U.S. ARMY TRADOC G2 Intelligence Support Activity

TRISA

Red Diamond

Contemporary Operational Environment and Threat Integration Directorate (CTID)

Fort Leavenworth, Kansas Volume 3, Issue 5 May 2012

YEMEN OE QUICK GUIDE

TRISA-CTID's Operational Environment Assessment (OEA) Team is introducing a new category of product. In addition to full OEAs that are dozens of pages in length, the OEA team will generate Operational Environment (OE) Quick Guides. OE Quick Guides provide a very brief overview of the Political, Military, Economic, Social, Information, Infrastructure, Physical Environment, and Time (PMESII-PT) variables of a given OE. Each of the PMESII-PT variables is covered in a brief, accessible format designed to quickly give the reader a comprehensive synopsis of the OE.

The OEA Team is pleased to introduce a new product to serve our customers, the OE Quick Guide, which provides a brief yet comprehensive overview of each of selected countries. These countries are in the *Top 10 Potential Operational Environments*, a forthcoming product.

The OE Quick Guides are based on TRISA's *Top 10 Potential Operational Environments*. The first OE Quick Guide covers Yemen. Yemen is the number three OE on TRISA'S Top 10 list as a location likely to require future Army brigade-level operations.

The OE Quick Guides give Soldiers, deploying units, scenario developers, trainers, and others a concise reference for an OE. While not as in depth as an OEA, the Quick Guides deliver the essential facts of the PMESII-PT variables. OE Quick Guides covering Indonesia and Egypt will follow the *Yemen OE Quick Guide*.

Tell us how we can help.

Email CTID at jon.s.cleaves.civ@mail.mil.

INSIDE THIS ISSUE

Red Diamond is produced monthly by the Contemporary Operational Environment and Threat Integration Directorate of the TRADOC Intelligence Support Activity (TRISA). Send suggestions and feedback to Ms. Penny Mellies (penny.l.mellies.civ@mail.mil).

BOMBING OF THE INDONESIAN EMBASSY IN PARIS

by Laura Deatrick, OEA Team

On 21 March 2012, a home-made bomb exploded outside the Indonesian Embassy in Paris, France. While authorities initially believed that the embassy was not the intended target, further investigation revealed a tie to a militant Islamist group based in Indonesia. Indonesian Embassy Bombing in Paris, a new OEA Team Threat Report, examines the details of the attack and possible training implications.

The Indonesian Embassy in Paris is located at the corner of Rue Cortambert and Rue Nicolo in the 16th arrondissement (quarter) of the city. Only a sidewalk separates the embassy from the street. During the quiet early-morning hours of the date in question, three individuals placed a package containing a homemade bomb outside the embassy building. After the bombers departed, the package was found by another person who moved it several yards away from the building. The bomb detonated shortly thereafter, shattering windows up to 50 meters (54 yards) away and damaging several cars, including two that caught fire. Fortunately, no one was injured.

Though authorities were initially uncertain of the actual target, intercepted e-mail and online chat communications led them to suspect a militant Islamist group with ties to Indonesia. The primary suspect is Frederic C. Jean Salvi, a Frenchman with ties to the Indonesian terrorist group Jemaah Islamiyah (JI). Salvi, on Indonesia's wanted list since 2010 for a planned car bombing, allegedly studied with Islamist militants in Indonesia and has a history of militant extremism in France. His perceived motivation was to dissuade Indonesia from continuing its current crackdown on Islamist militants.

Several aspects of this event will make it of interest to trainers and scenario writers. First, it is an excellent scenario for MI and MP units, and would be easy to mimic in the home-training environment. The lack of casualties allows participants to focus on incident investigation skills without the distraction or delay caused by medical response or crowd control requirements. The small number of local participants (outside of host-nation law enforcement personnel) allows for efficient use of role-players. The early discovery and moving of the bomb by a civilian prior to its detonation complicates the investigation as well. Conflicting witness accounts regarding the timeline of the event – who found the bomb, its original location, and when it exploded – present an additional challenge.

The Indonesian Embassy Bombing in Paris Threat Report provides information to deploying units, trainers, and scenario developers on the March bombing. It contains a detailed review of the event and its associated timeline. In addition, it discusses responsible parties and motives, training implications, apparent reporting contradictions, and offers a possible timeline of actual events.

BANNU, PAKISTAN PRISON ATTACK

by Rick Burns, OEA Team

On April 15, 2012, 150-200 members of the anti-government Tehrik-e-Taliban Pakistan (TTP) attacked the Bannu, Pakistan Central Prison with the primary goal of rescuing Adnan Rashid, eight years into a conviction for master-minding a failed attempt to assassinate then Pakistan president Pervez Musharrif. Understanding the dynamics of this type of attack is important as Soldiers have found, and will continue for the foreseeable future, to find themselves operating as small training and advisory teams in remote areas. This paper provides information on Bannu, Pakistan, the Bannu Prison setup prior to the attack, Adnan Rashid, the attack timeline, the immediate consequences of the attack, and a summary analysis.

Location of Bannu in Pakistan, map used with permission of BBC, http://www.bbc.co.uk/news/world-asia-16324616

Bannu, Pakistan has a long history as a market town and as a launching base for contending with the Afghanistan and Pakistan border tribes. Colonial Britain used Bannu as a major base of operation in actions against Afghan border tribes. Today, the town serves as a government administrative center and an army garrison with a population of over 35,000. Bannu, in close proximity to the Afghan border, is an important crossroad famous for its weekly Friday market. Bannu is also home to several technical colleges and universities and more than 300 primary, middle, and secondary schools for both girls and boys. Bannu is considered the gateway to North Waziristan, a tribal region along the Afghan border and a stronghold for Taliban insurgents and other militant groups.

The Bannu Prison seems secure on paper, but in actual practice reveals serious security concerns. The Bannu Prison is surrounded by open fields and within a ten minute drive of the Frontier Region; it borders Pakistan's volatile tribal areas. The prison itself is surrounded by cement walls and topped by barbed wire with three successive entry gates. The outer gate, called the Phatak gate, is located on the main road. One armed guard is deployed in each of four towers overlooking the search areas at the three entry gates. The Phatak gate has a total of five security personnel – three armed guards, one guard to register visitors and another to frisk anyone entering the prison. While not stated in available sources, it is likely that there was security at the second gate as well. At the third and last gate, there is one policeman with a baton. At full strength, on duty personnel at any one time should be 151 guards.

On the day of the attack, however, the prison suffered serious deficiencies. On 15 April 2012, there were 119 police on duty with only 21 performing their duties. Additionally, eight police were on loan to Dera Ismail Khan Jail, four were on detached duty to the Karak Jail, ten were on leave, and six were AWOL. In addition to being significantly undermanned at the time of the attack, reports stated that there were only five AK-47s available. Adnan Rashid, the target of the TTP rescue operation, had been allowed to use cell phones, Facebook, and blogs, undoubtedly communicating with those planning the attack on the prison that held him.

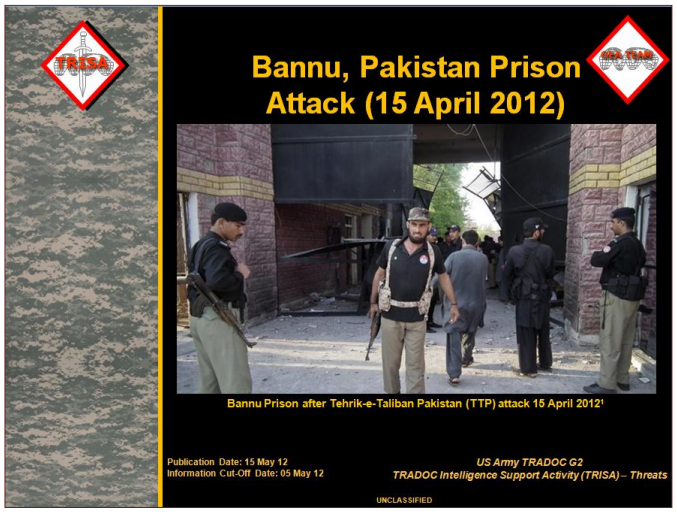
The TTP claimed responsibility for the attack on the Bannu Prison and stated that the rescue of Adnan Rashid from the prison was its primary purpose. Rashid was eight years into a death sentence for his conviction as the master-mind of a failed assassination attempt on then Pakistan president Pervez Musharrif in 2003 in Rawalpindi. At the time of the assassination attempt, Rashid was serving in the Pakistan Air Force. In 2011, Rashid was moved from the Adiala Prison in Rawalpindi to the Bannu Prison where he lived with as many 20 other dangerous and militant prisoners. Adnan Rashid developed a relationship with prison guards, such that he

was given use of cell phones and other social media type resources that allowed him to communicate with those planning the attack that rescued him.

