Strategy Research Project

THE DOOM OF MY ENEMIES: DARK NETWORKS AND TACTICAL ISR

BY

COLONEL PHIL A. STEWART
United States Air Force

USAWC CLASS OF 2011

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
06-04-2011	Strategy Research Project	

4. TITLE AND SUBTITLE

The Doom of My Enemies: Dark Networks and Tactical ISR

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Colonel Phillip A. Stewart

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Colonel Murray Clark

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT

Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

This project advances two propositions. First, that "dark" or "shadow" networks, which often operate from and within ungoverned areas, pose an increasing and significant threat to U.S. national interests. Understanding both the nature of ungoverned spaces and the types of organizations that create and perpetuate them will enable commanders and decision makers to optimize their use of available monitoring and targeting capabilities against these threats. Second, that tactical Intelligence, Surveillance, and Reconnaissance (ISR)--and the MC-12W "Liberty" aircraft in particular--constitutes a powerful capability for Combatant Commanders tasked by national leaders to locate and target shadow networks. Two important corollaries spring from this second proposition; primarily, that using the MC-12 in this role may quickly elevate the effects of "tactical" ISR to the strategic level. Finally, that integrating the four functions of the MC-12 ISR *system*—also known as the Four Pillars of tactical ISR—creates synergistic effects that reap great value for the nation across a surprising spectrum of likely uses. In light of predicted budget shortfalls, tactical ISR provides a relatively low-cost and flexible capability to counter many of the most elusive threats of the 21st century.

15. SUBJECT TERMS

Shadow Networks, Dark Networks, Ungoverned Areas, Failed States, Weak States, Tactical ISR, MC-12

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	32	

USAWC STRATEGY RESEARCH PROJECT

THE DOOM OF MY ENEMIES: DARK NETWORKS AND TACTICAL ISR

by

Colonel Phil A. Stewart
United States Air Force

Colonel Murray Clark
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Phillip A. Stewart

TITLE: The Doom of My Enemies: Dark Networks and Tactical ISR

FORMAT: Strategy Research Project

DATE: 6 April 2011 WORD COUNT: 6,565 PAGES: 32

KEY TERMS: Shadow Networks, Dark Networks, Ungoverned Areas, Failed States, Weak States, Tactical ISR, MC-12

CLASSIFICATION: Unclassified

This project advances two propositions. First, "dark" or "shadow" networks, which often operate from and within ungoverned areas, pose an increasing and significant threat to U.S. national interests. Understanding both the nature of ungoverned spaces and the types of organizations that create and perpetuate them will enable commanders and decision makers to optimize their use of available monitoring and targeting capabilities against these threats. Second, tactical Intelligence, Surveillance, and Reconnaissance (ISR)--and the MC-12W "Liberty" aircraft in particular--constitutes a powerful capability for Combatant Commanders tasked by national leaders to locate and target shadow networks. Two important corollaries spring from this second proposition; primarily, that using the MC-12 in this role may quickly elevate the effects of "tactical" ISR to the strategic level. Finally, that integrating the four functions of the MC-12 ISR *system*—also known as the Four Pillars of tactical ISR—creates synergistic effects that reap great value for the nation across a surprising spectrum of likely uses. In light of predicted budget shortfalls, tactical ISR provides a

relatively low-cost and flexible capability to counter many of the most elusive threats of the 21st century.

THE DOOM OF MY ENEMIES: DARK NETWORKS AND TACTICAL ISR

My eyes have seen the downfall of evil;
My ears have heard **the doom of my enemies**

- The Sabbath Psalm, Psalm 92, Verse 12

In April of 2008, Defense Secretary Robert Gates made a stunning announcement. He directed the Air Force to design, produce, and field a new weapon system to assist in the wars in Iraq and Afghanistan.[1] While the SECDEF often asks a military service to deliver new capability, in this case, the proposed timeline surprised his audience. Secretary Gates directed the Air Force to deliver this new aircraft to the warfighter in less than a year. In an era when major weapons programs take years, or even decades to deliver, delivering one to the field from scratch in a matter of months seemed unlikely. Yet the Air Force did just that.[2] The new weapons system was a tactical intelligence, surveillance, and reconnaissance (ISR) aircraft called the MC-12. The fielding of the MC-12 marked the fastest fielding of a major aircraft program since the P-51 in World-War II.[3] In addition, to complicate the task, due to the rapid timeline, the Air Force delivered the MC-12 direct from the factory to the front lines with no operational or developmental testing – another extremely risky undertaking. The successful fielding of the MC-12, from acquisition to combat maturity, is considered a huge success and the first year of combat operations in Iraq went amazingly well.[4]

Why was it necessary to deliver this capability to the warfighter so rapidly, and in so doing, accept such tremendous risk? Secretary Gates recognized the growing menace insurgents in Iraq and Afghanistan posed to our troops and was trying to give Combatant Commanders a tool to target them. Coalition forces in Iraq initially asked

the MC-12 leadership team for assistance in the search for improvised explosive devices (IEDs).[5] While successful in this mission, it quickly became apparent to warzone planners that the new MC-12 was capable of delivering much more to the warfighter. In fact, the military stumbled upon an even greater capability. Over the year, America's warriors discovered while the MC-12 team was good at detecting IEDs, they were exceptional at targeting dark networks. Most importantly, they learned Combatant Commanders can optimally use tactical ISR to achieve strategic effects by targeting the dark networks and the ungoverned spaces from which they operate.

This paper makes two propositions. First, a rapidly emerging threat – known as dark networks, operating from the sanctuaries provided by failed states and ungoverned spaces – poses a severe challenge to U.S. national interests. Second, this new capability, called tactical ISR, is best used by today's Combatant Commanders to target dark networks. In so doing, tactical ISR achieves strategic effects.

