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 10 Issue 1 Winter 2021

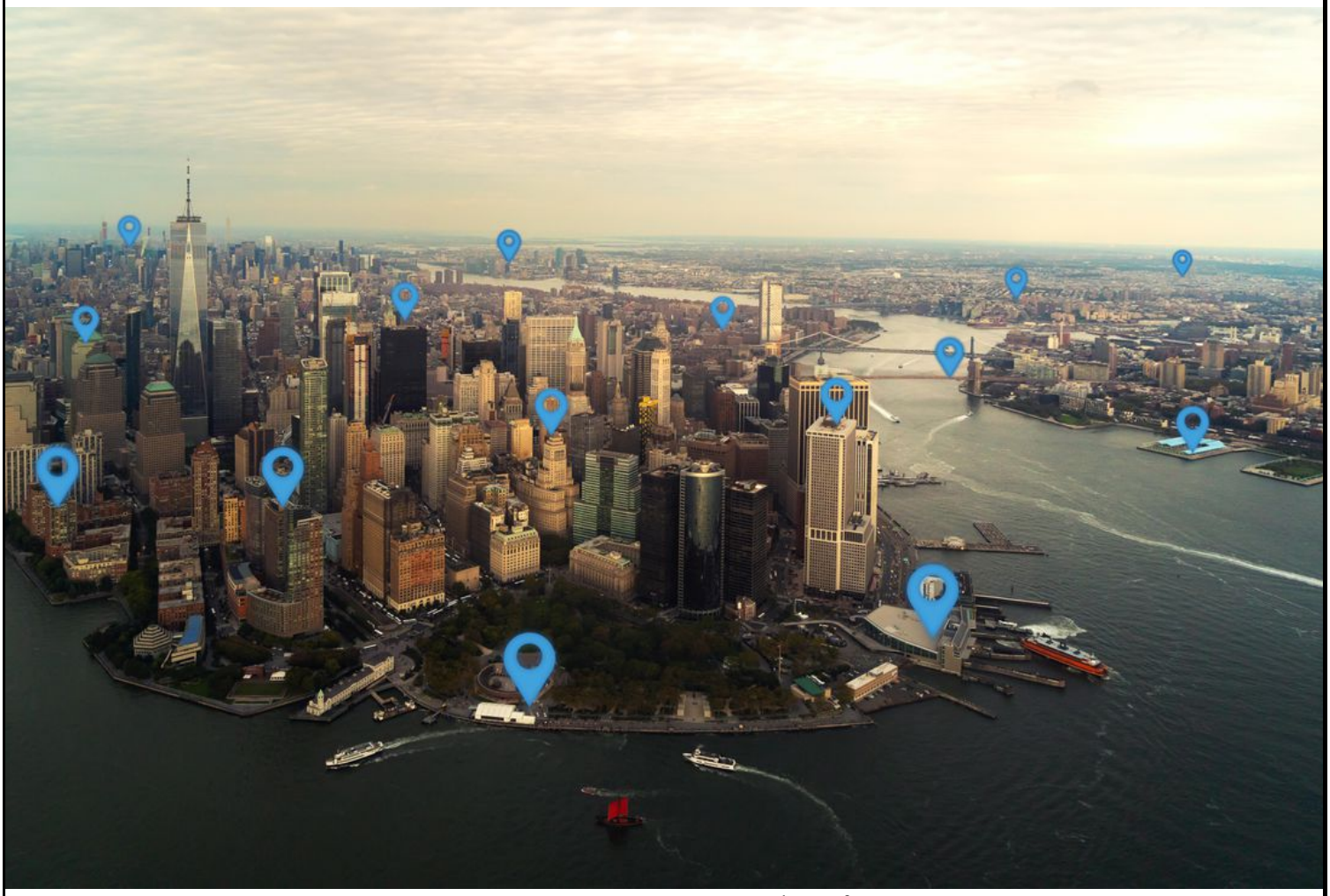

Photo from Getty Images

IN THIS ISSUE, FEATURED ARTICLE: BE SLEEK AND SILENT: HOW CHINA CENSORED BAD NEWS ABOUT COVID-19

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
LtCol David Lasseter, Deputy Director
LtCol Greg Ryan, Sensitive Activities Officer

