



Ex Verba Victoria

POVA LEAFLET DROP - JUNE 2023

PRESIDENT'S MESSAGE

Greetings and welcome to your June Leaflet Drop.

Your Board of Directors held our monthly meeting on 28 June. Attending: Brett Cox, Larry Dietz, Jesse Manning, Mike Rogers, Ham Salley, and Daniel Wood. Ray Ambrozak attended as a guest.

Anyone who would like a copy of the minutes can email me at: Dietz.POVA@gmail.com and I will send a copy. Our next meeting is 26 July at 1900 Eastern Time. Members are welcome to attend.

Here are the Statistics for the May Leaflet Drop

- Sends: 578
- Opens: 56%
- Clicks: 2%)
- Bounces: 9
- Unsubscribes: 0

On June 1 we welcomed Jacob Mellberg as a new serving member.

On June 16 I had the pleasure of meeting with BG (R) Ed Burley, a Life Member of POVA and a member of the Board the PRA for a cordial and productive discussion about the two organizations.

We have been unable to schedule a virtual office call with the CG of SWC who serves as the PSYOP Regiment Home Base Commander. If you are able to help in this effort, please contact me.

We continue the transition from our Michigan roots by establishing our banking relationship with the national firm, Edward James. Our end of June 2023 quarter balance was \$11,063.

Our new official mailing address is: POVA, 117 Bernal Road, Suite 70-338, San Jose, CA 95119.

Our Scholarship committee is exploring ways to streamline our scholarship process. If you are interested in helping out with this worthwhile effort feel free to contact Dan Wood at DWood1180@gmail.com.

The St. Louis Gateway Chapter of the Association of the United States Army (AUSA) awarded the Soldiers of the Year and the Senior NCO's of the Year from the commands in the St. Louis Region. POVA is pleased to congratulate SPC Christina Huff of the 318th POC and !SG Michael McCarty (not pictured) of the 308th POC on their amazing accomplishments and being designated as the best of the best to represent their Battalion in 2023. Hooah!

We would like to expand our coverage in the Leaflet Drop. If you have any appropriate military events coming up or information you would like to share with the PSYOP Community, please send the information to me at: Dietz.POVA@gmail.com and I will include it in our next issue.

Our next virtual POVA Board meeting is scheduled for 1900 Eastern time on 26 July via Google Meet. If you are interested in attending, please email me for an invite.

If you missed the May Leaflet Drop, you can find it at: <https://conta.cc/3N0tviW>

Larry

Lawrence D. Dietz
President

PSYOP NEWS - JUNE 2023

26 June 23

Trojan Horse Smartwatches Target Military Personnel

Using a ploy as old as the days of Troy, when the Greeks gifted the people of Troy with a magnificent hollow wooden horse in which Greek soldiers were hidden, an adversary of the U.S. is employing a modern-day slant to the infamous "Trojan Horse". Both the United States Army and Navy are advising all U.S. military personnel that unsolicited smartwatches are being sent to personnel and that these devices contain malware targeting the information on servicemember's devices.

<https://news.clearancejobs.com/2023/06/26/trojan-horse-smartwatches-target-military-personnel/>

25 June

Poll finds continued public support for Ukraine, Taiwan aid

A new [poll on national security issues](#) finds three-quarters of respondents believe it is important for Ukraine to win its war against Russia's invasion, but not all of them support [providing Ukraine military aid](#).

<https://www.defensenews.com/air/2023/06/25/poll-finds-continued-public-support-for-ukraine-taiwan-aid/>

24 June 23

Vladimir Putin Addresses Russia | Reports of Civil War, PsyOps, and CIA Involvement Saturate The Information Space

Just a few hours ago, Russian President Vladimir Putin made a speech describing an ongoing operation led by "external forces" who seek to "split the unity of the Russian people."

His speech comes after [news](#) that PMC Wagner Group Commander Yevgeny Prigozhin has seized control of the port city of Rostov-on-Don while demanding the resignation of Russian Defense Minister Sergei Shoigu.