The term "dark or shadow network" is explained in detail later, but in short, it refers to any network expressly designed for nefarious purposes. For example, terrorist networks, IED networks, insurgency networks, narcotics networks, kidnapping networks, and money-laundering networks are all examples of typical dark networks.

In addition, while the MC-12 is optimized for work with Special Operations Forces (SOF), it is also flexible enough to work with regular U.S. and coalition forces or indigenous foreign troops as well. This ability to work with troops of any experience level makes tactical ISR an extremely flexible and attractive asset to Combatant Commanders in nations with fledgling or under-developed democracies. Also, when allowed, the MC-12 is the ideal platform to support law enforcement forces (foreign or

domestic) and interagency units in a wide variety of operations.[6] Thus, tactical ISR in general – and the MC-12 specifically – is an amazingly flexible and adaptable platform, and should be the platform of choice for any geographic Combatant Commander interested in targeting and defeating dark networks and monitoring ungoverned spaces.

Dark Networks and Ungoverned Spaces

The last three decades have witnessed tremendous increase in globalization. The same technology improvements that, according to economist Thomas Friedman, have "flattened the world" and ignited global trade have enabled a parallel rise of organizations that would use similar technology advancements for sinister purposes.[7]

> The globalization of trade, finance and human travel across international boundaries in the commercial world has an analogous dark side as well. Criminal and terrorist networks are intermingling to construct their own "shadow globalization," building micro-markets, and trade and financial networks that will enable them to coordinate nefarious activities on a global scale.[8]

These networks, which are formed under shadow globalization, are called "dark networks" or "shadow networks."[9] Sometimes the press or media refers to them as non-state actors, but most non-state actors are not dark networks. Many non-state actors, such as Private Volunteer Organizations (PVOs) and Non-Governmental Organizations (NGOs) are positive forces in the international system. Dark networks are not.

The study of dark networks and their impact on society is a relatively new field. It began to evolve in the late 1990s and early 2000s as a subset of the study of social network theory. In their 2003 journal article "Dark Networks as Problems," Jorg Raab and H. Brinton Milward were among the earliest to focus exclusively on dark networks and to point out while there are "bright or collaborative networks…(which) are seen as appropriate devices to tackle public management and coordinate political, social, and

economic action"[10] there also appears to be a "realization that there is a set of individuals and organizations that constitute a network striving to achieve ends that create collective-action problems for governments all over the world."[11] These organizations, which created collective action problems, became known as dark networks.

Of significance, Raab and Milward wrote their paper in 2003, long after the 9-11 attacks. It indicates the world was caught flat-footed against the threat of dark networks. This isn't to say dark networks were not conceived of prior to 9-11. However, it merely points out the preponderance of study on dark networks is a post 9-11 endeavor and the impact of dark networks is still largely absent from much of U.S. military doctrine.

One possible reason the subject of dark networks is largely absent from much of U.S. warfighting doctrine is because, until recently, the military considered shadow networks to be criminal, not military, organizations. As such, they were a law-enforcement problem. This view has started to change. The 2011 "National Military Strategy of the United States" (NMS) points out United States' interests are increasingly tied to non-state actors.[12] The NMS goes on to say the changing distribution of world power "indicates a multi-nodal world characterized more by shifting, interest-driven coalitions…than by rigid security competition between opposing blocs" and "non-state actors such as criminal organizations, traffickers, and terrorist groups find a nexus of interests in exploiting the commons."[13] [14]

Today, we understand shadow networks comprise a large category of organizations including drug cartels, terrorists, insurgents, criminal organizations, and

any group that has sinister objectives. It is no longer possible, and probably counter-productive, to segregate them into "military challenges" and "law enforcement challenges." The nexus between the two groups has rendered the distinction irrelevant. This fact does not mean we should suspend *posse comitatus* and let the military engage in crime fighting, nor that police forces should engage in counter-insurgency operations. It merely indicates dark networks have identified a seam in U.S. security operations and this seam needs to be closed. In a recent study by the Center for a New American Security titled "Crime Wars," Bob Killebrew and Jennifer Bernal point out: "Crime, terrorism, and insurgency are interwoven in new and dangerous ways that threaten not just the welfare but also the security of societies in the Western hemisphere."[15]

Raab and Milward also highlight this apparent seam when they state: "There is increasing evidence of a close connection between Al Qaeda and the failed states of Liberia, Sierra Leone, and Burkina Faso in West Africa."[16] This is not because of any shared ideology between Al Qaeda and the leaders of these failed states. Instead, their relationship springs from Al Qaeda's need to exchange cash for diamonds and weapons to operate.[17] The world's nongovernmental organizations witnessed what the arm-for-diamonds trade was doing to destroy West Africa, and responded by coining the phrase "blood diamonds" in the early 2000s.[18] This awakening of world conscience, along with the 9-11 attacks, helped promote the study of dark networks and ungoverned spaces.

