Operational Environment Enterprise
US TRADOC G2 Intelligence Support Activity

Red Diamond

Complex Operational Environment
and Threat Integration Directorate

Fort Leavenworth, KS | Volume 5, Issue 9 | SEP 2014

INSIDE THIS ISSUE

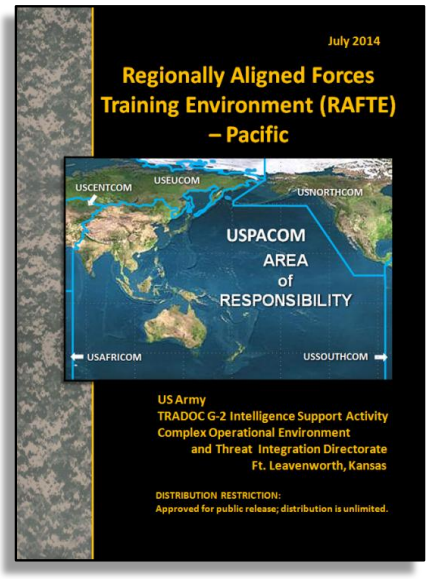
OEE *Red Diamond* published monthly by TRISA at CTID

Send suggestions to CTID
ATTN: *Red Diamond*
Dr. Jon H. Moilanen
CTID Operations
BMA Contractor
and
Angela Wilkins
Chief Editor
BMA Contractor

New Release: RAFTE-Pacific: Training for Readiness

by **Angela Wilkins**, TRISA CTID, Product Integration (BMA Ctr)

The Complex Operational Environment and Threat Integration Directorate (CTID) of the TRADOC G2 Intelligence Support Activity announces the availability of the 2014 Regionally Aligned Forces Training Environment (RAFTE) for the Pacific operational environment (OE). This product can be found on CTID's page on ATN.



A RAFTE provides a focused training environment for RAF readiness, and is designed to be used as a supplement to the Army's Decisive Action Training Environment (DATE) for training in a regional OE without a known specific OE. DATE is the base and the RAFTE provides regional flavor on the same terrain. In other words, this RAFTE must be used in conjunction with DATE for training in US Pacific Command; it cannot be used as a stand-alone training environment. For application to training, this construct enables re-use of exercise area signage, OPFOR uniforms, and other costly items versus retooling for each RAF training event. (*Continued* at p. 5)

The United States Pacific Command (USPACOM) Area of Responsibility (AOR) encompasses about half the earth's surface, stretching from the waters off the west coast of the US to the western border of India, and from Antarctica to the North Pole. There are few regions as culturally, socially, economically, and geo-politically diverse as the Asia-Pacific. The 36 nations that comprising the Asia-Pacific region are home to more than 50% of the world's population, 3,000 different languages, several of the world's largest militaries, and five nations allied with the US through mutual defense treaties.

US Pacific Command

RED DIAMOND TOPICS OF INTEREST

by **Jon H. Moilanen**, CTID Operations and Chief, *Red Diamond* Newsletter (BMA Ctr)

The cover article focuses on the recently published RAFTE-Pacific, and includes examples of how conditions can create and amplify considerations and uncertainties in an OE for training value. Another article reviews incidents in the ongoing conflict between Ukraine and the Russian Federation. A vignette recounts the Russian seizure of a Ukrainian command ship at Sevastopol.

The terrorism of kidnapping is a recurring incident in complex OEs. Threat motivations and actions use an incident vignette that can be adapted for antiterrorism and counterterrorism training.

Chemical weapons remain a significant threat from some state and/or non-state actors that are willing and able to use such weaponry. 4th generation chemicals are particular threats that can be masked in legitimate enterprise production until combined as a weapon.

The RPG-30 is a tandem precursor and main rocket propelled grenade system developed to defeat active protection systems on armored vehicles. Technicals are a simpler improvisation on commercial vehicles adapted as weapons carriers. These examples are two of the weapon system options available in the WEG.

The ISIL attack on Tabqa Airbase describes a succession of attacks using threat assault, fixing, breaching, and exploiting elements against regular Syrian forces. When ISIL elements seized the airbase, they executed prisoners and exploited ISIL atrocities in global social media.

Email your topic recommendations to:

Dr. Jon H. Moilanen, CTID Operations, BMA CTR
jon.h.moilanen.ctr@mail.mil
and
Angela M. Wilkins, Chief Editor, BMA CTR
angela.m.wilkins7.ctr@mail.mil

Director's Corner:
Thoughts for Training Readiness

by Jon Cleaves, Director, Complex Operational Environment and Threat Integration Directorate (TRISA-CTID)

Here at CTID, we work on a daily basis with organizations across DoD, the Intelligence Community, and our multinational partners. A good portion of this work is focused on helping our Combat Training Centers, Centers of Excellence, and unit home stations establish the very best threat environment for training. It is our principal charter to gather information and intelligence in real time on worldwide threats and provide that information and intelligence to our customer base in forms that allow rapid integration into training development and exercise design. We also provide an oversight function on behalf of the G2 and TRADOC Commander to ensure a consistent and relevant threat replication across all training venues.

In this age of unprecedented access to information, and with Soldiers always seeking to be as proactive as possible with respect to their craft, some may seek to go VFR direct to an external agency to get what might be perceived to be the very latest information and get that into training in the shortest time possible. On the surface, that seems awesome. And neither I nor anyone in my directorate would ever seek to stifle initiative. I would suggest, however, that it might be better to just simply come to us.

First, there is the issue, likely one you have encountered if you have participated in military service, that the "first report is often wrong." My analysts are trained to thoroughly source the threat information we provide to you. This means a deeper look than simply grabbing a headline. What might look like great threat information at first glance might be improperly reported (and be so for some significant amount of time) or even be part of someone's information warfare campaign and designed to misdirect or mislead.

Second, not all threat challenges are equal, and we do not have an unlimited budget with which to train. Threat action in a training event has a specific purpose—to challenge the execution of mission essential tasks. Not all threat actors are actually good enough to challenge all of our tasks in execution. Nor can we afford to execute every type and style and mode of threat action in every event. A threat action that challenges multiple ME tasks at once is more cost effective than several "hotter" but less challenging ones.

Third, we are training an Army to adapt to an uncertain future. We focus a great deal of effort on projecting likely threat actions from now out about 15 years. Threat actions from today's headlines are actually the "last war," even if we put them into training as soon as tomorrow. Analytical effort has to be applied to ensure the action is an enduring challenge that will get to the right kind of training objectives for units deploying in the future as well as causing the right kind of responses to build agile and adaptive leaders, Soldiers, and units.

Finally, we already come to the table with the right sort of connections across the IC and with our multinational partners also using the same training philosophy and products. Many disparate threat replication efforts will desynch our leadership's vision for Army training.

Bottom line—alert us to what is important to you, and let us do the homework.

JON

New Release: RAFTE-Pacific: Training for Readiness (Cont. from p.1)

RAFTE-Pacific identifies complex-dynamic CONDITIONS of the Pacific OE to enable training fidelity in a robust, realistic, relevant OE for selected Pacific areas. A RAFTE is organized into two sections.

The first section identifies conditions present in the identified OE—the Pacific in this case—that are not already present in the DATE. Section two identifies conditions that *are* in DATE that do not apply to the Pacific OE, and should not be factored into training scenarios. See figure 1 as an example of material in section 1—an Event that can be used for training.

Event	**Diplomacy with the West Driven by Threat of Nuclear Weapons**	
1. Related Activity	➢ **Capital investments diverted from social programs and infrastructure to military spending.**	
➢ **Possible Variable Conditions**	○ **Economic** ○ **Political** ○ **Information** ○ **Military**	➢ Shortages in basic needs such as food and fuel. ➢ Political unrest in areas hit most by food insecurity. ➢ Government focuses media messages on military prowess to divert attention from economy. ➢ Military is well-funded, well-fed, and loyal.
2. Related Activity	➢ **Due to widespread hunger and economic decline, large numbers of IDPs push across the borders into neighboring countries.**	
➢ **Possible Variable Conditions**	○ **Military** ○ **Information** ○ **Social**	➢ Military forces posted at borders to arrest IDPs and prevent further migration. ➢ Government media minimizes the number of IDPs and the size of the crisis, and paints the IDPs as disloyal. ➢ IDPs put into poorly-managed and -funded refugee camps where diseases begin to break out.
3. Related Activity	➢ **Nuclear weapon accidently explodes.**	
➢ **Possible Variable Conditions**	○ **Information** ○ **Social** ○ **Political**	➢ Government denies accident. ➢ Local residents relocated to poorly-run and -managed refugee camp. ➢ International pressure mounts for more transparency about the accident.
Possible Related METL Tasks	**Conduct Command and Control** (ART 5.0) ➢ Execute the Operations Process (ART 5.1) ➢ Integrate Information Engagement Capabilities (ART 5.3.1)	
	Conduct Information Protection (ART 6.3) ➢ Perform Information Assurance (ART 6.3.1) ➢ Perform Computer Network Defense (ART 6.3.2)	
	Conduct Critical Installations and Facilities Security (ART 6.5.2) ➢ Conduct Critical Installations and Facilities Security (ART 6.5.2)	
	Conduct Civil Affairs Operations (ART 5.4.6) ➢ Support Civil Administration (SCA) (ART 5.4.6)	

Figure 1. Excerpt from RAFTE-Pacific section 1

Significant conditions identified in the RAFTE-Pacific include "Young, inexperienced dictator with no announced succession plan" (political) as seen in North Korea, "no national or regional elections" (political) as seen in Brunei and Somoa, and a large number of government sponsored paramilitary groups (military) as seen in India. Again, these are conditions one would encounter in certain Pacific OEs that are not included in the basic DATE framework. See figure 2

for an example of a unique regional condition, how it can impact on a region, and how the condition can be represented for training in the DATE. The condition relates to the Event shown in Figure 1.

Unique Regional Condition: *Diplomacy with the West Driven by Threat of Nuclear Weapons*

Definition of Condition: For a small country, a nuclear weapons capability is a source of relevance and leverage for gaining a place at the negotiating table with larger countries. Developing a nuclear capability, however, means subordinating other national needs to military spending and expansion.

Regional Manifestation of Condition: North Korea's historical focus on the unsettled Korean War and international politics has driven a program of nuclear weapons development. Nuclear weapons development has come at a cost and sacrifice of other social and economic priorities that have left North Korea unable to take care of its basic food and fuel needs. North Korea continues to use its nuclear weapons program as a diplomatic bargaining chip and a means of finding a place of relevance in regional and international politics and diplomacy.

Application of Condition to DATE: With a historical distrust of the West and a desire to find regional legitimacy, Ariana has continued to develop nuclear weapons. Professing a need to protect itself, in recent years Ariana's nuclear efforts have increased at the expense of social programs and needed infrastructure maintenance. International and regional tensions have mounted, and demands for more transparency in its nuclear program have led to heated multilateral negotiations. Issues of most concern are the deteriorating economic conditions in Ariana and the safety of Arianian nuclear facilities.

