



OVERWATCH

*"The advancement and diffusion of knowledge is the only guardian of true liberty."
-James Madison*



THE JOURNAL OF THE MARINE CORPS INTELLIGENCE OVERSIGHT DIVISION

Volume 5 · Issue 1 · February 2016



Photo By: Lance Cpl. Tyler Ngiraswei

IN THIS ISSUE: FEATURE ARTICLE – BETTER INTELLIGENCE GATHERING, MILITARY MIGHT NEEDED TO COMBAT TERRORISM



Inspector General of the Marine Corps

The Inspector General of the Marine Corps (IGMC) will promote Marine Corps combat readiness, institutional integrity, effectiveness, discipline, and credibility through impartial and independent inspections, assessments, inquiries, investigations, teaching, and training.

The Intelligence Oversight Division

To ensure the effective implementation of Marine Corps-wide oversight of Intelligence, Counterintelligence, Sensitive activities (to include USMC support to law enforcement agencies, special operations, and security matters), and Special Access Programs. To establish policy and ensure their legality, propriety and regulatory compliance with appropriate Department of Defense/ Department of the Navy guidance.

Contact Information

Mail:

Director, Intelligence Oversight
Inspector General of the Marine Corps
Headquarters U.S. Marine Corps
701 South Courthouse Road
Building 12, Suite 1J165
Arlington, VA 22204

Intelligence Oversight Division Staff

GS15 Edwin T. Vogt, Director
Maj Christopher L. Doyle, Deputy Director

Inside This Issue

Features

- 3 A Message from the Director
- 4 Better Intelligence Gathering, Military Might Needed to Combat Terrorism
- 5 Time to Get Serious About Europe's Sabotage of US Terror Intelligence Programs
- 7 SITCC teaches language of aviation to Intelligence Marines
- 9 Intelligence Photographs in the News



Web Links

Senior Intelligence Oversight Official (SIOO)

<http://dodsioo.defense.gov/>

Marine Corps Inspector General

<http://www.hqmc.marines.mil/igmc/UnitHome.aspx>

Naval Inspector General

<http://www.ig.navy.mil/>

Message from the Director, Intelligence Oversight

I am pleased to announce that BGen (sel) Rick A. Uribe has assumed duties as the Inspector General of the Marine Corps. BGen Uribe is a KC-130 pilot and comes to IGMC from 3rd Marine Aircraft Wing, where he served as the Commanding Officer of Marine Aircraft Group-11. Welcome aboard Sir.



I am also pleased to announce that in coordination with and excellent support from Training and Education Command; we are nearing our goal to institute Intelligence Oversight training on MARINE NET. We hope to have it up and running within the next quarter. I ask that you have patience in the development process.

One of the articles this month argues for increased authorities by intelligence collection entities. A former member of the 9/11 Commission—calls on the President to “*use our intelligence assets more aggressively and act on them effectively.*” **Please note that the articles presented in these journals do not reflect the opinion of this office.** These articles are selected to provoke thought and discussion within our Marine Corps intelligence community. As always, we welcome suggestions or input from everyone.

Another article, an opinion piece, proposes US policy makers push back on European Union policies that will affect our ability to give and receive terrorism related intelligence to EU members. While we try to avoid political arguments, I believe this piece is important since it highlights the complexities of sharing with members of inter-governmental entities. When participating in multinational operations, we need to be aware of existing sharing agreements and foreign disclosure guidance. As always, when in doubt CYA...consult your attorney.

The Inspector General of the Marine Corps has recently upgraded all functional area checklists and removed those that do not provide a value to the commander. All Checklists will be attributed to the associated Standard Subject Identification Code (SSIC) for their respective orders. There will no longer be an FA 240 (Intelligence Oversight) checklist. The Intelligence Oversight checklist will now be the 3800 checklist. For Counterintelligence Marines, the Counter Intelligence checklist is in the process of revision and should be out in the very near future. Please contact IOC Branch at HQMC if you have input. This is the Inspector General’s effort to comply with the Commandant’s initiative to reduce the number of redundant training requirements or “lighten the pack.” The initiative gives commanders the ability to adjust training to the needs of their Marines.

