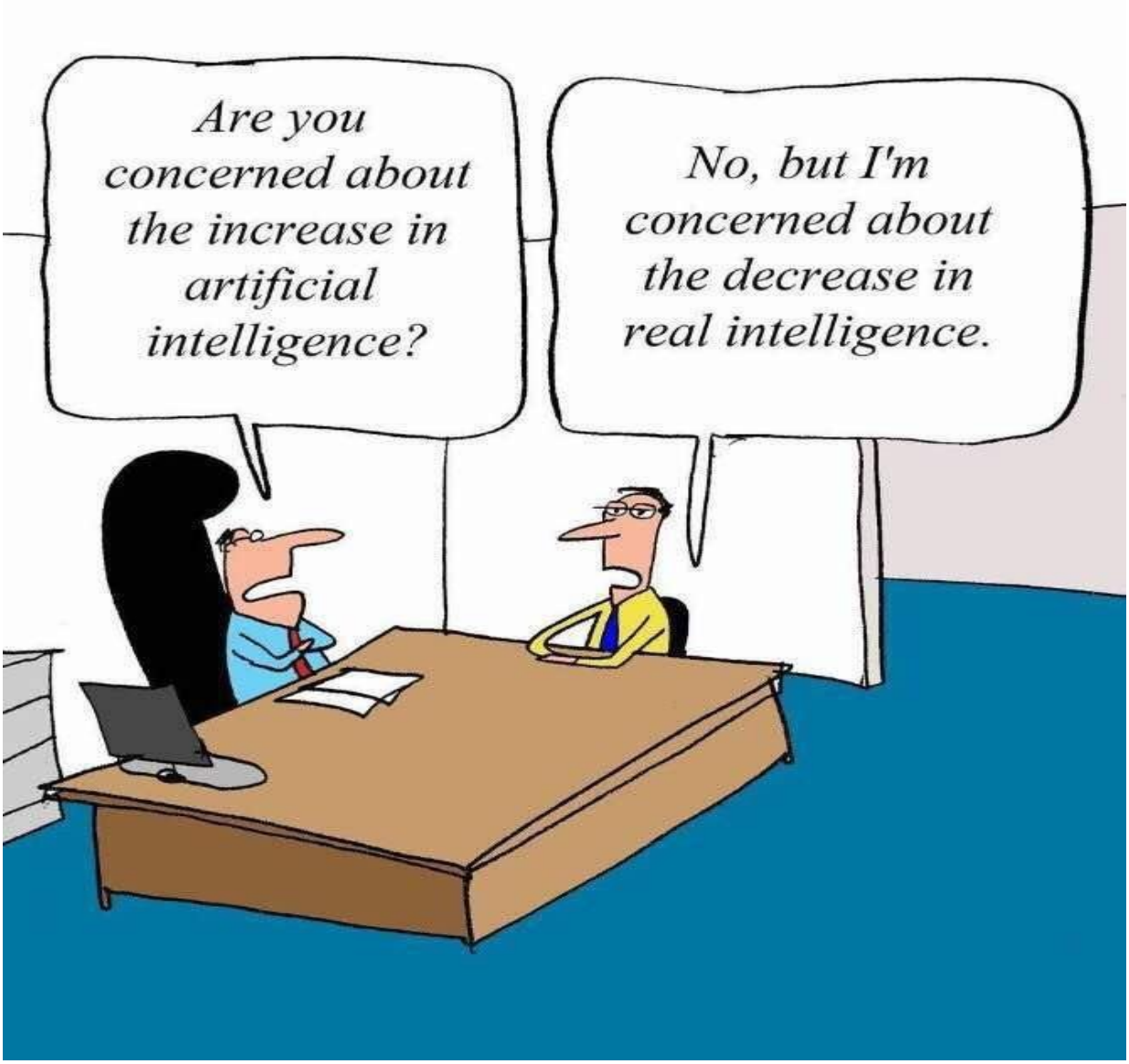
OVERWATCH

"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 16 Issue 3 FALL 2024

IN THIS ISSUE, FEATURED ARTICLE: US INTELLIGENCE AGENCIES' EMBRACE OF GENERATIVE AI IS AT ONCE WARY AND URGENT



Inspector General of the Marine Corps

The Inspector General of the Marine Corps (IGMC) facilitates Marine Corps efficiency, integrity, and institutional readiness through objective and independent assistance, assessments, inspections, and investigations to enhance the Marine Corps' mission success and the welfare of its Marines, Sailors, and their families.