Figure 2. Unique regional condition

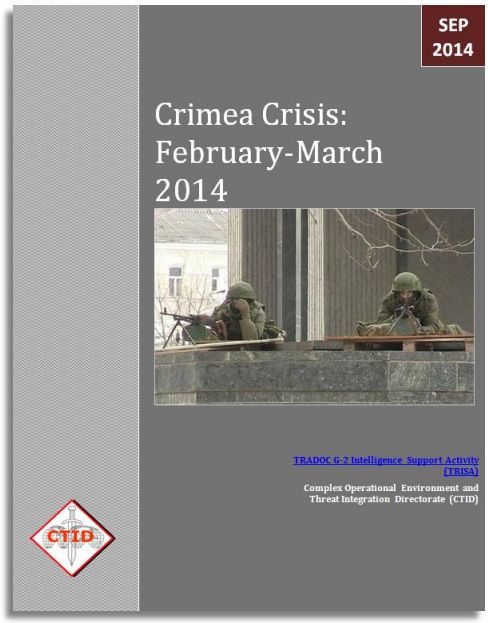
RAFTEs in general allow for the DATE framework to spotlight regionally different cultures, political dynamics, and military capabilities. Using a RAFTE is an efficient way to identify conditions for training during DATE-based exercised for CTCs and at home station. RAFTE products also exist for the North Korea and Africa OEs.

by **H. David Pendleton**, TRISA-CTID, Research and Analysis Team (CGI Ctr)

In less than a month's time starting in late February 2014, Russian and local militia elements took control of Crimea, defeated the approximately 25,000 Ukrainian military personnel stationed there, orchestrated the independence of the peninsula from Ukraine, and facilitated Crimea's eventual merger with the Russian federation. The lightning speed of the takeover caught the local Ukrainian military off guard. Seizure of strategic targets by pro-Russian paramilitary Crimean self-defense units augmented by highly-skilled and heavily-armed uniformed personnel of undeclared origin allowed the operation to run smoothly. Russian President Vladimir Putin later acknowledged these unidentified professional military augmentees to be Russian soldiers. Paralysis displayed by Ukrainian political leaders in Kiev resulted in only a token resistance by the country's military and contributed significantly to a successful Russian *fait accompli* in Crimea.

The Threat Report, *Crimea Crisis: February-March 2014*, (available soon on ATN) examines the events during the four-week run-up to the Russian seizure of Ukraine from strategic, operational, and tactical perspectives and provides historical context in analyzing the crisis.

Strategic Situation



At the strategic level, there are three major issues in play between Russia and Ukraine. First, historical friction between the two countries dates back many centuries. The area that now comprises Ukraine has been fought over by more powerful neighbors for at least 500 years. In the 14th century, Poland and Lithuania annexed most of what is now present-day Ukraine. In the 17th century, Russia and Poland divided most of Ukraine's territory lands between themselves. When Poland was subsequently partitioned, Russia appropriated almost all of Ukraine into its own empire. After a short-lived period of independence following the end of World War I, the Soviet Union seized the eastern two-thirds of Ukraine, converting the country to a Soviet Socialist State (SSR). After Nazi Germany's defeat in World War II, the Union of Soviet Socialist Republics (USSR) re-appropriated not only the former Ukraine SSR, but also territory comprising what is today the western third of Ukraine. When both Russia and Ukraine belonged to the USSR, the leaders in Moscow and Kiev usually found common ground. When the Soviet Union collapsed in the early 1990s, the relationship between the two former Soviet states became more strained as Ukraine found itself embroiled in a renewed competition for influence between Western Europe and Russia.

A second historical dimension of the present-day crisis is a longstanding language barrier that plagues Crimea's unique relationship with Russia. In order to foster a more cohesive bond between the heterogeneous peoples of the Soviet Union after World War II, the Soviet government decided that the Russian language should become the dominant vernacular throughout the USSR. For Ukrainians, this meant the suppression of the role played by their native tongue in sustaining the country's unique culture and traditions. In the eastern part of Ukraine, the predominance of the Russian language and culture resonated more among the local population than was the case throughout the western portion of the country.

In the two easternmost Ukrainian provinces, Donetsk and Luhansk, Russian is the primary instructional language in a majority of the schools. In Crimea, a part of Russia from the founding of Sevastopol in 1783 until 1954, only 8% of the students currently receive formal schooling imparted in the Ukrainian language. In the remainder of the country, Ukrainian is the primary language of education. Native Crimeans, reflecting the influence of a large indigenous ethnic Russian population as well as a sizeable Russian/Soviet military retiree population, tend to regard their province as part of Russia and not Ukraine. This attitude prevails despite 60 years of Ukrainian rule.

The final strategic problem affecting the current crisis is Ukraine's dependence on Russia for its hydrocarbon resources, especially natural gas. Ukraine produces no natural gas of its own, and imports 100% of its energy from Russia through the latter's gas company, GazProm. Since Ukraine became a nation-state in its own right in 1991, Russia has wielded the price of natural gas as both a carrot and a stick to keep its neighboring country in line politically. When Ukraine complies with Russian guidance or supports the Russian geopolitical party line, GazProm reduces the price of natural gas. Conversely, when Ukraine's leaders take exception to Russian policies or demonstrate support of policies tending to remove them from the Russian sphere of influence, GazProm raises the price of natural gas. Since Russian leaders believed that Ukraine supported Georgia in the 2008 Russo-Georgian Conflict, GazProm stopped all natural gas shipments to Ukraine before eventually striking an agreement that charged Ukraine a higher price. After a former pro-Russian Donetsk provincial governor, Viktor Yanukovych, won the Ukrainian presidency in February 2010, GazProm gave Ukraine a 30% discount in return for allowing Russia to station its Black Sea Naval Fleet in Crimea until at least 2042. In November 2013 Ukrainian leaders refused to sign a trade agreement with the European Union (EU). The following

month, GazProm cut its price of natural gas to Ukraine by an additional one-third. Yet almost immediately after the Ukrainian government impeached Yanukovych in February 2014, GazProm raised the price of natural gas sold to Ukraine by 80% through early April 2014, until GazProm finally halted all gas shipments to the country in June 2014.

Operational Level

At the start of the present crisis in late February 2014, Russia had about 16,000 military personnel stationed in Crimea, in comparison with Ukraine's 25,000-strong military establishment. Most of the personnel on both sides stationed in Crimea before mid-February 2014 were naval, with a few exceptions. Due to the treaty that allowed the Russian Black Sea Fleet to remain in Crimea, the Russians could station up to 25,000 military personnel in the province; these also enjoyed a freedom of movement that afforded them easy deployment from and redeployment to their home country.

Russia used the 25,000 strength level ceiling to bring in approximately 10,000 specialized military personnel, including airborne troops and special forces personnel just days prior to the military takeover that began on 27 February 2014. The Russians then invoked the treaty's freedom of movement clause to move their ground troops near strategic targets at the onset of the military maneuvers.

The Russians chose their targets thoughtfully, based on their experiences over the last 30 years, especially drawing from information gathered during their 2008 campaign in Georgia. Russians, in unmarked uniforms along with local defense groups that provided a front to create the impression of internal Crimean as opposed to external Russian involvement, captured 189 Ukrainian military facilities within a four-week period. Ukrainian military personnel either escaped to their country's mainland or defected; this was especially true for naval personnel. See figure 1 for selected targets.

Figure 1. Selected targets of Russian forces (Numbers correspond to actions as listed on next page)

The numbers on the map above correspond to the following targets in the order listed. This is not a complete list. Details of each action are in the Threat Report:

(1) 27 February 2014: Crimean parliament building and cabinet of minister's building.

(2) 27-28 February 2014: Simferopol civilian airport.

(3) 27-28 February 2014: Sevastopol military airport.

(4) 28 February 2014: Krym State Television Company and Urktelecom facilities throughout Crimea.

(5) 6 March 2014: Naval blockade of Donuzlav Lake.

(6) 6 March 2014: Remaining Ukrainian media stations.

(7) 8 March 2014: Warning shots fired at the Organization for Security and Cooperation in Europe (OSCE) observation teams.

(8) 10 March 2014: Targets of opportunity such as the Simferopol military hospital.

(9) 13 March 2014: Pro-Ukrainian and anti-Russian websites by blocking.

(10) 15 March 2014: Natural gas pipeline station to the Crimean peninsula.

(11) 18 March 2014: More difficult targets using overwhelming force.

(12) 19 March 2014: Capture and subsequent release of the Ukrainian Navy Commander.

(13) 21 March 2014: Ukrainian 174th Air Defense Regiment base with S-300 surface-to-air missiles.

(14) 21 March 2014: Prevention of Ukrainian ships that attempted to run the naval blockade.

(15) 22 March 2014: Belbek Airbase territory not already in Russian possession.

(16) 24 March 2014: Ukrainian 1st Marine Battalion.

The Russians used no tanks during this time, and the most advanced armored personnel carriers (APCs) used in these operations were BTR-80s. (See *The BTR Handbook-The Universal APC* for details on this APC's capabilities). The Russians and the Crimean militia used a combination of naval blockades, barricades to prevent soldiers leaving their bases, psychological warfare, intimidation, and bribery to convince most Ukrainian units to surrender without offering resistance. In units whose commanders initially refused to surrender, a few well-placed shots and a couple of resulting casualties typically sufficed to quickly change the resistors' minds. On 17 April 2014, Russian President Vladimir Putin finally revealed the worst-kept secret of the entire operation: Russian troops had been present in Crimea during the February/March 2014 military action. The Ukrainian government in Kyiv, however, refused to respond to the crisis even when the Ukrainian military held the upper hand in terms of personnel and heavy weapons. By the time the Ukrainian government decided to have their forces in Crimea resist, it was too late as Russia then held the advantage in both quantity and quality of the ground forces on the peninsula.

Tactical

One of the best examples of a tactical action reported in open sources was the seizure of the Ukrainian command ship *Slavutych* (U-510) in the Sevastopol Harbor on 22 March 2014. On 3 March 2014, five Russian tugboats positioned themselves behind the *Slavutych* and a neighboring ship, the U-209 *Ternopil*, to prevent them from leaving the docks. The Russians and local militia quickly took control of the *Ternopil*, but the *Slavutych*'s commander backed his ship 10 meters away from the pier to prevent hostile forces boarding via the landward side. Over the next few weeks, the *Slvautych's* crew kept their ship from being boarded by the enemy, primarily by using water cannons.

Two small Russian warships eventually relieved the tugboats and positioned themselves about 50 meters seaward from the *Slavutych*. Over the next three weeks, naval and ground forces kept a 24-hour watch on the Ukrainian command ship. After the Russian Black Sea Fleet commander boarded the *Ternopil* to inspect the captured vessel, the Russians gave the *Slavutych* in Sevastopol Harbor and the rest of the Ukrainian navy bottled up at Donuzlav Lake until Friday, 21 March 2014, to either surrender or join the Russian Navy. Using various psychological techniques that included urging

mothers of the sailors on board the *Slavutych* to call their sons' cell phones, up to 40% of the crew eventually deserted the ship. On the day of the Russian boarding, fathers also called, urging sons to stay in their cabins, unlock their doors, and leave them open, since the attackers would probably break down the doors anyway. Many of those on board were native Crimeans and felt little allegiance to Ukraine. Some of the sailors were not technically members of the Ukrainian military, but working as civilian contractors. Several of the sailors simply jumped overboard to escape; their mothers came, fished them out of the water, and took them home. Many sailors chose to join the Russian Navy, fearing that Ukrainian sailors who offered no resistance would be treated as deserters once they returned to Ukrainian-controlled territory. This was due in part to rumors indicating that some sailors who abandoned other ships had been arrested and were facing trial and possible prison sentences ranging from five to seven years. Other sailors simply chose to join the Russian Navy because they were native Crimeans, ethnic Russians, or married to local Crimean women; for them loyalty to family, heritage, or ship trumped national allegiance to Ukraine. (See figure 2.)