As professionals, we should continually seek to engage others and learn from their perspectives. Please pass along your perspectives on this newsletter, or anything else relevant to our lines of effort, to myself or Major Chris Doyle (Christopher.L.Doyle@usmc.mil). Additionally, please consider writing for *Overwatch*.

Semper Fidelis,

Edwin T. Vogt

Director, Intelligence Oversight Division

Office of the Inspector General of the Marine Corps

Ph: 703-604-4518 DSN: 664-4518 Email: Edwin.Vogt@usmc.mil

Feature Article

Better Intelligence Gathering, Military Might Needed to Combat Terrorism

Slade Gordon
The Seattle Times

MORE than 10 years ago, the 9/11 Commission determined that the American tragedy took place, at least in major part, because we ignored al-Qaida's explicit declaration of war against the United States and because of serious defects in our intelligence system.

The director of the CIA at the time summed up the situation in midsummer 2001 as "the system was blinking red." But no one predicted either the nature or the exact timing of the 9/11 attacks, so no real defenses were mounted.

U.S. actions and reforms after 9/11 are largely responsible for the fact that we have suffered nothing comparable to 9/11 for 14 years, a fact for which both administrations deserve credit. Still, these reforms have not prevented less elaborately planned but still horrific incidents like the San Bernardino attack and the Boston Marathon bombing. And those reforms do not guarantee against additional incidents or an even larger one.

So we face a challenge today both new and similar. While the San Bernardino attack could be inspired, rather than planned, by the Islamic State, that group claims that it has operatives in the U.S. ready to take action. In many respects "the system is blinking red" — but obviously with no more specifics available than we had in the summer of 2001.

So what do we do to defend more rigorously against the next such potential attack?

First, we should restore to the National Security Administration the right to practice its metadata programs. Remember that those programs involved collecting called- and calling-overseas numbers and

data about their time, date and length. The notion that our intelligence agencies need basic information on whether terrorism suspects overseas have been corresponding with people in the United States is clearly and eminently reasonable.

Only when that information provided a warning of potential terrorist activity could our government seek court authority to gain access to the full content of those communications.

Second, Congress should make clearly valid and permanent the roving wiretap authority to account for replaceable cellphones, together with the "lone wolf" authority to target terrorist would-be inspired by, but not under the command of, the Islamic State or al-Qaida.

Third, the administration should increase its use of its Foreign Intelligence Surveillance Act statutory authority to collect intelligence against foreigners outside of the United States who have no legitimate claim to protection under our Constitution.

Finally, President Obama should use our intelligence assets more aggressively and act on them effectively.

All this may raise concerns about privacy rights.

Alan Charles Rand, a former member of the Privacy and Civil Liberties Oversight Board, created at the recommendation of the 9/11 Commission, recently wrote about "the apparent absence of any political abuse of electronic surveillance." His conclusion and the board's advice should be given great weight.

But that is not enough.

In this conflict, intelligence is a defensive weapon only.

The 9/11 Commission's first recommendation was to attack terrorists and their organizations where they lived. The commission said: "The U.S. Government must identify and prioritize actual potential terrorist sanctuaries. For each, it should have a realistic strategy to keep possible terrorists insecure and on the run, using all elements of national power. We should reach out, listen to, and work with other countries that can help."

The principal sanctuary today is the self-proclaimed Islamic State caliphate in Iraq and Syria. Some 200 Americans have traveled there to join. According to our director of national intelligence, James Clapper, some 40 of them have returned, numbers constantly increasing and all presenting real challenges.

