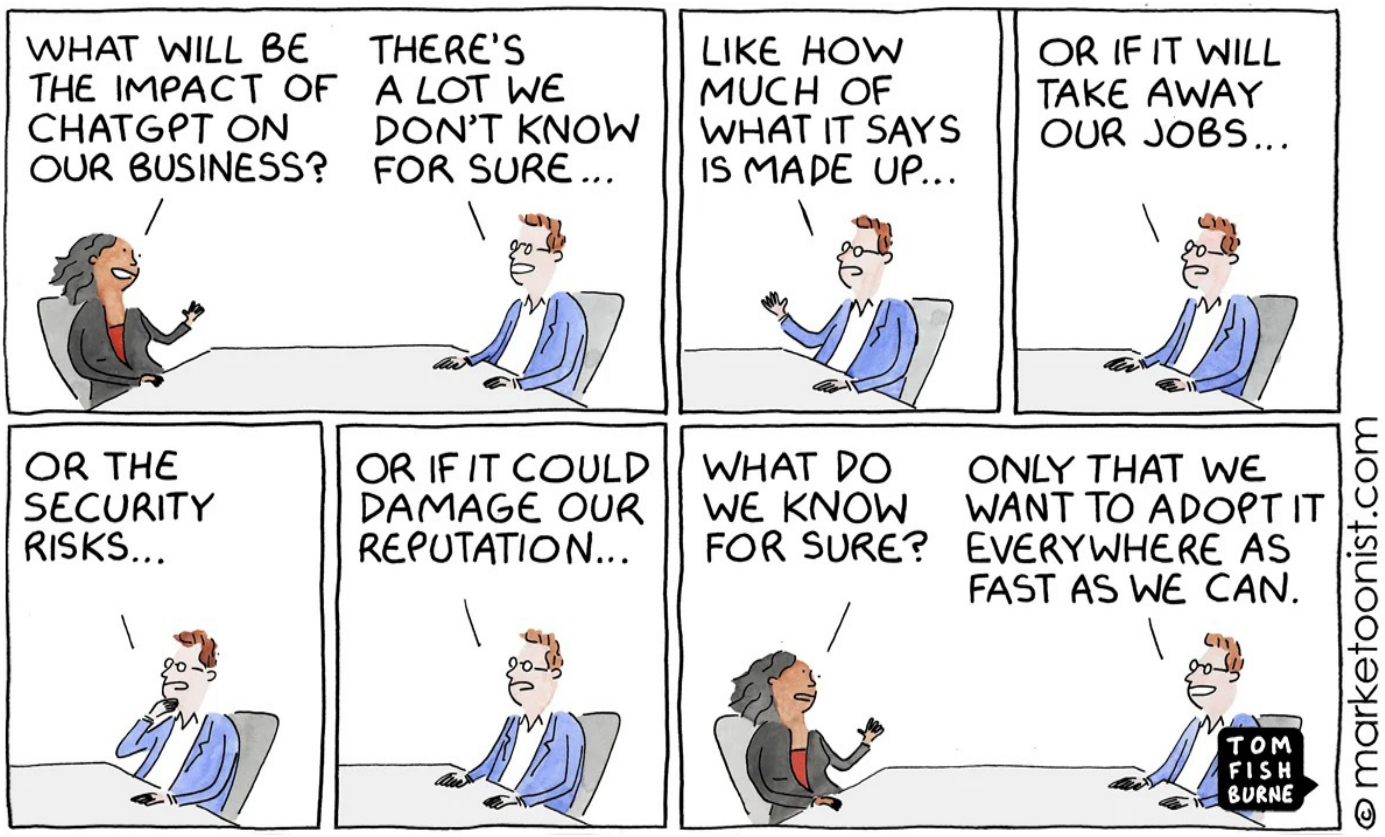
OVERWATCH

"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 17 Issue 4 WINTER 2024

IN THIS ISSUE, FEATURED ARTICLE: WAR AND PEACE IN THE AGE OF ARTIFICIAL INTELLIGENCE



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
Sensitive Activities Officer- Vacant

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

Intelligence News
INTEL - Home

A Message from the Director

Greetings from the Office of the Inspector General for the Marine Corps, Intelligence Oversight Division (IGO). This edition of *Overwatch* is the fourth of calendar year 2024 and my final newsletter to the fleet.

After two decades of service as the Director of IGO, the time has come for me to bid farewell to a community that has been my honor to serve alongside. Throughout these years, I have witnessed firsthand the dedication, professionalism, and unwavering commitment to excellence that define the Intelligence Community. Together, we have navigated complex challenges, upheld the highest standards of integrity, and ensured that our intelligence efforts remained grounded in law, ethics, and our national values. I am deeply proud of all we have accomplished and the relationships we've built along the way. As I move on to the next chapter, I leave with a profound sense of gratitude for the opportunity to serve and with the utmost confidence in the continued success and resilience of the United States Marine Corps and Intelligence Community. Thank you for your collaboration, your support, and your unwavering pursuit of excellence. Semper Fidelis.

