INSIDER ATTACKS AS ONE OF THE MAIN THREATS TO RESOLUTE SUPPORT PERSONNEL IN AFGHANISTAN

LTC Krystian Frącik, Ph.D.
War Studies University

The Author was appointed to the position of the Shift Director of Combined Joint Operations Centre (CJOC) in the Headquarters of NATO Resolute Support Mission in Kabul, Afghanistan from September 2015 to June 2016.

Summary

From July 2015, the International Security Assistance Force (ISAF) moved into the Resolute Support Mission (RSM) and started acting in the supporting role. From that time, one of the most important Security Force Assistance tasks has been maintaining and developing relationships with its counterparts in the Afghan Security Institutions (ASI) and Afghan National Defence Security Forces (ANDSF). Being aware of the importance of those connections, the enemies of Afghan society have attempted a tactic named Insider Attack (IA).

Insider Attack is not a new means of tactic. In the 19th and 20th centuries, Britain and the Soviet Union were victim to insider attacks. Insider attacks have a significant strategic impact on the campaign, as they erode the relationship between the Afghan National Defence Security Forces and Coalition Forces.

Insider attacks occur for numerous reasons, including personal grievances, insurgent influences, psychological distress, and ideological motivations. More than half of the attackers have insurgent ties. NATO utilises Target Focused Analysis & Neutralisation and Counter Intelligence Support Teams to screen, vet, and interview persons of interest, as well as collect, analyse, and exploit biometric data, documents, and media. Other measures implemented to mitigate insider threats are the threat Awareness and Reporting Programme (TARP) and the Terrorism Espionage and Sedition briefing to RSM personnel.

Incorporating appropriate lessons learned from the British, Russian and ISAF experience into RSM training and operations will have a positive impact on responding to Insider Attacks while reducing their frequency across the Combined Joint Operational Area - Afghanistan.

It is clear that the common approach to defeating Insider Threats must be holistic and each activity should be conducted according to equal principles.

The conceptual framework for countering Insider Threats has five functions: prepare, deter, detect, respond, recover and exploit.

This conceptual framework underpins the common approach and guides of counter - measures. While skills and drills are important, combatting Insider Threats is first and foremost about mindset and therefore it needs to be command-led. If proper preparation makes Coalition Forces members culturally adaptive, develops effective systems and procedures, and hones military skills and Tactics, Techniques, and Procedures, NATO will be able succeed in the Resolute Support Mission.

Introduction

On 18 June 2013, the International Security Assistance Force (ISAF) transferred lead security in Afghanistan to the Afghan National Defence Security Forces (ANDSF)[1]. After this important milestone, ISAF began its transition to a functionally oriented framework that focused on a self - sustainable ANDSF. From July 2015, the ISAF moved into the Resolute Support Mission (RSM)[2] and started acting the supporting role. From that time, one of the most important Security Force Assistance tasks has been in maintaining and developing relationships with its counterparts in the Afghan Security Institutions (ASI) and

1 **Afghan National Defense and Security Forces (ANDSF)**, there are approximately 173,000 soldiers, airmen, and Ministry of Defence (MoD) civilians serving in the Army; approximately 154,000 policemen and civilians serving in the Ministry of Interior (MoI); and more than 28,000 MoI Afghan Local Police (ALP) securing villages across Afghanistan, http://www.rs.nato.int/article/rs-news/afghan-national-defense-and-security-forces-operational-update.html (2016.07.24).

2 **Resolute Support Mission (RSM)** is a key component to the international community's engagement in Afghanistan, assisting Afghan authorities in providing security and stability, while creating the conditions for reconstruction and development. NATO-led mission to train, advise and assist the Afghan security forces and institutions. The mission was launched in 2015.

ANDSF. Being aware of the importance of those connections, the enemies of the Afghan society have attempted a new means of tactic named ***Insider Attacks (IA)***. These kinds of enemy activities are conducted in order to undermine common cohesion. Coalition Forces (CF) have undertaken extensive measures to counter this threat, leading to marked reductions in these types of attacks on Coalition personnel. However, the threat persists and requires continued vigilance. Based on historical trends in Afghanistan and other theatres, Insider Attacks increased as the Mission approached the end of direct combat activities. So, Coalition Forces must be ready nowadays to recognise the implications of such attacks, and commanders at every level ensure their commands are trained, equipped, and prepared to deal with them.