The Bannu Prison attack was a disciplined operation lasting only two hours and resulting in only three prison officers wounded and no known TTP casualties. The TTP arrived unopposed at the prison front gate in pickup trucks and cars between 1:30 and 2:30 a.m. on 15 April 2012. The TTP attacked the front gate using small arms fire, hand-tossed grenades, and rocket propelled grenades (RPGs). Due to smaller numbers and lack of weapons, prison guards offered little resistance. The TTP moved to the death row area of the prison using hand-held radios to coordinate their actions, freed Adnan Rashid, and opened the doors to all the other cells using hammers and small arms weapons to break the locks. Some reports claimed that the TTP forced other prisoners to flee at gunpoint. In the melee, some prison guards donned prisoner uniforms and "escaped" with prisoners to avoid personal harm. While some of the attackers moved to free approximately 384 prisoners, others moved to the prison office and burned prison records, ostensibly to create further confusion. Although three other jails lay within two miles of the Bannu Prison, requested support did not arrive in time to make a difference. In the aftermath of the attack, 103 prisoners returned voluntarily, most citing lack of food and water in the surrounding mountains or their relatively short remaining sentences as reason for their return. Security forces conducted raids in Bannu, Lakki Marwat, Karak and elsewhere resulting in the recapture of more than 24 escaped prisoners.

The effect of the Bannu Prison Attack and the resulting escape of dangerous and militant prisoners had an immediate effect and caused much political posturing. The Peshawar High Court chief justice ordered a judicial inquiry into the incident. Justice Dost Mohammed Khan constituted a two-member committee to investigate. A special five-member committee was set up by Chief Minister Amir Haider Khan Hoti, Chief Minister of Kyber Pakhtunkhwa (KPK) Province. Government Leaders reacted immediately by removing the following key prison officials from their posts – Commissioner Bannu Abdullah Khan Mehsud; Inspector General of Prisons, Arshad Majeed Mohmand; Deputy Inspector General Police Range Bannu, Mohammad Iftikhar Khan; and Deputy Superintendent Bannu Jail, Mohammad Zahid.

Additionally, the Bannu Prison attack had a chilling effect on Pakistan's efforts to create the appearance of positive internal security. The escape exposed Pakistan's inability to deal effectively with internal terrorism in contradiction to recent government pronouncements of success against anti-government militants. Such a brazen, disciplined, and successful attack against a supposedly fortified prison will decrease local confidence in the government's ability to provide local security, create a boon to insurgent efforts to create instability and generate a general lack of confidence in the Pakistan government and its security forces.



Beyond the disciplined, planned, and well-executed TTP attack, the Bannu Prison attack revealed a number of serious security lapses within the prison. These types of mistakes should be of particular concern for small training and advisory teams working with local security forces in places like Afghanistan and Pakistan. Of primary concern was the easy access Adnan Rashid (and possibly others) had to cell phones, social media, and blogging sites that allowed the TTP to obtain intelligence information to plan and execute the attack. Lack of adequate manning and a shortage of weapons for the guards further ensured a successful attack.

Consolidating dangerous and militant prisoners at a single prison so close to the uncontrolled Federally Administered Tribal Areas (FATA), provided the TTP a rich target with short attack and egress routes. Being so close to the FATA area, it is reasonable to assume that some of the local security forces have relationships with some TTP members that may have further compromised the security of the Bannu Prison. The poor response by the neighboring jails and other security forces points to either an inadequate coordination plan or collusion between security forces and the TTP; likely it was a combination of both. Attacks of this nature have been rare in Pakistan; however, due to the successful Bannu Prison attack, the impending reduction in NATO forces in Afghanistan, and growing international war fatigue,

the TTP will probably become more bold and aggressive in future attacks on the Pakistan government and its security forces.

The Bannu Prison attack is a realistic scenario faced by many small training and advisory teams assigned to work with military and police forces in remote areas. Training for these types of military roles should be built around ensuring proper vigilance by small remote training and advisory teams related to adequate security manning, vetting of security forces, development and enforcement of SOPs, support coordination, and intelligence gathering and analysis. In addition, attention should be paid to building skills in determining local support for insurgent groups and activities that might lead to an attack similar to the Bannu Prison attack.

For a more detailed treatment of the TTP, see TRISA Threat Report "Tehrik-e-Taliban Pakistan" (March 2012). See also, TRISA Threat Report "Taliban Attacks in Kandahar" (June 2011), for analysis of similar attacks in Afghanistan.

THE JEMAAH ISLAMIYAH—A SOUTH ASIAN TERRORIST GROUP

by H. David Pendleton, OEA Team

Many military personnel think that most Islamist terrorist groups operate as a single monolithic organization that not only possess the same goals, but completely agree about the methods for the organization to reach its aims. The Jemaah Islamiyah (JI), a Muslim group concentrated in South Asia, proves that this characterization of a group with a singular mindset is false. Instead, JI's history shows a series of differences in the ways and means to obtain its goals that created schisms. As a result, leaders often departed JI to start a new organization that better reflected the departed leader's views. Military personnel at the dirt combat training centers (CTC) and in home station can better understand these multi-faceted terrorist groups by reading the TRISA Threat Report, "Jemaah Islamiyah-Islamist Terrorist Group" and incorporating what they learn to make their role players more varied as they oppose U.S. forces in training exercises.

JI's history dates back to January 1993 when Abdullah Sungkar and Abu Bakar Ba'asyir, two Indonesian Muslim clerics and fugitives who lived in Malaysia at the time, founded their organization with its primary goal to institute a pan-Islamic caliphate (religious government) that encompasses the region's Muslim countries—Indonesia, Malaysia, Singapore, southern Thailand, and the southern Philippine Islands (Mindanao). The idea of a pan-Muslim country in South Asia dates back even futher to the *Darul Islam* (DI) movement that began in the 1950s after the Dutch left Indonesia and local Muslim leaders wished to institute a Muslim government in their country.

Differences in how JI should achieve its goal of a pan-Muslim country in South Asia created such intense conflict among members that Muslim leaders often left the organization to start another group more sympathetic to their own ways of thinking. In 1993, Sungkar and Ba'asyir left DI to begin a new group that would adopt their more radical interpretation of the Koran. Later, when JI leaders departed to form their own groups, governmental authorities sometimes recognized these divisions as new and separate groups, but often erroneously continued to view them as JI cells.

Even JI's primary leaders were not immune to the internal conflicts in the interpretation of the Koran. After Sungkar died in late 1999 soon after returning to Indonesia, JI's spiritual leader—Ba'asyir—left the group he founded to establish an even more radical Islamic group, the *Majelis Mujahidin Indonesia* (MMI). In 2008, after the MMI became too conservative for some of the group's members, Ba'asyir left MMI and created his third group in less than two decades, the *Jemaah Ansharut Tauhid* (JAT).

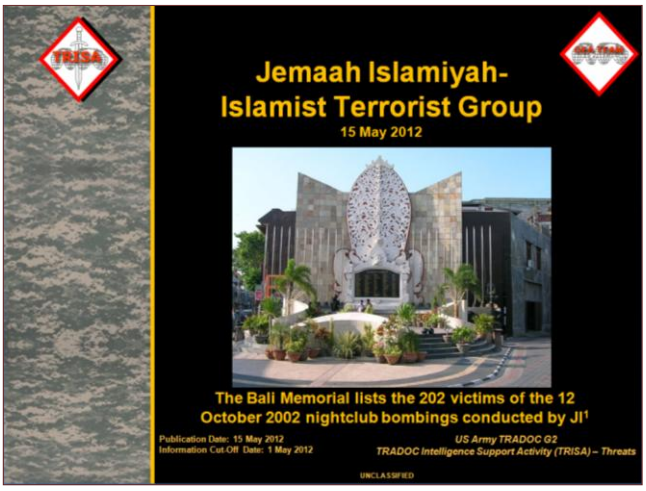
Other mid-level JI leaders also departed the organization due to divergent ideas, often upon the role of violence to achieve the group's objectives. JI eventually adopted, at least outwardly, a policy of non-violence to reach its goal of a Muslim caliphate in South Asia. Many other JI members disagreed. Malaysian Noordin Mohammad Top left JI soon after he helped in the successful 2002 bombings of two Bali nightclubs. Top's JI splinter group also carried out successful bombings of a Marriott Hotel in Jakarta in 2003, the Australian Embassy in Jakarta in

2004, and another attack on the Bali resorts in 2005. The third attack turned many tacit supporters away from JI and Indonesian neutrals began to support the governmental authorities, who wanted to end the terrorist attacks. Since Top was killed in a September 2009 shoot-out with police in Central Java, his former organization has failed to carry out another successful attack.

Umar Patek and Dulmatin, JI members who received training in al-Qaeda (AQ) camps in Afghanistan in the 1990s, left JI around 2002 and formed what became known as the Umar Patek Network. After the pair fled Indonesia for their role in the 2002 Bali bombings, they trained Abu Sayyaf Group members in the manufacture and use of improved explosive devices (IEDs) in the southern Philippines. Patek used contacts back in Indonesia to recruit both fighters and raise funds for the insurgents in the Philippines. In May 2010, Patek left the southern Philippines to visit Pakistan, where he was arrested in Abbottabad, the same city where Osama bin Laden was killed by U.S. Special Operations Command operatives only four months later. Patek's death put an effective end to his organization.