One notable effort to understand shadow networks in U.S. doctrine comes from the 2010 "Joint Operating Environment," (the JOE) published by U.S. Joint Forces Command. The JOE points out that shadow globalization has created "bazaars of

violence" whose ease of access and anonymity create virtual organizations supported by shadow financial organizations which can coalesce, plan, attack, and then dissolve all before the U.S. even knew they were a threat.[19] [20] In addition, the JOE points out "we should expect shadow globalization to encourage this outsourcing of criminality to interface increasingly with insurgencies, with perhaps hundreds of groups and thousands of participants."[21]

If you think dark networks are a trivial power on the world stage, think again. The current global financial impact of these shadow networks is $2-3 trillion annually, and economists predict that by 2030 dark networks could represent 1/3 of total global GDP.[22] In "Crime Wars," Killebrew and Bernal point out the power of shadow networks continues to rise, and in many cases, will trump the power of some nation-states.[23] Indeed, in several Combatant Commander's AORs, notably AFRICOM and SOUTHCOM, this has already happened. Guinea-Bissau, a country in West Africa, has become Africa's first narco-state, and Killebrew and Bernal consider Venezuela and Columbia to be along similar dangerous paths -- an issue which is sure to pose challenges for SOUTHCOM.[24] [25] Meanwhile, NORTHCOM must reckon with a growing narco-insurgency based in Mexico, our closest neighbor to the south.[26]

The terms narco-insurgency and narco-terrorist are relatively recent additions to the lexicon of military doctrine. Recently social scientists have begun to see a growing parallel between dark networks and insurgent networks. Indeed, the activities of criminal networks have in many places acquired the characteristics of an insurgency.[27] Military doctrine traditionally defines "insurgency" as an attempt to takeover or overthrow a government. In narco-insurgencies, however, that is not necessarily the

case. According to Killebrew and Bernal, during narco-insurgencies, shadow networks "attempt to *weaken or disrupt* the functions of government" not overthrow them.[28] Dr. Jennifer Hazen, a Research Fellow and Lecturer at the LBJ School of Public Affairs at the University of Texas, agrees with this significant distinction. Hazen, who has years of studying dark networks abroad, points out certain dark networks, such as narco-terrorists, do not seek political goals nor do they aim to overthrow governments. Instead they take measures to ensure they can continue their illicit and profitable activities unmolested.[29] They use corruption, intimidation, and secrecy to ensure their highly profitable operations can continue. As Hazen points out, "you don't see drug cartels marching on Mexico City, as you might an insurgent/rebel group."[30] This isn't to say narco-insurgents are not a threat—they are simply a *different* kind of threat. Hazen says these insurgencies are a threat to the nation's security, but not necessarily its sovereignty.[31] Killebrew and Bernal agree: "These are insurgencies not of power, but of greed…and profit is now a motivation for insurgency, along with religion, ideology, nationalism and other causes."[32]

One prerequisite these shadow networks need to operate effectively is access to a sanctuary of some sort. Even in the age of globalization, most shadow networks require a territorial base, either for the production of their illegal goods or as a refuge for planning, training and recovering.[33] Usually, they establish these sanctuaries in failed states or the ungoverned spaces of the world. Currently, narco-terrorists, drug cartels, and large criminal syndicates control and operate a large portion of the world's ungoverned spaces. Ironically, the term "ungoverned space" is a misnomer. Such places are usually governed, just not by any recognized nation-state. Instead criminal

cartels, drug runners, warlords, smugglers, or terrorist organizations govern them. Indeed, shadow networks often try to create and enable the conditions for these ungoverned spaces to exist, so that they can operate out of them unmolested.

In many parts of the world ungoverned spaces exist because shadow networks want them to exist. Indeed, shadow networks work hard to ensure ungoverned areas continue to exist in order to provide sanctuary and freedom, in the same manner the U.S. works to ensure it has access to the world's global commons for its trade and defense. To highlight this, Killebrew and Bernal point out that to ensure their access and to create ungoverned spaces, "Criminal cartels, gangs and other illegal armed groups are today spending hundreds of millions of dollars a year to undermine governments…when corruption proves insufficient, they turn to intimidation and violence."[34]

While the ungoverned spaces and failed states of the world provide sanctuary to various dark networks, perhaps the most fruitful sanctuary—from the perspective of a dark network—is actually a weak state. Prior to the 1980s, political scientists tended to refer to nation-states as either functioning or failed. As study on the subject matured, a third category--called weak states--began to emerge.[35] Eventually, political scientists began referring to different categories of ineffective governments as weak states, failed states, shadow states, and collapsed states.[36] Dr. Ken Menkhaus, a Political Science professor from Davidson College, in his paper "State Fragility as a Wicked Problem," argues that when dealing with a weak state, the most important analytic task for a strategic leader is to determine the government's level of political capacity and willingness on the part of its leaders to address their government's fragility.[37]

On the surface, this sounds like a simple task. Why would leaders of a struggling nation not want their state to be as strong as possible? The reality, according to Menkhaus, is actually much different. Sadly, many of the weak states of the world are failing because their leaders want them to.[38] Why? Because being an elite leader in a failed or weak state is often more profitable than having the same position in a successful nation. Indeed, "state fragility may be seen as an acceptable or even optimal solution, not as a problem to be solved."[39] Profits made from graft, kickbacks, laundering, and drugs often dwarf government tax revenues.[40] Menkhaus refers to these warlord, or narco-states as "able, but unwilling" states.[41] Their leaders are "able" to prevent their nation from being exploited, but "unwilling" to do so because the profits are too great. These warlord states prove to be fertile ground for dark networks.