<https://www.thegatewaypundit.com/2023/06/vladimir-putin-addresses-russia-l-reports-civil-war/>

22 June 23

White House mum on jailed Defense News correspondent

Senior White House officials said press freedom would be among the topics discussed this week by President Joe Biden and Indian Prime Minister Narendra Modi in private meetings, but would not commit to specifically intervening in the case of [Defense News contributor Vivek Raghuvanshi](#).

Raghuvanshi, a journalist and freelancer to Defense News for more than three decades, was [jailed in mid-May by India's Central Bureau of Investigation](#) on charges of espionage. The Indian government has released minimal information on his arrest.

<https://www.defensenews.com/congress/2023/06/22/white-house-mum-on-jailed-defense-news-correspondent/>

20 June 23

Chinese Next Generation Psychological Warfare

China views psychological warfare, centered on the manipulation of information to influence adversary decisionmaking and behavior, as one of several key components of modern warfare. The U.S. military's increased focus on China and preparations for a potential U.S.-China conflict mean that it is important to understand how Chinese psychological warfare capabilities may evolve and what they would mean for Chinese strategic behavior in a crisis or conflict. The author explores Chinese military thinking about next-generation psychological warfare. China is interested in both advanced computing, such as big data, and brain science for their potential military applications to improve future psychological warfare capabilities.

https://www.rand.org/pubs/research_reports/RRA853-1.html

20 June 23

SOCKOR Change of Command

Brig. Gen. Derek Lipson replaced Maj. Gen. Michael Martin as the commander of U.S. Special Operations Command – Korea (SOCKOR) during a change-of-command ceremony at Camp Humphreys, South Korea on June 12, 2023.

<https://sof.news/news/sockor-change-of-command-june-2023/>

17 June 23

Chinese Intelligence Army Quietly Operates ‘Service Centers’ in 7 US Cities

A Chinese intelligence agency quietly operates “service centers” in seven American cities, all of which have had contact with Beijing’s national police authority, according to state media reports and government records reviewed by the Daily Caller News Foundation.

<https://dailycaller.com/2023/06/17/china-intelligence-service-centers-ccp/>

16 June 23

Putin is prioritizing control over efficiency, and it’s not going to serve him well in the long run. It’s going to take weeks, or even months, before Ukraine and allies can confidently assess the status of Ukraine’s ongoing counteroffensive. But in the interim, Putin is responding to the increased military pressure by further tightening control over his population- both in terms of the military and civil society. He’s also doubling down on political alliances that might sound promising but are unlikely to offer Russia any long-term economic or political benefit.

<https://thearkingroup.com/highlights/>

16 June 23

Intelligence analysts confront the reality of deepfakes

The rise of AI — and what it means for the future of intelligence — was a hot topic at the recent GEOINT 2023 conference held in St. Louis.

During a panel discussion, officials from the National Geospatial-Intelligence Agency hailed the value of AI tools and machine learning to analyze thousands of satellite images and quickly unravel critical insights. They also alluded to the dark side of AI and the danger it creates when it’s exploited for misinformation.

“The future of geoint is about going faster; it’s about using artificial intelligence,” said James Griffith, NGA’s director of source operations and management. He noted that NGA is responsible for collecting, analyzing and distributing data in support of national security as well as civilian agencies.

<https://spacenews.com/intelligence-analysts-confront-the-reality-of-deepfakes/>

15 June 23

The Dynamics of the Ukrainian IT Army’s Campaign in Russia

Our understanding of cyber operations is almost entirely driven by defenders. Reports from cybersecurity companies, non-profit organizations, and government agencies offer a view into what and whom cyber operations target, but this perspective is partial, only catching bits and pieces of the overarching campaign. Leaked documents, most notably Edward Snowden’s leak of **Presidential Policy Directive 20** and **other documents** from the National Security Agency, and the occasional **statement** from U.S. Cyber Command offer some visibility into how and

where offensive operations are conducted, but still leave many gaps in understanding the landscape. However, the **Ukrainian IT Army**, a hacktivist group organized in response to the ongoing Russian invasion and likely affiliated with the Ukrainian government, offers a unique viewpoint into the decisions and actions of the offensive side and how cyberspace can be leveraged during a war.

<https://www.lawfareblog.com/dynamics-ukrainian-it-armys-campaign-russia>

15 June 23

Space Force Could Get a Guard Force and Part-Time Guardians, If House Lawmakers Get Their Way

The **Space Force** could soon have a Space **National Guard** -- as well as the addition of part-time Guardians -- if two different legislative proposals are approved by Congress.