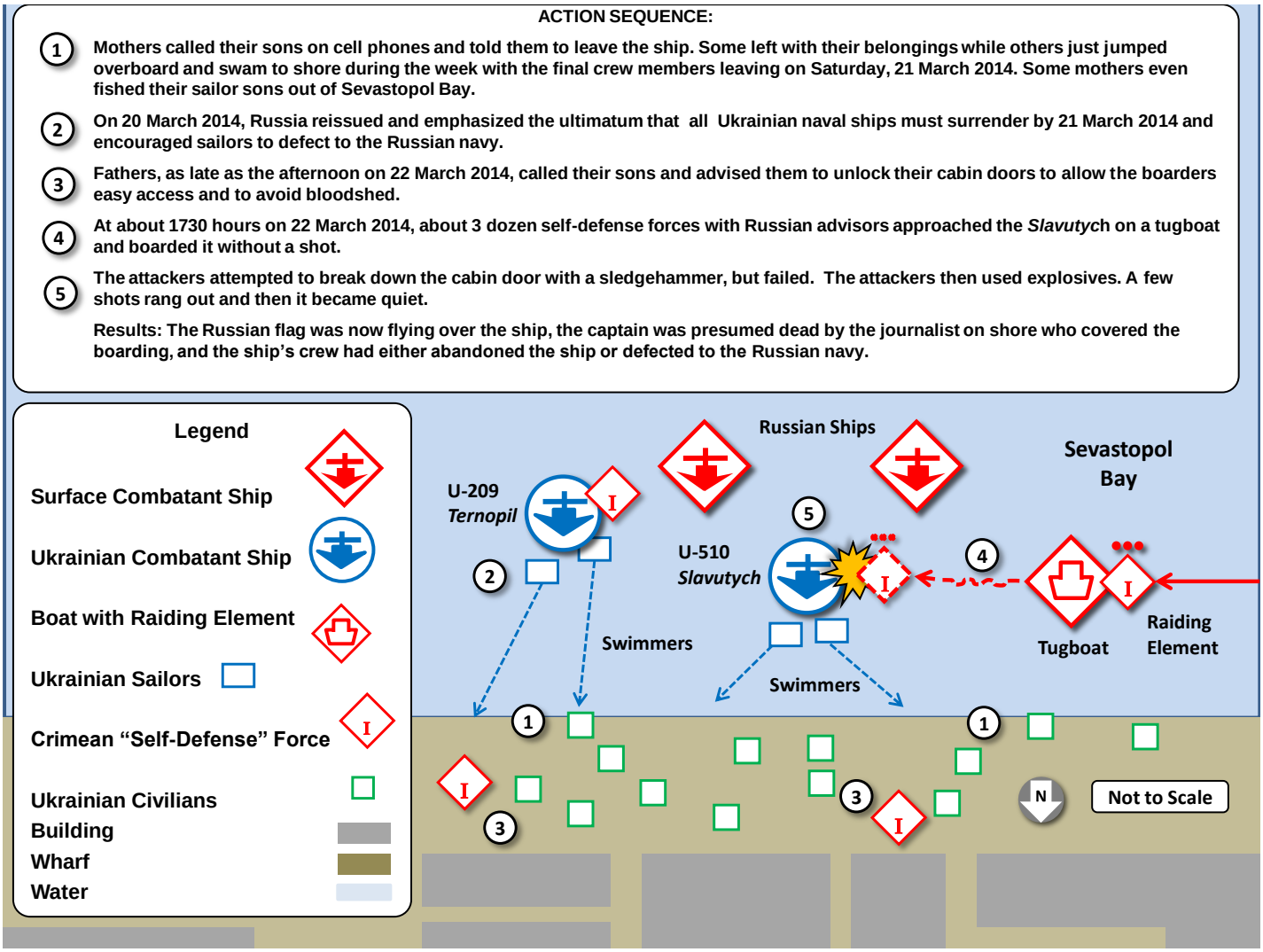


Figure 2. Storming of the Ukrainian command ship, U-510 *Slavutych*, on 22 March 2014

Despite all the psychological and family pressure, the *Slavutych's* captain and some of the crew refused to surrender their ship and remained loyal to the Ukrainian government in Kiev. Shortly thereafter it became apparent that the local defense forces would attack the *Slavutych* on the evening of Saturday, 22 March 2014. That afternoon, several of the ship's crew—some in uniform and some in civilian clothes—left the *Slavutych*, carrying their possessions in black plastic bags. At approximately 1730 hours local time, a tugboat with a few dozen men approached the Ukrainian ship while bystanders watched from the pier. While it appeared to some onlookers that the attackers were members of the self-defense forces, at least one witness alleged that the tugboat carried Russian special operations personnel. Sailors aboard the *Slavutych* used their loudspeaker system to warn the approaching vessel against illegally boarding the ship,

but to no avail. The Ukrainian ship then began to play the patriotic song *Varyag,* a heroic composition dating back to the Russo-Japanese War.

The attackers on the tugboat reached the *Slavutych* and then boarded it. By that time, almost everyone had surrendered except for the ship's captain, who had locked himself in his cabin. The attackers first tried to use a sledgehammer to break the door down. When that failed, they resorted to grenades. A few gunshots rang out after the sledgehammer echoes faded and the grenades exploded, but soon after the noise abated, the Ukrainian flag came down from the mast and the boarders raised a Russian flag in its place. The storming of the *Slavutych* was over in a matter of minutes.

The capture of the *Slavutych* is an excellent example of an attack to gain control of equipment, as described in Training Circular (TC) 7-100.2, Opposing Force Tactics. The only difference is that in this instance the attack occurred on water instead of land. While the Russians may call the units that participated in the attack by a variety of names, the attackers on the tugboat consisted of raiding, security, and support elements.

Summary

Since most of the Ukrainian military personnel stationed in Crimea were sailors as opposed to ground combat troops, there were few Ukrainian ground forces available to meet the military challenge posed by Russia and the local pro-Russian self-defense units. Although most of the Russian military personnel originally stationed in Crimea were sailors, sufficient ground forces entered Crimea by air and sea to convince most Ukrainian military personnel to surrender without a fight.

Once the pro-Russian forces seized selected strategic targets, the combination of Russian military and local self-defense forces systematically took control of the remaining military installations in Crimea. The Russians deployed soldiers in uniforms that bore no identifiable markings in an attempt to afford themselves plausible deniability, but almost immediately observers external to Crimea discerned the true nationality of the well-trained and well-armed invaders.

To lend an indigenous flavor to operations, the Russians assigned their advisors to local militia units and allowed the self-defense forces to seize many of the softer targets. For the more difficult or important objectives, the disguised Russian forces either took the objectives themselves or heavily augmented the local self-defense units. Ultimately, the failure of the Ukrainian government in Kiev to react decisively with military action to the events in Crimea lost them their province as much as the Russian-led forces won. With the ongoing conflict in eastern Ukraine, it is highly unlikely that Ukraine will regain possession of Crimea in the foreseeable future.

PREVENT AND PROTECT: *BE PROACTIVE—KNOW YOUR SURROUNDINGS*

by TRISA-CTID, Operations, Threats Terrorism Team

Situational Awareness—Situational Understanding

Kidnapping: Tactic-Technique and Terrorism in Complex OEs

by **Jon H. Moilanen**, TRISA-CTID Operations (BMA Ctr)

Operational environments (OEs), now and for the foreseeable future, will include criminal activity and terrorism that includes kidnapping with diverse motivations and rationales. Threat actors can include a host of state and non-state entities, military and law enforcement members, mercenaries, criminals, ideological extremists, renegade soldiers or security elements, and/or rogue citizens in a relevant population. This condition is not new. Assessments spanning recent decades note how these adversaries and/or enemies can apply tactics, techniques, and terrorism.[1]

Threat Actions in Complex Operational Environments

The US Army soldier will confront irregular warfare with tactics that will include terrorism, ambushes, kidnapping, and other criminal actions. The environment of armed conflict will change with more activity in urban areas. Adversaries and enemies will expand organizational connectivity in regional, international, and transnational affiliations. Access to modern technologies and weaponry and access to information, intelligence, and propaganda capabilities will complicate an already challenging and difficult mission set of offensive, defensive, or stability operations.

DIA, *Threat Assessment: Looking to 2016* (1997)

Kidnapping is a reality of contemporary times and will continue to be an ongoing threat in OEs for the foreseeable future. The 1997 Defense Intelligence Agency (DIA) assessment of threats, locales, levels of violence, propaganda, and effects of globalization are evident in current daily living as the Army operates in the second decade of the 21st century. Some regions of the world experience surges of kidnapping within what is already a normal criminal activity or terrorism tactic.

Other incidents are random acts of violence. Reasons for kidnapping vary. However, a consistent symptom from kidnapping is the psychological stress that the event causes to victims, their families, and friends. This uncertainty can ripple in negative effects across political, social, and economic aspects of a small community, a regional society, and/or a nation among nation-states.

Tactics, Techniques, and Terror

Tactics is often described as "the employment and ordered arrangement of forces in relation to each other."[2] Techniques complement tactics as "non-prescriptive ways or methods used to perform missions, functions, or tasks."[3] In the context of threat regular and irregular forces, tactics and techniques can focus on how threat actors approach the conduct of actions such as kidnapping.

Kidnapping is an abduction. The seizure affects not only the individual or individuals who are abducted, but generates anxiety in a larger group of people as location and welfare of the abducted target is unknown, as demands and actual intentions of abductors are frequently in doubt, and as the prospect of rescue or release is hazardous at best.

Tactic and Technique

Tactics. The ordered arrangement and maneuver of individuals or cells related to their enemy, each other, and terrain in order to achieve mission success.

Techniques. The general or detailed methods of using equipment and people to perform assigned missions and functions.

TRADOC G2 Handbook 1.07 C1, *Soldiers Primer on Terrorism TTP* (2012)

Theater is a metaphor sometimes used to describe the effects of terrorism. Kidnapping can be imagined as an unfolding drama. The final act can conclude in successful release of a victim or quickly degenerate into a tragedy ending in disaster.

Describing the Actions

Kidnapping is a difficult term to define precisely because many common and legal variations exist depending on the type of governance establishing laws and the conditions to describe kidnapping that may be specified, or purposely remain general in scope. A common dictionary defines *kidnapping* as an action "to seize and detain or carry away by unlawful force or fraud and often with a demand for ransom."[4] A legal dictionary includes phrases on kidnapping such as "forcible abduction" and "false imprisonment."[5] International organizations acknowledge the implications of kidnapping and the intention to prevent ransom payments or political concessions that favor terrorists."[6]

Kidnapping

Kidnapping is an act that unlawfully seizes, confines, moves, decoys, abducts, or carries away and holds for ransom or reward a person.

US Code, Title 18

Two common aspects in a criminal act of kidnapping are: (1) The movement or detention must be unlawful. Under various US state and federal statutes, not all seizures and movements constitute kidnapping. For example, civilian law enforcement officers may arrest and detain a person they suspect of a crime. Parents are allowed to reasonably restrict and control the movement of their children. (2) Some aggravating circumstance must accompany the restraint or movement of the victim. Examples include a demand for money or something of value, an attempt to affect a function of government, an attempt to inflict injury on the abducted person or persons, or an attempt to terrorize a third party.[7] Using the US Code (Title 18) to define *kidnapping* and its conditions, kidnapping is an act that unlawfully seizes, confines, moves, decoys, abducts, or carries away and holds for ransom or reward a person.[8] Some legal exceptions exist to an act qualifying as kidnapping as listed in the US Code.

Terrorism links to kidnapping in US Code (Title 18) under the general term of *terrorism* and also with the term of *international terrorism*.[9] Aspects of the US Code describe terrorism as an activity that involves a violent act or an act dangerous to human life that is a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or of any State and appears to be intended—(1) to intimidate or coerce a civilian population, (2) to influence the policy of a government by intimidation or coercion, or (3) to affect the conduct of a government by assassination or kidnapping.

