residents are much more likely to discuss difficult matters—such as suspicious individuals—with those they trust. NATO personnel should place strong emphasis on building close and trusted relationships with the partnered forces.

b. Enforce Access Procedures. Rigorous enforcement of security measures is essential to denying access to those not authorized to enter NATO facilities, such as those who seek to impersonate NATO or host-nation security forces personnel. Locally employed civilians, contractors, and interpreters should wear easily recognisable identification at all times.

c. Challenge. Although good security measures should ensure that only authorized personnel enter a NATO or host-nation location, no one should solely rely on access procedures to provide security. All personnel should remain alert to the possibility that an unauthorized person may gain access to a location where NATO personnel work. It is vital to have the moral courage to challenge anyone who appears out of place. When challenging, personnel should be prepared to respond.

d. Enforce Arming Policy. Arming policy directives mitigate a risk based on an identified vulnerability. These directives are an essential element of force protection and should be adhered to without exception.

e. Enforce Force Protection TTP. Force protection TTP present a visible posture, presence, and profile to deter both opportunist and planned attacks. They provide a mix of direct protection (e.g. wearing of personal protection equipment), indirect protection (e.g. alertness and weapons readiness) and actions to follow should an attack occur. Commanders should ensure that these TTP are trained, rehearsed, and followed.

Detect

0208. Detection is a continuous process during operations. Detection of a threat is everyone's responsibility and takes place at all levels. A systematic approach to detection is fundamental. Above the tactical level, vetting of HN personnel aims at detecting and rejecting those who present danger or vulnerability to hostile influence. Recognition and timely reporting of threat indicators enable pre-emptive action and de-escalation as well as feeding the intelligence effort at every level; this allows development of insider threat warnings. The rapid passage of threat warnings across the force is critical to force protection. At the tactical level, tasks within this function are:

a. Recognize Behavioural and Activity Indicators. At a basic level, detection is about spotting the presence of the abnormal or the absence of the normal. NATO personnel should be trained before, and throughout, their deployment to notice things that are out of place. Every member of the NATO coalition is a sensor and individual vigilance is key. HN members are likely to have the most success in spotting adverse indicators in other HN citizens. This reinforces the importance of building and maintaining good rapport between partners. Guardian angels have a specific responsibility for detection, and should consider themselves sensors first.

b. Conduct Biometric Enrolment and Screening of Host-Nation Security Force Personnel. If feasible, all members of the host nation's security forces should be biometrically enrolled as part of their recruitment, vetting, and screening process. This allows NATO personnel to pro-actively confirm the identity of those with whom they partner and detect impersonators. Initial CI screenings should be done on all HNSF, local interpreters, local contractors, and TCN workers as soon as advisors are collocated with HNSF. These CI screenings should be conducted by trained CI military personnel from NATO countries. Host nation personnel returning from leave, or a prolonged period of absence, should go through a routine reassessment to look for signs of potential co-option by insurgent or radical groups. Changes in behaviour, attitude, or performance may be linked to threats against the host nation service member or his family. Another potential indicator is an unexplained increase in wealth.

c. Report. Trust your instincts and act rapidly. It is vital that those who recognize indicators act upon them; even minor suspicions should be reported to the chain of command. Units should inform higher headquarters of any insider threat indicators. This is essential to building situational awareness and generating insider threat warnings that ensure everyone has current threat and risk awareness.

d. Investigate. CI personnel investigate insider threat indicators to generate situational awareness and issue-specific threat warnings. This is a key part of

the detection effort and a lynch-pin in the holistic effort to defeat insider threats. Teams on the ground make a vital contribution to this effort by providing timely and accurate reporting.

e. Disseminate Threat Warnings. Rapid dissemination of threat warnings ensures all personnel are informed of specific credible threats that have been identified through intelligence fusion. On receipt of threat warnings, commanders should reassess vulnerabilities and resultant risks and, where necessary, take actions in accordance with TTP and SOP. Host-nation security forces and NATO commanders should ensure that warnings, and actions to be taken, are disseminated rapidly within their units.