Please welcome Mr. Les Troudt as the new Director. He has extensive experience in the Intelligence Community, and I ask that you all support him with the same professionalism you have afforded me through the years.

I would also like to take this moment to thank Mr. Joseph Rutigliano, JAO Branch Head for his support over the last 20 years. His sage advice on critical matters was instrumental in our oversight mission.

As you read my last newsletter, I have concentrated on Artificial Intelligence articles and the challenges of providing effective oversight when AI is implemented. This has been my focus for the last several years and I hope it will continue to be a topic examined and reviewed carefully as the years go by.

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.

I hope my efforts of outreach with this newsletter throughout the last 20 years has provided everyone with issues to critically think about the value of intelligence oversight if this is your profession.

The first article discusses War and Peace in the age of Artificial Intelligence.

Our second article discusses a memo that Sets Rules for Artificial Intelligence and Americans' Private Data

.

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

Featured Article

War and Peace in the Age of Artificial Intelligence

What It Will Mean for the World When Machines Shape Strategy and Statecraft

By Henry A. Kissinger, Eric Schmidt, and Craig Mundie

November 18, 2024

From the recalibration of military strategy to the reconstitution of diplomacy, artificial intelligence will become a key determinant of order in the world. Immune to fear and favor, AI introduces a new possibility of objectivity in strategic decision-making. But that objectivity, harnessed by both the warfighter and the peacemaker, should preserve human subjectivity, which is essential for the responsible exercise of force. AI in war will illuminate the best and worst expressions of humanity. It will serve as the means both to wage war and to end it.

Humanity's long-standing struggle to constitute itself in ever-more complex arrangements, so that no state gains absolute mastery over others, has achieved the status of a continuous, uninterrupted law of nature. In a world where the major actors are still human—even if equipped with AI to inform, consult, and advise them—countries should still enjoy a degree of stability based on shared norms of conduct, subject to the tunings and adjustments of time.

But if AI emerges as a practically independent political, diplomatic, and military set of entities, that would force the exchange of the age-old balance of power for a new, uncharted disequilibrium. The international concert of nation-states—a tenuous and shifting equilibrium achieved in the last few centuries—has held in part because of the inherent equality of the players. A world of severe asymmetry—for instance, if some states adopted AI at the highest level more readily than others—would be far less predictable. In cases where some humans might face off militarily or diplomatically against a highly AI-enabled state, or against AI itself, humans could struggle to survive, much less compete. Such an intermediate order could witness an internal implosion of societies and an uncontrollable explosion of external conflicts.

Other possibilities abound. Beyond seeking security, humans have long fought wars in pursuit of triumph or in defense of honor. Machines—for now—lack any conception of either triumph or honor. They may never go to war, choosing instead, for instance, immediate, carefully divided transfers of territory based on complex calculations. Or they might—prizing an outcome and deprioritizing individual lives—take actions that spiral into bloody wars of human attrition. In one scenario, our species could emerge so transformed as to avoid entirely the brutality of human conduct. In another, we would become so subjugated by the technology that it would drive us back to a barbaric past.

THE AI SECURITY DILEMMA

Many countries are fixated on how to "win the AI race." In part, that drive is understandable. Culture, history, communication, and perception have conspired to create among today's major powers a diplomatic situation that fosters insecurity and suspicion on all sides. Leaders believe that an incremental tactical advantage could be decisive in any future conflict, and that AI could offer just that advantage.

If each country wished to maximize its position, then the conditions would be set for a psychological contest among rival military forces and intelligence agencies the likes of which humanity has never faced before. An existential security dilemma awaits. The logical first wish for any human actor coming into possession of superintelligent AI—that is, a hypothetical AI more intelligent than a human—might be to attempt to guarantee that nobody else gains this powerful version of the technology. Any such actor might also reasonably assume by default that its rival, dogged by the same uncertainties and facing the same stakes, would be pondering a similar move.

Short of war, a superintelligent AI could subvert, undermine, and block a competing program. For instance, AI promises both to strengthen conventional computer viruses with unprecedented potency and to

disguise them thoroughly. Like the computer worm Stuxnet—the cyberweapon uncovered in 2010 that was thought to have ruined a fifth of Iran's uranium centrifuges—an AI agent could sabotage a rival's progress in ways that obfuscate its presence, thereby forcing enemy scientists to chase shadows. With its unique capacity for manipulation of weaknesses in human psychology, an AI could also hijack a rival nation's media, producing a deluge of synthetic disinformation so alarming as to inspire mass opposition against further progress in that country's AI capacities.