Terrorism is defined differently within the US Federal government based on departmental purpose. One example of variance is the US Department of State and Department of Defense definitions of terrorism.

As a tactic or technique of employing terrorism, kidnapping can range the actions of a lone individual, a small group, or the operations of a highly organized transnational network. The context of this article addresses complex OEs for a wide range of threat actors committed to using kidnapping in order to achieve a desired outcome. Appreciating situational awareness and understanding to preclude or counter kidnapping often begins by narrowing attention to conditions that exist within a particular OE.

Terrorism Definitions

The premeditated, politically motivated violence perpetrated against non-combatant targets by subnational groups or clandestine agents.

US Department of State
Country Reports on Terrorism 2013 (2014)

The unlawful use of violence or threat of violence to instill fear and coerce governments or societies. Terrorism is often motivated by religious, political, or other ideological beliefs and committed in the pursuit of goals that are usually political.

US Department of Defense
DOD Dictionary of Military and Associated Terms JP 1-02 (2014)

Today's reality is a world of global interconnectivity and stage for near instantaneous information, intelligence, and/or propaganda. Kidnapping can prompt a sensational headline, extort political negotiations, compel military action or restraint of action, and/or divert scarce resources and capabilities from other important missions in a military area of operations. One kidnapping incident, minute in scope and singular in purpose, can amplify uncertain and complex conditions and quickly expand into an international incident and/or spotlight a particular agenda for transnational action.

Motivations for Kidnapping

Rationales for kidnapping typically include the use of coercion in order to obtain a concession. Intended outcomes may be as simple as a ransom or revenge; or attention to an organizational, political, social, or economic grievance. Other specific rationales include abduction of an individual or individuals to be bartered in human trafficking. A similar rationale of abduction can be children for use as child soldiers.

Kidnapping Motivations

- Coercion
- Ransom
- Revenge
- Social Grievance
- Political Grievance
- Economic Grievance
- Child Soldiers
- Human Trafficking
- Incite Retaliation
- Terrorism

Types of kidnapping can be focused as actions against an individual or group of individuals. Kidnapping can be an action to spotlight grievances about political positions or decisions, economic responsibilities, community or agenda leadership, or to achieve other visible notoriety in a regional, international, or global community.

A technique such as *tiger kidnapping* abducts an individual in order to coerce specific actions of another person or group.[10] Examples include coerced support to pay ransom or provide confidential information to assist other criminal activity. Other actions can be one individual coerced to participate physically in an illegal act based on the abduction of another person.

A more direct action is *express kidnapping* as an individual abduction in order to force withdrawal of personal or commercial funds from a local automated teller machine (ATM) as ransom.[11] This technique is used increasingly in large urban areas with easy access to ATMs. Variations of this technique include keeping the individual overnight with the intention of obtaining additional funds beyond a one-day withdrawal limit, and/or ransom demands communicated to family or business entities.

In another technique, the victim of *virtual kidnapping* is unaware of being a victim until after the criminal act is completed. The kidnapping is actually a scam.[12] The kidnapper knows when the victim will be not be able to be contacted, and initiates a demand for ransom to family or business associates during this period. Timing of the demand for immediate payment is fundamental to the success of this technique.

Kidnapping Techniques

- Individual
- Group
- Virtual
- Express
- "Tiger"

Kidnapping, in any of its forms, is a technique that causes anxiety and reaction in a larger relevant population. Effects can quickly expand from an isolated incident involving one person to an international and transnational crisis on political, social, and economic aspects of a nation-state and region.[13] When an adversary or enemy of a threat actor has formally announced significant retaliation in instances of kidnapping its citizens, the technique of kidnapping even one individual may be a viable method of instigating armed conflict, transnational intervention in regional affairs, and/or state or nonstate actor concessions in persistent conflict.[14]

Plans and Actions for Kidnapping

Understanding the goals and capabilities of a threat organization promotes a proactive approach to analyzing the transfer of goals to objectives, and objectives into operational plans and actions. While prediction is conditional, a plan for kidnapping considers target value and cost benefit required to successfully act. Location and timing are critical elements of conceiving, planning, and conducting the action. Identifying practical sites in which to conduct a kidnapping normally follows a deliberate process of initial reconnaissance and detailed surveillance that supports development of primary and enabling actions of a kidnapping.[15]

Daily routine can establish a template for surveillance and how much, if any, variation exists in routine actions of the target—the victim. If target behavior is less formally structured and lacks recurring cycles or easily noticeable patterns of activity, detailed data collection of daily lifestyle has an expectation of eventually identifying some noticeable pattern of activity. Focusing on location and timing applies simple analysis of conditions. When a target location is at a permanent home, temporary residence, or work place, the locale is clearly known and multiple aspects can be studied in and around that point of reference to identify vulnerabilities and plan the kidnap. A kidnapper evaluates what force protection measures are in effect in the vicinity of or with a target that indicates the degree of risk involved in a kidnapping task.

Analysis and current intelligence from surveillance and recurring evaluations confirms what weaknesses exist in a target's security and how to best exploit those vulnerabilities. See figure 1 for a general sequence of actions and explanations that, in many cases, is a continuum of refined practice and execution of action and enabling tasks.

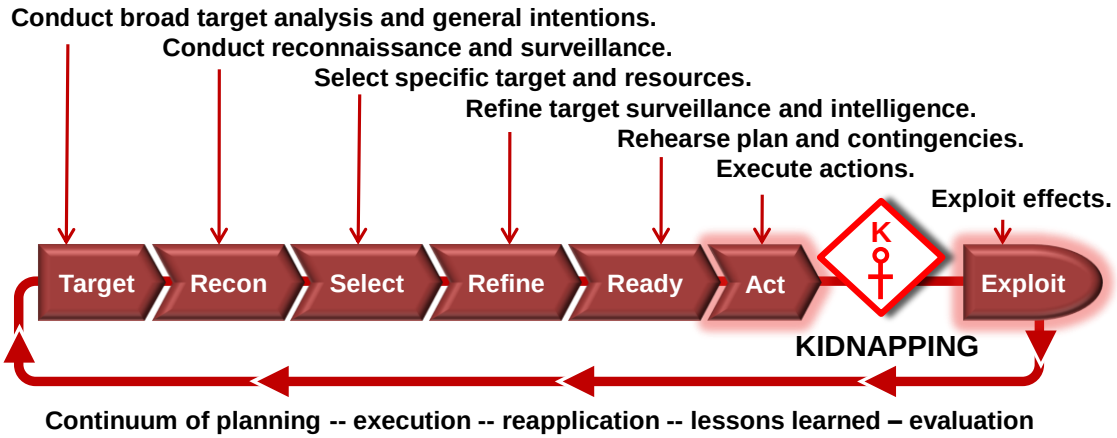


Figure 1. Deliberate planning-execution cycle for kidnapping

Location of the kidnapping site is selected for the optimum possibility of surprise, deception, rapid seizure of the victim or victims, and immediate movement from the site. Three typical points of reference such work place or office, home or temporary residence, and routes between these normal daily sites can be supplemented with other locations within a pattern of target behavior.

Action and Enabling Elements

Threat models for US Army training in the Training Circular 7-100 series describe threat missions with action, enabling, and/or special tasks.[16] The tasks correspond to the functions and outcomes required of each type of task. As the task or tasks of a particular element in a kidnapping change within a sequence of actions, the element's description also changes. For example, a deception element may transition to an assault element as part of a series of mission tasks.

- The *action* element of a kidnapping is responsible for performing the primary function or task that accomplishes the abduction.
- In relation to the action element, each additional element of a kidnapping task organization provides various enabling functions as an *enabling* element. However, each element with an enabling function is identified typically with a specific functional description it performs. Examples can include a *fixing*, *security*, *deception*, and/or *support* elements.
- A kidnapping can include *special* elements. These elements can be retained but not involved in initial primary or enabling actions, as in the case of a *reserve.* This allows the kidnapping mission leader the flexibility to influence unforeseen events or take advantage of developing opportunities.

Threat Kidnapping Options in Army Training

The threat task that most closely resembles kidnapping in TC 7-101, *Exercise Design* is a raid. A *raid* is "an attack against a stationary target for the purposes of its capture or destruction that culminates in the withdrawal of the raiding force to safe territory. Raids can also be used to secure information and to confuse or deceive the enemy. The keys to successful accomplishment of any raid are surprise, overwhelming force effects, and violence."[17] Rapid conduct is the norm of raid tasks. See table 1 as an aid in planning, conducting, and evaluating a raid task adapted to threat conduct of kidnapping in an Army training event.

Table 1. Threat kidnapping task option for Army training

Task 2.0 Raid (KIDNAPPING)		**As adapted from TC 7-101**
Task Description. An attack against a stationary target for the purposes of its capture that culminates in the withdrawal of the kidnapping elements to safe territory.		
Subtasks for a raid are—		
2.1	**Infiltrate**	• Conduct undetected movement through and/or into an area occupied by enemy forces to occupy a position of advantage.
2.2	**Isolate**	• Maneuver and deploy security element(s) to ensure additional enemy forces do not join the battle unexpectedly. (Security elements may become fixing elements.) • Continue to provide early warning. • Prevent the enemy from gaining further information. • Prevent enemy maneuver.
2.3	**Seize**	• Attack to seize personnel [adapted for kidnapping].
2.4	**Exfiltrate**	• Conduct undetected movement from areas under enemy control by stealth, deception, surprise, or clandestine means.

Actions on the objective—the kidnapping site—sequence through several main tasks of a raid with adaptations dependent on the particular US Army training circumstances. Appendix B of TC 7-101 provides a baseline tactical task, its subtasks, and measures to evaluate success of a raid. Key subtasks are to infiltrate into the objective area, isolate the

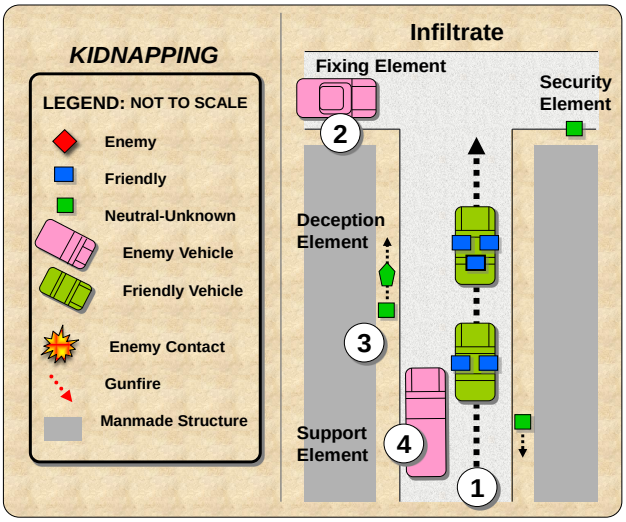
kidnap site, obtain access to the individual to kidnap, gain control of the victim, immediately remove the victim from the site, and exfiltrate to a safe haven.

The following training vignette is loosely based on the kidnapping of German industrialist Martin Schleyer in 1977 by members of the Red Army Faction (RAF).[18] This small group of terrorists used detailed surveillance to identify a vulnerable location to be exploited for the raid, and knew how to overwhelm the personal security and safeguards accompanying the target. The terrorists planned to surprise, deceive, and isolate the victim and security personnel, conduct a rapid and violent assault to murder the security personnel, and seize the kidnapping victim. The kidnapping was a success. Schleyer was held captive for over 40 days as the RAF stated demands and awaited release of imprisoned RAF members and a statement to be announced by the German federal government. When a separate hostage-taking act of terrorism was foiled by German authorities, Schleyer was murdered by his kidnappers.