In late 2007, Dulmatin separated from Patek and returned to Indonesia where he set up the *Lintas Tanzim*, an organization with many of his former JI comrades; members of KOMPAK, an Islamist organization founded by another former JI member; bombers from the Banten Ring, a Muslim group from the Indonesian city of the same name; and new terrorist recruits from Aceh, an Indonesian city in the northern tip of Sumatra. Lintas Tanzim members felt that Top's group caused too much collateral civilian damage while JI's pronouncement against violence was too much at the other end of the spectrum. While the Lintas Tanzim believed in the use of violent terrorist acts to achieve its goals, the violence needed to be both disciplined and surgical to achieve its aims without alienating the common people. Dulmatin's death along with nearly 100 of his followers in February-March 2010 in shootouts with governmental authorities effectively exterminated this JI splinter group.

Due to the effective campaign against terrorist groups over the last decade by many countries' police forces, the current JI *amir* (leader) is unknown, and less is known about the current JI leadership. The police arrested the last known JI leader, Zarkasih, in 2007 and he remains in custody. Over the last decade, a number of other prominent JI leaders have been killed or imprisoned. Supposedly, JI maintains a detailed leadership succession plan. Possible current JI amirs include two individuals, Para Wijayanto and Hadi Surya. Nothing much is known about either individual. The only other major JI leader both free and whose whereabouts are known remains Abu Jibril (Mohamad Iqbal Abdurraham), originally JI's primary recruiter, who is current an imam in Jakarta, Indonesia.



The Threat Report on the Jemaah Islamiyah terrorist group contains more detailed information on JI's leadership and organization, its history, and the tactics, techniques, and procedures (TTP) of its preferred attack methods. The report also includes a summary of the various recruiting practices that JI uses to coax new members to willingly join a terrorist organization and tell-tale signs of possible terrorist training camps based on past JI practices. CTCs could use the information to better prepare units as they rotate through the exercises by providing a more complex terrorist hierarchy with various agendas instead of a group working completely in unison to achieve the same goal.

INFOWAR:
IRREGULAR OPFOR METHODOLOGY FOR PERCEPTION MANAGEMENT ACTIVITIES

by Jerry England, OPFOR Doctrine Team

Perception management involves measures aimed at creating a perception of truth or stability that best suits opposing force (OPFOR) objectives. Perception management integrates a number of widely differing activities that use a combination of true, false, misleading, or manipulated information. Targeted audiences range from enemy forces, to the local populace, to world popular opinion. At the tactical level, the Irregular OPFOR seeks to undermine an enemy's ability to conduct combat operations through psychological warfare (PSYWAR) and other perception management activities aimed at deterring, inhibiting, and demoralizing the enemy and influencing civilian populations.

The various perception management activities include efforts conducted as part of—

- PSYWAR
- Direct action
- Public affairs
- Media manipulation and censorship
- Statecraft
- Public diplomacy
- Regional or international recruitment and/or fundraising for affiliated Irregular forces

The last three activities traditionally may be considered strategic or operational in nature and not suitable for the tactical level. However, information communications technology and global dissemination of the 24-hour news cycle has empowered the Irregular OPFOR to implement complex perception management activities such as social activism to effect change, garner global support, and generally shape the operational environment to their purposes. Often considered the bottom rung of political statecraft, grassroots activism involves groups that are willing to battle the establishment to obtain their objectives. The Irregular OPFOR can enable political and civic leaders at all levels to engage the population to accept their ideology and support the OPFOR cause.

The Irregular OPFOR at times will compete for limited resources either from its higher headquarters or from an external supporting state. This competition appears to the outside observer as disjointed or lacking the discipline needed for unity of effort. Individual leaders of the Irregular OPFOR, however, are allowed to develop their own lines of operation as they see fit given the unique set of circumstances of their area of responsibility and the means at their disposal. When a particular tactic is proven to be effective, it will be replicated as necessary in order to exploit success, increase the perception of legitimacy for the Irregular OPFOR cause, and to give the impression of progress. This sort of "groping in the dark" for a successful strategy means that the Irregular OPFOR is able to experiment to find what works and to receive rewards when it arrives at an effective tactic. The key is to open as many inroads as possible and to increase the likelihood of windows of opportunity for the Irregular OPFOR to exploit the political, economic, or social situation.

In some cases the operational variables of PMESII-PT will determine whether or not a local area will require all of the elements of statecraft for a complete perception management campaign. Important issues such as regional conflicts, underprivileged and underrepresented populations, and the location of political, commercial, or economic power all have the potential to be targets of an INFOWAR campaign plan. As the Irregular OPFOR assesses the local environment and the enemy's center of gravity is determined, INFOWAR planners will target select groups, organizations, and individuals for a variety of perception management activities.

Although the Irregular OPFOR maintains that perception management activities conducted at the tactical level must be consistent with, and contribute to, the OPFOR's operational and strategic goals, the Irregular OPFOR is allowed much more discretion on the ways and means of achieving its perception management objectives. For example, forming a partnership with a charitable organization or a local business leader in order to obtain secure lines of communication as well as a recruiting pool would be a natural extension of the strategic public diplomacy effort necessary to influence the local populace. If there is a religious or other ideological approach available, the OPFOR can leverage this to buy credibility by establishing educational organizations. The Irregular OPFOR provides a conduit for recruiting indoctrination and long-term influence. Additionally, the Irregular OPFOR has the freedom to provide immediate

assistance and disperse funds without delay during times of crisis or whenever there is an opportunity to meet a particular objective. This gives the Irregular OPFOR the opportunity to be the so called "first with the most" in the struggle for hearts and minds.

Social Activism

Local partnerships and projects are regarded by the OPFOR as enhancing the strategic and operational goal of the Irregular OPFOR but are not necessarily prescribed by the higher command. The objective is to provide a working solution that is culturally acceptable to the target population and does not compromise the core ideology of the OPFOR. The Irregular OPFOR seeks to integrate its activities into the target society and does this by providing the essential services for everyday life. Through cultural acceptance and shared goals, INFOWAR operators are able to develop trust and loyalty among the society and create opportunity for future projects. Other examples of grassroots assistance given to a disenfranchised segment of the population by the Irregular OPFOR could include—

Example: "Civic Dissension Intercede Committee" in S. Africa (Photo CC by Discott)

- Establishment or purchase of a local business or industry in order to buy influence, generate funds for military or paramilitary activities, and provide access to lines of communications
- Cash payments to victims of both natural and manmade disasters
- Support to religious, educational, or charitable institutions for public relations purposes and recruitment
- Provision of services such as welfare, disaster relief, or policing in order to delegitimize the existing government
- Monetary support to religious, political, academic, or business leaders who are willing to support the Irregular OPFOR cause
- Establishing a parallel legal process where the population can obtain a just resolution for disputes without unwanted corruption by external values

If properly employed, the results of perception management activities become ingrained into everyday life of the target population and can be viewed as a positive force. The targeted population gets the services denied to them by the current structure while the Irregular OPFOR is able to move freely among the population and establish a support structure for future operations. Perception management activities are regarded by the enemy as propaganda, despite the fact that the Irregular OPFOR enjoys more influence over the population than the existing government does. The Irregular OPFOR is able to maintain contact with the target population in an overt way that further legitimizes it. By providing opportunities for education, work, and charity, the Irregular OPFOR receives in return loyalty and support for its cause. The Irregular OPFOR may adopt a long-term strategy that allows it to fully integrate into all aspects of society. The fact that it administers resources and services that are unavailable to the targeted population increases its influence and makes affiliation with its cause a desirable end state.

INFOWAR: IRREGULAR OPFOR METHODOLOGY… *(continued)*

Disaster Response

Response to disaster, whether natural or manmade, is viewed by the Irregular OPFOR as another opportunity to gain influence and support in a region. Human suffering on a large scale sets the conditions for chaos and an over extension of the state's resources. In many regions of the area of operations, disaster relief services are inadequate, and there is usually an inordinate amount of suffering before any assistance becomes available. Because of its access to resources and support systems that are outside the government's bureaucratic structure, the Irregular OPFOR can enable a more comprehensive response to natural disasters in certain targeted areas. In some cases, it will augment the current regime's disaster relief and attempt to integrate and legitimize its role in assisting the population. In other situations it will supplant the existing structure and outperform the competition. The goal is to be the first with the most in terms of aid and assistance. Disaster response efforts may include—

Example: An Irregular Organization displays banners on a public street. (Photo CC by Aotearoa at pl.wikipedia)

- Evacuation of personnel from threatened areas
- Provision of humanitarian relief such as food and temporary shelter
- Long-term plans to rebuild structures destroyed by the disaster
- Cash payments to victims to pay for immediate needs or to compensate a loss

The combination of these services including grassroots activism, social services, and disaster response coupled with a political message and a strong military presence allows the Irregular OPFOR to establish its legitimacy and build support among the population to make inroads for future operations.

RECONNAISSANCE ATTACK EXAMPLE

For more information, with AKO access, go to **https://www.us.army.mil/suite/files/30894352.**

by Dr. Jon Moilanen, Threats Terrorism Team (T3) Integration

A *reconnaissance attack* is a tactical offensive action that locates moving, dispersed, or concealed enemy elements and either fixes or destroys them. However, a reconnaissance attack can also seize the initiative from the enemy by using surprise and deception. The purpose of a reconnaissance attack in this example is to obtain information on enemy coalition force capabilities by forcing a reaction to an attack.