The House's proposed defense authorization bill for the coming year aims to turn more than a dozen Air National Guard units into a Space National Guard. It's the third year that the move has been pushed forward in the annual policy bill, but the first time it has been included in the draft itself instead of being included as a separate amendment.

The draft legislation would also give the Space Force the option of a part-time, active-duty status for Guardians, replacing the conventional idea of a reserve force as a way to offer flexibility in serving. Getting it passed into law is one of the top priorities for the service.

<https://www.military.com/daily-news/2023/06/15/space-force-could-get-guard-force-and-part-time-guardians-if-house-lawmakers-get-their-way.html>

15 June 23

Senate Select Committee on Intelligence Passes Intel Act, Including Security Clearance and Classification Reform

The Senate Select Committee on **Intelligence** unanimously approved the **Intelligence Authorization Act for Fiscal Year 2024 (IAA)**, providing necessary funding, legal authorities, and enhanced oversight for the U.S. Intelligence Community (IC).

https://news.clearancejobs.com/2023/06/15/senate-select-committee-on-intelligence-passes-intel-act-including-security-clearance-and-classification-reform/?_hsmi=262645044&_hsenc=p2ANqtz-9z6mY9ae528hwX4cv78BYsIPq0KVzY_OHJy5SbAJdeIVSqYfh4NxaTJzkRx_6rwiDK-41r_k7hUeTiaHcywEdv0ZTLWw

14 June 23

Exposed: Disturbing details of the Pentagon "Perception Management" Office
Despite its low-key rollout, IPMO looks set to be a hugely influential new DoD agency in the future, waging ceaseless information warfare at home and abroad. What makes the new venture all the more sinister is that such capabilities are nothing new; the Pentagon has managed multiple similar, if not identical, operations in the past and continues to do so, despite significant controversy and public backlash.

Indeed, the DoD's **official dictionary** has a dedicated definition of "perception management", linking the practice to "psychological operations," which are defined as actions intended to influence the "emotions, motives, objective reasoning, and ultimately the behavior" of target governments, organizations, groups, and individuals:

Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning as well as to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover and deception, and psychological operations.

<https://mronline.org/2023/06/14/exposed-disturbing-details-of-the-pentagon-perception-management-office/>

14 June 23

Let's Stop Pretending Spying is a Big Deal

When U.S. officials **complained** at the annual Shangri-La Dialogue in Singapore early this month that a Chinese naval vessel had dangerously cut off a U.S. destroyer in international waters as it passed through the Taiwan Strait, China's defense minister had a ready-made answer for how such hazards could best be avoided in the future.

"For China, we always say mind your own business, take good care of your own vessels, your fighter jets, take good care of your own territorial airspace and waters," **said** Gen. Li Shangfu. "If that is the case, then I don't think there will be future problems."

<https://foreignpolicy.com/2023/06/14/us-china-spying-cuba-international-waters-taiwan/>

10 June 23

The Role of Special Operations Forces in Irregular Warfare within the Framework of Great Power Competition

In an era defined by increasing geopolitical tensions and evolving threats, irregular warfare emerges as a salient component of global conflict. The United States Special Operations Forces (SOF) stand at the crux of this irregular warfare landscape, uniquely equipped to respond to diverse challenges and ensure national security interests. However, the question arises whether SOF should be the leading effort in American irregular warfare across the globe within the context of great power competition.

<https://www.linkedin.com/pulse/role-special-operations-forces-irregular-warfare-within-sal-artiaga/>

9 June 23

US cyber experts sent to Latin America on hunt-forward' mission

McLEAN, Va. — U.S. cyber specialists were sent south to identify digital weaknesses on foreign networks and expose tools hackers employ, according to an official with Cyber Command.

The so-called hunt-forward mission, handled by experts on the **Cyber National Mission Force**, was conducted inside Southern Command's area of responsibility, which comprises more than two-dozen countries such as Argentina, Brazil, Jamaica and Nicaragua.