The purpose of this article is to provide basic information concerning current threats toCoalition Forces from Insider attacks and to describe measures to counter them.

Challenges with Current Definitions

Insider Attacks are tactical actions that may have strategic implications and direct influence on Afghan public confidence and national will. They also strike at the relationship with the local population and institutions being supported by Coalition Forces.

This part of the article aims at clarifying confusing and partially misleading terminology in the context of deliberate attacks on CF by ANDSF members or people posing as ANDSF members without major changes to existing terminology - often referred to as ***Insider Threat, Insider Attack, Inside the Wire Threat*** or ***Green-on-Blue*** incidents.

Insider Threat (IT) is usually defined by NATO as the potential for an attack by, or facilitated by, a person (or persons) who hold a position of trust with the Combined Team (CT)[3] personnel because of their employment, status, access, or affiliation.

3 Combined Team (CT) includes both Afghan National Security Forces and Resolute Support Coalition Forces.

Another term used in several of the publications is ***Inside the Wire Threat.*** This term refers to non - Coalition Forces (non-CF) members with whom CF are partnered or in regular contact who have committed a breach of trust. *Inside the Wire* includes those individuals who are not members of an organisation (i.e. non-CF members), but, due to a professional or employment relationship, have access to the organisation's personnel, facilities and or activities. Very often the term *Inside the Wire* itself is misleading in that it implies a geographical location such as the interior of Forward Operating Bases (FOBs), Combat Operating Bases (COBs), or other bases. Rarely that definition is connected with a threat that is occurring at a Checkpoint (CP) or on a road; however, these cases are explicitly included

Inside the Wire Threat is often used synonymously with *Insider Threat* but based on a proposal of the Deputy of Chief of Staff Operations (DCOS OPS) at the Headquarters of the International Security Assistance Forces (HQ ISAF), the term *Insider Threat* is used to replace the term *Inside the Wire Threat.*

Insider Attack occurs when a person, or persons, in a position of trust initiates an act of violence against the CF member. Perpetrators of an Insider Attack possess motive, intent, and capability and need opportunity in order to attack. Insider Attacks are characterised by surprise, speed, and shock.

In accordance with the above, *Insider Attacks* can be categorised as:
- ***personally motivated:*** caused by ideology, stress, argument, volunteerism or other personal or cultural grievances;
- ***insurgent manipulated***: co-option, coercion, or infiltration;
- ***criminally motivated***: normally related to the protection of corruption;
- ***unknown*****:** when the perpetrator is killed or escapes, his motivation often remains unknown, the insurgency is quick to take credit for such attacks to continue their narrative and attack the Combined Team Center of Gravity (CoG).

Whatever factor, or combination of factors, caused an Insider Attack, the insurgents will seek to claim it and exploit its consequences. The response of the CT, both ANDSF and ISAF, must be cohesive, synchronised, and resolute.

Green-on-Blue (GoB) events are defined as an ANDSF member who knowingly attacks, attempts to attack and/or helps facilitate an attack against CF with the

intent to maim or kill CF personnel. The distinctive feature of this kind of attack is the initial affiliation of the perpetrator. In order to be considered a *GoB* incident, the initial affiliation of the perpetrator is the ANDSF. For *Insider Attacks* where the initial affiliation of the suspect is insurgent, it is classified as of *INS Origin*

The following figure visualises the categorisation of (deliberate) *Insider Threats.*