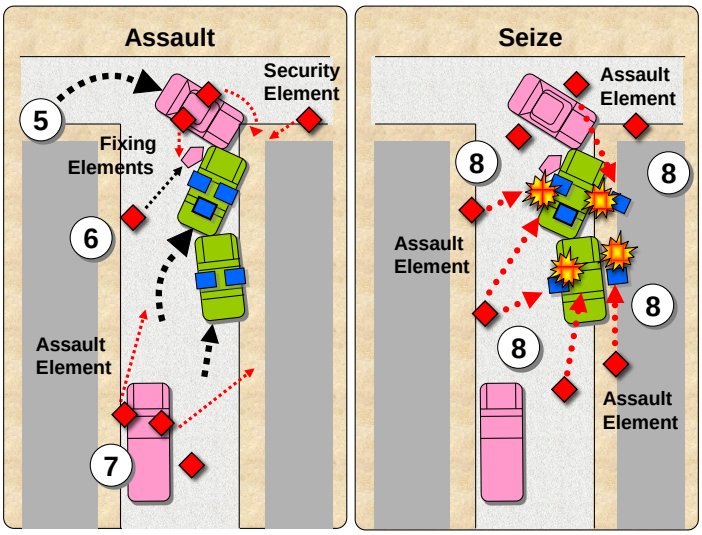
Training Vignette – Kidnapping

This vignette focuses on several subtasks within the task of kidnapping. After selecting and rehearsing the kidnapping, key action and enabling actions include—

- Infiltration to the site well prior to the assault in order to blend into the local environment.
- Emplacement of terrorist *security* elements and/or observers to alert on any conditions that may affect the assault and kidnapping.
- Confirmation that all kidnapping elements are ready to act on order of the leader.
- Isolation (blocking) of the kidnapping target by a *fixing* element.
- Creation of a *deception* concurrent with the isolation that compounds the *surprise* of a fixing element on target vehicles.
- Conduct rapid *assault* and seizure of the victim.
- Movement from the kidnapping site by a *support* element of all kidnapping elements and the victim to a safehouse.



This vignette allows for multiple possible outcomes of a kidnapping that can include release, rescue, and/or escape of the victim, and also considers that a kidnapping victim may be murdered rather than released. Observers could also remain in the kidnapping site area to report on actions and timing of response forces to the kidnapping.



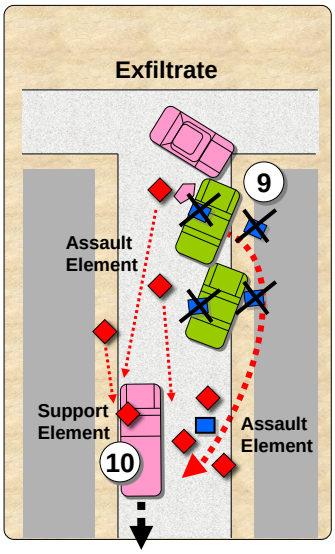
1. The terrorists select a one-way street with restrictive lateral egress as the assault site. Having confirmed the victim's normal route of travel and a norm of riding in a lead (victim) vehicle accompanied by a trail security vehicle, the terrorists select a most vulnerable location site for the kidnapping.

2. The terrorists position a vehicle prepared to *isolate* and fix the lead vehicle from any forward egress. Security elements observe multiple approaches into the objective area as early warning and/or reporting the approach of the two-vehicle target.

3. The terrorist position a woman with a baby carriage [empty] who prepares to *deceive* and surprise the lead vehicle and prevent lateral egress by pushing the baby

carriage into the victim's vehicle.

4. The terrorists park a vehicle nearby as *support* to secure the victim and rapidly move from the kidnapping site.



5. The *fixing* element vehicle swerves in front of the victim's vehicle and fixes movement from the front. The abrupt halt causes of the security vehicle to ram the back of the kidnap victim's vehicle and pins the lead vehicle between the terrorist and security vehicles in the restricted street area.

6. The woman terrorist pushes the baby carriage from the sidewalk into the road, screams, and wedges the baby carriage into the victim's vehicle.

7. Simultaneously, other terrorists are approaching both the lead and trail vehicle and preparing to *assault* and shoot the lead vehicle driver and security personnel.

8. The terrorists rush the two vehicles and quickly murder the lead driver and three security personnel with massed small arms fire from pistols, an automatic weapon, and a shotgun.

9. The terrorists pull the kidnapping victim from the lead vehicle and move to the *support* vehicle.

10. The terrorists run to the *support* vehicle with their victim and quickly exfiltrate from the kidnapping site. The entire kidnapping sequence takes two to four minutes from the initial fixing of vehicles and the terrorist's exit from the site.

Training Implications—Use Kidnapping Vignettes in Training: Risk Assessment-Situational Awareness

From a threats perspective, terrorism intent and capabilities indicate possible and probable types of threat action that may be directed against US military members, units, and organizations. Factors other than military power may place limitations or restrictions on both threats and friendly forces. Commanders, organizational leaders, and other military members must know the threat in an OE, and instill situational awareness and understanding of the conditions that may be conducive to an act of kidnapping.

- Publicize kidnapping as a threat to US military members, family members, Department of the Army Civilians (DAC), and contractors in support of Army missions. Threats may extend to coalition partners and local citizens at institutional locations such as training and education sites, installations, support facilities, and mission areas of operations.
- Relate appropriate levels of protection of the force, operational security (OPSEC), and kidnapping prevention and countermeasures at installations, activities, and units. Include kidnapping threat as integral to vulnerability analyses for US forces, citizens, and support activities when—
    - Deployed on an operational mission.
    - In-transit to or from an operational mission.
    - Designated as installation or institutional support and not normally deployed in the conduct of the organization's mission.
- Ensure a recurring threat assessment is relevant to probable and known vulnerabilities to protect key personnel or other individuals who have been targeted for kidnapping. Plan appropriate situational awareness; vehicle protection; and security personnel equipment, weapons, communications, and techniques adequate to counter or preempt known or projected threat capabilities of a kidnapping. *Know the Threat—Know the Enemy*.

Notes

[1] US Department of Defense, Defense Intelligence Agency, Threat Assessment: Looking to 2016 (Washington, D.C.: Defense Intelligence Agency, 1997).
[2] Tactics. DOD Dictionary of Military and Associated Terms, Joint Publication 1-02, 08 November 2010, as amended through 15 June 2014.
[3] Techniques, DOD Dictionary of Military and Associated Terms, Joint Publication 1-02, 08 November 2010, as amended through 15 June 2014.
[4] Kidnapping, Merriam-Webster Dictionary [online].
[5] Kidnapping, The Law Dictionary: Black's Law Dictionary Free Online Legal Dictionary 2nd Ed.
[6] Kidnapping-Ransom Payments-Political Concessions, United Nations Security Council, Resolution 2133 (2014).

[7] Kidnapping, The Free Dictionary.
[8] Kidnapping, Title 18, Part I, Chapter 55, Section 1201, Cornell University Law School US Code Collection.
[9] International Terrorism. Title 18, Part I, Chapter 113B, Section 2331, Cornell University Law School US Code Collection.
[10] Tiger Kidnap, Police Service of Northern Ireland.
[11] Margaret Cauley, "Rise of 'Express' Kidnappings Sign of Colombia's Criminal Evolution," In Sight Crime, 25 March 2014.
[12] Michelle Lee (FBI Special Agent), "'Virtual Kidnapping' Extortion Calls on the Rise," 6 August 2014.
[13] Jacob Zenn, "Boko Haram and the Kidnapping of the Chibok Girls," Combating Terrorism Center at West Point, 29 May 2014.
[14] Andrew Chadwick, "The 2006 Lebanon War: A Short History," Small Wars Journal, 11 September 2012. See also, Scott Farquhar, Back to Basics: A Study of the Second Lebanon War and Operation CAST LEAD, US Army Combat Studies Institute, 2009.
[15] US Department of the Army, Training Circular 7-100.3, Irregular Opposing Force, 17 January 2014.
[16] Ibid., para. 2-52 to 2-57.
[17] US Department of the Army, Training Circular 7-100.2, Opposing Force Tactics , 9 December 2011.
[18] Global Security, The Kidnapping/Assassination of Hanns Martin Schleyer.

WHERE TO FIND THE THREAT TRAINING LITERATURE ON ARMY TRAINING NETWORK

Complex Operational Environment and Threat Integration Directorate (CTID)

Chemical Weapons Remain— A Serious Threat: 4th Generation Chemicals

by **Walter L. Williams**, TRISA-CTID, Exercise and Training Support Team (DAC)

The May 2012 edition of the Red Diamond included an article on chemical weapons, "The Non-Traditional Chemical, Biological, Radiological, and Nuclear (CBRN) Portrayal in Potential Operational Environments (OEs)." That article focused on the differences in chemical weapon employment by terrorist and insurgent entities versus conventional military forces. This article is a follow-on discussion to the aforementioned article with the intent of briefly discussing the definition, development, and stockpile of 4th Generation Chemicals.

A chemical agent is a substance that produces an effect on humans, animals, and plants by virtue of its toxic chemical properties. When used as weapons, chemical agents may be aimed or targeted against humans, 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. A chemical agent can either be a toxic (blood/chocking, 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.

4th Generation Chemicals are considered to be chemical agents developed by the former Soviet Union (and later Russia) in the 1980s. Information revealed by Russian military chemists indicates that a new generation of nerve agents was developed over two-three decades beginning in the 1970s. The creation of the nerve agents, called *novichoks* (Russian for "newcomer"), resulted from a top secret program called Foliant.

One of the chemists from the Foliant program, Dr. Vil Mirzayanov, attested that the novichok nerve agents were stronger than the G- and V-series agents because they were more resistant to treatment and therefore more deadly. "Agent 230 [a novichok], which was adopted as a chemical weapon by the Russian Army, is 5-8 times more poisonous than VX gas. It is impossible to cure people who are exposed to it."[1] Table 1 provides a brief illustration of the various chemical agents developed from World War I to the present.

Table 1. Generations of chemical agent development

GENERATION	TIME PERIOD	CHEMICAL AGENT TYPES	EXAMPLES
First	World War I	Choking, Blood, or Blister	Chlorine, Hydrogen Cyanide, Lewisite, Mustard
Second	Prior to World War II	G-Series Nerve	Sarin, Soman, Taben
Third	1950s	V-Series Nerve	VX
Fourth	1980s	INA	INA

One should consider employment considerations for 4th Generation Chemicals in terms of reasonable, feasible, and plausible. The methods of employment may involve both traditional and non-traditional means with various actors. For

example, an approach is for a state or non-state actor to use the existing infrastructure of a target country and employ the agent using improvised delivery or dissemination techniques.

An example of this approach is the 20 March 20 1995 Sarin (second generation agent) gas attack of the Tokyo subway system by the Japanese terrorist group Aum Shinri Kyo. The terrorist group was well financed and organized. They were able to obtain an amount of the Sarin agent and disperse it on crowded subway trains inflicting casualties as well as spreading fear amongst the population.

On the other hand, a traditional method of employment could be by a state actor with a conventional force structure supporting the dissemination of the chemicals in attacks. The dissemination methods may range from aerosol sprays by aircraft to bombs, missiles, rockets, and artillery projectiles.