0209. A predictive classification concept that may aid in identifying an insider threat employs a multi-layered analysis and inference process that progresses logically from data to observations to indicators to behaviours, as depicted in Figure 2-2.[4] A more comprehensive listing of useful observations, indicators and behaviours is contained in Annex A.

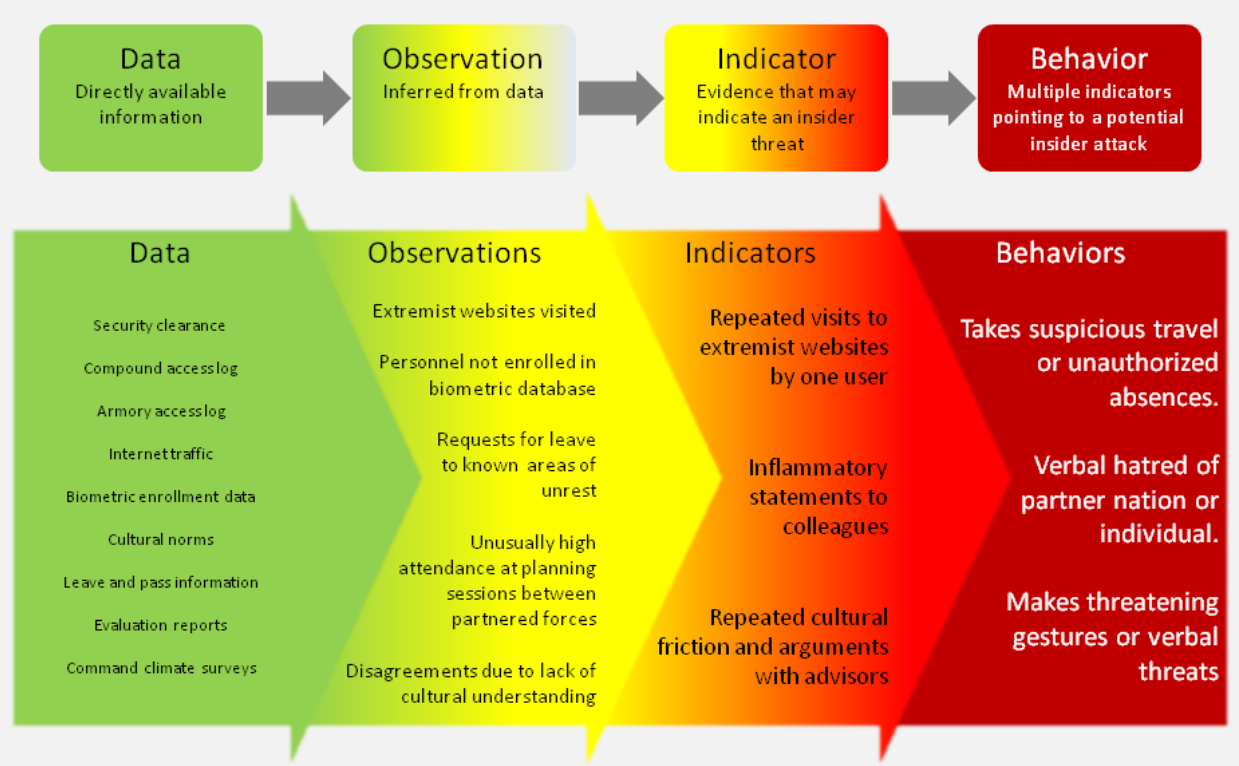

Figure 2-2 Predictive Classification

[4] Much of this section, to include the graphic, is adapted from the predictive modelling approach developed by the Pacific Northwest National Laboratory publication:
US Department of Energy. (2009). *Predictive Modelling for Insider Threat Mitigation, 5-7*, Retrieved from http://www.pnl.gov/cogInformatics/media/pdf/TR-PACMAN-65204.pdf

a. The data that forms the base of this model is directly available information and comes in many forms, i.e.; statements to colleagues; correspondence; reading material; clearance and access to sensitive locations and NATO personnel; and, email traffic. Commanders may employ as many collection techniques as available to begin sifting this data, whether it is through information technology monitoring or an active counter-intelligence collection effort when a legal basis exists.