It will be hard for countries to get a clear sense of where they stand relative to others in the AI race. Already the largest AI models are being trained on secure networks disconnected from the rest of the Internet. Some executives believe that AI development will itself sooner or later migrate to impenetrable bunkers whose supercomputers will be powered with nuclear reactors. Data centers are even now being built on the bottom of the ocean floor. Soon they could be sequestered in orbits around Earth. Corporations or countries might increasingly "go dark," ceasing to publish AI research so as not only to avoid enabling malicious actors but also to obscure their own pace of development. To distort the true picture of their progress, others might even try deliberately publishing misleading research, with AI assisting in the creation of convincing fabrications.

AI in war will illuminate the best and worst expressions of humanity.

There is a precedent for such scientific subterfuge. In 1942, the Soviet physicist Georgy Flyorov correctly inferred that the United States was building a nuclear bomb after he noticed that the Americans and the British had suddenly stopped publishing scientific papers on atomic fission. Today, such a contest would be made all the more unpredictable given the complexity and ambiguity of measuring progress toward something so abstract as intelligence. Although some see advantage as commensurate with the size of the AI models in their possession, a larger model is not necessarily superior across all contexts and may not always prevail over smaller models deployed at scale. Smaller and more specialized AI machines might operate like a swarm of drones against an aircraft carrier—unable to destroy it, but sufficient to neutralize it.

An actor might be perceived to have an overall advantage were it to demonstrate achievement in a particular capability. The problem with this line of thinking, however, is that AI refers merely to a process of machine learning that is embedded not just in a single technology but also in a broad spectrum of technologies. Capability in any one area may thus be driven by factors entirely different from capability in another. In these senses, any "advantage" as ordinarily calculated may be illusory.

Moreover, as demonstrated by the exponential and unforeseen explosion of AI capability in recent years, the trajectory of progress is neither linear nor predictable. Even if one actor could be said to "lead" another by an approximate number of years or months, a sudden technical or theoretical breakthrough in a key area at a critical moment could invert the positions of all players.

In such a world, where no leaders could trust their most solid intelligence, their most primal instincts, or even the basis of reality itself, governments could not be blamed for acting from a position of maximum paranoia and suspicion. Leaders are no doubt already making decisions under the assumption that their endeavors are under surveillance or harbor distortions created by malign influence. Defaulting to worst-case scenarios, the strategic calculus of any actor at the frontier would be to prioritize speed and secrecy over safety. Human leaders could be gripped by the fear that there is no such thing as second place. Under pressure, they might prematurely accelerate the deployment of AI as deterrence against external disruption.

A NEW PARADIGM OF WAR

For almost all of human history, war has been fought in a defined space in which one could know with reasonable certainty the capability and position of hostile enemy forces. The combination of these two attributes offered each side a sense of psychological security and common consensus, allowing for the informed restraint of lethality. Only when enlightened leaders were unified in their basic understanding of

how a war might be fought could opposing forces determine whether a war should be fought.

Speed and mobility have been among the most predictable factors underpinning the capability of any given piece of military equipment. An early illustration is the development of the cannon. For a millennium after their construction, the Theodosian Walls protected the great city of Constantinople from outside invaders. Then, in 1452, a Hungarian artillery engineer proposed to Emperor Constantine XI the construction of a giant cannon that, firing from behind the defensive walls, would pulverize attackers. But the complacent emperor, possessing neither the material means nor the foresight to recognize the technology's significance, dismissed the proposal.

Unfortunately for him, the Hungarian engineer turned out to be a mercenary. Switching tactics (and sides), he updated his design to be more mobile—transportable by no fewer than 60 oxen and 400 men—and approached the emperor's rival, the Ottoman Sultan Mehmed II, who was preparing to besiege the impermeable fortress. Winning the young sultan's interest with his claim that this gun could "shatter the walls of Babylon itself," the entrepreneurial Hungarian helped the Turkish forces to breach the ancient walls in only 55 days.

The contours of this fifteenth-century drama can be seen again and again throughout history. In the nineteenth century, speed and mobility transformed the fortunes first of France, as Napoleon's army overwhelmed Europe, and then of Prussia, under the direction of Helmuth von Moltke (the Elder) and Albrecht von Roon, who capitalized on the newly developed railways to enable faster and more flexible maneuvering. Similarly, blitzkrieg—an evolution of the same German military principles—would be used against the Allies in World War II to great and terrible effect.

"Lightning war" has taken on new meaning—and ubiquity—in the era of digital warfare. Speeds are instantaneous. Attackers need not sacrifice lethality to sustain mobility, as geography is no longer a constraint. Although that combination has largely favored the offense in digital attacks, an AI era could see the increase of the velocity of response and allow cyberdefenses to match cyberoffenses.

In kinetic warfare, AI will provoke another leap forward. Drones, for instance, will be extremely quick and unimaginably mobile. Once AI is deployed not only to guide one drone but to direct fleets of them, clouds of drones will form and fly in sync as a single cohesive collective, perfect in their synchronicity. Future drone swarms will dissolve and reconstitute themselves effortlessly in units of every size, much as elite special-operations forces are built from scalable detachments, each of which is capable of sovereign command.