In Menkhaus' example above, the states unwillingness to provide law and order creates a symbiotic relationship enjoyed by both the shadow networks that are provided sanctuary, and the government elites who welcome them. In the 1990's, Liberia under Charles Taylor was a classic example of a warlord state. In exchange for vast profits, Taylor provided sanctuary for a host of shadow networks, including Al Qaeda. He provided diplomatic passports, flagged their planes and ships to give a certain degree of legitimacy to their smuggling, and made huge profits trading cash for diamonds, weapons, and gold.[42]

The critical question for today's strategic leader when dealing with the elites of a weak or failing state is: Are you dealing with an "able, but unwilling," or an "unable, but willing" state? The difference when framing the environment or performing operational design could be massive. In certain war torn places of the world, most notably Africa,

"the point of war might not actually be to win it, but instead to engage in profitable crime under the cover of warfare…violence becomes central to the advancement of those with a vested interest."[43] To make matters worse, "able, but unwilling" states often use their condition of failure as a lure for state-building assistance, which is then pocketed by local elites for private gain.[44] The strategic point Menkhaus drives home is "state-building policies designed for tame cases of state failure, but applied instead to wicked cases (able, but unwilling) are destined to fail and possibly make matters worse."[45]

Emerging dark networks, and the ungoverned spaces in which they lurk, pose a growing and serious threat to U.S. National Interests. The attacks on September 11th, nearly ten years ago, demonstrated the catastrophic destruction a dedicated and sophisticated shadow network can unleash on an unprepared government. The 9-11 attacks were not sponsored by any nation-state, and were not organized or financed by any recognized, legitimate authority. At the time of the attacks, Al Qaeda was a mature shadow network, operating under the sanctuary of an "able, but unwilling" Taliban government, with access to large sums of money through a mature financial shadow network. In the decade that has followed those attacks, while the Taliban has been overthrown and Al Qaeda greatly weakened, other shadow networks have increasingly flourished and the corresponding threat from those networks has also grown. Pirate networks operating off the Horn of Africa are an example of this. Since 2007, 640 ships have reported pirate attacks in the vicinity of the HOA, and Somali pirates have taken over 3,150 hostages and received over $180 Million in ransom payments.[46] In addition, the sinister, but highly profitable activity has raised concerns that profits from piracy and

ransom will undermine regional security and could possibly contribute to other threats, including terrorism.[47]

Shadow and dark networks currently pose a serious threat to all areas of U.S. national interests (not just security) and the threat will continue to grow.[48] In the latest National Security Strategy, President Obama addressed the rising power of dark networks and our need to confront them. President Obama states: "We need to disrupt and dismantle transnational terrorist and criminal organizations; and ensure our national resilience in the face of the threat and hazards."[49] In addition, the NSS points out:

> The threat to our people, our homeland, and our interests has shifted dramatically in the last 20 years. Competition among states endures, but instead of a single nuclear adversary, extremists who may not be deterred now threaten the United States. Instead of a hostile expansionist empire, we now face a diverse array of challenges, from a loose network of violent extremists to states that flout international norms or face internal collapse. In addition to facing enemies on traditional battlefields, the United States must now be prepared for asymmetric threats, such as those that target our reliance on space and cyberspace.[50]

Understand the threat from non-state actors comes not only from today's violent extremists and third world insurgencies. The very existence of shadow organizations--and the ungoverned spaces they create and--works counter to all U.S. national interests in ways that go beyond just a threat to our national security.

Shadow networks undermine our economic prosperity by piracy and the siphoning of billions of dollars a year in oil (called oil bunkering).[51] Pirate shadow networks menace the waters in areas from which the U.S. will be importing over 25% of its oil by 2015 – over twice the amount it currently gets from the Middle East.[52] This is not just a United States concern. Crime and insecurity in the maritime domain interfere

with open sea lines of communication, can limit global trade, and have damaged the global economy.[53]

These non-state actors undermine our diplomatic efforts to support fledgling democracies all over the world by fueling corruption which de-legitimizes local governments. According to Dr. Hazen shadow networks pose a threat to democracies because the corruption they bring means politicians are making decisions based on cash flow, not on good governance or the need of citizens.[54] This corruption can be devastating to young democracies and has caused a phenomenon known as "retreat from the state" in many African nations."[55] This eroding of democracy works directly to counter National Security Presidential Directive 50 (NSPD 50), signed by George H.W. Bush which "commits U.S. policymakers to consolidate democratic transitions and bolster fragile states, promote regional stability, and stimulate African economic development and growth."[56]

Also, to ensure access the ungoverned spaces they desperately need, dark networks work counter to the "promotion of our values" by promoting rape, torture, and murder as intimidation tools. The Janjaweed militia in Darfur, the *Fuerzas Armadas Revolucionarias de Colombia (*FARC) in Colombia, and the brutal drug cartels in Asia and Mexico are all examples of this.[57]

Due to their negative impact on so many of our national interests, shadow networks are sure to pose a huge challenge in every Combatant Commander's AOR. To make matters more difficult, the U.S. military has been very slow to recognize the threat dark networks present and to posture itself accordingly.[58] As a result, today's Combatant Commander's have very few tools to counter dark networks when our

national leaders task them to do so -- something which may become more common in the upcoming decade as we drawdown from Iraq and Afghanistan and get more involved in Africa and South America as threats there grow.

As pointed out above, the U.S. was slow to recognize the growing menace posed by dark networks – focusing instead on classic state-versus-state confrontation, and the weapons systems required to fight them -- yet we have begun to wake up to it. In a September 2010 speech to the American Legion, The Secretary of the Air Force, Michael Donley, pointed out:

> …the future is shaped by the broad scope of potential threats and uncertainties in the global environment – from terrorist movements to newly developing nuclear powers, from failed states and ungoverned areas…and it is being shaped by the globalization of information and other technologies and the rapid pace of technological change.[59]

Senior military leaders also recognize the rising and threat. The 2010 Combat Air Force Strategic Plan, authored and endorsed by the three and four-star Combat Air Force Generals states:

> Rapidly evolving technology enables a single individual (sic) act or person to generate strategic effects…from non-state actors, terrorists, and criminal networks exploiting the seams created by ungoverned spaces…the complexity of the global security environment is changing.[60]

While the military may have been slow to recognize the threat of dark networks, they have acted rapidly to help counter it. The Air Force has recently taken several dramatic steps to posture itself to assist Combatant Commanders in the fight against shadow networks. Most notably, they completely revolutionized the way they deliver ISR capability to the Combatant Commanders by restructuring ISR organizations. The result is a much more empowered, flexible, and capable network of ISR organizations

called Distributed Common Ground Stations (DCGS).[61] Another initiative was the rapid fielding of a capability known as tactical ISR to provide immediate assistance to geographic Combatant Commanders. Tactical ISR units and DCGS's are the most effective way for Combatant Commanders to target shadow networks and monitor ungoverned spaces.