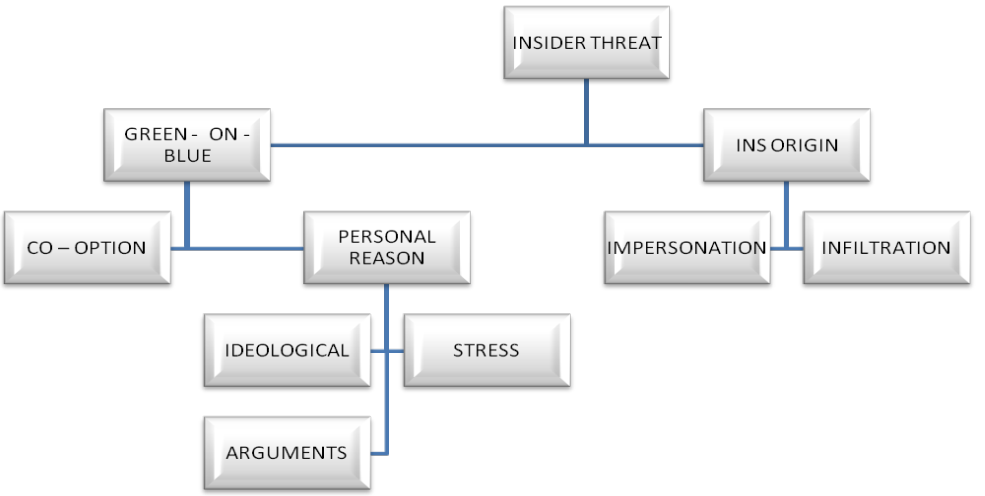

Figure 1. Categorisation of (deliberate) Insider Threats

The single categories mentioned on the above figure are defined as follows:

Co-option is defined as an existing ANDSF member who is recruited to assist or act on behalf of the insurgency. A member can be recruited through multiple means, including ideological pressures, financial incentives, intimidation, extortion, or familial and tribal ties.

Personal Reasons occur when an ANDSF member acting intentionally as an individual independent perpetrator, without direct guidance, command, or pre-planning from external entities. Further classification breaks the personal reasons category into three subcategories:

– *Ideological reasons:* the individual is motivated by a desire to become a martyr or support the cause of the insurgency.
– *Stress:* there is variety of conditions which push the individual to break with reality or act, such as intercultural misunderstanding, lack of appropriate

emotional intelligence, stress as a result of combat operations, narcotics use, or exhibition of signs of depression and/or mental health issues.
– *Arguments:* when disagreements between ANDSF and CF members escalate to violence.

Impersonation takes place when an insurgent or non-ANDSF member poses as an ANDSF member to conduct attacks.

Infiltration occurs when an existing insurgent member joins the ANDSF through the standard recruitment process in order to support the insurgency.

Unknown takes place if there is evidence that indicates the perpetrators had ties to the insurgency, but not enough to determine whether the attackers were infiltrators or co-opted. The other reason to name the attack as *Unknown* is when the event is still pending an investigation or there is a significant lack of evidence to suggest a dominant motivational factor for the attack.

According to above, Resolute Support Mission's members must be ready to counter the threat through focused awareness, military professionalism and cultural adaptability of all participations of the Mission. It is necessary to fully leverage the technical and tactical skills, adhere to high standards, empathise with the unique challenges faced by Afghan society and deepen the understanding of the way they work.

Historical Context

Insider Threat has existed in Afghanistan for as long as foreign interventions have occurred. It is not a new phenomenon or even a new tactical concept within the country. During recent history, there are two significant periods: *the Anglo-Afghan wars of the 19th Century* and *the Soviet occupation from 1979 to 1989*.

The first periods include three British wars in Afghanistan and numerous counterinsurgency campaigns in the Northwest Frontier region of India, employing advisors to lead Afghan units. During this period, British officers observed that Afghan soldiers would return to their tribal homelands after they had been discharged or had deserted and employ the tactics they had learned against

their former allies. Based on their intimate knowledge of British procedures and organisation, Afghans were also able to develop their own tactics for use against the British-Indian Army, thereby increasing their effectiveness. During this extended period, the British suffered numerous Insider Attacks against military advisors, diplomats, and their family members.

A British officer in charge of Pashtun tribesmen wrote in his diary that they performed exceptionally as irregular cavalry, and that it was the treatment they received from their advisors which will make them either cheerful and zealous soldiers or a useless rabble. *He continued that* there is none, however, who can less bear rudeness or offensive language and he must never be submitted to either. He must feel that he is certain of being well-received by his officer. Nothing in treatment or obedience should be imposed on, or required of the Soldier which may tend to lower him in his own estimation or in that of his fellows in or out of service. An officer who has not had much intimacy with natives of this description, even with the best intentions, may unwillingly offend and annoy them from his very ignorance.