Background Situation

The local insurgent organization observes the coalition forces establishing police stations along the surfaced roadway of Highway 3 and positioning coalition police teams at traffic control posts (TCPs) in villages of the valley. The enemy governing authority continues to demonstrate a presence in the rural valley and provides security for truck convoys through the province. The TCPs monitor the flow of commerce between the

unimproved roads and trails and the highway. The TCPs also observe known routes for insurgent movements from the border mountain region. Insurgent reconnaissance indicates that the police station is forming a quick reaction force (QRF) in an assembly area near the highway.

Functional Organization for a Reconnaissance Attack (See Figure A)

With his resources marshaled and rehearsed in a mountain area safe haven, the local insurgent leader ① orders a reconnaissance attack on the coalition force QRF and a TCP of the police station. The plan is to attack a coalition TCP ② and cause the employment of the police station's QRF. Reaction time of the QRF ③ and what routes the QRF uses are critical intelligence for the insurgent leader to determine when and where to attack the QRF in his local area of responsibility (AOR). The result of the reconnaissance attack is to destroy the police QRF and a TCP.

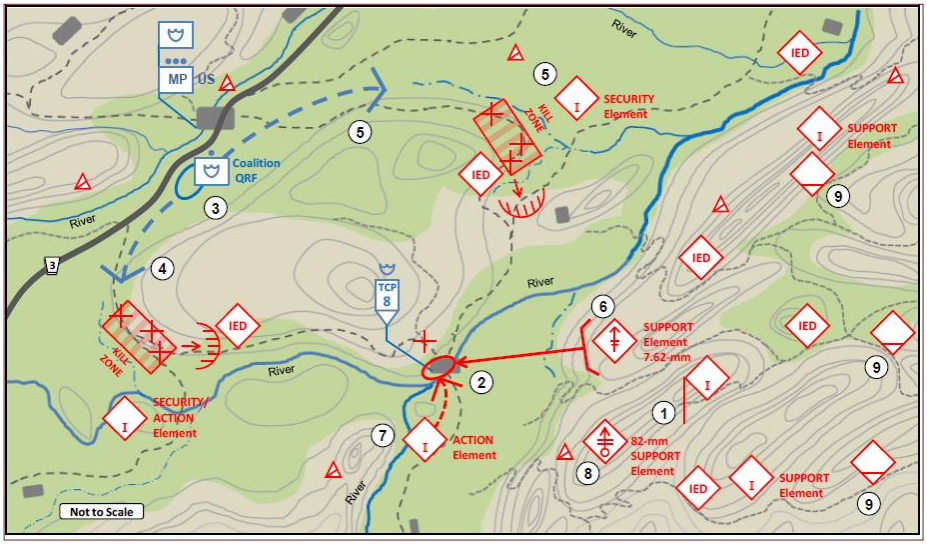


Figure A. Insurgents initiate a reconnaissance attack

Depending on the situation, the insurgent leader organizing a reconnaissance attack may designate reconnaissance, security, security/action, and/or support elements. There may be more than one of each type element. Various types of support elements may be organized for a particular mission.

Reconaissance Elements

The leader organizes several *reconnaissance elements* in the form of observation posts. Their role is to locate and report on enemy elements in the AOR. They will maintain surveillance of actions at the police headquarters on the highway, track the approaching enemy QRF, and keep security and support elements informed of enemy locations. In this example, the reconnaissance elements do not engage the enemy; the reconnaissance elements report.

Security Elements

The insurgent leader task-organizes sufficient combat power to engage enemy coalition elements on the routes ④ and ⑤ that can be used by the enemy QRF. A security element may also be described as an *action element* when it attacks the QRF. The *security elements*, working in conjunction with reconnaissance, support, and action elements, plan to use kill zones to fix and destroy the enemy QRF with direct and indirect fires. An attack on a TCP will cause the QRF to employ from its assembly area along one of two routes.

Action Element(s)

The insurgent leader organizes *action elements* to conduct specific actions in conjunction with support elements. One support element ⑥ initiates the attack on a TCP with direct fire of a light machinegun. An action element ⑦, on order, attacks the police TCP. This action element is to kill the enemy, acquire useful weapons and equipment, collect documents, and destroy any materiel left at the TCP before exfiltrating into the mountains. There is no expectation to take prisoners in this attack.

Once the TCP has been destroyed, the insurgent leader will direct when security elements are to exfiltrate if not in contact with the enemy coalition forces, or disengage if in contact with the enemy and exfiltrate on designated routes in the valley. Some elements will rendezvous before continuing to a safe haven in the mountainous terrain near the international border. Some reconnaissance elements will remain in the valley near villages to conduct surveillance and report on subsequent police actions.

Support Element(s)

One or more *support elements* can perform various supporting tasks. In this reconnaissance attack, the insurgent leader task-organizes elements and plans for capabilities as follows:

- Fire support
- Air defense
- Logistics
- Information warfare (INFOWAR)

Fire Support

Indirect fires of the medium mortar team ⑧, in conjunction with direct fires, are to destroy the QRF. Then, the mortar team will cover the withdrawal of security and/or action elements with mortar fires if the enemy attempts to follow and engage the withdrawing insurgents in the valley.

Air Defense

The local insurgent organization has no sophisticated air defense weapon systems. The leader has rehearsed his cells for an "all-arms air defense" concept if enemy helicopters or fixed-wing aircraft intervene during the attack. One light machinegun team, two antitank grenade launcher (ATGL) teams with the security elements, and all insurgents within small arms weapons range will use their weapons against an aircraft if it comes within effective engagement range. Rehearsals emphasized that the intent is to mass weapons fire that a helicopter or plane flies through. Even though the likelihood of crippling or catastrophic hits on an aircraft is low, the barrage of weapons fire can disrupt effective use of aircraft weapons and/or observation. (See TC 7-100.2, chapter 11, for more information on all-arms air defense.) The air defense anticipates likely air avenues of approach if enemy aircraft attempt to locate insurgents exfiltrating into the mountain passes.

Logistics

The local insurgent organization establishes a group of caches ⑨ of ammunition, food, and medical supplies along routes into the mountains. The insurgent plan expects a rapid movement away from the TCP site if the police QRF is able to maneuver through the security/action element kill zone. Wounded insurgents are to be evacuated with the elements and teams moving into the mountain passes. No insurgent casualties, wounded or killed, are to be left in the valley.

INFOWAR

INFOWAR activities in this reconnaissance attack are directed at the local rural population and the police force. INFOWAR cell members circulate among the valley farmers and ensure them protection from the illegal taxing that has occurred by local police officers. An attack on the police station is promised in the near future. In return for this protection, the cell obtains detailed information on how the interior of the police station is organized, the daily shift schedule, and a description of the communications equipment it operates. The INFOWAR cell has also posted a written warning on the wall of the police station and on the highway road surface.

Reconnaissance Attack on Coalition Police Forces (See Figure B)

Insurgent elements infiltrate to designated positions and wait for the insurgent leader's command to initiate the attack. Reconnaissance elements ① provide periodic reports of the police presence on the highway and at the TCP. As the early evening shadows start to cover the valley floor, machinegun fire erupts from the ridgeline. The policemen of the TCP at the ford site take cover in a mud building next to the river, and return fire with their automatic weapons. The TCP leader immediately notifies the police station that they are under attack and requests assistance.

Insurgent reconnaissance elements near the police station at the highway observe the reaction of the police forces. Actions appear confused and the crews of the QRF have difficulty loading some equipment in their vehicles. Two of the vehicles have inoperative radios that are being replaced in the vehicles. The QRF leader is shouting and even kicks one of the policemen. As the vehicles depart their motor park, they move to the south at a high rate of speed. The orientation of weapons on the vehicles looks haphazard and is not providing all-around security as the vehicles continue down the trail to the southeast.

Security elements on the northern ② and southern ③ routes listen to situation reports with their handheld

radios and learn that the QRF is using the southern approach to the TCP. The security elements pre-position improvised explosive devices (IEDs) at the kill zones. Reconnaissance and security elements remain alert for any relief forces that might approach from along the highway.

The southern security/action element prepares to call for mortar fire as the QRF nears the kill zone. The QRF is not using any sense of security with its lead vehicle as it detonates an IED ④ on the trail. Mortar fires start to impact ⑤ in the kill zone, and the security/action element rakes the vehicles with direct fires as they stop and stack up on the trail. An intermittent stream bed on one side of the trail and a steep cut in the bank on the other side do not allow any lateral movement for the vehicles.