What is Tactical ISR?

No doctrinal definition of "tactical ISR" exists in Joint Publications and tactical ISR is such a new arrival to modern battlefields that writers of doctrine have yet to tackle exactly what it is, and what it is not. Tactical ISR was officially born when the Air Force fielded an asset called the MC-12 in 2009. The fielding of the MC-12, combined with the DCGS, created important new battlefield synergies. These synergies were united into a single enterprise called tactical ISR. Tactical ISR has only been on the battlefield since roughly 2009 and it differs greatly from its cousins, operational and strategic-level ISR.

Differentiating between the strategic, operational, and tactical levels of ISR is often as difficult as differentiating between the strategic, operational, and tactical levels of modern warfare. Intelligence experts generally consider either satellites or the U.S. high-altitude reconnaissance fleet – such as the U-2 and the Global Hawk – as strategic level ISR assets. Similarly, operational level ISR assets are MQ-1 Predators, MQ-9 Reapers, or our heavy-fixed-wing assets – such as the RIVET JOINT, AWACS, and J-STARS aircraft. Tactical ISR assets, however, are normally propeller driven, light-fixed-wing airframes. For this reason, senior leaders in the Pentagon sometimes refer to them as "Light ISR."[62]

We distinguish tactical ISR from operational and strategic level ISR in two main ways. The first characteristic that distinguishes tactical ISR from operational and strategic ISR is the organizational level of the supported user. Tactical ISR operates in support of small tactical units, almost always providing real-time information and feedback. Real-time feedback means there is usually little requirement for post mission analysis. Unlike traditional ISR assets that process, exploit, and disseminate (PED) at a later time, tactical ISR mission PED teams normally produce a "play-by-play" of the unfolding action. To facilitate this, higher headquarters usually task Tactical ISR teams in direct support to ground units below the battalion level. Conversely, strategic level ISR assets may never be tasked to a particular ground unit, and instead provide theater-level imagery at the direction of theater commanders to the Corps or Division headquarters.

The manner in which the Air Force presents Tactical ISR units to the supported Combatant Commander is the second, and most important, characteristic that distinguishes tactical ISR from other forms of ISR. Strategic or operational-level ISR assets -- such as the U-2, the Global Hawk, or satellites -- are never tasked OPCON or TACON to the supported commander. Under Joint Doctrine, the STRATCOM Commander always retains OPCON of these strategic and operational-level intelligence platforms. On the other hand, tactical ISR units are forward deployed directly into the AOR and are attached COCOM to the Combatant Commander, OPCON to the JFACC, and TACON to the supported unit, for integration with other assigned theater assets.

The exact definition of tactical ISR is much like the Supreme Court definition of pornography: "Hard to describe, but you know it when you see it."[63] Tactical ISR is a

new and unique branch of ISR – separate and distinct from both operational and strategic-level ISR.

Tactical ISR is so valuable to the warfighter—and so useful when targeting dark networks--because it fuses four traditional ISR functions into a single team. This team – united under a single commander to achieve unity of effort – creates powerful battlefield synergies. These unified functions are called the four pillars of tactical ISR. The four pillars are: Full Motion Video (FMV), Signals Intelligence (SIGINT), Intelligence, and Integration.[64] These "pillars" have existed for years; however, the MC-12 program was the first to unite them under a single commander and meld them into a cohesive unit.

Full motion video (FMV) describes the capability to capture and broadcast live video of the battlefield and exploit it real-time by intelligence analysts, while also disseminating both the video and exploited product to the user in near-real-time. For example, imagine the broadcast of O. J. Simpson in the white Ford Bronco. The camera on the bottom of the helicopter captured the video and the news reporter who narrated the action provided the exploitation (interpreted it and told you what was occurring). That is a simplified version of FMV. FMV captures the data, intelligence analysts exploit and analyze the data, and the entire product is then broadcast to the user. The ability to do this in near-real-time has proven a huge asymmetrical advantage in combat by helping to lift the fog of war.

FMV capability answers questions such as: Is that a car with insurgents, or a car with families going to pray? Is that a farmer carrying a shovel, or a paramilitary guard carrying a gun? Is that a construction crew fixing a pothole ahead of the convoy, or is it an insurgent group planting an IED? Is that an ambush ahead, or a broken down truck?

FMV answers these questions. In recent years, warfighter demand for FMV capability has exploded. Just five years ago, FMV overhead was considered “nice to have.” Now, elements of the military will no longer go into combat without it. Ground units now see FMV as a battlefield necessity, and demand will only continue to grow.[65]

FMV has a significant limitation, however. It is reactive in nature. FMV is wonderful about showing the user what has happened, but it is almost impossible to use FMV to prevent something from occurring in the first place. It can monitor, but not anticipate. Thus it is reactive in nature. The ability to be proactive requires an additional capability, such as SIGINT.