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
Deputy Director – LtCol James Kim
LtCol Bessie Bernstein -Sensitive Activities Officer

Inside This Issue

3 A Message from the Director

4. US intelligence agencies' embrace of generative AI is at once wary and urgent

6. The U.S. counterintelligence head says the list of threats is long and getting longer

7. Intelligence History

10. Intelligence Photographs in the News

Web Links

Senior Intelligence Oversight Official (SIOO)
https://dodsioo.defense.gov/

Marine Corps Inspector General
https://www.hqmc.marines.mil/igmc//

Naval Inspector General
https://www.secnav.navy.mil/ig

Intelligence News
INTEL - Home

A Message from the Director

Greetings from the Office of the Inspector General for the Marine Corps, Intelligence Oversight Division. This edition of *Overwatch* is the third of calendar year 2024. As always, the articles provided in this issue do not represent the opinion of Intelligence Oversight Division or the Office of the Inspector General. The articles are meant to inspire thought and create a space for discussion.

This issue welcomes a familiar face to the USMC Intelligence enterprise with LtGen Jerry Carter taking the mantle of Deputy Commandant for Information (DC/I) and a new Executive Assistant, Col Brendon Harper. Both have extensive experience within HQMC Intel Department and are eager to take the enterprise to the next level.

SECNAVINST 3820.F, INTELLIGENCE OVERSIGHT WITHIN THE DEPARTMENT OF THE NAVY is currently in rewrite and will be published shortly. Please keep an eye out for it. MCO 3800.2C is also moving through the process to be updated. The Functional Area Checklist 3800 INTELLIGENCE has been modified and in final stages of review before being published. Additionally, MCO 3800.2C, OVERSIGHT OF INTELLIGENCE ACTIVITIES is still making its way through the process and hope to have it published soon.

The annual training requirement for Intelligence Oversight can be fulfilled by successful completion of the online Annual Intelligence Oversight Training course currently available via Marine Net at: https://portal.marinenet.usmc.mil/content/mnet-portal/en/catalog/coursedetails.html?courseid=cb536883-529f-453d-bbad-3d186063d5d0

The course takes approximately one hour to complete. Completion status will be captured in personnel's Marine Net profile and recorded in the Marine Corps Total Force System (MCTFS) for unit training managers' documentation. Note that course completions remain valid for one year from completion.

I am very pleased at the amount of personnel utilizing this new training format. Numbers of personnel taking the training is rising exponentially.

The first article discusses the Intelligence Community embrace of generative artificial intelligence.

Our second article is a report from the head of US Counterintelligence regarding threats to the homeland.

Last, we have our section on Intelligence History which this issue continues with excerpts on the Birth and Early Years of Marine Corps Intelligence.

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

Featured Article

US intelligence agencies' embrace of generative AI is at once wary and urgent.

ARLINGTON, Virginia (AP) — Long before generative AI's boom, a Silicon Valley firm contracted to collect and analyze non-classified data on illicit Chinese fentanyl trafficking made a compelling case for its embrace by U.S. intelligence agencies.

The operation's results far exceeded human-only analysis, finding twice as many companies and 400% more people engaged in illegal or suspicious commerce in the deadly opioid.

Excited U.S. intelligence officials touted the results publicly — the AI made connections based mostly on internet and dark-web data — and shared them with Beijing authorities, urging a crackdown.

One important aspect of the 2019 operation, called Sable Spear, that has not previously been reported: The firm used generative AI to provide U.S. agencies — three years ahead of the release of OpenAI's groundbreaking ChatGPT product — with evidence summaries for potential criminal cases, saving countless work hours.