"We had our first defend-forward mission, a hunt-forward mission, in SOUTHCOM just recently, which is amazing," Brig. Gen. Reid Novotny said June 8 at the Potomac Officers Club's Cyber Summit in McLean, Virginia. "The whole point of the

defend-forward mission is to learn something on someone else's network, a partner network, another nation's network, so we can bring back that information and make sure our networks are more secure."

<https://www.c4isrnet.com/cyber/2023/06/09/us-cyber-experts-sent-to-latin-america-on-hunt-forward-mission/>

7 June 23

Chinese 'Volt Typhoon' hack underlines shift in Beijing's targets, skills
WASHINGTON — For **decades**, Chinese hackers focused on wholesale and **often ham-handed** theft of Western trade secrets, what then-NSA director Gen. Keith Alexander called in 2012 "**the greatest transfer of wealth in history**." But in recent years, the NSA and independent experts agree, the Chinese have gotten a lot subtler — and some of their best hackers have changed tactics, moving from using cyberspace for theft to using it to prepare the battlefield of a future conflict.

This shift, years in the making, became unmistakable last month, when news broke of a widespread security breach of US critical infrastructure, particularly around the strategically crucial island of **Guam**. While it's not not a harbinger of impending apocalypse or a major breakdown in an increasingly fraught relationship, experts told Breaking Defense that the activity serves as a scary sign of a kind of new normal, where both superpowers are using cyber capabilities to prepare for a potential open war.

<https://tinyurl.com/3j9eu8hc>

6 June 23

What ChatGPT Can and Can't Do for Intelligence

The prospects of ChatGPT for intelligence are mixed. On the one hand, the technology appears "**impressive**," and "**scarily intelligent**," but on the other hand, its own creators **warned** that "it can create a misleading impression of greatness." In the absence of an expert consensus, researchers and practitioners must explore the potential and downsides of the technology for intelligence.

<https://www.lawfareblog.com/what-chatgpt-can-and-cant-do-intelligence>

5 June 23 Special Operations Forces News Update

CA Officer Assignment. Brig. Gen. Andree G. Carter, deputy commanding general, U.S. Army Civil Affairs and Psychological Operations Command, Fort Bragg, North Carolina, will be assigned as the commander, 350th Civil Affairs Command, Pensacola, Florida.

193rd SOW and ACE. Agile Combat Employment or ACE is a concept that the 193rd Special Operations Wing is incorporating into its training program. The wing is exploring expansion of its course offerings at Fort Indiantown Gap in Pennsylvania. Read more in "**Wing eyes Regional Training Site as location for national Agile Combat Employment instruction**", *193rd SOW*, June 2, 2023.

FBNC Now Fort Liberty. A big chunk of Airborne and Special Forces heritage has gone away as the long-time name of Fort Bragg **has now been struck from the history books**. ([Military.com](https://www.military.com), June 2, 2023).

Chinese PSYOP. A report by RAND Corporation provides information on the psychological warfare capabilities of the Chinese military and some of its emerging operational concepts. China views the manipulation of information to influence adversary decisionmaking and behavior as a key component of modern warfare. *Chinese Next-Generation Psychological Warfare*, RAND, June 2023, PDF, 224 pages.

https://www.rand.org/pubs/research_reports/RRA853-1.html

2 June 23

Information Operations and the new Commandant Marine Corps (CMC)

Compass Points reported yesterday on the nomination of General Eric Smith to be the next Commandant of the Marine Corps. Perhaps as a part of his preparation for confirmation hearings and meetings, the incoming Commandant might want to broaden his preparation by reviewing the nearly three-hundred prior posts on Compass Points, all of which encourage broader thinking, deeper understanding, and better decisions, for a stronger Marine Corps. If the next CMC is looking for better answers to tougher Congressional questions, Compass Points is here to help. In the upcoming weeks, Compass Points will feature a variety of issues – old and new – the incoming Commandant may want to explore.

<https://bit.ly/45YUB2D>

1 June 23

U.S., ROK Agencies Alert: DPRK Cyber Actors Impersonating Targets to Collect Intelligence.

FORT MEADE, Md. - The National Security Agency (NSA) is partnering with several organizations to highlight the Democratic People's Republic of Korea's (DPRK) use of social engineering and malware to target think tanks, academia, and news media sectors.