Inside This Issue

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

A Message from the Director

Greetings from the Office of the Inspector General for the Marine Corps, Oversight Division. This edition of *Overwatch* is the first of calendar year 2021. As always, the articles provided in this issue do not represent the opinion of Intelligence Oversight Division or the Inspector General's Office.

There is new training available on MARINENET for intelligence oversight located at https://elearning.marinenet.usmc.mil/moodle/course/view.php?id=3598. You must have a MARINENET account to participate. You may use this for your annual refresher training. Also, the new SECNAVINST 5000.34G, Oversight of Intelligence Activities, Intelligence-Related Activities, Special Access Programs, and Sensitive Activities Within the Department of the Navy was published on January 19, 2021. This instruction can be found at: https://www.secnav.navy.mil/doni/Pages/Dashboard.aspx.

The first article was written by New York Times journalists Raymond Zhong, Paul Mozur, Jeff Kao, and Aaron Krolik. The article discusses how the Chinese government prevented accurate dissemination of information regarding the COVID-19 origins and its health implications.

The next article by Daniel Klaidman was written in 2013 about the recently Senate confirmed Director of National Intelligence, Avril Haines. Ms. Haines took an atypical path into the intelligence community which is highlighted in this article. She is now the Nation's most senior intelligence officer.

Next, Homeland Security Today highlights the release of the new ODNI and U.S. Attorney General procedures for conducting intelligence activities.

Last, Charlie Savage of the New York Times reports on the Defense Intelligence Agency's purchase and use of commercial smartphone location data associated with American citizens.

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

Be Sleek and Be Silent: How China Censored Bad News About COVID*

By Raymond Zhong, Paul Mozur, Jeff Kao, and Aaron Krolik
www.nytimes.com
December 2020

Thousands of internal directives and reports reveal how Chinese officials stage-managed what appeared online in the early days of the outbreak.

In the early hours of 7 February, China's powerful internet censors experienced an unfamiliar and deeply unsettling sensation. They felt they were losing control.

The news was spreading quickly that Li Wenliang, a doctor who had warned about a strange new viral outbreak only to be threatened by the police and accused of peddling rumors, had died of COVID-19.

Grief and fury coursed through social media. To people at home and abroad, Li's death showed the terrible cost of the Chinese government's instinct to suppress inconvenient information.

Warning of the "unprecedented challenge" Li's passing had posed and the "butterfly effect" it may have set off, officials got to work suppressing the inconvenient news and reclaiming the narrative, according to confidential directives sent to local propaganda workers and news outlets.

They ordered news websites not to issue push notifications alerting readers to his death. They told social platforms to gradually remove his name from trending topics pages. And they activated legions of fake online commenters to flood social sites with distracting chatter, stressing the need for discretion: "As commenters fight to guide public opinion, they must conceal their identity, avoid crude patriotism and sarcastic praise, and be sleek and silent in achieving results."

The orders were among thousands of secret government directives and other documents that were reviewed by *The New York Times* and *ProPublica*. They lay bare in extraordinary detail the systems that helped the Chinese authorities shape online opinion during the pandemic.

At a time when digital media is deepening social divides in Western democracies, China is manipulating online discourse to enforce the Communist Party's consensus.

To stage-manage what appeared on the Chinese internet early this year, the authorities issued strict commands on the content and tone of news coverage, directed paid trolls to inundate social media with party-line blather and deployed security forces to muzzle unsanctioned voices.

Though China makes no secret of its belief in rigid internet controls, the documents convey just how much behind-the-scenes effort is involved in maintaining a tight grip. It takes an enormous bureaucracy, armies of people, specialized technology made by private contractors, the constant monitoring of digital news outlets and social media platforms: and, presumably, lots of money.