"You wouldn't be able to do that without artificial intelligence," said Brian Drake, the Defense Intelligence Agency's then-director of AI and the project coordinator.

The contractor, Rhombus Power, would later use generative AI to predict Russia's full-scale invasion of Ukraine with 80% certainty four months in advance, for a different U.S. government client. Rhombus says it also alerts government customers, who it declines to name, to imminent North Korean missile launches and Chinese space operations.

U.S. intelligence agencies are scrambling to embrace the AI revolution, believing they'll otherwise be smothered by exponential data growth as sensor-generated surveillance tech further blankets the planet.

But officials are acutely aware that the tech is young and brittle, and that generative AI — prediction models trained on vast datasets to generate on-demand text, images, video and human-like conversation — is anything but tailor-made for a dangerous trade steeped in deception.

Analysts require "sophisticated artificial intelligence models that can digest mammoth amounts of open-source and clandestinely acquired information," CIA director William Burns recently wrote in Foreign Affairs. But that won't be simple.

The CIA's inaugural chief technology officer, Nand Mulchandani, thinks that because gen AI models "hallucinate" they are best treated as a "crazy, drunk friend" — capable of great insight and creativity but also bias-prone fibbers. There are also security and privacy issues: adversaries could steal and poison them, and they may contain sensitive personal data that officers aren't authorized to see.

That's not stopping the experimentation, though, which is mostly happening in secret.

An exception: Thousands of analysts across the 18 U.S. intelligence agencies now use a CIA-developed gen AI called Osiris. It runs on unclassified and publicly or commercially available data — what's known as open-source. It writes annotated summaries and its chatbot function lets analysts go deeper with queries.

Mulchandani said it employs multiple AI models from various commercial providers he would not name. Nor would he say whether the CIA is using gen AI for anything major on classified networks.

"It's still early days," said Mulchandani, "and our analysts need to be able to mark out with absolute certainty where the information comes from." CIA is trying out all major gen AI models – not committing to anyone -- in part because AIs keep leapfrogging each other in ability, he said.

Mulchandani says gen AI is mostly good as a virtual assistant looking for "the needle in the needle stack." What it won't ever do, officials insist, is replace human analysts.

Linda Weissgold, who retired as deputy CIA director of analysis last year, thinks war-gaming will be a "killer app."

During her tenure, the agency was already using regular AI — algorithms and natural-language processing — for translation and tasks including alerting analysts during off hours to potentially important developments. The AI wouldn't be able to describe what happened — that would be classified — but could say "here's something you need to come in and look at."
Gen AI is expected to enhance such processes.

Its most potent intelligence use will be in predictive analysis, believes Rhombus Power's CEO, Anshu Roy.

"This is probably going to be one of the biggest paradigm shifts in the entire national security realm — the ability to predict what your adversaries are likely to do."

Rhombus' AI machine draws on 5,000-plus data streams in 250 languages gathered over 10-plus years including global news sources, satellite images and data cyberspace. All of it is open source. "We can track people, we can track objects," said Roy.

AI bigshots vying for U.S. intelligence agency business include Microsoft, which announced on May 7 that it was offering OpenAI's GPT-4 for top-secret networks, though the product must still be accredited for work on classified networks.

A competitor, Primer AI, lists two unnamed intelligence agencies among its customers — which include military services, documents posted online for recent military AI workshops show. It offers AI-powered search in 100 languages to "detect emerging signals of breaking events" of sources including Twitter, Telegram, Reddit and Discord and help identify "key people, organizations, locations." Primer lists targeting among its technology's advertised uses. In a demo at an Army conference just days after the Oct. 7 Hamas attack on Israel, company executives described how their tech separates fact from fiction in the flood of online information from the Middle East.

Primer executives declined to be interviewed.

In the near term, how U.S. intelligence officials wield gen AI may be less important than counteracting how adversaries use it: To pierce U.S. defenses, spread disinformation and attempt to undermine Washington's ability to read their intent and capabilities.