b. Observations are derived as the data is collected and starts to coalesce and infer indicators, i.e. vague statements of dissatisfaction to colleagues; extremist reading material quoted or distributed; and claimed relationships with members of extremist or terrorist organizations.

c. Indicators use observations as cues to observe insiders and assess a potential insider threat. Specifically, an indicator is defined as an action or event that is a precursor of an actual insider attack. A member of a foreign security force may read extremist literature or access it via the internet in an attempt to understand the enemy further while a member distributing that same literature or commenting in online forums about their desire to serve the cause exhibits the indicator to a higher degree. Not every person who falls into this category actually poses a threat. Individuals may display the indicators of an insider threat for many reasons, only some of which involve the actual intention to commit an insider attack.[5]

d. Behaviours are sequences of activities for achieving the specific purpose of carrying out an insider attack. Isolated indicators do not point directly to an insider threat. If the individual has experienced cultural friction with a NATO advisor, spoken repeatedly and angrily about it with other personnel, and that individual has frequent access to NATO members during time periods where advisors have demonstrated a lower force protection posture, then he represents a clear risk and his behaviour indicates that he may carry out targeted violence.

Respond

0210. Regardless of the effectiveness of NATO deterrence and detection efforts, determined insider attacks may still occur; therefore, NATO should be prepared to respond. The respond function lasts from the time an insider attack is identified or an imminent attack is perceived, until that threat has been neutralized and local safety has been restored. The basis of the respond function is the implementation of established and rehearsed TTP and SOP; these ensure the fastest possible

[5] Fein, R.A., Vossekuil, B., and Holden, G.A. (1995). Threat Assessment: An Approach to Prevent Targeted Violence. *National Institute of Justice: Research in Action*. 2. Retrieved from https://www.ncjrs.gov/pdffiles/threat.pdf

response when under the surprise and shock of an attack. At the tactical level, tasks within this function are:

a. Concentrate Force Rapidly. Immediate and decisive concentration of force will protect personnel and deter expansion of an attack. Guardian Angel(s) are the first planned response and much may depend on their alertness and the quality of their training. Everyone should react to the attack immediately and decisively to neutralize the threat acting within the rules of engagement. Commanders should consider use of all available assets including the quick reaction force; intelligence, surveillance, target, acquisition, and reconnaissance; neighbouring combined team fires; and medical evacuation.

b. Gain and Maintain Control. The surprise, speed, and shock of an attack are likely to lead to a temporary reduction in coalition force control in that immediate vicinity. The initiative should be rapidly regained with strict adherence to ROE, effective identification, and fire control measures. The many assets called to assist should be coordinated and controlled in order to maximize their combined effectiveness. An increase in local force protection measures and access control should be implemented.

c. Warn and Report. Information should be passed rapidly to all personnel in the area. Higher HQs, subordinate units, and neighbouring units should be informed as the situation develops.

d. Contain and Neutralize the Threat. The incident should be contained to limit the attacker's freedom of movement. Containment is not enough to neutralize the threat because within the containment, attackers are likely to continue to engage NATO personnel. Therefore, responders should enter and clear within the containment area until the threat has been fully neutralized.

e. Conduct a Joint Response. Wherever possible, all available personnel should be involved in the response. The host-nation security forces provide better local knowledge, language skills, and cultural understanding than NATO members alone and therefore can be more effective in responding to, recovering from, and exploiting an insider attack. This requires careful coordination or de-confliction.

Recover and Exploit

0211. The recover and exploit function should commence as soon as the on-scene commander is content that the threat has been neutralized and a safe and secure local environment has been re-established. Recover and exploit are inextricably linked and conducted in tandem—and so are treated as one function. The foundation of the recover and exploit function is implementation of established and rehearsed SOP.