We Americans will not destroy the Islamic State threat by “leading from behind” or delegating our duty to Vladimir Putin’s Russia or the ayatollah’s Iran. Nor have our occasional air attacks seriously undercut the Islamic State’s strength or its appeal. Only true U.S. leadership and military power can do that.

Such leadership could inspire effective assistance from France, many other NATO allies and from Arab states as well, many of which are more profoundly threatened by the Islamic State than we are. Doing nothing on our part would result in nothing being done.

For the next year, only President Obama can build this coalition and advance its cause. But each serious candidate for the presidency should be required to weigh in on what he or she would do to meet the increasing challenge of terrorism here at home.

Time to get serious about Europe’s sabotage of US terror intelligence programs

Stewart Baker
Washington Post

The intelligence tools that protect us from terrorism are under attack, and from an unlikely quarter. Europe, which depends on America’s intelligence reach to fend off terrorists, has embarked on a path that will sabotage some of our most important intelligence capabilities. This crisis has been a long time brewing, and up to now, the US has responded with a patchwork of stopgap half-solutions.

That’s not likely to work this time. We need a new strategy. And most of all, we need to get serious about defending U.S. interests.

It’s no surprise that the US fight against terrorism depends crucially on the so-called 702 program, which allows the government to serve orders on social media, webmail, and electronic service providers who store their global customers’ data in the United States.

The intelligence we gather in this way protects Europe as much as the United States. Within days of the Paris attacks, the US agreed to give France direct access to much raw intelligence. Even more recently, the German government credited US (and French) intelligence with helping it thwart planned suicide bombings in Munich over the New Year holiday. The British communications intelligence agency, GCHQ, has a deeply integrated intelligence sharing arrangement with NSA. None of these countries, let alone the smaller members of the European Union, can hope to match the American intelligence resources that are now marshaled in their defense.

So it might seem odd that the European Union poses a threat to these capabilities. Odd but true. The problem has deep roots in Europe’s dysfunctional governance structure and in the mix of dependence and resentment that shape its relationship to the United States. In the name of protecting privacy, the EU has long insisted that personal data may not be exported to other countries unless those countries provide “adequate” legal guarantees for privacy, and it has frequently threatened to cut off data flows to the United States because of differences in US and EU data protection law.

The threats were grounded partly in economic interest – keeping data processing jobs and companies in Europe – and partly in a European enthusiasm for expressing its moral superiority to the United States. The EU and US have always been able to negotiate a solution as these crises have been created, but the dynamic changed this fall when the European Court of Justice (ECJ) was asked to rule on the adequacy of US privacy

law. Relying in part on irresponsible and inaccurate statements by the European Commission, the ECJ declared that the Commission had not justified a conclusion that United States surveillance oversight is “adequate.” It overturned the “Safe Harbor” that had allowed US companies to send customer data across the Atlantic. Just as important, it authorized individual data protection agencies in each member state to adjudicate the lawfulness of data transfers to the United States. While the decisions of those agencies can be appealed, the EU has reached agreement on penalties for data protection violations that are a percentage of companies’ global revenue – billions of dollars in the case of big tech companies like Google and Microsoft. With those penalties hanging over their head, few companies will want to gamble that they’ll be vindicated on appeal. The data protection agencies, meanwhile, are delighted to have the US and its tech companies in their sights; they’ve said that enforcement actions are likely to begin at the end of January.

The European Commission has been trying to reach a new agreement with the United States to reinstate the Safe Harbor; the US has provided assurances that our intelligence oversight meets European standards. (Indeed, it far exceeds anything that French or German or British intelligence agencies put up with.) But the Commission’s authority to bind the data protection authorities is in doubt, and it is increasingly under the thumb of a reflexively anti-American European Parliament, which will be inclined to reject or cavil at whatever it negotiates. As a result, the Commission has dug in its heels, demanding wide access to (and implicit authority over) US intelligence programs. There’s a high probability that no deal, or at least no good deal, can be reached with the Commission.