Signals Intelligence, or SIGINT, is the second pillar of tactical ISR. Almost all SIGINT functions of the MC-12 are classified though, and can’t be discussed in detail here. Simply put, SIGINT finds the enemy (ideally before they act) and enables the tactical ISR team to be proactive. In addition, special software on the MC-12 fuses inputs from the FMV and SIGINT operators to achieve even more synergy. Operators can work together to eliminate false trails and explore leads more quickly – all in an attempt to close the find-fix-finish-exploit-asses (F3EA) loop more quickly – and get that information to the user. Basically, SIGINT finds the target, and FMV fixes the target. This fusion of information is incredibly powerful. In the past, teams often relied on Human Intelligence (HUMINT) or other less reliable methods to find the target. Using SIGINT is less risky and more reliable. Using FMV to positively identify the target adds fidelity to the endeavor.

Intelligence is the third pillar of tactical ISR. Intelligence teams play a critical role in tactical ISR squadrons. The first function of the Intelligence team is to provide all the

processing, exploitation, and dissemination (PED) of the intelligence to the user. An ISR exploitation cell (ISREC) performs this function. The ISREC works seamlessly with the aircrew to provide information to the user via PED in near-real-time.

Second, the Intelligence team helps the user determine who to target or monitor in the first place. This can be key when targeting shadow networks because their command structures are usually very nebulous. Imagine an enemy's organizational chart, with organizational structure, command relationships, and order-of-battle. At first, the boxes and lines would be blank. The Intelligence team works to fill in those blanks, using a multitude of available sources, and provides this information to the user. In addition, once the wiring diagram starts to fill in, the Intelligence team determines which connections or boxes are exploitable or targetable, as well as continuously updates and refines the information based on the results of ongoing missions. Finally, Intelligence teams interact continuously with the ISREC and the supported user to refine and update the picture and enhance situational awareness.

The ability to determine whom to target is important, but how does the tactical ISR team determine what to target in the first place? Which segment of the shadow network is most vulnerable? Here, integration comes into play. Integration is the fourth, and most important, pillar of tactical ISR. Tactical ISR units deploy forward and attach using COCOM to the AOR Combatant Commander. Normally, they are OPCON to the Joint Force Air Component Commander (JFACC) and can even be imbedded directly with the supported user in a TACON role. Members of the tactical ISR integration team liaison directly with the supported user to assist the supported commander in determining what and who to target to achieve maximum desired effect.

An example of successful integration occurred during the Iraqi election in March of 2010. At the time, the supported commander -- an army Division Commander -- was worried insurgents in his AOR would use vehicular IED's to disrupt the election process. His intelligence teams indicated his AOR was highly susceptible to this type of intimidation, and indeed, history suggested IED attacks were likely. The MC-12 integration team worked directly with the staff of the supported commander to target the IED network in the AOR. Then, the Air Force MC-12 Intelligence team plugged directly into the existing Army Intelligence network and worked with them to develop and gather information on the network. The tactical ISR team exploited this IED network over a six-week period leading up to the elections. The details of the operation are classified; however, the results are not. On the day of the Iraqi national elections, as predicted, insurgents placed multiple IED's throughout Iraq to intimidate voters and disrupt the process. However, in the AOR supported by the MC-12s and in which the supported commander had a plan to target and disrupt this tactic, not a single IED exploded on Election Day.[66] This example highlights both the importance of staff integration by forward deployed teams and planning integration to the overall execution process of tactical ISR. The importance of integration cannot be overstated and the same level of teamwork generated cannot be achieved using traditional "reach back," which is common with Air Force ISR units.[67]

To summarize how the four pillars of tactical ISR work: The integration team works with the supported commander who determines <u>what</u> to target to achieve the desired effects. The Intelligence team works with the supported user to determine <u>whom</u> to target and also provides the real-time PED. The SIGINT team finds the target.

The FMV team fixes and identifies the target for follow-on action. The supported unit determines the follow-on action. The four pillars of tactical ISR, united under a single commander to provide unity of action, and forward deployed into the AOR to integrate with the supported commander's planning staff, allows unmatched synergy and effectiveness and makes the MC-12 squadrons a unique, powerful, and flexible tool for the combatant commander. They are the perfect weapon against shadow networks.

How Can Tactical ISR Help Combatant Commanders?

Tactical ISR in general--and the MC-12 specifically—has the unique capability to target shadow networks, and is the weapon of choice to do so. Its fusion of SIGINT, FMV, and Intelligence make it ideal to lead the fight. When Combatant Commanders decide to target dark networks as a means to a broader objective, the MC-12 stands alone. MC-12 squadrons and detachments are rapidly deployable, self-sustaining, and fit seamlessly into any existing organizational structure, or act as a stand-alone capability. They can work with Special Operations or conventional U.S. Forces and can also work with indigenous troops, if desired. The aircraft are customized, but rugged, and require very little specialized equipment to operate and maintain. They can operate out of almost any paved runway in the most austere situations (security conditions permitting). The bottom-line is tactical ISR should be at the top of any Combatant Commanders "wish list" when tasked with the inevitable challenge of targeting shadow networks.

MC-12 units provide flexibility and have many wartime uses even beyond targeting dark networks. Their unique blend of FMV, SIGINT, and intelligence also make them ideal for a range of other combat roles and missions. For example, tactical

ISR teams are a great personnel recovery asset. They are an invaluable resource for providing overwatch to troops in the field, or convoy escort duty.[68] In addition, they can provide world-class assistance to civilian authorities during a disaster response, as they did during the Haiti earthquake assistance effort. FMV capability is one of the first and most important assets needed by JTF commanders in a disaster response, and unmanned RPVs may not be initially suited to this task due to airspace congestion caused by incoming humanitarian relief.[69] [70] Instead, manned tactical ISR is a much better choice. Indeed, geographic commanders are sure to find a multitude of uses for this newest tool in their toolkit. Tactical ISR is flexible, tailorable, and capable.