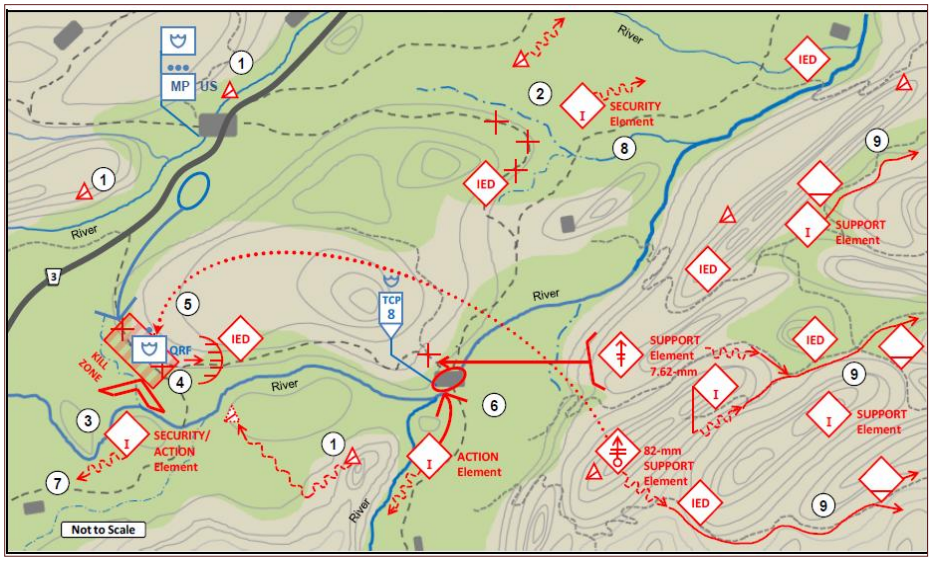


Figure B. Reconnaissance attack on coalition police forces

Simultaneously, the machinegun fire on the TCP shifts just north of the TCP as planned in order to contain the policemen in the mud building at the TCP. The action element attacks the TCP ⑥. After a brief engagement with automatic weapons and ATGL fires, the policemen of the TCP are killed. The action element clears the TCP; gathers useable weapons, equipment, and documents; and quickly starts to exfiltrate along the river bed to the south.

Return fire from the QRF had been ineffective. At least one vehicle was destroyed by an IED, and two other vehicles were damaged by the mortar, small arms, and ATGL fires. Evening darkness precludes observing any accurate count of enemy wounded or killed, but the security/action element leader reports that the QRF is destroyed. The insurgent leader directs the southern security/action element to exfiltrate ⑦.

The northern security element ⑧ reports no observed enemy movements in its AOR. The reconnaissance elements near the police station report that no additional vehicles have arrived from the south or north along the highway. The insurgent leader directs the machinegun team and the mortar team to withdraw to the rendezvous. The insurgents exfiltrate ⑨ on separate routes. Insurgents also emplace IEDs along the insurgent exfiltration routes. If conditions provide the ability to successfully ambush pursuing enemy elements, these IEDs will be used to initiate ambushes. The IEDs on the trails can be command detonated if enemy forces attempt to pursue the insurgent elements into the mountains.

The insurgents do not disturb the caches as they continue their movement to the east and higher mountain ridges. Reconnais-sance elements remain in the valley and along the ridgeline to observe and report any coalition force actions.

Effects of the Reconnaissance Attack

The insurgent leader accomplishes his mission task. He destroys the QRF and a TCP of the police station. These actions reinforce a negative psychological effect on the local police force, and reinforce his authority with the relevant population along this section of valley floor and adjacent mountain ridges. The villagers and farmers of the area continue to provide information and intelligence on activities of the governing authority, do not dispute the level of insurgent taxes on food in return for insurgent protection, and provide several recruits for insurgent operations.

Insurgent casualties are minimal. One insurgent in the southern security element is slightly wounded by small arms fire in a shoulder, but is able to exfiltrate with the element with no assistance. One insurgent is peppered with rocks and debris when he walks into the backblast of an ATGL as the grenadier fires his weapon. The wounded insurgent is temporarily blind with swollen eyes and a heavily bruised face. With his face covered and bandaged, he exfiltrates on the back of another insurgent.

RECONNAISSANCE ATTACK EXAMPLE *(continued)*

The governing authority's credibility in the rural valley district is in jeopardy. The local insurgent organization leader gains status with the higher insurgent organization as an individual who uses his initiative with available resources and manpower in his local AOR. His successes in INFOWAR techniques and tactical actions are evident in the improved support and human intelligence (HUMINT) from the villagers along the valley plain and farming communities. The intelligence is a significant addition to the higher insurgent organization's collection plan on the governing authority's infrastructure and vulnerabilities for future attacks in the rural region.

THE NONTRADITIONAL CHEMICAL, BIOLOGICAL, RADIOLOGICAL, AND NUCLEAR (CBRN) PORTRAYAL IN POTENTIAL OPERATIONAL ENVIRONMENTS (OES)

by Walt Williams, Training-Education-Leader Development Team

"In 1346, plague broke out in the Tartar army during its siege of Kaffa [present day Feodosia in Crimea]. The attackers hurled the corpses of plague victims over the city walls; the plague epidemic that followed forced the defenders to surrender, and some infected people who left Kaffa may have started the 'Black Death' pandemic which spread throughout Europe." (USAMRIIDS Medical Management of Biological Casualties Handbook, page 1)

The use of chemical and biological weapons isn't just a twentieth or twenty-first century phenomenon. These types of weapons have been an effective combat weapon for centuries. History is replete with examples of biological and chemical use. Toxic fumes were used in India as early as 200 B.C. and during the Sung Dynasty in China. There are accounts by Thucydides of the burning of pitch and sulfur during the sieges of Plataea in 429 B.C. and of Delium in the 424 B.C. Peloponnesian War to produce poisonous fumes.

The Romans dumped the corpses of dead animals in their enemy's water sources to deny the use of the water. Confederate soldiers shot horses and other farm animals in ponds as a way to contaminate the water sources. By the end of the nineteenth century, the world witnessed the British use of artillery projectiles laced with picric acid against the Boers. Throughout the twentieth century, revolutionary scientific advancements brought CBRN warfare to a high state of conventional or traditional employment by military forces in a symmetric setting. However, recent past and current events of adaptive or nontraditional employment of CBRN by unconventional forces such as insurgents or terrorists demonstrates that we cannot close the book on this phenomenon.

The intent of this article is to highlight how terrorist and insurgent incidents involving chemical, biological, and toxic industrial chemicals (TIC) differ from incidents involving conventional weapons and threats. It is important that we review the definitions before we continue the discussion.

A chemical agent is defined as a substance that produces an effect on humans, animals, and plants by virtue of their toxic chemical properties. During training exercises the conventional wisdom or event is for chemical agents to be employed against humans. However, when used as weapons, chemical agents are not necessarily aimed or targeted to humans, but also at crops and animals. The destruction of poppy fields through aerial dissemination of chemicals is an example of a chemical attack against crops. The agent can appear as a vapor, aerosol, or liquid. The agent can either be a toxic (blood/choking, blister, nerve) or incapacitating agent. It is important to note that riot control agents, smoke, and flame materials are generally excluded from consideration as traditional chemical warfare agents.

TICs are chemical substances with acute toxicity that are produced in large quantities for industrial purposes. Exposure to some industrial chemicals can have a lethal or debilitating effect on humans. The near-universal availability of large quantities of highly toxic stored materials, their proximity to urban areas, their low cost, and the low security associated with storage facilities make them a potentially attractive option for use. Employing a TIC against an opponent by means of a weapon delivery system, whether conventional or unconventional, is considered a chemical warfare attack with the TIC used as a chemical agent. The target may be the enemy's military forces or his civilian population.

Biological agents are defined as microorganisms that cause disease in humans, plants, or animals or cause the deterioration of material. Unlike chemical agents, biological agents have the capability to reproduce themselves, and thus are less predictable than chemical agents.

An Operational Environment

Every potential operational environment consists of multiple actors or players such as the enemy, friendly forces, non-combatants, governmental and nongovernmental organizations, terrain, weather, and other factors. The traditional and nontraditional employment of CBRN can occur at any point of the range of military operations. A typical paradigm or mindset is for one to expect the traditional forms of CBRN employment during combined arms maneuver (CAM) operations. On the other hand, one may expect a higher frequency of nontraditional forms of CBRN employment to occur during wide area security (WAS) operations. However, it is important to note that the Army core competencies of offense, defense, and stability operations each require a combination of CAM and WAS. None of the core competencies of offense, defense, and stability is conducted in total isolation. Thus, it is conceivable to expect both traditional and nontraditional forms of CBRN employment during both CAM and WAS.

Using the OE variables (PMESII-PT) as a framework, one is able to understand the various factors such as politics, military capabilities, or economics that may dictate the rationale for the type of CBRN employment. Figure 1 illustrates the various actors in relation to the traditional and nontraditional employment of CBRN with regard to the range of military operations. The figure shows that the actors (within the clouds) are not limited to any one part of the range of military operations. State actors along with terrorists and insurgents may choose to use the supply networks of underground or criminally-based activities for the acquisition and transport of chemical and biological agents as well as components such as fuzing and pressure devices.