The second period concerns the Soviet Union occupation of Afghanistan from 1979 to 1989. During that time, the Afghan Army faced constant defections, as not only individuals and small units but also whole divisions went over to the Mujahedeen, taking their personal equipment, small arms, tanks, and armoured vehicles with them. When units were ordered to operations, there was always the risk they might defect. Like the British before them, Soviet advisors also suffered from Insider Attacks, their casualties, however, were initially the result of Afghan units revolting en masse and killing their advisors who they viewed as representatives of the central regime. When the Soviets transitioned operations to Afghan leadership (January 1987), they began a two-year period of withdrawal. During this time, Afghan soldiers, unsure as to the future viability of the Afghan state, sought to gain influence with the Mujahedeen by killing their advisors and switching sides. The Soviet response to these Insider Attacks was to take violent retribution against their families, which minimised the number of Insider Attacks.

Countering the Insider Threats

Insider Threats is not unique to current RSM. Incorporating appropriate lessons learned from the British, Russian and ISAF experience into RSM training and operations will have a positive impact on responding to Insider Attacks while reducing their frequency across the Combined Joint Operational Area - Afghanistan (CJOA-A).

It is clear that a common approach to defeating *Insider Threats* must be holistic and each activity should be conducted according to equally principles

The conceptual framework for countering *Insider Threats* has five functions (Figure 2):

– prepare;
– deter;
– detect;
– respond;
– recover & exploit.

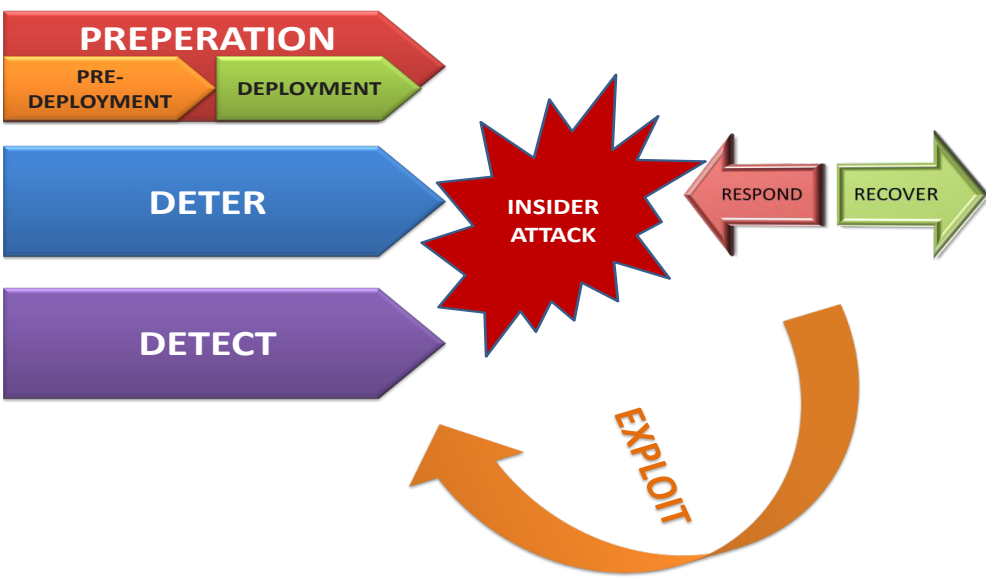

Figure 2. Functions of the conceptual framework for countering Insider Threats

Preparation starts prior to deployment and continues throughout operations. The main tasks within this function are:

– ***During Pre-deployment:***
  - *Conduct Threat Awareness Training.* All personnel must understand the nature of the threat;
  - *Develop and Practice Counter IT Tactics, Techniques, and Procedures (TTPs).* TTPs are critical in countering Insider Attacks. Drills are *essential for developing rapid responseand exploitation capabilities and should feature prominently in training;*
  - *Conduct Advanced Weapons Training.* It is required to enhance speed of response, controlled weapons handling, and accurate shooting;
  - *Select for Aptitude.* It must be ensured that personnel in key advisory and mentoring roles have the appropriate skills and motivation for working alongside partners of different cultures. Personnel who are not suitable for such key roles may be employed in supporting roles;
  - *Conduct Cultural Training.* All personnel must be culturally adaptive. The key characteristics of good cultural adaptability are cultural awareness, empathy, skillful rapport-building, respectfulness, self- reflection, and self-control.