0212. Recover aims at stabilizing the situation so that operations may continue. At the tactical level, tasks within this function are:

a. Manage Consequences. In any incident where there has been violence between partners, or there is a perception that such violence has occurred, the consequences can be severe; negative public opinion creates a strategic risk. The establishment of facts and communication of those facts is essential to dispel misinformation and rumours and de-escalate heightened emotions. Messaging at all levels should be well-informed and coherent. Partnered personnel and their families should be reassured that everything possible is being done to determine the cause, to bring those responsible to justice, to restore good relationships, and to continue the mission.

b. Engage Partners. Following an insider attack, relationships between partners will be strained. Commanders should consider timely liaison and key leader engagement to explain the incident, the response, and the future. Good rapport built before the event and a joint response to the event will significantly ease tension and speed a return to normal operations.

c. Reinforce Morale. Morale will be damaged as a result of an insider attack. Firm leadership is essential in restoring morale amongst partners. Determining facts through investigation and communication of those facts to all personnel, especially highlighting that the insider attack was the action of an individual and not a unit, will help rebuild confidence and cohesion.

d. Resume Mission. Commanders should resume their assigned mission as rapidly as possible. The effectiveness of the insider attack will be rendered operationally ineffective once full partnering returns to pre-incident levels; this not only signals trust to our host-nation partners, it also demonstrates commitment to the campaign. Based on statistics from recent NATO operations in Afghanistan, another attack is likely to take place somewhere within theatre inside of 48 hours. Commanders should remain aware of this and adjust force posture and profile appropriately.

0213. Exploit involves military pursuit operations, technical pursuit operations to gather evidence, and the lessons process. At the tactical level, tasks within this function are:

a. Conduct Follow-on Operations. This can involve both pursuit and technical investigation. Investigative results can in turn lead to follow-up operations. Pursuing escapees and accomplices and bringing them to justice may result in wider successes against insurgent networks.

b. Investigate. Once the operational circumstances allow, incident evidence should be secured as a crime scene objective, not a military objective, in order

to preserve it and allow exploitation. This includes the immediate area of the attack, bodies, witnesses, detained personnel, and equipment used to perpetrate the attack. The evidence should be exploited to establish who did what, to identify perpetrators and accomplices, and to determine cause. The successful preservation of evidence will support future judicial proceedings. Commanders need to be aware of the scale of this; units should be prepared to receive several investigative agencies within hours of an insider attack.

c. Exploit Lessons. The investigation may identify changes to the prepare, detect, deter, respond, recover, and exploit functions in order to reduce risks and strengthen NATO forces against future insider attacks. Lessons are identified as a result of investigations, but lessons are only learned when deliberate action is taken to change or maintain something, e.g. policies, TTP, and SOP. Commanders should implement a review process so that learning can take place. Implicit within all this is the sharing of lessons between partners.

Summary

0214. Insider threats are not a new phenomenon. Understanding the serious strategic risk insider threats pose to NATO missions emphasizes the imperative to defeat this threat. Understanding the context will prevent the spectre of insider threats from having a corrosive effect on the NATO partnerships with HNSF. This conceptual framework should underpin NATO forces approach and guide counter-measures. While TTP are important, combating insider threats is first and foremost about mind-set and therefore it needs to be command-led.

INTENTIONALLY BLANK

ANNEX A – OBSERVATIONS, INDICATORS, AND BEHAVIOURS

Annex A provides some examples of observations, indicators, and behaviours that a potential insider threat may exhibit. This is not a comprehensive list and is meant to be used as a guide.

Observations

A01. The following observations are gleaned from available data and demonstrate that the individual in question might be an insider threat. None of these by themselves are worth formally investigating however, they do merit monitoring of the individual's actions and/or discussion with the individual.

- Complains about other nations and/or religions.
- Advocates violence beyond what is the accepted norm.
- Abrupt behavioural shift.
- Desires control.
- Socially withdraws in some occasions.
- Appears frustrated with partner nations.
- Experiences personal crisis.
- Demonizes others.
- Lacks positive identity with unit or country.
- Reclusive.

Indicators

A02. The following indicators are cues that an individual may be an insider threat. As noted in Chapter 2, indicators may serve as precursors to an actual insider attack. At a minimum, the chain of command should be notified that these indicators are being displayed. If deemed appropriate, notify counter-intelligence assets.