And because Silicon Valley drives this technology, the White House is also concerned that any gen AI models adopted by U.S. agencies could be infiltrated and poisoned, something research indicates is very much a threat.

Another worry: Ensuring the privacy of "U.S. persons" whose data may be embedded in a large-language model.

"If you speak to any researcher or developer that is training a large-language model, and ask them if it is possible to basically kind of delete one individual piece of information from an LLM and make it forget that -- and have a robust empirical guarantee of that forgetting -- that is not a thing that is possible," John Beieler, AI lead at the Office of the Director of National Intelligence, said in an interview.

It's one reason the intelligence community is not in "move-fast-and-break-things" mode on gen AI adoption.

"We don't want to be in a world where we move quickly and deploy one of these things, and then two or three years from now realize that they have some information or some effect or some emergent behavior that we did not anticipate," Beieler said.

It's a concern, for instance, if government agencies decide to use AIs to explore bio- and cyber-weapons tech.

William Hartung, a senior researcher at the Quincy Institute for Responsible Statecraft, says intelligence agencies must carefully assess AIs for potential abuse lest they lead to unintended consequences such as unlawful surveillance or a rise in civilian casualties in conflicts.

"All of this comes in the context of repeated instances where the military and intelligence sectors have touted "miracle weapons" and revolutionary approaches -- from the electronic battlefield in Vietnam to the Star Wars program of the 1980s to the "revolution in military affairs in the 1990s and 2000s -- only to find them fall short," he said.

Government officials insist they are sensitive to such concerns. Besides, they say, AI missions will vary widely depending on the agency involved. There's no one-size-fits-all.

Take the National Security Agency. It intercepts communications. Or the National Geospatial-Intelligence Agency (NGA). Its job includes seeing and understanding every inch of the planet. Then there is measurement and signature intel, which multiple agencies use to track threats using physical sensors.

Supercharging such missions with AI is a clear priority.

In December, the NGA issued a request for proposals for a completely new type of generative AI model. The aim is to use imagery it collects — from satellites and at ground level – to harvest precise geospatial intel with simple voice or text prompts. Gen AI models don't map roads and railways and "don't understand the basics of geography," the NGA's director of innovation, Mark Munsell, said in an interview.

Munsell said at an April conference in Arlington, Virginia that the U.S. government has currently only modeled and labeled about 3% of the planet.

Gen AI applications also make a lot of sense for cyberconflict, where attackers and defenders are in constant combat and automation is already in play.

But lots of vital intelligence work has nothing to do with

data science, says Zachery Tyson Brown, a former defense intelligence officer. He believes intel agencies will invite disaster if they adopt gen AI too swiftly or completely. The models don't reason. They merely predict. And their designers can't entirely explain how they work.

Not the best tool, then, for matching wits with rival masters of deception.

"Intelligence analysis is usually more like the old trope about putting together a jigsaw puzzle, only with someone else constantly trying to steal your pieces while also placing pieces of an entirely different puzzle into the pile you're working with," Brown recently wrote in an in-house CIA journal. Analysts work with "incomplete, ambiguous, often contradictory snippets of partial, unreliable information."

They place considerable trust in instinct, colleagues and institutional memories.

"I don't see AI replacing analysts anytime soon," said Weissgold, the former CIA deputy director of analysis.

Quick life-and-death decisions sometimes must be made based on incomplete data, and current gen AI models are still too opaque.

"I don't think it will ever be acceptable to some president," Weissgold said, "for the intelligence community to come in and say, 'I don't know, the black box just told me so.'"

The U.S. counterintelligence head says the list of threats is long and getting longer.

April 12, 2024, 5:01 AM ET

As the head of American counterintelligence, Mike Casey sees daily the scope of foreign spying operations, cyberattacks and economic espionage against the United States.

"The scale is impressive and terrifying," said Casey, who stepped into his current job last year after working for more than two decades in Congress. He finished up his time on the Hill as the staff director for the Senate Intelligence Committee, so he already had deep understanding of the array of threats facing the U.S.

What's changed now, though, is it's his responsibility to keep those secrets safe.