It is much more than simply flipping a switch to block certain unwelcome ideas, images or pieces of news. China's curbs on information about the outbreak started in early January, before the novel coronavirus had even been identified definitively, the documents show. When infections started spreading rapidly a few weeks later, the authorities clamped down on anything that cast China's response in too "negative" a light.

The United States and other countries have for months accused China of trying to hide the extent of the outbreak in its early stages. It may never be clear whether a freer flow of information from China would have prevented the outbreak from morphing into a raging global health calamity.

But the documents indicate that Chinese officials tried to steer the narrative not only to prevent panic and debunk damaging falsehoods domestically. They also wanted to make the virus look less severe — and the authorities more capable — as the rest of the world

was watching.

The documents include more than 3,200 directives and 1,800 memos and other files from the offices of the country's internet regulator, the Cyberspace Administration of China, in the eastern city of Hangzhou.

They also include internal files and computer code from a Chinese company, Urun Big Data Services, that makes software used by local governments to monitor internet discussion and manage armies of online commenters.

The documents were shared with *The Times* and *ProPublica* by a hacker group that calls itself CCP Unmasked, referring to the Chinese Communist Party. *The Times* and *ProPublica* independently verified the authenticity of many of the documents, some of which had been obtained separately by *China Digital Times*, a website that tracks Chinese internet controls.

The CAC and Urun did not respond to requests for comment.

"China has a politically weaponized system of censorship; it is refined, organized, coordinated and supported by the State's resources," said Xiao Qiang, a research scientist at the School of Information at the University of California, Berkeley, and the founder of *China Digital Times*. "It's not just for deleting something. They also have a powerful apparatus to construct a narrative and aim it at any target with huge scale."

"This is a huge thing," he added. "No other country has that."

*Please visit nytimes.com for the entire story.

Avril Haines, The Least Likely Spy*

By Daniel Klaidman
Newsweek
June 26, 2013

The morning light was just breaking over Washington, D.C. At the White House, the early cleaning shift was already on the job. As Avril Haines walked through the quiet, darkened halls, she smiled and waved to a worker pushing a polishing machine, buffing the marble floors. It was 5:30 a.m. in mid-May and Haynes was *leaving* work. She would return by 7, after a shower and change of clothes at her Capitol Hill home—and after picking up her habitual iced grande whole milk latte at the local Starbucks, where the baristas are on a first-name basis with her.

The past few weeks had been a grueling run for Haines, the top lawyer for the National Security Council. On this morning, she was laboring over the "playbook," President Obama's massively complex and bureaucratically contentious effort to reform the administration's lethal drone program. But the truth is, it was only a slight departure from Haines's typically relentless work routine. Since becoming the National Security Council's legal adviser in 2011, she had been working on a wide array of highly complicated and legally sensitive issues—generally until 1 or 2 in the morning, sometimes later—that go to the core of U.S. security interests. Among them were the legal requirements governing U.S. intervention in Syria and the range of highly classified options for thwarting Iran's nuclear program. All the while, Haines was sometimes summoned in the middle of the night to weigh in on whether a suspected terrorist could be lawfully incinerated by a drone strike.

Earlier this month, Obama selected Haines to be deputy director of the CIA, where she will serve under the new CIA director, John Brennan. In some respects, picking Haines made a lot of sense, given her national-security credentials and her well-known work ethic. But in another respect, it was a surprising choice. Ask around about Haines, and colleagues will often describe some character traits not usually associated with the CIA—or, for that matter, with rapid ascent inside the Beltway: a sweet personality, humility bordering on shyness, a deep empathy for

others. "She may quite literally be the nicest person any of us have ever met," says Deputy National Security Adviser Benjamin Rhodes, who has worked closely with Haines.