In addition, AI will provide similarly speedy and flexible defenses. Drone fleets are impractical if not impossible to shoot down with conventional projectiles. But AI-enabled guns firing rounds of photons and electrons (instead of ammunition) could re-create the same lethal disabling capacities as a solar storm that can fry the circuitry of exposed satellites.

AI-enabled weapons will be unprecedentedly exact. Limits to the knowledge of an antagonist's geography have long constrained the capabilities and intentions of any warring party. But the alliance between science and war has come to ensure increasing accuracy in instruments, and AI can be expected to make more breakthroughs. AI will thus shrink the gap between original intent and ultimate outcome, including in the application of lethal force. Whether land-based drone swarms, machine corps deployed in the sea, or possibly interstellar fleets, machines will possess highly precise capabilities of killing humans with little degree of uncertainty and with limitless impact. The bounds of the potential destruction will hinge only on the will, and the restraint, of both human and machine.

In kinetic warfare, AI will provoke a huge leap forward.

That being so, the AI age of warfare will be reduced primarily to an assessment not of an adversary's capabilities but rather of its intentions and their strategic applications. In the nuclear age, we have already entered such a phase—but its dynamics and

significance will come into much sharper focus as AI proves its worth as a weapon of war.

With such valuable technology involved, humans may not even be the primary targets of AI-enabled war. AI could in fact remove humans as a proxy in warfare entirely, making war less deadly but potentially no less decisive. Similarly, territory alone seems unlikely to provoke AI aggression—but data centers and other critical digital infrastructure certainly could.

Surrender, then, will come not when the opponent's numbers are diminished and its armory empty but when the survivors' shield of silicon is rendered incapable of saving its technological assets—and finally its human deputies. War could evolve into a game of purely mechanical fatalities, the deciding factor being the psychological strength of the human (or AI) who must contest to risk, or forfeit to prevent, a breakthrough moment of total destruction.

Even the motives governing the new battlefield would be alien, to some extent. The English writer G. K. Chesterton once quipped that "the true soldier fights not because he hates what is in front of him, but because he loves what is behind him." An AI war is unlikely to involve love or hate, let alone a concept of soldierly bravery. On the other hand, it may still incorporate ego, identity, and loyalty—although the nature of those identities and loyalties may not be consistent with those of today.

The calculation in warfare has always been relatively straightforward: whichever side first finds intolerable the pain of battle will likely be conquered. The consciousness of one's own shortcomings has in the past produced restraint. Without such awareness, and with no sense for (and thus a great tolerance of) pain, one cannot but wonder what, if anything, would prompt restraint in an AI that has been introduced into warfare, and what would conclude the conflicts it wages. A chess-playing AI, if it had never been informed of the rules dictating the end of the game, could play to the very last pawn.

GEOPOLITICAL RESTRUCTURING

In every age of humanity, almost as if in obedience to some natural law, there has emerged, as one of us (Kissinger) once put it, a unit "with the power, the will, and the intellectual and moral impetus to shape the entire international system in accordance with its own values." The most familiar arrangement of human civilizations is that of the Westphalian system as conventionally understood. The idea of the sovereign nation-state, however, is only a few centuries old, having emerged from treaties that are collectively known as the Peace of Westphalia in the mid-seventeenth century. It is not the preordained unit of social organization, and it may not be suited for the age of AI. Indeed, as mass disinformation and automated discrimination trigger a loss of faith in that arrangement, AI may pose an inherent challenge to the power of national governments. Alternatively, AI may well reset the relative positions of competitors within today's system. If its powers are harnessed primarily by nation-states themselves, humanity could be forced toward a hegemonic stasis, or else toward a new equilibrium of AI-empowered nation-states. But the technology could also be the catalyst of an even more fundamental transition—a shift to an entirely new system, in which state governments would in turn be forced to abandon their central role in the global political infrastructure.

One possibility is that the companies that own and develop AI will accrue totalizing social, economic, military, and political power. Today's governments are forced to contend with their difficult position both as cheerleaders for private corporations—lending their military power, diplomatic capital, and economic heft to promote these homegrown firms—and as supporters of the average citizen suspicious of monopolistic greed and secrecy. That may prove an untenable contradiction.

Meanwhile, corporations could form alliances to consolidate their already considerable strength. Those alliances might be built on complementary advantages and the profit of amalgamation or, alternatively, on a shared philosophy of development and deployment of AI systems. These corporate alliances might take on traditional nation-state functions, though rather than seeking to define and expand bounded territories, they would cultivate diffuse digital networks as their domains.

AI may pose an inherent challenge to the power of national governments.