"Fortunately for me, and unfortunately for everybody else, counterintelligence, it turns out, is a growth business," he told NPR in an interview. "More players are getting into it with more tools, going after more targets."

The list of concerns is a long one. The usual suspects — China, Russia, Iran, and North Korea — lead the way, he says, but there are other actors, including private sector entities and cybercriminals who are also getting involved.

"It's not just the Russians stealing secrets from the State Department anymore," Casey said. "It's everybody trying to steal all sorts of intellectual property, going after critical infrastructure. Just the list goes on and on."

For all the changes, one foreign adversary still stands out, he says, for the ambition and scale of its espionage efforts against the U.S.: the People's Republic of China.

The kinds of U.S. targets China chases

Casey says Beijing has studied American history and has concluded that the U.S. achieved greatness, in part, by helping craft the world system that emerged from the ashes of World War II and the rules that govern it.

"And they have a view of national greatness that essentially says, 'If we can supplant the United States in key technology, both military and non-military, and help establish sort of the international regulatory scheme for all that, then we will become the preeminent player in the international area,' " Casey says.

That interpretation influences how China's intelligence officers operate and the kind of targets they go after in the U.S.

"It's not so much a guy in a black hat breaking into the plant and stealing the tank armor out the back," Casey says. "It's much more of a hacking operation or hiring a scientist."

He points to a recent Justice Department case charging a former Google engineer with stealing the building blocks of the company's AI technology. The defendant, a Chinese national, was allegedly secretly working for two China-based technology companies while he was pilfering files from Google.

The case is just the latest in what American officials say is a relentless campaign by China to try to steal American trade secrets, cutting-edge research, and technology as well as intellectual property.

U.S. officials and lawmakers have spent a lot of time in recent years meeting with American businesses and

universities to try to keep them informed about what the government says are China's efforts against them.

Casey says that conversation has changed from five years ago.

"The question then you got was, 'Really, how bad is it? I'm not sure I believe you.' The question now is, 'What do I do?' And that's a fundamental change," he said. "I think the threat has been absorbed, and you're much more in the practicalities of how I deal with this as a private sector entity."

Russia is another top concern. The Kremlin presents a different sort of threat from China. Moscow, for one, doesn't target U.S. economic secrets like Beijing does.

"Certainly not to the same extent," Casey says. "They're still much more in their classic model of government secrets, military secrets."

In 2018, the Trump administration expelled 60 Russian diplomats that the U.S. had identified as intelligence officers. The move was a response to a nerve agent attack in the United Kingdom against a retired Russian intelligence officer.

Asked whether Russia has managed to rebuild its intelligence operations in the U.S. since then, Casey replied with "a qualified somewhat, yes."

"I think what we believe is that they have managed to rebuild some of that stable," he said. While China and Russia are two of the top concerns for Casey, a recent Justice Department case demonstrated that smaller nations can't be overlooked, either.

A former U.S. ambassador, Victor Manuel Rocha, was arrested and charged late last year with spying for Cuba. Rocha has since pleaded guilty. The fact that a one-time ambassador was spying was bad enough. But Rocha did so undetected for 40 years.

How big of a counterintelligence failure was that? "Obviously not a small one," Casey says. "But we don't actually know how big it was yet until we go through and do the damage assessment. The IC [intelligence community] will take a hard look at whatever was compromised and whatever damage it did, but certainly, somewhere, we dropped the ball."

Rocha's spying pre-dates Casey's time in the job. Still, it's a reminder of a point Casey makes about the spying business: Never assume that you know everything and that you've got it all in hand.

"We're counterintelligence," Casey says. "Paranoia is kind of what we do."

Intelligence In History

The below is the continuation of a series of articles on the history of military intelligence.

Post–World War I Reorganization of the Marine Corps

By Michael H. Decker and William MacKenzie

Military Intelligence Section Activities

In 1922, Brigadier General Feland wrote in the *Marine Corps Gazette* that he saw the Division of Operations and Training as essential for the Marine Corps to mitigate future losses in combat and increase organizational readiness. He stated that the Military Intelligence Section's principal function was the "collection and compilation of intelligence useful to the Marine Corps, in carrying out its mission."