That personality plays out every day in Haines's interactions with top national-security officials in some of the most charged, high-stakes settings in government. She is known for her deferential style—Attorney General Eric Holder has occasionally admonished her to call him "Eric" rather than "Mr. Attorney General"—and tends to eschew the Washington habit of self-aggrandizement.

Even under normal circumstances, these traits might seem an odd fit at an agency tasked with deception and death. But they are especially surprising at a moment when the White House is attempting a far-reaching, and controversial, plan to rein in the CIA's role in the war on terror. Haines, in many ways the ultimate outsider, will be working to reform a proud and deeply insular culture. To be sure, not every top CIA official of recent vintage has come from within the agency. But none has been quite like Haines. She will be the first woman to hold the deputy job at an agency that is still dominated by men. And she will be a lawyer in a culture of forward-leaning operators who fret about their hands being tied by risk-averse attorneys. Moreover, she has spent most of her career in government working at the State Department, an agency that does not typically share the same outlook as the CIA. (Indeed, when Obama tapped Haines for the CIA position, her nomination to be State Department legal adviser was pending before the Senate. It has since been withdrawn.)

*Please visit newsweek.com for entire article.

ODNI Releases ODNI Attorney General Procedures for Conducting Intelligence Activities

Homeland Security Today
January 2021

The Office of the Director of National Intelligence (ODNI) released new procedures approved by the DNI and the Attorney General governing the conduct of ODNI intelligence activities.

As required by Executive Order 12333, these procedures, commonly referred to as the "Attorney General (AG) Guidelines," provide the core protections for ODNI's collection and handling of information concerning U.S. persons in the conduct of lawful intelligence activities. The Guidelines also prescribe the limited circumstances in which ODNI personnel may participate in a U.S. organization without disclosing their ODNI affiliation.

Until the effective date of the new ODNI AG Guidelines on March 23, ODNI will continue to conduct intelligence activities within established National Counterterrorism Center or CIA AG Guidelines.

"As intelligence professionals, our first duty is to the American people," said Director of National Intelligence John Ratcliffe. "We must continue to ensure that we always conduct our intelligence activities lawfully, appropriately integrate intelligence in support of national security, and protect the privacy and civil liberties of every American. ODNI's AG Guidelines provide the framework for executing that mission."

The new ODNI AG Guidelines are part of a multi-year effort to update comparable sets of procedures across the Intelligence Community (IC). They ensure the IC takes a consistent approach to protecting privacy and civil liberties while integrating information across many different intelligence elements and disciplines.

Consistent with the Principles of Intelligence Transparency for the IC, the ODNI's AG Guidelines are unclassified and proactively released in their entirety here. In addition, a narrative document describing key provisions of the Guidelines, including the authorities and restrictions that govern ODNI's

collection, evaluation, retention and dissemination of information, as well as the oversight mechanisms that ODNI will use to ensure compliance with these protections, is available here.

Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says

By Charlie Savage
New York Times
January 2021

A military arm of the intelligence community buys commercially available databases containing location data from smartphone apps and searches it for Americans' past movements without a warrant, according to an unclassified memo obtained by The New York Times.

Defense Intelligence Agency analysts have searched for the movements of Americans within a commercial database in five investigations over the past two and a half years, agency officials disclosed in a memo they wrote for Senator Ron Wyden, Democrat of Oregon.

The disclosure sheds light on an emerging loophole in privacy law during the digital age: In a landmark 2018 ruling known as the Carpenter decision, the Supreme Court held that the Constitution requires the government to obtain a warrant to compel phone companies to turn over location data about their customers. But the government can instead buy similar data from a broker — and does not believe it needs a warrant to do so.

"D.I.A. does not construe the Carpenter decision to require a judicial warrant endorsing purchase or use of commercially available data for intelligence purposes," the agency memo said.

Mr. Wyden has made clear that he intends to propose legislation to add safeguards for Americans' privacy in connection with commercially available location data. In a Senate speech this week, he denounced circumstances "in which the government, instead of getting an order, just goes out and purchases the private records of Americans from these sleazy and unregulated commercial data brokers who are simply above the law."