And there is still another alternative. Uncontrolled, open-source diffusion could give rise to smaller gangs or tribes with substandard but substantial AI capacities, sufficient to administer to, provide for, and defend themselves within some limited scope. Among human groups that reject established authority in favor of decentralized finance, communication, and governance, such technology-enabled proto-anarchy could win out. Or such groupings might incorporate a religious dimension. After all, in terms of reach, Christianity, Islam, and Hinduism have all been larger and longer-lasting than any state in history. In the age to come, religious denomination, more than national citizenship, might conceivably prove the more relevant framework for identity and loyalty.

In either future, whether dominated by corporate alliances or diffused into loose religious groupings, the new "territory" that each group would claim—and over which they would fight—would not be inches of land but a digital landscape, seeking the loyalties of individual users. Linkages between these users and any administration would subvert the traditional notion of citizenship, and agreements between the entities would be unlike ordinary alliances.

Historically, alliances have been forged by individual leaders and have served to augment a nation's strength in case of war. By contrast, the prospect of citizenships and alliances—and perhaps conquests or crusades—structured around the opinions, beliefs, and subjective identities of ordinary people in times of peace would require a new (or very old) conception of empire. It would also force a reassessment of the obligations entailed in pledging allegiance and the cost of exit options, if indeed any were to exist in the AI-entangled future.

PEACE AND POWER

The foreign policies of nation-states have been built and then adjusted by balancing idealism and realism. The temporary balances struck by our leaders are seen in retrospect not as end-states but as only ephemeral (if necessary) strategies for their time. With each new age, this tension has produced a different expression of what constitutes political order. The dichotomy between the pursuit of interests and the pursuit of values—or between a particular nation-state's advantage and the global good—has been part of this unending evolution. In the conduct of their diplomacy, leaders of smaller states historically have responded straightforwardly, prioritizing the necessities of their own survival. By contrast, those responsible for global empires, with the means to realize additional goals, have faced a more agonizing predicament.

Since the beginning of civilization, as human units of organization have grown, they have simultaneously achieved new levels of cooperation. But today, perhaps because of the scale of planetary challenges as well as to the material inequalities evident among and within states, a backlash against this trend has surfaced. AI could prove commensurate to the demands of this still-grander scale of human governance, capable of seeing with granularity and fidelity not merely the imperatives of the country but also the interplay of the globe.

We harbor a hope that AI, deployed for political ends at home and abroad, might do more than just illuminate balanced tradeoffs. Ideally, it could provide new, globally optimal solutions, acting on a longer time horizon and with greater precision than humans are capable of, and thus bringing competing human interests into alignment. In the coming world, machine intelligences navigating conflict and negotiating peace might help clarify, or even surmount, traditional dilemmas.

However, if AI were indeed to fix problems that we should have hoped to solve ourselves, we could face a crisis of confidence—of both overconfidence and the lack of confidence. To the former, once we understand the limits of our own ability for self-correction, it may be difficult to admit that we have come to cede too much power to machines in handling existential issues of human conduct. To the latter, the realization that simply removing human agency from the handling of our affairs has been enough to solve our most intractable problems might reveal too explicitly the shortcomings of human design. If peace has always been but a simple

voluntary choice, the price of human imperfection has been paid in the coin of perpetual war. To know that a solution has always existed but has never been conceived by us would be crushing to human pride.

In the case of security, unlike that of the displacement of people in scientific or other academic endeavors, we may more readily accept the impartiality of a mechanical third party as necessarily superior to the self-interestedness of a human—just as humans easily recognize the need for a mediator in a contentious divorce. Some of our worst traits will enable us to exhibit some of our best: that the human instinct toward self-interest, even at the expense of others, may prepare us for accepting AI's transcendence of the self

Spy Agency Memo Sets Rules for Artificial Intelligence and Americans' Private Data

By Charlie Savage

Charlie Savage writes about national security and legal policy for the NY Times

A previously confidential directive by Biden administration lawyers lays out how military and spy agencies must handle personal information about Americans when using artificial intelligence, showing how the officials grappled with trade-offs between civil liberties and national security.
The results of that internal debate also underscore the constraints and challenges the government faces in issuing rules that keep pace with rapid advances in technology, particularly in electronic surveillance and related areas of computer-assisted intelligence gathering and analysis.

The administration had to navigate two competing goals, according to a senior administration official, Joshua Geltzer, the top legal adviser to the National Security Council: "harnessing emerging technology to protect Americans, and establishing guardrails for safeguarding Americans' privacy and other considerations."

The White House last month held back the four-page, unclassified directive when President Biden signed a major national security memo that pushes military and intelligence agencies to make greater use of A.I. within certain guardrails.

After inquiries from The New York Times, the White House has made the guidance public. A close read and an interview with Mr. Geltzer, who oversaw the deliberations by lawyers from across the executive branch, offers greater clarity on the current rules that national security agencies must follow when experimenting with using A.I.

A.I. AND PRIVACY

Read the guidance to intelligence agencies.
The answers they reached, the document shows, are preliminary. Because the technology is evolving quickly, national security lawyers for Mr. Biden decided the government must revisit the guidance in six months — a task that will now fall to the Trump administration.