Current and future U.S. adversaries will seek ways to offset U.S. advantages. These asymmetric means range from the simple use of information to shape world and U.S. opinion to the employment of niche and low-level technologies. An added complexity is adaptive employment of chemical and biological agents. The situation becomes even more complex when the enemy employs CBRN in large metropolitan or urban areas or terrain. For example, large urban areas such as Seoul, Korea (21 million people); Lagos, Nigeria (9 million people); or Manila, Philippines (14 million people) pose a unique challenge to forces conducting military operations. U.S. forces conducting military operations in these urban areas can expect the adversaries to use adaptive methods of employing chemical and biological agents. For example, a terrorist plot was foiled in Jordan that involved the use of vehicle-borne improvised explosive devices (VBIEDs) along with additional vehicles loaded with household chemicals and pharmaceuticals. Additionally, we witnessed several attacks in Iraq involving the use of artillery projectiles filled with Mustard and Sarin chemical agents using an IED as the detonating device. The public disclosure of these actions produces both concern among the coalition force and fear among the general population.

There is an assumption that employment of chemical and biological weapons involves tactics, techniques, and procedures (TTP) conducted by special-purpose force units operating in a conventional force construct as illustrated in the example (presented in the red center box).

Shrouded by darkness, the man of Unit 124 approached the fence of the base and donned gas masks and large black rubber gloves. After testing the wind, the members of this sensitive biological weapons detachment opened the metal canisters near the perimeter fence. When the task was complete, they fled north on foot…Peyton spoke slowly and without emotion. "This is an anthrax outbreak."

The Next War, *pages 16-17.*

However, one could see that in the latter half of the twentieth century, it was just the opposite. What we see today is not necessarily a high-tech arena requiring specialized equipment or core materiel. Instead, we see an application of basic high school and college biology and chemistry coupled with motivation and innovative means of delivery. The use of IEDs is one of many innovative means of delivery. IEDs are devices placed or delivered and fabricated in an improvised manner incorporating explosives or destructive, lethal, noxious, pyrotechnic, or incendiary chemicals. They are designed to destroy, disfigure, distract, or harass. It is possible to categorize an IED by the type of container (i.e., car bombs), by the method of initiation (i.e., electric or nonelectric), or as open or closed devices (depending on whether or not they are concealed). An IED normally consist of a filler (explosive, incendiary, or chemical), container, fuze, detonator, and power source, depending on method of initiation. The predominant numbers of IEDs are homemade or specifically assembled for the intended target. It is not unusual for international terrorists to use military explosives, especially the malleable or sheet plastic type, in the construction of an IED. Detection and recognition of an IED is becoming steadily more challenging, because of the variety of devices being assembled, the sophisticated designs, the imaginative use of commonly available materials, and clever packaging.

Any munition would require a fuze and burster assembly that would provide either an air or ground burst for a chemical agent and have sufficient power in the burster to disseminate, but not destroy, the chemical agent. The weapon's ballistics should provide for proper angle of impact to optimize the agent distribution (the rocket-propelled grenade [RPG] is a direct fire weapon which could malfunction when mated to an indirect fire mortar round). The insurgent would have to do some testing prior to actual use to develop the required gunnery techniques. For most agents or chemicals employed, minimal safety gear or special equipment is required for limited scale production. To modify existing high-explosive antitank (HEAT)/HE mortar or RPG rounds to carry a biological or chemical payload, terrorist or extremist forces need the following:

- A method to remove the current HE fill
- A chemical payload to replace the HE fill
- A properly designed burster/fuze combination that will disseminate the chemical payload without destroying it
- Safety techniques and equipment to cope with the explosive removal process and loading the chemicals

The thought of using human cadavers as "biological bombs" is in the minds of many, beyond the imagination of twenty-first century man. It is important for us to transform or broaden our mindset to understand that traditional chemical and biological agents and weapons can be developed for terrorist purposes. Even TICs which are manufactured for everyday use can be applied in weapons that can be extremely hazardous, even fatal. The potential for intentional use of industrial chemicals as weapons may be illustrated by examples in the Balkans. During the period of 1993-1995, Serbian forces in the Balkans attacked the Petrochemia facility, which stored large quantities of anhydrous ammonia and a variety of other potentially hazardous chemicals, near Kutina, Croatia. The Serbs attacked the facility six times using rockets, bombs, artillery, and mortars. Serbian Forces also intentionally targeted the pesticide production facility at Sisak and the natural gas refinery in Ivanic. Also, during the siege of Muslim forces in Tuzla by the Serbs, the Muslims threatened to release large quantities of chlorine gas from railroad cars under their control. Although there would have been a high number of friendly casualties from such an action, the Muslims vowed they would release the gas if the city were assaulted. Subsequent U.S. modeling efforts indicated that had the attacks destroyed existing stored chemical containers, lethal concentrations of chemicals could have covered a wide area.

Potential U.S. adversaries including terrorists and insurgents understand that chemical and biological agents may be virtually undetectable while they are in transit. For example, a terrorist may transport the agent in every day baggage (gym bags, backpacks, etc) since there is no mechanism used during routine searches of individuals such as bomb, border or immigration, or drugs. The most prudent method of detection is a physical search of the person(s) or vehicle/equipment by a well-trained and very lucky searcher. The wide spectrum of chemical and biological agents and delivery methods combined with the inadequate supply of medical prophylactics measures (such as antidotes and vaccinations) available to the general population within a given theater increases the difficulty of the U.S. to properly protect and respond to each attack. Unless the U.S. is forewarned of a potential attack against the population, it could be perceived as impotent thus increasing the likelihood and frequency of the events.

Unconventional Capability

Developing countries and transnational organizations are those limited in terms of infrastructure, materiel, and resources and are not likely to independently develop a robust, organized chemical warfare or biological warfare program. Instead, they would more than likely develop chemical or biological agents or toxic chemicals or substances in a way that would reduce the risk of detection. One approach to minimize detection is to produce laboratory quantities using the existing infrastructure of the target country and employ the agent by improvised delivery or dissemination techniques. All of the information necessary to produce toxic chemicals and poisons at an unconventional level is available to transnational organizations. There are three levels of proficiency in production of unconventional chemical and biological agents:

- High-level capabilities are characterized by the ability to produce and employ second- and third-generation chemical agents and complex biological agents. This end of the spectrum represents the most dangerous of the three ad hoc levels. Terrorist or insurgent groups located on this end of the spectrum are generally large in nature, well financed and sophisticated, and possibly state-supported.
  - For example, in 1984 Paris police raided a suspected German Red Army Faction safe house and discovered a bathtub containing many flasks filled with the biological agent Clostridium Botulinum. Clostridium Botulinum produces a bacterial toxin as a severe form of food poisoning. An infected victim becomes ill with stomach pains, diarrhea, visual disturbances, giddiness, and muscular weakness within a day. The whole body, including the respiratory muscles, becomes paralyzed leading to death within a few days. The police also found many documents that revealed a strong working knowledge of lethal biological agents.
  - The Japanese terrorist group Aum Shinri Kyo is another example of a well-financed organization. On March 20, 1995, the group was able to conduct an attack of the Tokyo subway system using the chemical nerve agent, Sarin. On March 28, 1995 Tokyo police conducted a series of several raids against Aum Shinri Kyo facilities. The police discovered large quantities of the biological agent Clostridium Botulinum.
- Intermediate-level capabilities are characterized by the ability to optimize the available procedures for the production of toxic compounds and poisons and also procedures on testing the products. Terrorist or insurgent groups located on this portion of the spectrum are generally smaller in nature, less sophisticated, and possibly use chemical and biological agents that are readily available for use.
  - For example, in 1992, followers of the Bhagwan Shree Rajneesh cult acquired Salmonella typhi samples from an Oregon hospital. The cult contaminated salad bars in local restaurants in Oregon with Salmonella typhi. This capability suited their purposes in that it was simple to deliver (hand spray bottles) and would temporarily incapacitate the victims to prevent them from voting.
- Low-level capabilities concentrate on following written procedures and seeking to employ toxic industrial chemicals without modifications or an understanding of how to enhance their effects. Smaller groups or individuals with very limited targets use the chemical and biological agents in murder plots or to create chaos.
  - Recently Israeli Security officials of the Shin Bet secret service were able to thwart a Palestinian terrorist plot to detonate and AIDS bomb. The plot involved the Palestinian Tanzim terrorist groups plan to obtain AIDS infected blood from Palestinian hospitals and attach the blood to a suicide bomber vest. The suicide bomber would then conduct an attack in a designated Israeli city. According to Israeli medical personnel, the probability of casualties (from the blast) being infected by the AIDS blood was extremely low.

Chemical/Biological Convention Relevance

The intent of the various CBRN warfare conventions, treaties, or protocols is to make it difficult for a nation-state or transnational entity to produce, stockpile, weaponize, or employ CBRN weapons to the extent that military forces would be subject to a significant threat or would be significantly constrained from executing operational and tactical missions. This does not mean that the CBRN convention, treaty, or protocol can be verified with 100 percent confidence. The enforcement or verification provisions enable the signatories to monitor, verify, and enforce the treaty with a reasonable confidence level. However, the enforcement or verification provisions of these conventions, treaties, or protocols do not rule out the use of CBRN by terrorists or insurgents, nor do they rule out isolated incidents of CBRN employment. Isolated tactical incidents of CBRN employment as well as CBRN employment by terrorist or insurgents present a dilemma of potential retaliation for signatories. What is the appropriate measured

response? Do we conduct a strike against a particular terrorist or insurgent training camp or base? Do we conduct a strike against a rogue state sponsor of terrorism?