- Verbally defends radical groups and/or ideologies.
- Speaks about seeking revenge.
- Associates with persons who have extremist beliefs.
- Exhibits intolerance.
- Personally connected to a grievance.
- Cuts ties with unit, family, or friends.
- Isolates himself from unit members.

- Intense ideological rhetoric.
- Attempts to recruit others.
- Choice of questionable/subversice reading materials in personal areas.
- Is in contact (e.g., personal, email, phone, courier) with known insurgents.

Behaviours

A03. If an individual is exhibiting the following behaviours, immediate action is required as an insider attack may be imminent. Appropriate action runs the gamut from removing that individual's access to a weapon up to forcible detention.

- Advocates violence as a solution to problems.
- Shows a sudden shift from "upset" to normal.
- Takes suspicious travel or unauthorized absences.
- Stores or collects ammunition or other items that could be used to injure or kill multiple personnel.
- Verbal hatred of partner nation or individual from partner nation.
- Exhibits sudden interest in partner nation headquarters or individual living quarters.
- Makes threatening gestures or verbal threats.

LEXICON

PART I – ACRONYMS AND ABBREVIATIONS

AJP	Allied joint publication
ATP	Allied tactical publication
COIN	counter-insurgency
HN	host nation
HNSF	host-nation security forces
ID	identification
NATO	North Atlantic Treaty Organisation
ROE	rules of engagement
SFA	security force assistance
SOP	standard operating procedures
TCN	troop-contributing nation
TTP	tactics, techniques, and procedures

PART II – TERMS AND DEFINITIONS

counter-insurgency
Comprehensive civilian and military efforts made to defeat an insurgency and to address any core grievances. (NTMS-NATO Agreed)

counter-intelligence
Those activities which are concerned with identifying and counteracting the threat to security posed by hostile intelligence services or organisations or by individuals engaged in espionage, sabotage, subversion, or terrorism. (NTMS-NATO Agreed)

force protection
All measures and means to minimize the vulnerability of personnel, facilities, equipment and operations to any threat and in all situations, to preserve freedom of action and the operational effectiveness of the force. (NTMS-NATO Agreed)

host nation
A nation which, by agreement: a. receives forces and materiel of NATO or other nations operating on/from or transiting through its territory; b. allows materiel and/or NATO organizations to be located on its territory; and/or c. provides support for these purposes.. (NTMS-NATO Agreed)

insider
A person who has a position of trust within an organization or access to personnel, facilities, and equipment. (This term and definition are only applicable in this publication.)

insider threat
A threat from within with the potential for an attack by, or facilitated by, an insider. (This term and definition are only applicable in this publication.)

insider attack
An attack that occurs when an insider initiates an act of violence against NATO forces. (This term and definition are only applicable in this publication.)

physical security
That part of security concerned with physical measures designed to safeguard personnel, to prevent unauthorized access to equipment, installations, material and documents, and to safeguard them against espionage, sabotage, damage, and theft. (NTMS-NATO Agreed)

References

Except where specifically noted by footnotes, the following publications were used as reference material for this publication.

NATO DOCTRINE

AAP-6, NATO Glossary of Terms and Definitions (English and French)

AAP-15, NATO Glossary of Abbreviations Used in NATO Documents and Publications

AJP-01(C), Allied Joint Doctrine

AJP-2, Allied Joint Intelligence and Security Doctrine

AJP-2.2, Counter-intelligence and Security Procedures

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

AJP-3.2 Allied Joint Doctrine for Land Operations.

AJP-3.4.1 Allied Joint Doctrine for Peace Support Operations.

AJP-3.4.4 Allied Joint Doctrine for Counterinsurgency (COIN).

AJP-3.14 Allied Joint Doctrine for Force Protection

OTHER PUBLICATIONS

NATO International Security Assistance Force, *Security Force Assistance Guide*, March 2013

United States Army Center for Army Lessons Learned Handbook, *Insider Threats – Afghanistan,* November 2012

NATO International Security Assistance Force, *COIN Common Sense, Volume 3, Issue 4*, December 2012

ATP-3.16.1(A)(1)