The A.I. systems that private sector companies are developing, like OpenAI's large language model, Chat GPT, apparently far surpass anything the government can do. As a result, the government is more likely to buy access to an A.I. system rather than create its own. The guidance says that such a system will count as being "acquired" if it is hosted on a government server or if officials have access to it beyond what anyone could do on the internet.

Training A.I. systems require feeding them large amounts of data, raising a critical question for intelligence agencies that could influence both Americans' privacy interests and the ability of national security agencies to experiment with the technology. When an agency acquires an A.I. system trained by a private sector firm using information about Americans, is that considered "collecting" the data of those Americans?

The answer determines whether or when long-existing limits for what a national-security agency can do with personal data about Americans, developed for surveillance programs, kick in.

Rules for what an agency employees can do with domestic information it has collected include limiting when they may retain such data, how they must store it, the date by when they must delete it, under what circumstances their analysts may query it, and when and how the agencies may disseminate it to other parts of the government.

Many of those limits were developed in the context of older technologies like wiretapping phone calls. The Biden legal team, Mr. Geltzer said, worried that applying those privacy rules at the point when A.I. systems are acquired would severely inhibit agencies' ability to experiment with the new technology.

As a result, the guidance says that when an intelligence agency acquires an artificial intelligence system that was trained using Americans' data, that does not generally count as collecting the training data — so those existing privacy-protecting rules, along with a 2021 directive about collecting commercially available databases, are not yet triggered.

Still, the Biden team was not absolute on that question. The guidance leaves open the possibility that acquisition might count as collection if the agency has the ability to access the training data in its original form, "as well as the authorization and intent to do so."

The use of sensitive information in training an A.I. system — especially when it is capable of spitting that data back out in response to a prompt — has raised novel and contested issues on other fronts. The Times and several other news organizations are suing OpenAI and Microsoft over their use of copyrighted news articles to train chatbots.

The Biden team also addressed what it would mean if an agency uses data about Americans already in its possession to modify or augment an A.I. system. That could be fine-tuning the system's training to change how it weighs certain factors or connecting it to additional data and tools without altering its underlying processes.

In that case, the document says, longstanding attorney general guidelines about spy agencies' using, querying, retaining, and disseminating Americans' information kick in — as do laws that can further limit what the government may do with domestic information, like the Privacy Act.

The guidance requires intelligence agencies to consult with senior legal and privacy officers before any such action. And it raises caution about feeding an A.I. system with information gathered by the Foreign Intelligence Surveillance Act: Officials are required to consult the Justice Department and the Office of the Director of National Intelligence first. In the world of national security surveillance, there are rules limiting when an analyst may query a database of raw intercepts in search of information about Americans. The guidance examined a similar issue: when an intelligence official may prompt an A.I. system by asking it a question about an American.

If, in response to such a prompt, an A.I. system spits out information that an intelligence agency did not already have, the guidance says, that counts as collection if the analyst decides to copy, save or use that new information. In that case, the limits on handling Americans' personal information kick in. The guidance also encourages intelligence agencies to consider steps that could make oversight efforts easier. But the guidance does not require such precautions.

For example, it tells agencies to explore possible ways to mark information about Americans collected by an A.I. system and any intelligence reports containing that information. And it asks agencies to "consider what documentation, if any, is appropriate" that would log when analysts have submitted a prompt that was designed to return Americans' information.

The guidance governing personal information about Americans' personal privacy joins a separate memo released in October that outright bans the use of A.I. in some circumstances, such as by requiring humans to remain in the loop when carrying out a presidential decision to launch or terminate a nuclear strike.

That earlier memo also laid out "high impact" activities that military and intelligence agencies could in theory do with the technology — but only with more intensive safeguards like rigorous risk assessments, testing and human oversight. Those included using A.I. to track people based on biometrics for military or law enforcement action, classifying people as known or suspected terrorists and denying entry to a foreign visa applicant.

"These documents will enable the executive branch to use artificial intelligence more fully and at the same time more responsibly to advance public safety and national security, while also requiring executive branch lawyers to revisit key legal considerations in light of evolving technology and the findings from

particular use cases," Mr. Geltzer said.

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

Service in ONI

The ONI was established in the Bureau of Navigation in March 1882 by *Navy Department General Order No. 292 , nearly 40 years before the fledgling Headquarters* Military Intelligence Section. Marines served at ONI prior to the creation of the Corps' Military Intelligence Section, with the first Marine, First Lieutenant Lincoln Karmany, being assigned to ONI in January 1893. Captain (later Major) William L. Reddles served as assistant naval attaché in Tokyo, Japan, from 1915 to 1918 and then served as a lieutenant colonel in ONI from 1920 to 1921. In the 1930s, there were often three to five Marine officers at ONI, most often serving in or leading the Far East and Latin American sections. For example, Captain Ronald Aubry Boone, who served as S-2, 4th Marine Regiment, in Shanghai at the start of the Sino-Japanese War in 1937, was promoted to major and assigned to ONI in 1939 as assistant head of the Far East Section.