Weirdly, the European institutions that have created this mess have no serious responsibility for stopping terrorism or for collecting and using intelligence. The European security agencies that have that responsibility are powerful in individual countries but have little sway in Brussels. This means that the machinery set in motion by the European Court of Justice will grind forward, with everyone doing what they’ve done before: The

Commission will seek maximum concessions from US intelligence agencies. The European Parliament will deem the concessions insufficient. The data protection agencies will do all they can to punish American tech companies. Without a deal, tech companies may have to move their data centers out of the United States – making counterterrorism intelligence unavailable to our government. And they will be under heavy pressure to break with the US government on intelligence issues – to encrypt even more data to foil US intercepts, and to fight US intelligence orders in court and in Congress. US intelligence will suffer, perhaps greatly, and European and Americans will be at greater risk of terrorist attacks.

In short, if all the players in this drama just keep doing what they’ve always done, the result will be a disaster for US (and European) counterterrorism efforts. If we want to stave off that disaster, we have to shake up the peculiar European structures that are driving this outcome. We have to make clear that continued attempts to hold American company’s hostage over intelligence collection is simply unacceptable to the United States. Up to now, the Administration has tried to appease Europe; it has not played hard ball. And Congress has been disappointingly inactive, except for the House of Representatives, which has gone from inactive to supine in a related dispute, proposing to amend US law to give greater privacy rights to Europeans without demanding even before the negotiations are complete.

What could the US do to change Europe’s negotiating calculus? It’s not that hard, if we have the will. Congress (or, frankly, the President) could simply prohibit the sharing of intelligence with any country whose data protection agencies take action that has the effect of undermining US intelligence capabilities; this would certainly include punishing private companies that send data to the United States. Such a measure would make clear the connection between European data protectionism and our lost counterterrorism insights. While it is harsh to cut off intelligence to countries that are often allies against terrorism, the fact is that their policies will slowly cut off US access to terrorism intelligence. (We don’t have to cut off access across

the board; the measure could allow exceptions when the President certifies the need to share particular intelligence, but broad intelligence sharing would be barred with any country that takes action against US data access.)

Such a measure has the advantage of putting the onus of solving the problem on individual member states – the entities responsible for national security and for the actions of the data protection agencies. (It’s notable that data protection authorities have rarely or never tried to regulate their own national intelligence agencies; they don’t have the clout. Which strongly suggests that those agencies can bring the data protectors to heel if their access to US intelligence depends on it.) Negotiations with individual European nations, then, are far more likely to produce responsible results than negotiations with the neutered European Commission.

That’s one way of making clear to Europe that we’ve had enough. Here’s another. The US and Europe have been negotiating a Transatlantic Trade and Investment Partnership for years, and it’s likely that a deal will be presented to Congress for approval in 2016. This is part of the Obama administration’s ambitious effort to lock in a host of environmental, intellectual property, labor and trade policies via large multinational deals. You’d think that any effort to restrict protectionism and foster trade would address Europe’s data export restraints – probably the biggest trade issue between the US and the EU in the last fifteen years. You’d be wrong. Both the European Commission and the European Parliament have taken data protectionism off the table in this trade deal, insisting that their current rules must be untouched. The result is a trade deal that as a practical matter blesses the current EU attack on our counterterrorism intelligence programs. Unlike the European Parliament, Congress has said nothing about the issue, strengthening the European hand. Yet it is Europe that likely needs a trade deal far more than the US. Europe’s economy has lagged ours in growth and employment for decades, with the one economic bright spot being a consistently large trade surplus with the US. Congress should take a page from the European Parliament’s book,

adopting a resolution stating that no transatlantic trade deal will be approved if it permits the EU’s current interference with both US technology trade and US counterterrorism capabilities.