– ***While Deployed:***
  - *Plan Each Operation.* Plans, orders, and rehearsals for every interaction between Combined Team partners must take account of IT and Force Protection (FP). The planning of operations must consider risks associated with specific dates or events, for example: religious holidays and anniversaries;
  - *Assess Threat, Vulnerability, and Risk.* The attacker possesses motive, intent, and capability and needs opportunity to carry out an attack. Motive, intent, and capability are identified through threat assessments; opportunity is identified through vulnerability assessments. Risk assessment examines threat and vulnerability to gauge probability and impact. These assessments must be carried out both in fixed locations and while on operations to mitigate the identified risk;
  - *Implement Risk Mitigation Measures.* Once a risk assessment has been completed, commanders must mitigate the risks. This implementation process must cover day-to-day internal operations of RS bases;

- *Develop Messaging.* After Insider Attack, the insurgency will seek to capitalise on it to attack cohesion. So, responsive messaging must be coherent, convey the facts of an incident, and reinforce resolve;
- *Rehearse.* In order to ensure successful implementation, Counter - IT plansTTPs, and Standard Operating Procedures (SOPs) must be rehearsed;
- *Learn Lessons.* All aspects of Insider Attacks should be dynamically informed by lessons identified from operations. As part of an agile and responsive lesson process, risk assessments, force posture, TTPs, and SOPs should all be reviewed and, where necessary, amended and rehearsed;
- *Conduct Threat Awareness Training.* Threat awareness training should be provided after arrival in the deployed location, and then at least every six months.

Deterrence is conducted simultaneously and continually. It ranges from strategic communications to continuous rapport-building between Combat Team partners to the rigorous application of visible Force Protection measures. Based on the assumption that RS personnel are being observed at all times, following these steps demonstrates preparedness to defeat *Insider Attacks.* There are some tasks within the deter function:

– *Enforce Access Procedures*: rigorous enforcement of security measures is essential to denying access to those not authorized to enter RS bases, non-coalition personnel (locally employed civilians, contractors, and interpreters) must wear recognised identification at all times;
– *Challenge:* although good security measures should ensure that only authorised personnel enter an RS or Government of the Islamic Republic of Afghanistan (GIRoA) location, no one should solely rely on access procedures to provide security. All personnel must remain alert to the possibility that an unauthorised person may gain access to a location where RS 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;
– *Enforce arming policy:* arming policy directives mitigate a risk base, enforce army policy, enforce force protection Tactics, Techniques and Procedures (TTPs); build and maintain rapport;
– *Enforce Force Protection TTPs.* Commanders should ensure that Force Protection TTPs are trained, rehearsed, and followed. TTPs present a visible posture, presence, and profile to deter both opportunist and planned attacks;

– *Build and Maintain Rapport.* All RS personnel should place strong emphasis on building close and trusted relationships with their Afghan partners. Afghans are much more likely to discuss difficult matters (e.g., suspicious individuals) with those they trust. Establishing rapport provides protection at multiple levels.

Detection. Detection of a threat is everyone's responsibility and takes place at all levels. All personnel should detect and reject those who present danger or vulnerability to hostile influence. Recognition and timely reporting of threat indicators enable preemptive action. The rapid passage of threat warnings across the force is critical to Force Protection. The main tasks within this function are:

– *Recognise Behavioural and Activity Indicators.* At a basic level, detection is about spotting the presence of the abnormal or the absence of the normal. Troops should be trained before, and throughout, their deployment to notice things that are out of place. Every soldier is a sensor and individual vigilance is key. Afghans are likely to have the most success in spotting adverse indicators in other Afghans. This reinforces the importance of building and maintaining good rapport between CT partners. Force Protection soldiers have a specific responsibility for detection and should consider themselves sensors first.
– *Conduct Biometric Enrollment and Screening of ANSF Personnel.* It is a part of recruitment, vetting and screening process for all members of the ANDSF to be biometrically enrolled. This allows RS personnel to detect impersonators. ANDSF personnel should go through a routine reassessment after returning from leave, or a prolonged period of absence. Changes in behaviour, attitude, or performance may be linked to threats against the RS members
– *Report.* All personnel who recognise indicators, even minor suspicions should be reported to the chain of command. This is essential to building situational awareness and generating *Insider Threats* warnings that ensure everyone has current threat and risk awareness.
– *Investigate.* In order to generate situational awareness and issue-specific threat warnings, Counter Intelligence personnel investigate incoming *Insider Threats* indicators. Teams on the ground make a vital contribution to this effort by providing timely and accurate reporting.
– *Disseminate Threat Warnings.* Dissemination of threat warnings ensures all personnel are informed of threats that have been identified. On receipt of

threat warnings, commanders must reassess vulnerabilities and resultant risks and, where necessary, take actions in accordance with TTPs and SOPs.