While we do not have evidence that duty at ONI was viewed as career enhancing by Marines of that era, we do know that many Marines who served at ONI were later promoted to colonel and general officer ranks. A future Commandant (1934–37), Major John H. Russell Jr., came to ONI in 1913 after serving as commander of the Marine Detachment, American Legation, Peking (Beijing), China. In 1916, Major Russell worked with Navy Commander Dudley W. Knox on a reorganization plan for ONI that was approved by Secretary of the Navy Josephus Daniels on 1 October 1916. In early 1917, Major Russell took charge of Section A, Organization and Control of Agencies for the Collecting of Information, which included debriefing of commercial travelers as well as control of hired agents and informants. Lieutenant Colonel John C. Beaumont served in ONI in 1920, was promoted to colonel in 1926, commanded 4th Marines in 1933, and was promoted to brigadier general in 1935.

Brigadier General Dion Williams is considered the father of amphibious reconnaissance based on his book *Naval Reconnaissance*, which he wrote in 1905–6 while a major on the instructor staff at the Naval War College. He served as a staff intelligence officer in ONI and on intelligence duty abroad from November 1909 to March 1913. From 1924 to 1925, as a brigadier general, he was director of operations and training at Headquarters and supervised the Military Intelligence Section.

U.S. Naval Attachés Abroad

In 1910, the first of many Marines was sent to Tokyo to serve as assistant American Legation U.S. naval attaché in Tokyo for language training. Most notably, Captain Ralph Stover Keyser, who later served as Major General Lejeune's G-2 in France, served as assistant naval attaché at the American embassy in Tokyo from January 1912 to February 1915. Marine officers served in Tokyo, gaining Japanese language capability, through summer 1941, when the decision was made to withdraw the naval attaché office from Japan. The two Marines evacuated in 1941 were Captain Bankson T. Holcomb Jr. and First Lieutenant Ferdinand W. Bishop. Holcomb would go on to serve as director of intelligence at Headquarters in 1957.

Marines were normally assigned as assistant naval attachés. Lieutenant Colonel James C. Breckinridge was the first Marine to serve as the naval attaché, being assigned to Christiania (now Oslo), Norway, in 1917 with the added duty of covering Denmark and Sweden. In the interwar years, more Marines served in unique or first-time attaché roles. Captain David R. Nimmer was sent to Moscow in March 1934 as the assistant naval attaché but ended up as the second Marine naval attaché because the Navy officer assigned as naval attaché to Moscow turned down his orders. Perhaps the most famous Marine of this period to serve as an assistant naval attaché was Colonel Pedro A. del Valle, who later commanded the 11th Marine Regiment (Artillery) at Guadalcanal and the 1st Marine Division at Okinawa and would retire as a lieutenant general. Colonel del

Valle served as assistant naval attaché in Rome, Italy, from 1935 to 1936 and was a military observer with the Italian Army during its campaigns in Ethiopia.

Communications Intelligence

Department of the Navy communications intelligence began in the fashion of one-at-a-time, on-the-job training for experienced communications and linguist personnel. This activity was controlled by the director of naval communications within the Communications Security Section, which was formed in 1922. By 1926, the Communications Security Section began to conduct small training classes for officers, and the first class included Captain Leo F. S. Horan. By 1928, Communications Security Section began classes for enlisted intercept operators in a classroom that was constructed on the roof of the main Navy building in Washington, DC, earning intercept operators who graduated the course the nickname "On-the-Roof Gang" or OTRG. Two of the classes were entirely comprised of Marines.

Some of the Marines detailed to Japan for foreign language training did follow-on tours of duty at radio intercept stations. First Lieutenant Alva B. Lasswell was sent to Tokyo for Japanese language training from 1935 to 1938, to the 16th Naval District's C Station radio intercept station (Corregidor) in 1938–39, and Shanghai in 1939. Lasswell's tour at C Station exposed him to the technical aspects of communications intelligence: cryptanalysis, traffic analysis, and translation since all were performed at Corregidor in support of both the Asiatic Fleet and Army General Douglas MacArthur.[32]

Although not an activity of the interwar years, it is worth noting that experience gained by this small group of linguists and cryptologists in Japan and China directly contributed to the success of the U.S. Pacific Fleet in World War II (WWII). Alva Lasswell was the linguist and cryptologist who later decrypted and translated the message traffic in 1942 that led to the Battle of Midway and the 1943 traffic that led to the downing of Admiral Isoroku Yamamoto's plane. It is also interesting to note that Marines were assigned to Fleet Radio Unit Pacific performing communications intelligence as WWII began, with Marines such as Bankson Holcomb taking a "direct support" radio intercept unit aboard USS *Enterprise* (CV 6) for the February 1942 Marshalls–Gilberts raids.