There is ample evidence of the Military Intelligence Section collecting and compiling information. Many Marines are familiar with the legend of Lieutenant Colonel Ellis writing *Advanced Base Operations in Micronesia* in 1921 and then being found dead in Palau in 1923 while on an intelligence or reconnaissance mission. What few Marines may know is that with no professional or career intelligence officers, all officers in the Division of Operations and Training could move between sections and perform a variety of duties as needed. Ellis, for example, simultaneously headed the Military Intelligence Section and wrote those advanced basing plans that guided Marine Corps war planning for the subsequent 25 years.

As evidenced by the Headquarters letter forwarding the 1920 Army doctrinal publication *Intelligence Regulations*, the Military Intelligence Section also took part in the Division of Operations and Training's other efforts, such as "organization of units, matters of training, choice of most suitable arms and equipment, military schooling, etc."

On 10 January 1921, a month after the Military Intelligence Section was formed, it promulgated a "List of Intelligence Regulations, etc. Transmitted to Certain Marine Corps Units." The list included items such as the Intelligence *Regulations*, along with various other military orders, articles, and reports. A few excerpts from items on the list high- light the type of things this 40-day-old Headquarters office determined would be of use to Marine Corps Schools and "certain" field units.

Front Line Intelligence, extract from an article in the *Marine Corps Gazette*, December 1920, by Major Ralph Stover Keyser." Major Keyser had served as commanding officer of 2d Battalion, 5th Marines, June–July 1918 during battles in the Château-Thierry sector and the Aisne-Marne offensive; then, August 1918–August 1919, he served as Major General Lejeune's assistant chief of staff, G-2 (Intelligence Department), in the 2d Division, AEF. The article was a tour-de-force of tactical intelligence support on intelligence functions at the division, regiment, and battalion level. Major Keyser noted, "Military intelligence is more than reliable information, it is reliable information furnished in time to permit appropriate action."

"Intelligence Service in the Bush Brigades and Baby Nations, Extracts from a 1920 report by Major Earl Ellis." Ellis noted, "In executing the intelligence functions stated the most difficult problem of all is to force the personnel to realize that their mission is not to gather information of any kind and place it on file, as is generally the custom, but to gather pertinent information, put it in proper form for use and then place it in the hands of the person who can use it to best advantage—and this as quickly as possible."

"Functions of Intelligence Officers in War Plans, Extract from U.S. Army Instructions to Intelligence Officers by Military Intelligence Department, 1921." This Army doctrine stated, "As the plan is built up, every portion should be submitted to you for attack as the enemy's representative—this for the purpose of providing the means of disinterested construction [*sic*] criticism. Your mental attitude in doing this work should be that of the enemy's Chief of Staff, who, supposedly having captured the plan, strives to plan to circumvent it.

These examples show how the combined lessons of small wars and the AEF in World War I instructed these officers that newly formed Marine Corps intelligence staffs should focus on tactical and operational intelligence support that was very practical and directly tied to current operational planning and decision making. However, the Military Intelligence Section was dividing its time between this type of "force development" activity (as it might be called today) and the need to do other longer-range planning and interagency coordination.

Brigadier General Feland noted that the Division of Operations and Training "has been charged with certain responsibility in regard to the policy to be followed in selecting the personnel for assignment to certain duties." Examples of this would include detailing of Marines to the ONI, naval attaché duty, special training in areas such as communications intelligence, and special reconnaissance missions.