Very little is known about the continued development, production, and stockpile of 4th Generation Chemicals. There remain concerns by Western nations (particularly the United States) about the declaration as well as the accuracy of Russia's reporting of their chemical weapon stockpiles. An August 30, 2005 Bureau of Verification and Compliance report stated the following:

> Since 1992, Russian scientists familiar with Moscow's chemical warfare development program have been publicizing information on a new generation of agents, sometimes referred to as 'Novichoks'. These scientists report that these compounds, some of which are binary agents, were designed to circumvent the Chemical Weapons Convention and to defeat Western detection and protection measures. Furthermore, it is believed that their production can be hidden within commercial chemical plants. There is concern that the technology to produce these compounds might be acquired by other countries. [2]

Russia became a signatory to the Chemical Weapons Convention with a legal obligation to not only destroy their chemical weapons stockpiles but to cease the development and possession of chemical weapons. The Russian Duma passed and Russian President Boris Yeltsin signed the Russian Federal Law on Chemical Weapons Destruction in May 1997. The Federal Law was based upon a 1996 Russian-developed implementation plan for chemical weapons destruction. Changes or adaptations to the implementation plan were made in June 2002 and 2003. It is suspected that Russia's destruction of their declared chemical weapons stockpiles is slow due to both financial and bureaucratic reasons. For example, "with international assistance, Russia in April 2003 completed the destruction of one percent of its Category 1 CW stockpile three years after the original CWC deadline for completing such destruction."[3]

Thus, there is a possibility for the continued development and production of 4th Generation Chemicals by Russia, but no one knows for sure. It is strongly suspected that Russia is continuing to destroy their inventory of an array of nerve agents in both weaponized and bulk form.

References

Bureau of Verification and Compliance. "Arms Control Compliance". 30 August 2005.
Ciottone, Gregory R, ed. "Disaster Medicine". Mosby Incorporated. 2006.
Counterproliferation Program Review Committee. "Activities and Programs for Countering Proliferation and NBC Terrorism." May 2006.
Pike, John. "Weapons of Mass Destruction Intelligence Assessments." FAS. 7 February 2012.
Soutter, Will. "Nano Technology in Chemical Warfare." AZoNano.com. 16 February 2013.
Tucker, Jonathan B. "The Future of Chemical Weapons." The New Atlantis. Fall 2009-Winter 2010.

Notes

[1] Jonathan B. Tucker, "The Future of Chemical Weapons," The New Atlantis, Fall 2009-Winter 2010.
[2] Bureau of Verification and Compliance, "Arms Control Compliance," 30 August 2005.
[3] Bureau of Verification and Compliance, Arms Control Compliance," 30 August 2005.

RPG-30 Kryuk "Hook" Russia's Solution to Active Protective Systems (APS)

by Mike Spight, TRISA-CTID, Exercise and Training Support Team (CGI Ctr)

Since World War I and the introduction of the tank and armored vehicles on the battlefield, armies have sought out methods for small units or individual soldiers to damage or destroy those particular threats. Until World War II and the introduction of systems such as the German Panzerfaust and the US M1 Rocket Launcher (Bazooka) the primary ways to kill a tank were with another tank, anti-tank mines, anti-tank gun systems, massed artillery fires, or aerial bombs dropped from aircraft. In the case of the US Army's M1 system, it was an awkward system to carry and operate and realistically required two soldiers (a loader and a gunner) to effectively employ it against enemy armored vehicles. However, the German Panzerfaust, issued to both Wehrmacht and Waffen SS infantry units, was truly capable of being operated by a single soldier and was extremely portable in comparison to the M1 Rocket Launcher. Additionally, the Panzerfaust 30, and its follow-on variants (60 and 100) introduced the concept of a disposable launcher. The rocket was fired at an enemy vehicle, and the German soldier could then drop the launcher and leave it behind as he moved to a new position. This evolutionary concept was eventually adopted by the US Army in 1963 with the introduction of the M72 Light Armor Weapon (LAW), the first disposable launcher rocket propelled grenade (RPG) developed by the US, and the former Soviet Union's development of the RPG 18 (adopted in 1972 and depicted in Figure 1) as their first disposable launcher RPG.

As a result of the proliferation of anti-armor systems that can be easily carried and operated by individual soldiers or other combatants, states have adapted both their tactics and armored vehicles to counter the effectiveness of modern RPGs. Within the past 30 years, improvements in armor, such as the composite armor found on the M1 Abrams and other nations' modern main battle tanks (MBT), have increased the level of protection offered to the crews, and greatly reduced the chance that an RPG (particularly the older variants) will damage, much less kill, a modern MBT or infantry fighting vehicle (IFV).

Early variant RPG projectiles were commonly only 64-66mm, and these improvements in armor protection drove the development of new RPGs, particularly in the former Soviet Union, with 105mm (RPG-27 and RPG-29), and later 125mm (RPG 28) projectiles. As these more powerful RPGs with greatly increased capability to penetrate heavy armor proliferated, the appearance of explosive reactive armor (ERA) and APS mounted on MBTs and IFVs become the norm for some new tier 1 or 2 systems. Plus, ERA is commonly installed on even tier 3 or 4 systems in an effort to upgrade protection for crews. The development of ERA directly led to development of the tandem warheads found on modern RPGs and some anti-tank guided missiles (ATGMs).

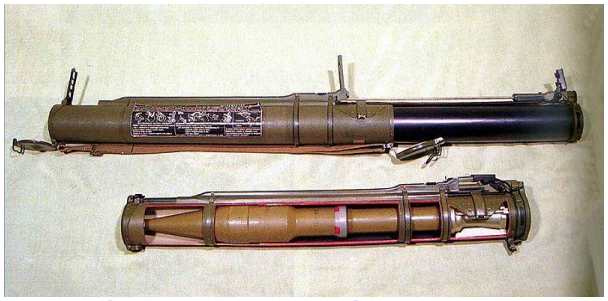


Figure 1. RPG-18 Kryuk or Common Designation "Hook"

APS has recently been shown to be extremely effective in defeating RPGs and even ATGMs. The Israeli Defense Force (IDF) is equipping its Merkava MBTs with the Trophy APS which has proven effective in Gaza within the past few months as it has successfully detected and destroyed incoming RPGs and ATGMs. The IDF documented multiple incidents in which Trophy APS-equipped Merkavas were engaged not only with RPG-29s, but also with advanced ATGM systems like Kornet-E and Konkurs. In every case, the Trophy APS detected and defeated the incoming RPG or missile.

The Russian defense industry, anticipating the ability of APS to defeat existing anti-tank systems, developed the RPG-30 to specifically counter existing or future APS systems. Developed by the State Research and Production Enterprise (Bazalt) in 2008, it was tested and eventually adopted by the Russian military in 2012 and it is a singularly simple concept. The RPG-30—a cutaway variant is shown below in Figure 2—fires a decoy, sub-caliber rocket milliseconds before the primary projectile, a 105mm high explosive, tandem warhead anti-tank (HEAT) rocket.

Figure 2. Cutaway of 105-mm and Decoy RPGs

In theory, the target vehicle's APS will detect the incoming sub-caliber decoy round, lock on, and then fire its counter-measure projectiles at the incoming decoy rocket. As typical APS require somewhere between .2 to .4 of a second to reset and be ready to detect and engage the next incoming rocket, this results in a gap in the APS coverage, and the main 105mm HEAT rocket is then free to exploit and strike the now exposed armor plate of the target vehicle, perhaps resulting in a heavily damaged or destroyed vehicle. This is certainly a simple, adaptive solution, but to date, there are no reports as to how effective the RPG-30 is against an actual APS-equipped MBT. As the RPG-30's 105mm rocket is similar in performance to the RPG-29's PG-29V 105mm rocket, it would be safe to assume that its ability to damage or even destroy an MBT after defeating ERA is virtually assured. And, of course, the designed ability to defeat APS makes it a truly formidable RPG. Figure 3 depicts how the RPG works against an APS-equipped MBT.

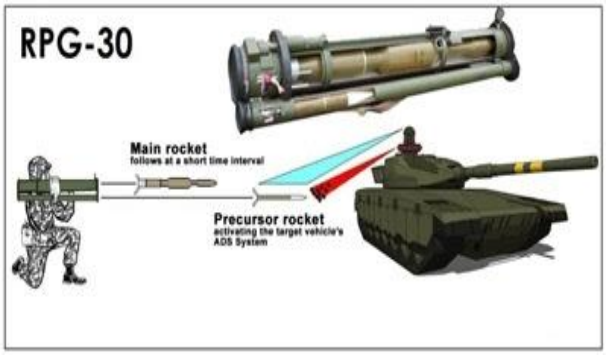


Figure 3. Precursor and Main Grenade Functions

The RPG-30 has the following estimated performance characteristics: effective range of 200 meters; can penetrate approximately 600mm (approximately 24") of rolled, homogeneous armor (after ERA); and a rocket velocity of 120m per second.

The IDF is aware of the threat posed by the RPG-30 and has reportedly developed an upgraded APS named Trench Coat, which is intended to fire enough projectiles to destroy both the incoming precursor sub-caliber rocket and the main 105mm HEAT round. Trench Coat is designed to offer 360 degree protection around the MBT, but will not cause collateral damage to other friendly vehicles or exposed dismounts near the targeted MBT. [Type a quote from the document or the summary of an interesting point. You can position the text box anywhere in the document. Use the Text Box Tools tab to change the formatting of the pull quote text box.]

How effective the RPG-30 will be against modern APS remains to be seen. The only engagements of APS-equipped MBTs currently reported have occurred in Gaza and Israel, and the IDF's Trophy system proved to be extremely effective. If the RPG-30 is exported to Syria, Gaza, and/or Hezbollah at some point (something that Israel is very interested in knowing), then the effectiveness of the IDF's new Trench Coat system will certainly be thoroughly tested at some point by the IDF's implacable enemies.

by **Kristin Lechowicz**, TRISA-CTID, Current Operations Team (DAC)

The Complex Operational Environment and Threat Integration Directorate (CTID) of the Training and Doctrine Command (TRADOC) Intelligence Support Activity (TRISA) is assigned the mission to examine and capture relevant, real-world threats and challenging operational environments (OEs) for the training community. CTID's research provides the proper conditions for threat portrayal and the representation of a realistic US Army training environment. One facet of CTID's research incorporates evolving or new technologies of threat systems/equipment into the US Army TRADOC G2 Worldwide Equipment Guide (WEG).

The three-volume WEG is updated annually and posted to the Army Training Network. With a common access card (CAC), the WEG is available at the "Hybrid Threat and OPFOR Doctrine" button on the ATN front page. The WEG identifies capabilities and limitations of weapons and equipment derived from observations and lessons learned from real-world threats, not unlike the ongoing conflict in Syria and Iraq. The WEG supports live, virtual, constructive, and gaming (LVCG) simulations for concept development, training, education, and leader development.

A current example of threat capabilities is how the Islamic State of Iraq and the Levant (ISIL) uses civilian pickup trucks mounted with heavy weapons systems as improvised fighting vehicles. (See figure1.) The media and military analysts often refer to these makeshift combat vehicles as "technicals." The technical, as a concept or as an expression, is not new to persistent conflict. The term became popular during Operation RESTORE HOPE in Somalia. Other real-world threats such as Taliban insurgents, Somali warlords, and ISIL extremists have used technicals for years. Recent examples of regular and irregular forces in a hybrid threat continue to transform various types of commercial vehicles into mobile and sometimes armored weapons carriers. Weaponry mounted in technicals can range medium caliber or millimeter machine guns to large antiaircraft guns, large-caliber recoilless rifles, or large rocket launchers.