He called the practice unacceptable and an intrusion on constitutional privacy rights. "The Fourth Amendment is not for sale," he said.

The government's use of commercial databases of location information has come under increasing scrutiny. Many smartphone apps log their users' locations, and the app makers can aggregate the data and sell it to brokers, who can then resell it — including to the government.

It has been known that the government sometimes uses such data for law enforcement purposes on domestic soil.

The Wall Street Journal reported last year about law enforcement agencies using such data. In particular, it found, two agencies in the Department of Homeland Security — Immigration and Customs Enforcement, and Customs and Border Protection — have used the data in patrolling the border and investigating immigrants who were later arrested.

In October, BuzzFeed reported on the existence of a legal memo from the Department of Homeland Security opining that it was lawful for law enforcement agencies to buy and use smartphone location data without a warrant. The department's inspector general has opened an internal review. The military has also been known to sometimes use location data for intelligence purposes.

In November, Vice's Motherboard tech blog reported that Muslim Pro, a Muslim prayer and Quran app, had sent its users' location data to a broker called X-Mode that in turn sold it to defense contractors that work with the U.S. military. Muslim Pro then said it would stop sharing data with X-Mode, and Apple and Google said they would ban apps that use the company's tracking software from phones running their mobile operating systems.

The new memo for Mr. Wyden, written in response to inquiries by a privacy and cybersecurity aide in his

office, Chris Soghoian, adds to that emerging mosaic.

The Defense Intelligence Agency appears to be mainly buying and using location data for investigations about foreigners abroad; one of its main missions is detecting threats to American forces stationed around the world.

But, the memo said, the unidentified broker or brokers from which the government buys bulk smartphone location data does not separate American and foreign users. The Defense Intelligence Agency instead processes the data as it arrives to filter those records which appear to be on domestic soil and puts them in a separate database. Agency analysts may only query that separate database of Americans' data if they receive special approval, the memo said, adding, "Permission to query the U.S. device location data has been granted five times in the past two and a half years for authorized purposes."

Mr. Wyden asked Avril D. Haines, President Biden's new director of national intelligence, about what he called "abuses" of commercially available locational information at her confirmation hearing this week. Ms. Haines said she was not yet up to speed on the topic but stressed the importance of the government being open about the rules under which it is operating.

"I would seek to try to publicize, essentially, a framework that helps people understand the circumstances under which we do that and the legal basis that we do that under," she said. "I think that's part of what's critical to promoting transparency generally so that people have an understanding of the guidelines under which the intelligence community operates."

Mr. Wyden's coming legislation on the topic appears likely to be swept into a larger surveillance debate that flared in Congress last year before it temporarily ran aground after erratic statements by President Donald J. Trump, as he stoked his grievances over the Russia investigation, threatening to veto the bill and not making clear what would satisfy him.

With Mr. Biden now in office, lawmakers are set to resume that unresolved matter. The legislation has centered on reviving several provisions of the Patriot Act that expired and whether to put new safeguards on them, including banning the use of a part known as Section 215 to collect web browsing information without a warrant.

Intelligence Photographs in the News

Cpl Tryston Compton, a geospatial intelligence analyst with Special Purpose Marine Air-Ground Task Force - Southern Command, launches an RQ-11B Raven during an RQ-11B Raven Operator Course at Marine Corps Base Camp Lejeune, North Carolina. SPMAGTF-SC Marines participated in the course to test their knowledge and skills when employing a small unmanned aircraft system.

Information courtesy of Marine Forces Reserve. Photo by Sgt. Andy O. Martinez.

Avril Haines testifies on January 19, 2021 before the United States Senate Select Committee on Intelligence during her confirmation hearing to be the Director of National Intelligence (DNI). The following day the Senate confirmed her nomination by a vote of 84-10. She is the first female to serve as DNI.

Photo courtesy of C-SPAN

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):** 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 3820.3F, 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.