Finally, tactical ISR platforms are also relatively inexpensive, easy to maintain, and have a great role in building partnership capacity (BPC) with friendly nations. Developing nations who wish to acquire an inexpensive ISR capability could acquire MC-12's and assist the United States with building partnership capacity. One of the first capabilities a young Air Force requires, after light-airlift, is a light-ISR capability (removing the SIGINT element turns "tactical ISR" into "light-ISR").[71] An MC-12 costs roughly $17 million, and an entire squadron of MC-12s can be purchased for the same cost of a few 5th generation F-22 fighter aircraft. Also, propeller-driven light-fixed-wing aircraft are relatively inexpensive to operate, and have much smaller operating and maintenance budgets than large jet-engine airplanes. In addition, with mission-capability rates well into the 90%s – they are reliable. In short, MC-12s provide tremendous value. They are inexpensive to buy, cheap to operate and maintain, and very flexible and reliable. In the fiscally constrained defense budgets of the future, tactical ISR units, such as the MC-12 will be a wise investment.

Conclusion

This paper began with two main premises. First, dark and shadow networks operating in the failed states and ungoverned places of the world pose a rising and significant threat to all categories of U.S. national interests. Second, tactical ISR in general, and the MC-12 in particular, is the weapon system of choice for any and all Combatant Commanders who are tasked by national leaders with the daunting task of targeting these shadow networks.

In support of my first premise, I showed how the rising menace of non-state actors, particularly in the form of dark and shadow networks, pose a severe threat to U.S. national interests. Shadow networks not only threaten our national security, but also pose a threat to our economic prosperity, our values, and international interests as well. They are a threat in every geographic combatant commander's AOR and it is becoming increasingly urgent to target these shadow networks more aggressively.

Doctor Jakub Grygiel, an International Relations professor at Johns Hopkins, explains why it is more important today to monitor ungoverned spaces and target dark networks than it was in years past. In his 2009 "Vacuum Wars," Dr. Grygiel explains how in the pre 9-11 world, United States' intervention into the failed states of the world was mainly driven by humanitarian concerns, not concerns for our national security.[72] Grygiel writes: "Interventions such as in Somalia, Bosnia, or Haiti were driven by a Western public shocked by vivid images of suffering and slaughter rather than by a sense that collapsed states directly threatened U.S. national security."[73] The 9-11 attacks and the growth of dark networks in the days since have changed this perception. According to Grygiel, the United States government now realizes these

ungoverned spaces, and the shadow networks which lurk inside, are a serious threat because the mischief created in failed states "starts from within them and subsequently spills over to others."[74] They are not only humanitarian disasters, but security threats as well.[75] U.S. intervention in failed states may become much more commonplace in the upcoming years due to this realization. Why? To paraphrase noted author Thomas Friedman: "The lesson of 9/11 is that if we do not visit the world's bad neighborhoods …they will surely visit us."[76]

In support of my second premise, I explained how a new capability, called tactical ISR, has emerged rapidly in the form of a weapons system called the MC-12. MC-12 units are uniquely suited to assist Combatant Commanders in their struggle against dark networks and ungoverned spaces. Today's Combatant Commander can use tactical ISR to achieve strategic effect by targeting and eliminating those non-state actors and shadow networks in their AOR.

Finally, I pointed out while MC-12 units are ideally suited to target dark networks, they are also capable of a wide and flexible array of missions all which provide much-needed and inexpensive capability to today's Combatant Commanders. Not only can they help target dark networks such as pirates in Somalia, drug cartels in Mexico, and insurgents in Iraq and Afghanistan, but they can also assist Combatant Commanders with critical missions such as personnel recovery, overwatch, humanitarian relief, and building partnership capacity. Clearly, if used optimally by strategic leaders, tactical ISR can be a global game changer and enhance national security by enabling the doom of my enemies.

Endnotes

[1] Tom Vanden Brock, “Newest manned spy plane scores points in war effort,” USA Today, June 2nd, 2010

[2] Tamir Eshel, “U.S. Air Force Deploys the Last MC-12 to Afghanistan,” Defense Update, July 13th, 2010

[3] Ibid.

[4] Ibid…in addition, the MC-12 program has been the DoD’s nomination, and finalist, for the Collier Trophy for the last two years. The Collier Trophy is an annual aerospace industry award given for the most outstanding aerospace feat for that year. Last year, the MC-12 finished second, behind the International Space Station.

[5] Personal recollection of Phillip Stewart, Colonel, USAF, Commander of the unit, and author of this paper.

[6] *Posse Comitatus* not withstanding

[7] Thomas L. Friedman, *The World is Flat: A Brief History of the Twenty-First Century*, (New York: Farrar, Straus and Giroux, 2005)

[8] U.S. Joint Forces Command, *Joint Operating Environment, 2010* (Norfolk, VA, March 2010), 61.

[9] The terms “dark network” and “shadow network” are used interchangeably throughout the paper, and can be considered synonyms. The person who coined the term is unknown, but the origination of the theory of dark networks will be explored later in the paper.

[10] Jorg Raab and H. Brinton Milward, “Dark Networks as Problems,” *Journal of Public Administration and Theory,* (Oct 2003): 237

[11] Ibid., 239

[12] Michael G. Mullen, Admiral, U.S. Navy, *The National Military Strategy of the United States of America*, (Alexandria, VA: The Pentagon, February 2011), 1.

[13] Ibid., 2.

[14] Ibid., 3

[15] Bob Killebrew and Jennifer Bernal, “Crime Wars,” Center for a new American Security, (September 2010): 6

[16] Raab and Milward, “Dark Networks as Problems,” 249

[17] Ibid., 425

[18] Ibid., 428

[19] U.S. Joint Forces Command, *Joint Operating Environment, 2010* (Norfolk, VA, March 2010), 61.