Special Reconnaissance

Special duty assignments—in this case of intelligence, reconnaissance, and related missions—were accounted for in the U.S. Navy regulations of 1920, which stated in article 127, section 2, of its chapter on general in- structions to officers that "no officer of the Navy or of the Marine Corps shall proceed to a foreign country on special duty connected with the service except un- der orders prepared by the Bureau of Navigation or by the Major General Commandant as the case may be, and signed by the Secretary of the Navy."[34] While records do not note how many Marines were detailed to special duty assignments in the interwar years, the provision of Navy regulations citing the Major General Commandant's authority to prepare such orders indicates anticipation that Marines would be used in this manner. Perhaps the most famous special duty assignment of a Marine during this period is the mission of Lieutenant Colonel Ellis to survey islands in East Asia. Ellis's special duty was approved by the Major General Commandant and the secretary of the Navy. Unfortunately, the mission ended with Ellis's death in Palau in 1923.

Another example of a special duty reconnaissance mission is the work of then-major William Arthur Worton in China from 1935 to 1936.[36] Major Worton, who as a platoon commander during World War I had been badly wounded in a gas attack in Belleau Wood, was assigned to ONI's Far East Section after several tours of duty in China, including completion of the State Department's Chinese language course in Beijing and a tour as an intelligence officer in 3d Brigade under Major General Smedley Butler. While serving at ONI, Worton proposed the fleet intelligence officer of the Asiatic Fleet be assigned an assistant who would be based in Hong Kong or Shanghai to recruit and deploy foreign agents to Japanese ports to observe and report on the Japanese Navy. Worton was sent to Shanghai to execute his plan, which he did undercover as a businessman. Worton was able to set up an agent network, but he recommended successive Marines assigned to this duty be designated assistant naval attachés because the proximity of Shanghai's international settlement to the 4th Marines often meant running into fellow Marine officers who did not always believe he was there to start a business.

Intelligence Photographs in the News

Service members with the Philippine Marine Corps, and U.S. Marines with Marine Rotational Force-Southeast Asia, pose for a group photo during an intelligence subject matter expert exchange as part of Exercise Sama Sama 2024 at Fort Bonifacio, Manila, Philippines, Oct. 10, 2024. Sama Sama is a bilateral exercise hosted by the Philippines and the United States, with participants from Australia, Canada, France, and Japan, designed to promote regional security cooperation, maintain and strengthen maritime partnerships, and enhance maritime interoperability. MRF-SEA is a rotational unit executing a Marine Corps Forces Pacific operational model that involves training events and exchanges with partner military subject matter experts, promotes security goals with Allied and partner nations, and ensures a persistent I Marine Expeditionary Force presence west of the International Date Line. (U.S. Marine Corps photo by Cpl. Tyler Wilson)

Photo by Cpl. Tyler Wilson
Marine Rotational Force - Southeast Asia

10.17.2024
Photo by Sgt. Amelia Kang
15th Marine Expeditionary Unit

U.S. Marine Corps Sgt. Colin Clark, left, a mortarman assigned to Bravo Company, Battalion Landing Team 1/5, 15th Marine Expeditionary Unit, and a native of Texas, and a Philippine Marine assigned to Intelligence Company, 3rd Marine Brigade, walk to a firing point to employ a NightFighter S counter-unmanned aerial vehicle system during a subject matter expert exchange as part of exercise KAMANDAG 8 at Tarumpitao Point, Palawan Province, Philippines, Oct. 17, 2024. KAMANDAG is an annual Philippine Marine Corps and U.S. Marine Corps-led exercise aimed at enhancing the Armed Forces of the Philippines' defense and humanitarian capabilities by providing valuable training in combined operations with foreign militaries in the advancement of a Free and Open Indo-Pacific. This year marks the eighth iteration of this exercise and includes participants from the French Armed Forces, Royal Thai Marine Corps, and Indonesian Marine Corps; including continued participation from the Australian Defense Force, British Armed Forces, Japan Ground Self-Defense Force, and Republic of Korea Marine Corps. (U.S. Marine Corps photo by Sgt. Amelia Kang

Photo by **Lance Cpl. Joaquin Carlos Dela Torre**
U.S. Marine Corps Training and Education Comman

U.S. Marine Corps Maj. Jacqueline Fischer, recipient of the William J. Donovan Intelligence Writing Award, center, poses for a photo during the 2023-2024 Academic Awards Ceremony on Marine Corps Base Quantico, Virginia, June 3, 2024. The award is presented to the student with the most outstanding paper on intelligence or an intelligence-related topic. Marine Corps University hosted the ceremony to recognize service members from across the globe for their achievements for this past academic year. (U.S. Marine Corps photo by Lance Cpl. Joaquin Dela Torre)

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.