Figure 1. Civilian vehicle mounting heavy machine gun ISIL Technical

Due to successful operations of the improvised fighting vehicles in events such as the Arab Spring, a CTID analyst produced a WEG data sheet on the Toyota Helix converted into a technical fighting vehicle. This WEG data sheet is one of many resources readily available to create and/or enhance the challenging conditions of a diverse and adaptive threat in complex OEs.

Volume 1 of the WEG discusses improvised fighting vehicles within two of its chapters: “Infantry Fighting Vehicles” and “Improvised Military Systems.” The US Army and joint community can use the WEG to support complex and ad hoc threat arrays in preparation for and readiness in contemporary and future conflicts. The example of a WEG sheet in figure 2 (below) features a baseline for how a civilian vehicle can be adapted into a “technical’” weapons carrier.

Toyota (Double Cab) Hilux “Technical” Multi-Role Vehicle (Example)

SYSTEM
Alternative Designations:
Date of Introduction: Originally 1968
Proliferation: Widespread (Worldwide)

Description: Pickup truck with multiple models, cab size, engine type/transmission, and styles.
Troop Capacity: 5 in front, 6+ in rear
Weight (mt): 2.81
Gross Vehicle Weight: 2810 kg
Curb: 1840 kg (automatic trans)
Length Overall (m): 526
Height Overall (m): 186
Width Overall (m): 183.5
Payload on/off Highway (kg): 1060
Number of Axles: 2
Drive Formula: 4x4
Ground Clearance (mm): unknown (dependent)
Turning Radius (m): 12.4 -13.0 (circle) Power Assisted Rack and Pinion
Wheels:
Size (in): 15-17 (dependent)
Central Tire Pressure Regulation System: No
Run Flat: Available; however, uncommon for most technicals. Due to the use of common civilian vehicles.

AUTOMOTIVE

Engine: (V-6 Petrol model) Six cylinders, V-formation, chain-driven DOHC, four valves per cylinder, all alloy with cross-flow cylinder heads
Cooling: yes
Cruising Range (road) (km): 436.17 (based on 21.17 MPG and 20.1 Gallons)
Speed (km/h): (dependent on load) 100-113

Fuel Capacity (liters): (petrol model) 76
Towing Capability (kg): 2500 (with trailer breaks) 700 (without)
Fording Depths (m): 70 (wading)
Trench Crossing Width (mm): N/A
Winch: Dependent (available)

CARGO SPACE

Height (mm): 420
Width (mm): 1515
Length (mm): 1520

1.
ARMAMENT: The Toyota Hilux can be “up-armored;” however, Most of the technicals that will be encountered by U.S. forces will be regular civilian vehicles used by an irregular force. There have been reports that drug cartels have used up-armored pickup trucks in the past.

2. VARIANTS and ANALYSIS:
A technical can be almost any civilian truck or vehicle that can be armed with versus different weapons systems (rockets, air defense guns, or heavy machineguns). The Toyota Hilux is a good example of a technical based on reporting from Libya, Syria, Afghanistan, and Mali. Irregular forces use these particular type of vehicles because of the vehicle’s reliability in hostile conditions. Many technicals are trucks or 4x4 vehicles (most likely due to mobility in restrictive terrain and availability). The pictures above are from Libya and Afghanistan that illustrate examples of technicals with a DShK heavy machinegun (for additional information on that system see Vol. 1 of the World Wide Equipment guide). The use of common civilian vehicles makes t easy for threat forces to blend into the civilian population and makes it difficult for friendly forces to target. These types of vehicles allow the Threat to be agile, fast, and move freely within a set population (with the only downside of having limited armor protection.

Figure 2. TRADOC G2 Worldwide Equipment Guide: Technical multi-role vehicle (example)

References

Cave, Damien. "Monster Trucks on the Road, From Gangs in Mexico." The New York Times. 7 June 2011.
Einzemark. "Toyota Hilux, A Brief History."
Fox News Latino. "Mexican Cartels Moving Drugs in Armored Vehicles ." 18 January 2012.
Rosemberg, Hernan. "Cartel Violence Helps Boost Armored Car Sales In US." Fronteras. 26 January 2012.
Top Speed. "2009 Toyota Hilux." 4 September 2008.
Wikicommons. "Brega checkpoint [technical]." Picture 1 (WEG sheet, upper left). 25 November 2011.
Wikicommons. "A Private Afghan Security Company truck armed with a DShK heavy machine gun." Picture 2 (WEG sheet, upper right). 11 February 2010.
Wired. "The Tools of Mexico's Drug Cartels, From Landmines to Monster Trucks."

Note. For more information, contact artilce author.

ISIL Attack on the Tabqa Airbase, Syria

by **Rick Burns**, TRISA-CTID, Fusion Team (CTR BMA)

Introduction

Despite air superiority, Syrian regime forces were unable to hold on to the last base in the Raqqah Governate. In recent months, the Islamic State of Iraq and the Levant (ISIL) has consolidated its hold on this northern province, finally capturing the Tabqa base after a steady week-long series of attacks. Over the preceding weeks, ISIL forces captured and occupied villages surrounding the Tabqa base in preparation for an assault on the base. Using its signature suicide bombers as breaching forces, ISIL finally forced an evacuation from the base.

Essentially controlling the Raqqah governate adds to the growing ISIL narrative that it is the legitimate protector and leader of the caliphate. With uncontested geography, ISIL is free to implement its radical form of governance and intimidation. For the Syrian security forces, it means another defeat and the looming reality that ground will not be easily taken back from ISIL. (See figure 1.)

Figure 1. Map of Raqqah Governate

Unmanned Aerial Vehicles (UAV)

In the recent Raqqah Governate fighting, ISIL added a new reconnaissance capability to its fighting by utilizing UAVs. A recent ISIL video, meant for propaganda, shows that it is capable of and interested in utilizing technology to gain an advantage. The commoditization of reconnaissance-capable UAVs has made them an inexpensive and useable, if limited, means of gaining intelligence. Both Hezbollah and Hamas have used UAVs over Israel. Iran recently claimed to have shot down an Israeli UAV within its borders. The next logical step in the use of UAVs will be to use them as an IED or as a means to drop ordnance from a distance.

Tabqa Air Base Attack

Figure 2 provides an overview of the Taqba Airbase in relation to Ayad Kabir. Figure 3 (next page) illustrates the general tactical actions sequence as reported in open source data. Specific dispositions between ISIL and Syrian government forces are assumed based on open source reports and are not intended to be a definitive depiction of the combat. This visualization and the following narrative focus attention on the main breaching actions and attacks at the airbase's north gate. Syrian forces and ISIL fighters continued to engage each other throughout the period of these main attacks. The Syrian Air Force (SAF) was particularly aggressive in bombing ISIL positions and infrastructure around the base and within nearby cities such as Tabqa and Raqqa. ISIL forces conducted operations against other points of the airbase perimeter during the attacks.

The Tabqa base is key terrain for both ISIL and the Syrian regime. Both sides fought tenaciously with Syrian forces using air assets and ISIL using its suicide bombers and exploitation element to attempt breaches at the main gate. Around 10 August 2014, ISIL began attacking the base. On 17 August, the SAF conducted over 20 air strikes in and around Tabqa and the city of Raqqah. On 18 August, SAF continued air strikes in Raqqah City, damaging the Raqqah city water plant. Anticipating sustained ISIL attacks, the Syrian regime sent reinforcements and large quantities of ammunition and food to the Tabqa airbase. In the preceding days, ISIL captured nearby villages from which to launch attacks.

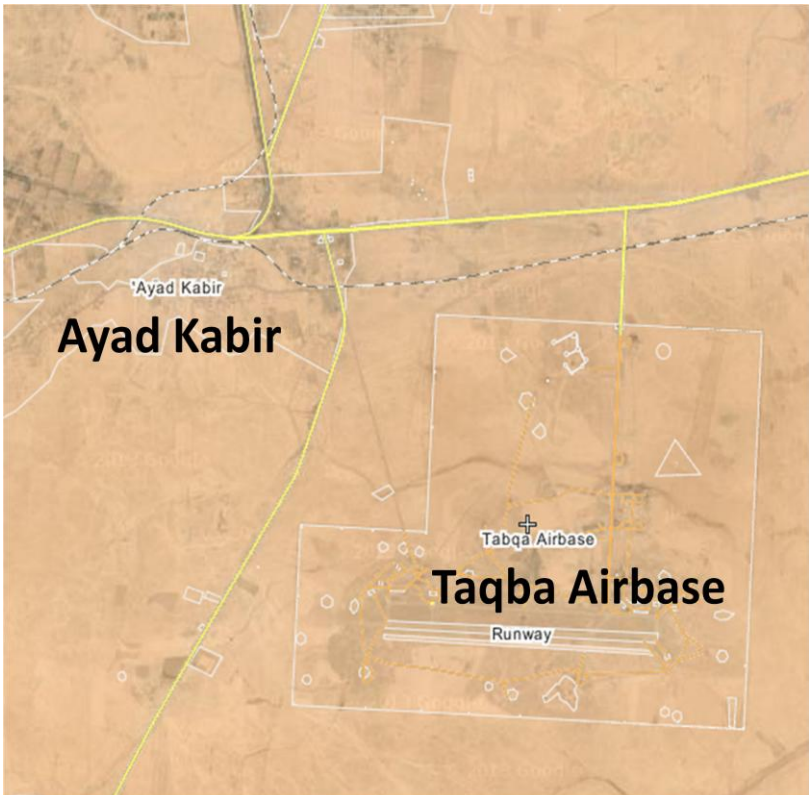


Figure 2. Map of Tabqa Airbase

The first main assault began on the night of 20 August. ISIL used rockets and mortars as a fixing element. A breaching comprised of two suicide vehicle borne IEDs (SVBIED) attacked the main gate and were followed by an exploitation element of up to 200 fighters. This assault was stopped at the gate by Syrian defenders. The first SVBIED was detonated at a distance from the gate by either the Syrian guards or was caused by a premature detonation. The second SVBIED detonated close to the gate, but produced little damage. The exploitation element met with sufficient resistance from airbase defenders, and withdrew from the immediate area.

Fighting subsided during the morning of 21 August 2014 after which a second assault was launched. This second assault included a fixing element of rockets and mortars and an action element with the mission of attacking and penetrating the front gate.

Syrian special operation forces, recognizing the staging of ISIL fighters, anticipated their movement and planted mines in their attack axis. In addition, Syrian forces massed heavy indirect fires and air strikes against the ISIL combatants. The ISIL force retreated again. Fighting continued into the morning of 22 August 2014 when ISIL managed to capture a checkpoint outside the base. ISIL failed, however, to capture the base.

On the evening of 22 August 2014, ISIL received reinforcements and attempted to breach the entry to the base in the same manner it had begun the attack on the Tabqa airbase on 20 August. An SVBIED attempt to breach the gate failed again, and the exploitation element failed to penetrate the gate.