[20] Ibid., 61

[21] Ibid., 61

[22] Ibid., 61

[23] Killebrew and Bernal, "Crime Wars," 6.

[24] Andre Le Sage, PhD, "Nonstate Security Threats in Africa: Challenges for U.S. Engagement," *Prism* Vol. 2 No. 1 (December 2010): 68.

[25] Killebrew and Bernal, "Crime Wars," 7

[26] Ibid., 8

[27] Ibid., 7

[28] Ibid., 8

[29] Jennifer Hazen, PhD, Researcher and Lecturer, LBJ School of Public Affairs, University of Texas, Interviewed by author, Carlisle Pennsylvania, February 23, 2011

[30] Ibid.

[31] Ibid.

[32] Killebrew and Bernal, "Crime Wars," 8

[33] Raab and Milward, "Dark Networks as Problems," 431

[34] Killebrew and Bernal, "Crime Wars," 7

[35] Kenneth Menkhaus, PhD, "State Fragility as a Wicked problem," Prism, Vol 1, No. 2, (March 2010): 87

[36] Ibid., 87

[37] Ibid., 85

[38] Ibid., 98

[39] Ibid., 89

[40] Ibid., 94

[41] Ibid., 89

[42] Raab and Milward, "Dark Networks as Problems," 428

[43] Ibid., 428

[44] Menkhaus, “State Fragility as a Wicked problem,” 97

[45] Ibid., 98

[46] “Updating U.S. Counterpiracy Action Plan Gains Urgency as Piracy Escalates off the Horn of Africa,” United States Government Accountability Office, Testimony before the subcommittee on Coast guard and Maritime Transportation, March 15th, 2011, 4.

[47] Ibid., 1

[48] The four areas of U.S. National Interests are usually considered to be defense of the nation, economic prosperity, promotion of our values and promotion of our way of life.

[49] Barak Obama, *National Security Strategy* (Washington DC: U.S. Government Printing Office, May 2010), 15.

[50] Ibid., 17

[51] Le Sage, “Nonstate Security Threats in Africa: Challenges for U.S. Engagement,” 63

[52] Ibid., 64

[53] Ibid., 68.

[54] Jennifer Hazen, Op Cit

[55] Le Sage, “Nonstate Security Threats in Africa: Challenges for U.S. Engagement,” 68

[56] Ibid., 73

[57] Ibid., 74

[58] Killebrew and Bernal, “Crime Wars,” 5.

[59] Michael B. Donley, Keynote Speech presented at American Legion’s 92nd Annual National Convention, September 1st, 2010

[60] 2010 United States Combat Air Force Strategic Plan, “Securing The High Ground: Agile Combat Power,” Air Combat Command, Langley Air Force Base, VA, June 2010, 3

[61] Michael C. Sirak, “ISR Revolution,” Air Force Magazine, Vol. 93, No. 6, June 2010

[62] Norton A. Schwartz, “CSAF Vector 2010,” July 4th, 2010, 4. Light ISR is also usually lumped into a category with “Light Mobility Aircraft,” and “Light Attack Aircraft,” so called because they all operate on a light-fixed-wing platform. Practitioners in the field, however, prefer the term “tactical ISR,” which is a much more accurate description of its effect, and how it is referred to in this paper.

[63] Supreme Court Justice Potter Stewart, concurring opinion in *Jacobellis v. Ohio* 378 U.S. 184 (1964), regarding possible obscenity in the movie *The Lovers.*

[64] The Four Pillars of Tactical ISR is a model invented by the author.

[65] Robert M. Gates, "Quadrennial Roles and Missions Review Report," U.S. Department of Defense, January 2009, 25

[66] Personal recollection of the author, who was the commander of the unit and present throughout the entire operation. Details are classified and left vague on purpose.

[67] "Reachback," also known as "Remote Split Operations" refers to the Air Force practice of flying Remotely Piloted Vehicles (RPV's) in overseas AOR's from CONUS locations. Reachback is required in some cases because the Air Force currently forward deploys the vast majority of its ISR assets. The only way to do that is with reachback. The positive aspects of reachback are that it gives the service the ability to forward deploy large numbers of assets for long periods of time. The drawback is that reachback is less user friendly and inhibits the building of personal relationships, which the author argues are critical to success. The Air Force needs reachback, but it also needs some forward deployed personnel as well. Both capabilities are critical.

[68] In Iraq, no unit which had overwatch provided by MC-12's was ever surprised by an ambush or suffered casualties as the result of an IED…granted that was a less kinetic environment than Afghanistan, but in many cases tactical ISR was able to point out "possible danger ahead" to convoys and troops in the field successfully. Personal recollections of Col Stewart and documented on his end of tour citation.

[69] RPV's are Remotely Piloted Vehicles. Such as the MQ-1 Predator and the MQ-9 Reaper.

[70] Lt Col Rick Berryhill, Director of Operations, 186th ARW, Mississippi Air National Guard, telephone interview by author, March 17th 2011

[71] As a note, the C-12 aircraft, on which the MC-12 platform is based, also can provide a great light-airlift platform to emerging countries. Perhaps the two capabilities could be packaged, and when combined with a light attack capability (also in development), provide a small, flexible, and inexpensive start-up Air Force.

[72] Jakub Grygiel, PhD, "Vacuum Wars," *The American Interest,* August 2009, 40

[73] Ibid., 41

[74] Ibid., 41

[75] Ibid., 42

[76] Thomas L. Friedman, "9/11 Lesson Plan," *New York Times*, September 4, 2002