There will be opposition to either of these measures. Many American businesses expect to get specific benefits from a trade deal, and they are reluctant to upset the apple cart. Refusing to share terror intelligence, meanwhile, has a cold-hearted air. But if we fail to deal with Europe’s data protectionism in this trade deal, we may never have another chance; that will be bad for US industry, which will increasingly be held hostage or forced to accept uneconomic restrictions on how they manage their data. And cutting off counterterrorism intelligence sharing with countries that are undermining the foundation on which that intelligence rests is simply a matter of self-preservation.

If Europe wants to cripple its intelligence agencies, it is free to make that choice. We should not let it cripple ours.

SITCC teaches language of aviation to Intelligence Marines

Story by Cpl. Jason Jimenez

MARINE CORPS AIR STATION CHERRY POINT, N.C. - Intelligence Marines from across the 2nd Marine Aircraft Wing and 3rd MAW had the opportunity to become increasingly proficient in aviation operations during a Squadron Intelligence Training and Certification Course here, Feb. 1 - Feb. 25.

During the SITCC, 30 students of various ranks were introduced to multiple facets of Marine Corps aviation to familiarize themselves with aviation combat intelligence, as it plays a vital role in the success of an Aviation Wing during combat operations.

“Right now, there is a gap in training for intelligence Marines that are going to aviation units,”

said 1st Lt. David Cox, the officer in charge for the course. “SITCC is the best thing to fill that gap, short of having a separate MOS for aviation intelligence Marines”

To date, the course has certified more than 300 Marines enabling them to better integrate into the Marine Air –Ground Task Force. The course squeezes approximately 18 months of on-the-job training into 20 training days, “said Cox.

Even experienced ground intelligence Marines that come to the air wing, have to start learning again because it is very different; a new warfare community, explained Cox. “Throughout my career, I’ve had different jobs, but on the ground, we don’t really care if it’s rainy, cloudy or foggy - it doesn’t affect me kicking in the enemy’s door,” said Gunnery Sgt. Michael Brewster, intelligence chief with MAG-39 and SITCC student.

“When it comes to aviation, you need to take that all into consideration because it affects the Aviation Combat Element.”

The ACE focuses on a different aspect of the enemy, according to Brewster.

The course combines classroom instruction as well as intense student intelligence evaluation and briefing requirements followed by practical application events in direct support of live aviation requirements. Topics included coverage of handling threats to the MAGTF, functions of Marine aviation, along with information on different types of aircraft.

“They have to learn a whole new language,” said Brewster. “They have a three-month course in the schoolhouse, and in that curriculum, only one week is devoted to air intelligence – which is not enough to be basically proficient.”

The wing supports the ground and Intelligence supports the wing, so the more assistance Intelligence Marines give to the aviators, the better the aviators can support the ground units, explained Brewster.

“We are trying to get the SITCC course to be a

formalized school so Aviation Intelligence Marines must come here right after basic training similar to Marine Combat Training,” explained Timothy D. Andres, intelligence coordinator for the Marine Aviation Training Standardization Squadron. “Some Intelligence Marines do not know what a MAW consists of, they don’t know what they don’t know and this course opens their eyes.”

The graduation, held on Feb. 26, certified the 30 Marines as Aviation Intelligence Marines.

“SITCC is not just an Aviation Intelligence solution for a shortcoming in training ... this is a MAGTF solution,” said Col. Robert Plevell, 2nd MAW intelligence officer.

They can now pass their knowledge on to other Marines and spread what they have learned to better support the MAGTF, according to Plevell.

“Of course the students feel a bit challenged, but after the course is completed, they always say thank you for teaching us, we learned a lot,” said Andres.