Next up- Service in the Office of Naval Intelligence

Intelligence Photographs in the News

U.S. Marines with 3rd Intelligence Battalion, III Marine Expeditionary Force Information Group, receive instruction for the course of fire during a 3rd Intelligence Battalion field exercise on Camp Hansen, Okinawa, Japan, May 11, 2024. The field exercise was held to test the capabilities and functions of the support elements, giving them a better understanding of how to work together. (U.S. Marine Corps photo by Cpl. Alora J. Finigan)

From left, U.S. Marine Corps Cpl. Isaac Torres, and Lance Cpl. Alan Garza, both rifleman with 3rd Intelligence Battalion, III Marine Expeditionary Force Information Group inspect a maritime radar system during exercise Resolute Dragon 24 at Ie Shima Training Facility, Okinawa, Japan, July 30, 2024. The maritime surveillance screening was conducted to refine the Marines ability to act as an early warning system for allied forces. RD 24 is an annual bilateral exercise in Japan that strengthens the command, control, and multi-domain maneuver capabilities of Marines in III MEF and Japan Self-Defense Force personnel, with a focus on controlling and defending key maritime terrain. Havana is a native of California and Garza is a native of Idaho. (U.S. Marine Corps photo by Sgt. Marcos A. Alvarado)

U.S. Marine Corps Cpl. Ava Hamilton, left, a geospatial intelligence analyst, and Sgt. Gage Revell, a small arms repair technician, both with U.S. Marine Corps Forces, Korea, ground fight during a Marine Corps Martial Arts Program Instructor Course at U.S. Army Garrison Humphreys, South Korea, June 7, 2024. MCMAP is an integrated, weapons-based training system that incorporates the full spectrum of the force continuum on the battlefield and contributes to the mental and physical development of Marines. (U.S. Marine Corps photo by Cpl. Dean Gurule)

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

i. **INTELLIGENCE OVERSIGHT (IO):** Intelligence Oversight ensures that all activities performed by intelligence units and personnel are conducted in accordance with federal law, Presidential Executive Orders, DoD directives, regulations, policies, standards of conduct, and propriety References: E.O. 12333, DoDM 5240.01, DoD Reg 5240.1-R, SECNAVINST 3820.3F,SECNAVINST 5000.34G, MCO 3800.2B

ii. **INTELLIGENCE RELATED ACTIVITY**. Activities that are not conducted under the authority of Executive Order 12333 that involve the collection, retention, or analysis of information, and the activities' primary purpose is to: a. train intelligence personnel; or b. conduct research, development, or testing and evaluation for the purpose of developing intelligence-specific capabilities. Reference: SECNAVINST 5000.34G.

iii. **SENSITIVE ACTIVITIES:** Operations, actions, activities, or programs that are generally handled through special access, compartmented, or other sensitive control mechanisms because of the nature of the target, the area of the operation, or other designated aspects. Sensitive activities also include operations, actions, activities, or programs conducted or supported by any DoD component, including the DON, that, if compromised, could have enduring adverse effects on U.S. foreign policy, DoD or DON activities, or military operations; or cause significant embarrassment to the United States, its allies, the DoD, or DON. Reference: SECNAVINST 5000.34G.

iv. **SPECIAL ACCESS PROGRAM (SAP):** A program activity that has enhanced security measures and imposes safeguarding and access requirements that exceed those normally required for information at the same level. Information to be protected within the SAP is identified by a security classification guide. DoD SAPs are divided into three categories: Acquisition SAP; Intelligence SAP; or Operations and Support SAP. Reference: SECNAVINST 5000.34G.

v. **QUESTIONABLE INTELLIGENCE ACTIVITY:** Any intelligence or intelligence-related activity, when there is reason to believe such activity may be unlawful or contrary to any Executive Order, Presidential Directive, Intelligence Community Directive, or applicable DoD policy governing that activity. Reference: SECNAVINST 5000.34G.

vi. **SIGNIFICANT OR HIGHLY SENSITIVE MATTER (S/HSM**): An intelligence or intelligence-related activity (regardless of whether the intelligence or intelligence-related activity is unlawful or contrary to an E.O., Presidential directive, Intelligence Community Directive, or DoD policy), or serious criminal activity by intelligence personnel, that could impugn the reputation or integrity of the Intelligence Community, or otherwise call into question the propriety of intelligence activities. Such matters might involve actual or potential Congressional inquiries or investigations, Adverse media coverage, Impact on foreign relations or foreign partners, Systemic compromise, loss, or unauthorized disclosure of protected information.