The respond function lasts from the time an *Insider Attack* is identified or an imminent attack is perceived until that threat has been neutralised and a safe and secure local environment has been re-established. Regardless of the effectiveness of RS deterrence and detection efforts, determined individuals will still carry out Insider Attacks; therefore, all RS personnel should be prepared to respond. The basis of the Respond functions are:

– *Concentrate Force Rapidly.* Everyone who can react to the attack should do so immediately and decisively to neutralise the possible threat. Concentration of force will protect personnel and deter expansion of an attack. It is necessary to use all available assets including the Quick Reaction Force (QRF), Intelligence Surveillance and Reconnaissance (ISR), neighbouring Combined Team fires, and Medical Evacuation (MEDEVAC).
– *Gain and Maintain Control.* In the event of *Insider Attack,* the initiative should be rapidly regained. The surprise and shock of an attack are very likely to lead to a temporary reduction of self-control. The many assets called to assist must be coordinated and controlled in order to maximise their combined effectiveness.
– *Warn and Report.* HQs, subordinate units, and neighbouring units should be informed about the current situation. Information should be passed rapidly to all personnel in the area. It is far better to provide incomplete information in frequent, short reports, than to wait until completed information is available.
– *Contain and Neutralise the Threat.* Containment is not enough to neutralise the threat because, within the containment, attackers are likely to continue to engage RS personnel. Therefore, responders should enter and clear within the containment area until the threat has been fully neutralised. The incident should be contained to limit the attacker's freedom of maneuver.
– *Conduct a Combined Response.* CF and ANDSF should give a combined response to an *Insider Attack,* only if it is possible.

The last conceptual function of framework for countering *Insider Threats* is **Recover and Exploit.** Taking **Recover** into consideration**,** the main aim of the function is to stabilise the situation so that operations may continue, it should

take place as soon as the threat has been neutralised and a safe and secure local environment has been re-established. The basis of the Recover functions are:

– *Manage Consequences.* It is obvious that the consequences of any incident where there has been violence between CT partners can be severe, create negative public opinion and strategic. It can lead to misinformation and rumours and de-escalate heightened emotions. So it is necessary to reassure CT personnel and their families that everything possible is being done to determine the cause.
– *Engage CT Partners.* In the event of an Insider Attack, relationships between CT partners will be strained, so it is necessary to explain the incident, the response, and the future as soon as possible. Good rapport built before the event and a joint response to the event will significantly ease tension and speed a return to normal operations.
– *Reinforce Morale.* Insider Attack usually damages morale among CT partners. The essential responsibility belongs to each leader to restore the morale. It can be done by determining facts through investigation and communicating those facts to all personnel. It will help rebuild confidence and cohesion of team members, especially if it is highlighted that the Insider Attack was the action of an individual and not a unit.
– *Resume Mission.* The effectiveness of the Insider Attack will be rendered operationally ineffective once full partnering returns to pre-incident task. It is necessary to resume their assigned mission as rapidly as possible to send signals of trust to Afghan partners. It can also demonstrate commitment to the campaign.

At the tactical level, tasks within Exploit are as follows:

– *Conduct Follow-up Operations.* Investigative results can in turn lead to follow-up operations. Evidence Based Operations (EvBO) is conducted to pursue escapees and accomplices and to bring them to justice. EvBO may result in wider successes against insurgent networks.
– *Investigate.* Incident evidence should be secured as a crime scene objective, not a military objective, in order to preserve it and allow collecting all available evidence: bodies, witnesses, detained personnel, and equipment used to perpetrate the attack. It is necessary to establish who did what, to identify perpetrators and accomplices, and to determine cause. Full preservation of evidence will be able to support future judicial proceedings. Commanders need

to be aware of the scale of this response. Units should be informed of several investigative agencies that will appear within hours of an Insider Attack.