The Information Campaign

One would ask if the Tartars were successful in using disease as method of breaking the siege. The answer is simply yes. First, the illness caused the city of Kaffa to surrender to the Tartars. Second some medical historians have speculated that the Tartars' means of catapulting plague infested bodies into the city resulted in the bubonic plague epidemic spreading across medieval Europe causing approximately 25 million people to perish. Third, an immeasurable effect is the "biological bomb" psychological impact on the populace.

A terrorist or a tactical event conducted by conventional or irregular forces resulting in many casualties in any locale will receive immediate local and national media attention. If the event involves the use of chemical or biological agents or weapons (to include toxic industrial chemicals), there is a heightened concern among the populace and the government. Even though the attack may be small scale and may result in limited illness and fatalities, the psychological impacts from such an attack could be severe. The attack may generate substantial media attention, incite terrorist or insurgent rhetoric, and force a heightened interest into the perceived use of chemical and biological weapons by friendly and threat forces. For this heightened awareness of chemical and biological weapons to take place, there has to be a seed planted of previous use of these types of weapons by either side or a sense of distrust among the populace. For example, an insurgent group may seek to poison food supplies as a means to produce illness or fatalities among the targeted populace to induce fear and a lack of confidence in the outsiders' agricultural and medical techniques.

Another example is if a non-governmental agency or entity is using herbicides or insecticides for agricultural purposes, they may become the target of hostility by the population. A plausible example of a recent world event would be as follows: The Syngenta herbicide "Paraquat" is currently thought to be a major source of poisoning in West Africa. The company markets the herbicide under the name "Gramoxone." The herbicide is generally used on agricultural farms or sites such as fruit (pineapple or banana), coffee, and rubber plantations. At the request of the country of Burkina Faso, the Secretariat of the Rotterdam Convention added "Paraquat" to the list of severely hazardous pesticides in December 2010. The Burkina Faso request was based upon a Rotterdam Convention study that showed 18% or (54 of 296 cases) of the pesticide poisonings were attributed to the use of Gramoxone. As a result of the request, nine Western African nations took steps to ban the herbicide.

The use of protective clothing and equipment may be expensive and very difficult to wear in hot climates within developing countries. The lack of the proper clothing and equipment for workers increases their chances of the side effects of severe illness or death due to prolonged exposure to the herbicide. Training, education, and resources (clothing and equipment) for workers may more than likely mitigate the health concerns as a result of the use and exposure to the herbicide. But, here lies a golden opportunity for an insurgent group or organization to use the media as a way to build on the tragic side effects (serious health problems and even death) of the herbicide as a method to build and sustain mistrust between the non-governmental agency and the population.

The government or military use of insecticides and herbicides as a defoliant or to destroy narcotics crops can lead to an effort to produce fear. One would only have to look at the efforts by despots in developing countries to induce the belief that the herbicides or insecticides were being introduced to control the population growth and even as a method of low-level genocide.

Along with bombings and shootings, one must consider the brutal reality of a chemical and biological hot zone. Biological mass casualties on a single scene are unlikely because biological effects take days or weeks to manifest themselves. Patients will appear in ones and twos throughout a region, state, nation, or the world. Chemical attacks are another story. First, the initial information reports probably won't paint a clear picture. The event may begin with a report of a single patient in respiratory distress in a school, mosque or church, market, stadium, auditorium, or airport. Additionally, there is a possibility that the usual indicators of a hazardous materials incident may not be present. The location may not have identifiable containers, placards, material safety data sheets, or shipping papers. Therefore, responding personnel may not immediately recognize a biological or chemical incident or the personnel responsible for the incident. It may take days to accurately identify the substance and the individual or group responsible for the incident. In the meantime, media personnel may produce reports with contradictory or inflammatory material to incite the populace.

Media coverage of chemical and biological events additionally presents a security challenge. It is conceivable that the media coverage may result in the broadcast of U.S. strategies and tactics throughout the world. For example, during the 1996 anthrax hoax at the B'nai B'rith headquarters in Washington, D.C., the media showed HAZMAT deployment and decontamination procedures in vivid detail. Additionally, at a pipe bomb incident in Florida, the media exhibited close-ups of classified procedures for disarming the device.

The key for U.S. forces is a proactive information warfare campaign that establishes credibility and trust while simultaneously discrediting the efforts of the insurgents. The ideal campaign involves the use of medical personnel, international organizations, and the local populace.

Summary

Lessons learned from Operation New Dawn (formerly Operation Iraqi Freedom) and Operation Enduring Freedom indicate the need or requirement for flexible and adaptive organizations within the U.S. military. These organizations must be able to readily accept the challenges by enemy forces of both traditional and nontraditional forms of CBRN employment. The organizations also must be able to immediately respond to these employments in unified land operations. This requires a cultural shift in the training and education of leaders and soldiers.

In most cases the Combat Training Centers (CTCs) make use of chemicals through the traditional means of a mortar or artillery strike but there is evidence of the CTCs using the adaptive or nontraditional employment of chemical munitions. For example, the Joint Readiness Training Center (JRTC) uses biological agents to affect water sources. They also use chemical rucksack bombs, chemical truck or VBIEDs, chemical sprayers, and chemical land mines. The training objective is to introduce and familiarize the training unit to the various nontraditional forms of chemical and biological employment during unified land operations. Though the introduction of chemical and biological weapons may be on a small scale, it is important to consider the training effects and outcomes from secondary and third order implications of such an attack, such as the media and/or the handling of civilian causalities.

Train the Trainer Coming this September

TRISA-Threats will host its annual Hybrid Threat "Train the Trainer" (TTT) Course of Instruction (COI) from 17-21 September 2012 at the Mission Training Complex, Leavenworth, Kansas. This week-long course covers Hybrid Threat and associated opposing force (OPFOR) application as depicted in the new Army TC 7-100 series (e.g. organization, equipment, and tactics). The intent of this COI is to train a limited number of attendees who will return to their installation and/or command to teach the material to others.

Clearances are not required. Contractors and foreign military students are welcome to attend. All interested participants or organizations are requested to submit names as soon as possible, but no later than 1 August 2012, to the course administrator: patrick.madden@us.army.mil or 913-684-7997 (DSN 552). Seating is very limited. Students will be provided all course material. This includes our latest approved and draft OPFOR publications.

WEG HIGHLIGHT: RUSSIAN 7.62-MM GENERAL PURPOSE MACHINEGUN PKM AND PECHENEG

The Worldwide Equipment Guide (WEG) was developed to support OPFOR equipment portrayal across the training community. The WEG is not a product of the U.S. intelligence community. The WEG is a TRADOC G-2 approved document. Annual WEG updates are posted on the Army Knowledge Online (AKO).

Russian 7.62-mm General Purpose Machinegun PKM and Pecheneg

Ammunition Types	Typical Combat Load
7.62-mm cartridge Ball Ball-tracer Incendiary-ranging API API-T	**INA**

SYSTEM
Alternative Designations: (see VARIANTS)
Date of Introduction (PKM/PKT): 1971/1968
Proliferation: Widespread

Description:
Crew: 2
Weight (kg):
- Empty (w/o magazine) (PKM/PKT) (kg): 8.4/10.66
- Loaded (with magazine): Varies with magazine
- Ammo box (only) with 100/200-rd belt (kg): 3.9/8.0

Tripod (lightweight) (kg): 4.75
Length (mm):
- Overall (PKM/PKT): 1,160/1,080
- On tripod (PKS): 1,267
- Barrel: 658

Barrel Change: Yes
Mount Type: Pintle, coaxial, bipod or tripod (Stepanov)
Mounted On: (see VARIANTS)
Rate of Fire (rd/min):
- Cyclic: 650
- Practical: 250 for PKM. Bursts to 600 for Pecheneg/PKP

Fire Mode: Automatic
Operation: Gas
Feed: Belt, 100-rd belt carried in a box fastened to the right side of the receiver. 25-rd belts can be joined in several combination lengths (100/200/250)

SIGHTS
Name: INA
Type: Open iron sights
Sighting range (PKM/PKT) (m): 1,500/2,000
Magnification: None
Night Sights Available: Yes

VARIANTS
PKM: Squad machinegun
PKT: Vehicle mounted MG with solenoid electric trigger, remote sight, and a longer heavier barrel. It lacks a stock and, bipod. Some are coaxial to a main gun and use its sights. Others operate separately. They generally do not dismount for ground use.
PKS: Lightweight tripod-mounted infantry weapon
PKMS: Lightweight tripod-mounted variant of the PKS
PKB (PKBM): Pintle-mounted on APCs, SP guns, BRDM, BTRs, has butterfly trigger rather than solenoid, double space grips, and front and rear sights

Pecheneg/PKP/6P41: Modernized PKM with longer service life and lower recoil. Improved accuracy to 1,500 m reduces firing error 80% versus PKM. The barrel rear is steal-jacketed and ribbed with muzzle break air vents, for full-length barrel cooling and longer bursts (to 600 rounds) with no barrel change needed. The carry handle with built in rear sight (and telescopic sight mount) eliminates blurred sight image due to heat shimmer. The bipod is fitted to the barrel for better balance.