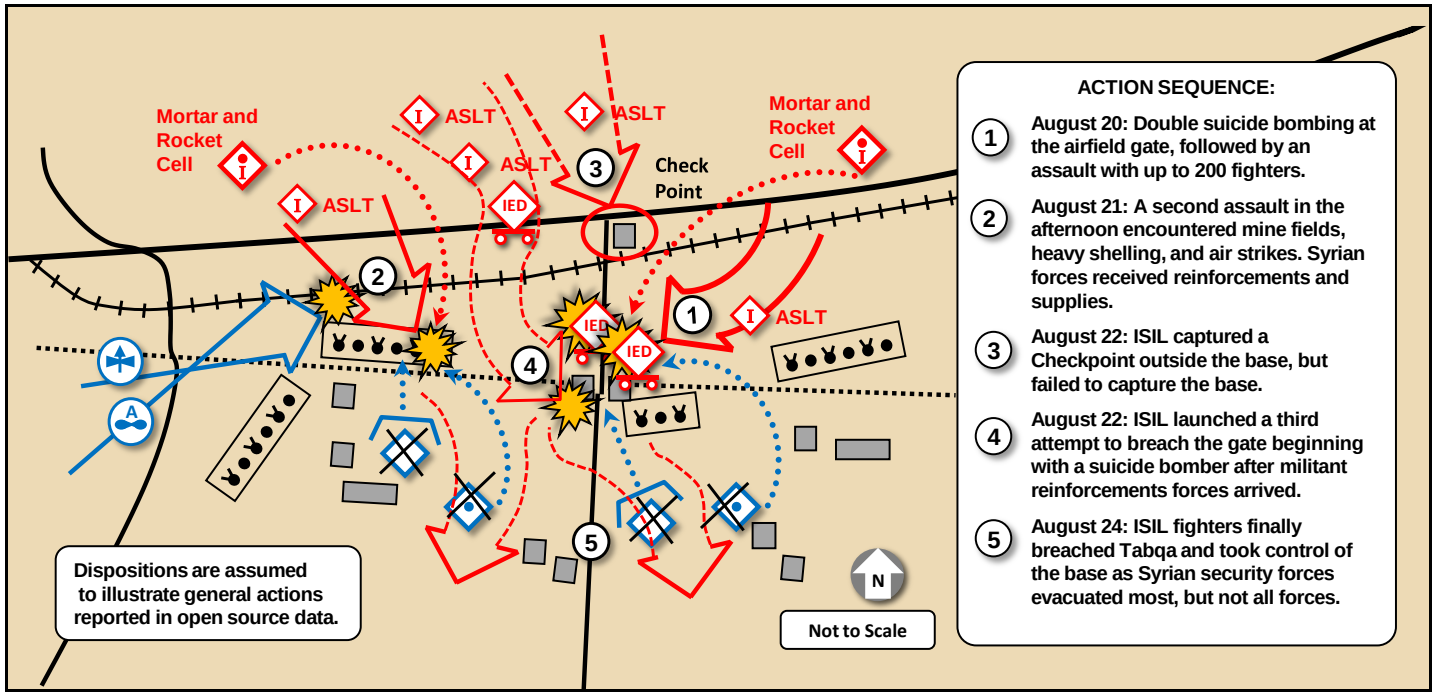


Figure 3. ISIL attack on Tabqa Airbase

Over the next two days, the SAF began evacuating the base. On 24 August 2014, ISIL finally breached the Tabqa base. To this point, approximately 170 government forces were killed and 150 were captured. Around 346 ISIL fighters were killed in the attacks. ISIL executed the Syrian defenders that were captured. Both ISIL and the SAF sides attempted to explain the events at Tabqa Airbase to their advantage. The Syrian regime painted the evacuation as a planned regrouping of forces. ISIL claimed victory and used it as further evidence of its growing strength.

Training Implications

As outlined in TC 7-100.2, *Opposing Force Tactics*, threat forces fight with a degree of predictability. ISIL attacked Tabqa using a combination of fixing, breaching, and exploiting elements. Although unsuccessful in actually breaching the base gate, the SVBIEDs had an effect. Understanding that Syria's casualty risk calculation is much different than ISIL's suggests that ISIL was ready and willing to attack with additional fighters and more SBVIEDs. Syria's response was to launch air strikes and reinforce the base defenses to some degree on the ground, but eventually it evacuated most of its defenders, allowing ISIL to seize the Taqba Airbase. Considered in this light, the evacuation, defeat, and/or capture of the Syrian forces and key terrain was inevitable.

References

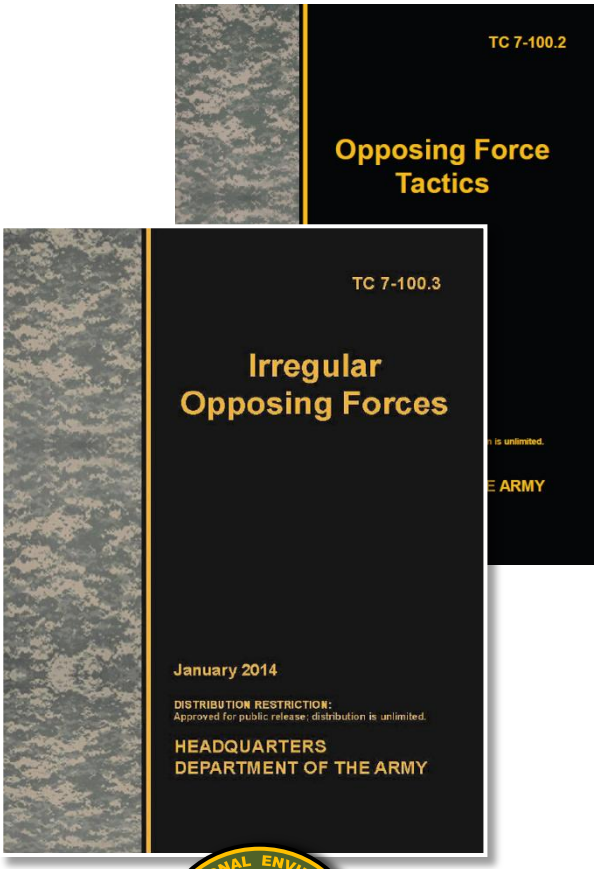
"Al Raqqa Province: Warplanes Went In." Syrian Observatory for Human Rights. 25 August 2014.
Ali, Abdullah Suleiman. "After Tabaqa Airport, What is IS' Next Target?" Al Monitor. 25 August 2014.
Ali, Abdullah Suleiman. "IS attacks Syrian army's last outpost in Raqqa." Al Monitor. 21 August 2014.
Ali, Abdullah Suleiman. "IS continues attacks on Tabaqa airport in Raqqa." Al Monitor. 22 August 2014.
Bergen, Peter and Emily Schneider. "Now ISIS Has Drones?" CNN. 25 August 2014.
Fadel, Leith. "200+ Islamic State Fighters Killed at Tabqa Airbase." Al Masdar News. 21 August 2014.
Fadel, Leith. "Breaking News from Tabqa Airbase: Syrian Army No Longer Encircled." 23 August 2014.
Fadel, Leith. "Syrian Republican Guards Newly Formed 124th Arrives at Tabqa Airbase." Al Masdar News. 21 August 2014.
Hubbard, Ben. "ISIS Tightens Its Grip with Seizure of Air Base in Syria." The New York Times. 24 August 2014.
Iqbal, Muhammad, "Syrian Troops Defending Last Stronghold in Raqa Province." *Business Recorder.* 21 August 2014.
"ISIS Captured and Executed Dozens." Syrian Observatory for Human Rights. 28 August 2014.
"ISIS Claims to Have a Surveillance Drone in New Video." ABC News. 26 August 2014.
Karam, Zeina. "Islamic State Militants Attack Major Air Base In Eastern Syria." The World Post. 20 August 2014.
Lister, Charles. Twitter Entry. 25 August 2014.
Magnier, Elijah. Twitter Entry. 18 August 2014.
Magnier, Elijah. Twitter Entry. 17 August 2014.

Magnier, Elijah. Twitter Entry. 19 August 2014
Magnier, Elijah. Twitter Entry. 24 August 2014.
"More than 500 Dead in Battle for Syria's Tabqa Airport." The Citizen. 16 September 2014.
Mroue, Bassem. "Reports: Syria Troops Kill Scores of Jihadis." AP. 21 August 2014.
"Syria Conflict: ISIS 'Overruns' Raqqa Military Base." BBC. 25 July 2014.
"Syrian Forces Hit Islamic State in Raqqa, Destroy Water Plant." Reuters. 18 August 2014.
"Syrian Jets Hammer Islamic State Stronghold." Aljazeera. 17 August 2014.
Westall, Sylvia. "Hundreds Dead as Islamic State Seizes Syrian Air Base – Monitor." Reuters. 24 August 2014.

Army Antiterrorism Awareness

TRISA **Threats Terrorism Team Advisory**

Do you *know*
The THREAT?



TRADOC G2 Operational Environment Enterprise (G2 OEE)
TRADOC G2 Intelligence Support Activity (TRISA)

—What CTID Does for YOU—

- Determine Operational Environment (OE) conditions for Army training, education, and leader development.
- Design, document, and integrate hybrid threat opposing forces (OPFOR) doctrine for near-term/midterm OEs.
- Develop and update threat methods, tactics, and techniques in HQDA Training Circular (TC) 7-100 series.
- Design and update Army exercise design methods in HQDA TC 7-101.
- Develop and update the US Army *Decisive Action Training Environment (DATE)*.
- Develop and update the US Army *Regionally Aligned Forces Training Environment (RAFTE)* products.
- Conduct Threat Tactics resident course at TRISA, Fort Leavenworth, KS.
- Conduct Threat Tactics mobile training team (MTT) at units and activities.
- Support terrorism-antiterrorism awareness in threat models and OEs.
- Research, author, and publish OE and threat related classified/unclassified documents for Army operational and institutional domains.
- Support Combat Training Centers (CTCs) and Home Station Training (HST) and OE Master Plan reviews and updates.
- Support TRADOC G-2 threat and OE accreditation program for Army Centers of Excellence (CoEs), schools, and collective training at sites for Army/USARR/ARNG.
- Respond to requests for information (RFIs) on threat and OE issues.

CTID Points of Contact

Director, CTID	Jon Cleaves	DSN: 552
jon.s.cleaves.civ@mail.mil		913.684.7975
Deputy Director, CTID	Penny Mellies	
penny.l.mellies.civ@mail.mil		684.7920
Operations-Analyst	Dr Jon Moilanen	
jon.h.moilanen.ctr@mail.mil	BMA	684.7928
Product Integration-Analyst	Angela Wilkins	
angela.m.wilkins7.ctr@mail.mil	BMA	684.7929
Research & Analysis	DAC Jennifer Dunn	
jennifer.v.dunn.civ@mail.mil		684.7962
Worldwide Equipment Guide	John Cantin	
john.m.cantin.ctr@mail.mil	BMA	684.7952
Military Analyst	H. David Pendleton	
henry.d.pendleton.ctr@mail.mil	CGI	684.7946
Fusion	DAC Jerry England	
jerry.j.england.civ@mail.mil		684.7934
UK LNO	Warrant Officer Matt Tucker	
matthew.j.tucker28.fm@mail.mil		684-7994
Military Analyst	Laura Deatrick	
laura.m.deatrick.ctr@mail.mil	CGI	684.7925
Military Analyst	Rick Burns	
richard.b.burns4.ctr@mail.mil	BMA	684.7897
Exercise-Training Spt	DAC Walt Williams	
walter.l.williams112.civ@mail.mil		684.7923
Military Analyst	DAC Steffany Trofino	
steffany.a.trofino.civ@mail.mil		684.7943
LNO to JMRC & JRTC	Mike Spight	
michael.g.spight.ctr@mail.mil	CGI	684.7974
LNO to MCTP	BMA Pat Madden	
patrick.m.madden16.ctr@mail.mil		684.7997
Current Operations	LTC Shane Lee	
shane.e.lee.mil@mail.mil		684.7907
Threat Tactics & CoEs LNO	CPT Ari Fisher	
ari.d.fisher.mil@mail.mil		684.7939
Intel Specialist-NTC LNO	DAC Kris Lechowicz	
kristin.d.lechowicz.civ@mail.mil		684.7922
Intel Specialist-Analyst		(TBD)