– *Exploit Lessons.* In order to reduce risks and strengthen RS personnel against future Insider Attacks, the investigation should identify changes that CT should make to the Prepare, Detect, Deter, Respond, Recover, and Exploit functions. 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, TTPs, and Standing Operating Procedures (SOPs). Commanders must implement a review process so that learning can take place. Implicit within all this is the sharing of lessons across the CT.

Summary and Conclusion

According to the above, Insider Threats are not a new problem among CF members in Afghanistan, but it is necessary to understand the serious strategic risk IT poses to the NATO military mission. Understanding the context, in particular the miniscule percentage of ANDSF involved in attacks against CF, will prevent it from having a corrosive effect on the Combined Team. This conceptual framework underpins the common approach and guides of counter - measures. While skills and drills are important, combatting IT is first and foremost about mindset and, therefore, it needs to be command-led. If proper preparation makes CF members culturally adaptive, develops effective systems and procedures, and hones military skills and TTPs, NATO will be able succeed in the Resolute Support mission.

For many CF members who stand *shoulder to shoulder* with the Afghan National Defense Security Force in the mission, having an awareness of Afghan culture is not enough. These Coalition personnel must go further, bridging gaps and blending together our best practices to create enduring solutions for the ANDSF. These cultural adaptive skills must be trained, rehearsed and reinforced at every opportunity. Through this professionalism, we mitigate the Insider Threat and contribute to the continued viability of a free and independent Afghanistan.

Acronyms

ANA:	Afghan National Army
ANDSF:	Afghan National Defense Security Force
ANP:	Afghan National Police
ASI:	Afghan Security Institutions
CF:	Coalition Forces
CJOA-A:	Combined Joint Operational Area - Afghanistan
COB:	Combat Operating Base
CoG:	Center of Gravity
CP:	Checkpoint
CT:	Combined Team (RS and ANDSF)
DCOS OPS:	Deputy to Chief of Staff Operations
EvBO:	Evidence Based Operations
FOB:	Forward Operating Base
FP:	Force Protection
GIRoA:	Government of the Islamic Republic of Afghanistan
GoB:	Green-on-Blue
HQ:	Headquarters
INS:	Insurgent
ISAF:	International Security Assistance Force
ISR:	Intelligence Surveillance and Reconnaissance
ISTAR:	Intelligence, Surveillance, Target Acquisition and Reconnaissance
IT:	Insider Threat
IA:	Insider Attack
MEDEVAC:	Medical Evacuation
non-CF:	Non-Coalition Forces
QRF:	Quick Reaction Force
RS:	Resolute Support

RSM:	Resolute Support Mission
SFA:	Security Force Assistance
SOP:	Standing/Standard Operating Procedure
TTP:	Tactics, Techniques, and Procedures

References

CJ2 Information Paper: Combating the Insider Threat, *NATO Training Mission Afghanistan, 4 Aug 2011.*

HQ ISAF SOP 331, Theatre Force Protection.

HQ ISAF SOP 332 - Insider Threat Risk Mitigation and Insider Incidents Handling Procedure.

HQ ISAF SOP 333 - Insider Incident Handling Procedures. COMISAF Insider Threat Tactical Directive, *02 March 2012.*

http://www.rs.nato.int/article/rs-news/afghan-national-defense-and-security-forces-operational-update.html

IJC / NTM-A Joint Desk Note - *Inside the Wire Threat Analysis,* 05 August 2012.

Inside the Wire Threats - Afghanistan: Green on Blue, US Center for Army Lessons Learned (CALL) Handbook No. 12-07, , February 2012.

Inside the Wire Threats-Afghanistan: Green on Blue, *CALL Handbook No. 12-07.*

Insider Threat Prevention Model Effective Practices*; CAAT Special Report, 5 Nov 2012.*

Insider Threat: A Real and Present Danger, COIN Common Sense, Vol 4, Iss 1, 20 Feb 2013.

Insider Threats in Partnering Environments*; Asymmetric Warfare Group*, Jun 2011.

Threat Awareness and Reporting Program*; Army Regulation 381-12*, 4 Oct 2010.