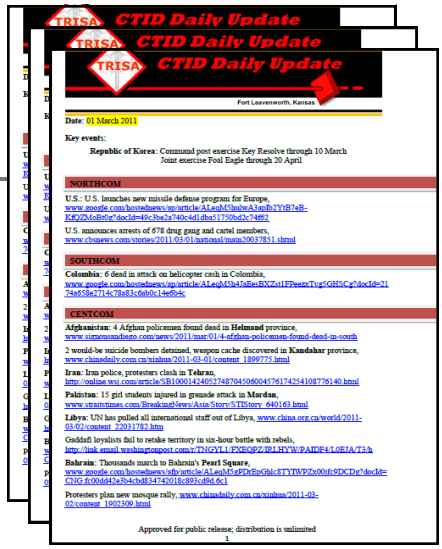
AMMUNITION

Name: 57-N-323S
Caliber and Length: 7.62x54-mm rimmed
Type: Ball
- Max Range (PKM/PKT) (m): 3,800/4,000
- Practical Range (PKM/PKT) (m):
  - Day: 1,000/2,000
  - Night: 300/INA
- Armor Penetration @ 0° obliquity
  - @ 500 range (mm): 8
  - steel plate @ 520 m (mm): 6
  - Flak vest: 110 m
- Muzzle Velocity (PKM/PKT) (m/s): 825/855

Name: 7BZ-3
Caliber and Length: 7.62x54-mm rimmed
Type: Armor piercing incendiary
- Max Range (PKM/PKT) (m): 3,800/4,000
- Practical Range (PKM/PKT) (m):
  - Day: 1,000/2,000
  - Night: 300/INA
- Armor Penetration
  - @ 200 range (mm): 10
- Muzzle Velocity (PKM/PKT) (m/s): 808

NOTES
The 7.62-mm general-purpose machinegun (PKM) is a gas-operated, belt-fed, sustained-fire weapon. The basic PKM is bipod-mounted but can also fit in vehicle firing ports. It is constructed partly of stamped metal and partly of forged steel. Compared to the US M-60, the PK-series machineguns are easier to handle during firing, easier to care for, and lighter. The 7.62x54R is a more powerful cartridge than the US with a slightly shorter effective range.

MONTHLY WRAP-UP OF CTID DAILY UPDATES



CTID analysts produce a daily *CTID Daily Update* to help our readers focus on key current events and developments across the Army training community. Available on AKO, each *Daily Update* is organized topically across the Combatant Commands (COCOMs). This list highlights key updates during May 2012. The *Daily Update* is a research tool, and an article's inclusion in the *Update* does not reflect an official U.S. Government position on the topic. Also, CTID does not assume responsibility for the accuracy of each article.

There were no *CTID Daily Updates* 2-8 May.

01May—**Syria**: Both sides violating Syria cease-fire, (includes video)
01May— **Malaysia**: Malaysia orders 32 armored vehicles from Indonesia
01May—**Turkey**: 3 PKK members killed in **Doğubayazıt, Ağrı**
01May—**UK**: Seven arrested in Britain on suspicion of financing terrorism
09May—**Cyber Security**: Spear-phishing attacks hit **U.S.** gas pipeline networks
09May—**Sudan**: Rebels seize **Girayda, Darfur**
10May—**Mexico**: Mexico's deadliest female assassin captured
10May—**Pakistan**: Pakistan test fires Hatf III Ghaznavi missile
10May—**Chine**: China launched a new Yaogan-14 spy satellite
11May—**Al-Qaeda**: Qaeda chief urges **Somali** fighters to defy peace bid
11May—**Russia**: Russia threatens to destroy U.S. missile shield in Europe
14May—**Afghanistan**: Spy balloons become part of the Afghanistan landscape
14May—**Uganda**: Uganda captures high-ranking Lord's Resistance Army member
15May—**Space Operations**: Pentagon wants to use disposable satellite clusters for intelligence
15May—**Iran**: More than 60 nuclear experts at work building Iranian nuclear bomb
15May—**Italy**: New generation AW169 helicopter completes its maiden flight
16May—**Taiwan**: Taiwan to build prototype missile frigate
16May—**South Sudan**: South Sudan to receive anti-aircraft missiles within months
16May—**Venezuala**: Venezuela border clash points to Colombia spillover violence
17May—**U.S.**: Pentagon to assign Army brigade to Africa to do training, military exercises
17May—**Cambodia**: Dengue fever kills 14 children in 4 months, 2277 cases so far
18May—**Al-Qaeda**: AQ chief urges **Saudis** to rise up against rulers
18May—**Bahrain**: Thousands of Bahrainis demonstrate against Saudi union
21May—**Falkland Islands**: British nuclear submarine sent to Falklands in show of strength as tensions rise ahead of 30th anniversary of conflict
21May—**Syria**: Syria forces kill 9 deserters as NATO nixes intervention
22May—**Japan**: Japan buttresses missile defense to counter North Korea
22May—**Germany**: German extradited from Turkey on 'terror' charges

Disclaimer: CTID does not assume responsibility for the accuracy of each article shown on this page. Also, the views and opinions expressed in Red Diamond articles are those of the authors and do not necessarily reflect the official policy or position of any Department of Defense or government entity.

YOUR Easy e-Access Resource

Director, CTID DSN: 552
Mr Jon Cleaves FAX: 2397
jon.s.cleaves.civ@mail.mil 913.684.7975

OE & OPFOR Doctrine & Training Lit.
Senior Analyst CTID: Dr Don Madill 684.7926
donald.l.madill.civ@mail.mil

OPFOR Doctrine Team
SME: Mr Rick McCall 684.7960
richard.g.mccall.civ@mail.mil

Intelligence Specialist
SME: Mr Kris Lechowicz 684.7922
kristin.d.lechowicz.civ@mail.mil

Intelligence Specialist
SME: Mr Jerry England 684.7934
jerry.j.england.civ@mail.mil

Worldwide Equipment Guide (WEG)
SME: Mr Tom Redman BAE 684.7925
thomas.w.redman.ctr@mail.mil

Threats Terrorism Team (T3) Integration
SME: Mr Jon Moilanen L3-MPRI 684.7928
jon.h.moilanen.ctr@mail.mil

Operational Environment Analysis
SME: Ms Penny Mellies 684.7920
penny.l.mellies.civ@mail.mil
SME: Angela Wilkins L3-MPRI 684.7929
angela.m.wilkins7.ctr@mail.mil

Training-Education-Leader Development
SME: Mr Walt Williams 684.7923
walter.l.williams112.civ@mail.mil

National Training Center - OPFOR
SME: LTC Terry Howard USAR 684.7939
terry.d.howard.mil@mail.mil

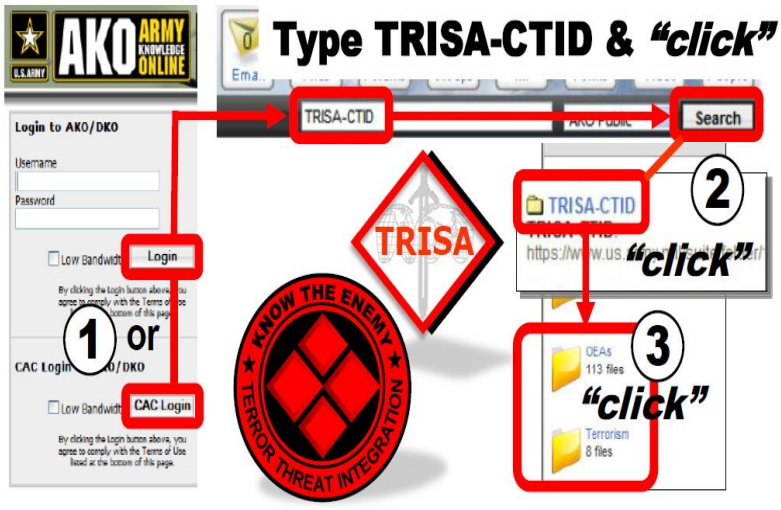
Joint Readiness Training Ctr - OPFOR
SME: Mr Marc Williams BAE 684.7943
james.m.williams257.ctr@mail.mil

Joint Maneuver Readiness Ctr - OPFOR
SME: Mr Mike Spight BAE 684.7974
michael.g.spight.ctr@mail.mil

Mission Command Training Program - OPFOR
SME: Mr Pat Madden S3 Inc 684.7997
patrick.m.madden16.ctr@mail.mil

Threats Website-Support Operations
SME: Mr Charles Christianson 684.7984
charles.e.christianson.civ@mail.mil

AKO *Three "Click"* Drill-Down



Find Your Topic – Do Your Research

What We Do for YOU

- ***Determine OE Conditions***
- ***Publish Operational Environment Assessments (OEAs)***
- ***Publish OE Threats in FSO***
- ***Publish Army OPFOR Doctrine***
- ***Assess Threat-Enemy & TTP***
- ***Support Terrorism Awareness***
- ***Produce the Decisive Action Training Environment (DATE—previously Full Spectrum Training Environment)***

All CTID products can be found on AKO. Check out all of our products at:
www.us.army.mil/suite/files/11318389