USMC



Intelligence Photographs in the News



Lithuania - Marines introduced the concept of Company Level Intelligence Cells to Land Forces brigade officers and noncommissioned officers of the Baltic allies in Lithuania from Nov. 24- Dec. 3, 2015. The training was conducted as part of U.S. Marine Corps Forces Europe and Africa's focused implementation plan for military intelligence engagements. In both Baltic nations, small military intelligence corps can benefit from increasing their tactical information-gathering capabilities using concepts like CLIC. **Courtesy Photo**

Marine Corps Base Camp Lejeune, N.C. - Sgt. Ian Rivera, an intelligence analyst with Headquarters Company, 2nd Battalion, 8th Marine Regiment, is responsible for the rescue of two people, including an Army captain, during a vehicular accident that occurred on Interstate 95, Nov. 25, 2015. Rivera is a native of Virginia Beach, Va. **Photo By: Cpl. Paul S. Martinez**



Edinburgh, Scotland, United Kingdom - U.S. Marines with 2nd Intelligence Battalion and British soldiers search for a checkpoint during Exercise Phoenix Odyssey II near Edinburgh, U.K., Oct. 30, 2015. The service members executed a three-mile conditioning hike and shooting competition as part of the exercise, which is designed to enhance joint intelligence operations. **Photo By: Cpl. Lucas Hopkins**

Intelligence Oversight Division

MISSION: To ensure the effective implementation of Marine Corps-wide Oversight of Intelligence, Counterintelligence, Sensitive activities (to include USMC support to law enforcement agencies, special operations, and security matters), and special Access Programs. To establish policy and ensure their legality, propriety and regulatory compliance with appropriate Department of Defense/ Department of the Navy guidance.

Examples of sensitive activities include:

- Military support to Civil Authorities
- Lethal support/training to non-USMC agencies
- CONUS off-base training
- Covered, clandestine, undercover activities
- Intelligence collection of information on U.S. persons

SECNAVINST 5430.57G states:

"...personnel bearing USMC IG credentials marked 'Intelligence Oversight/Unlimited Special Access' are certified for access to information and spaces dealing with intelligence and sensitive activities, compartmented and special access programs, and other restricted access programs in which DON participates. When performing oversight of such programs pursuant to Executive Order, they shall be presumed to have a 'need to know' for access to information and spaces concerning them."

WHAT IS INTELLIGENCE OVERSIGHT?

Intelligence Oversight ensures that intelligence personnel shall not collect, retain, or disseminate information about U.S. persons unless done in accordance with specific guidelines, proper authorization, and within only specific categories ([See References](#)).

DEFINITIONS

- INTELLIGENCE OVERSIGHT (IO):** Ensures that intelligence personnel shall not collect, retain, or disseminate information about U.S. persons unless done in accordance with specific guidelines, proper authorization, and within only specific categories. References: [E.O. 12333](#), [DoD Dir 5240.01](#), [DoD Reg 5240.1-R](#), [SECNAVINST 3820.3E](#), [MCO 3800.2B](#)
- SENSITIVE ACTIVITY OVERSIGHT:** Any activity requiring special protection from disclosure which could embarrass compromise or threaten the DON. Any activity which, if not properly executed or administered, could raise issues of unlawful conduct, government ethics, or unusual danger to DON personnel or property. These activities may include support to civilian law enforcement. Reference: [SECNAVINST 5000.34E](#)
- SPECIAL ACTIVITIES OVERSIGHT:** As defined by Executive Order 12333, activities conducted in support of national foreign policy objectives abroad which are planned and executed so that the role of the United States Government is not apparent or acknowledged publicly, and functions in support of such activities, but which are not intended to influence United States political processes, public opinion, policies or media, and do not include diplomatic activities or the collection and production of intelligence or related support activities. Reference: [SECNAVINST 5000.34E](#)
- SPECIAL ACCESS PROGRAM (SAP):** Any Program imposing need-to-know or access controls beyond those normally required for Confidential, Secret or Top Secret information. Such a program includes but is not limited to a special clearance, more stringent adjudication or investigation requirements; special designation of officials authorized to determine need-to-know; or special lists of persons determined to have a need-to-know. A special access program may be a sensitive activity.
- QUESTIONABLE ACTIVITIES:** Any conduct that may constitute a violation of applicable law, treaty, regulation or policy.