To help protect against these DPRK attacks, NSA and partners are publicly releasing the Cybersecurity Advisory (CSA), "[North Korea Using Social Engineering to Enable Hacking of Think Tanks, Academia, and Media.](#)"

<https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3413621/us-rok-agencies-alert-dprk-cyber-actors-impersonating-targets-to-collect-intell/>

1 June 23

Private Eyes: China's Embrace of Open-Source Military Intelligence

The People's Liberation Army (PLA) is using new collection, processing, and analysis technologies to exploit the massive amount of open-source information available from the internet and other sources for military intelligence purposes. A growing ecosystem of private companies, state-owned enterprises, state-run research organizations, and universities is supporting the PLA's push to leverage open-source intelligence (OSINT) by providing research services, platforms, and data. The PLA almost certainly views OSINT as an increasingly valuable source of

military intelligence that can support decision-making and necessitates the use of new collection, processing, and analysis technologies, which the PLA and China's defense industry are actively developing.

<https://bit.ly/45IYiZW>

30 May 23

NATO intel chief: Russia's war on Ukraine and a hybrid war aimed at us

Military Times' Senior Managing Editor Kimberly Dozier sat down with [David Cattler, NATO's assistant secretary general for intelligence and security](#), on the sidelines of the [2023 Lennart Meri Conference in Tallinn, Estonia](#), earlier this month. Cattler started as a naval surface warfare officer, patrolling the Pacific and taking part in [Operation Southern Watch](#), aimed at keeping Iraq dictator Saddam Hussein from harming U.S. Iraqi Shiite allies in the south of his country. Cattler now wrangles some 80 intelligence organizations from 31 NATO members, organizing their efforts somewhat like the [director of national intelligence provides guidance to U.S. intelligence agencies](#). His main focus right now? [Russia's all-out war on Ukraine](#) and its hybrid war against Ukraine and NATO, as well as the rest of Europe. This conversation has been edited for brevity and clarity. <https://www.c4isrnet.com/cyber/2023/05/30/nato-intel-chief-russias-war-on-ukraine-and-a-hybrid-war-aimed-at-us/>

24 May 23

The Case for a Deepfake Equities Process

Experts around the world are concerned with the explosive growth of deepfakes: digitally altered videos and audio that change a person's appearance and words to spread false information or are otherwise created with malicious intent. Most deepfakes are harmless, such as [AI-generated images of the Pope](#). Other uses, [such as non-consensual deepfake pornography](#), are far more disturbing. A Congressional Research Service [report](#) predicts that hostile intelligence services might use deepfakes to embarrass adversary political leaders and create false "evidence" of war crimes, among other dangers. Academic experts Robert Chesney and Danielle Citron [warn](#) that the spread of deepfakes may allow dishonest leaders to dismiss genuine evidence of fraud or other criticisms as a deepfake. Rapid advances in artificial intelligence have made deepfakes far easier to create, and they are spreading rapidly throughout the internet.

<https://bit.ly/3Wzdm0N>

24 May 23 China Hacks US Critical Networks in Guam, Raising Cyberwar Fears
As state-sponsored hackers working on behalf of Russia, Iran, and North Korea have for years wreaked havoc with disruptive cyberattacks across the globe, China's military and intelligence hackers have largely maintained a reputation for constraining their intrusions [to espionage](#). But when those cyberspies breach critical infrastructure in the United States—and specifically a US territory on China's doorstep—spying, conflict contingency planning, and cyberwar escalation all start to look dangerously similar.

On Wednesday, Microsoft [revealed in a blog post](#) that it has tracked a group of what it believes to be Chinese state-sponsored hackers who have since 2021 carried out a broad hacking campaign that has targeted critical infrastructure

systems in US states and Guam, including communications, manufacturing, utilities, construction, and transportation.

<https://bit.ly/3qIW823>

15 March 23

A year of Russian hybrid warfare in Ukraine

Prior to Russia's full-scale invasion of Ukraine on February 24, 2022, many observers expected that a Russian-led hybrid war, like that observed when Russia invaded Donbas and illegally annexed Crimea in 2014, would involve marrying cyber weapons, influence operations, and military force to swiftly overrun Ukrainian defenses. Now, one year after its full-scale invasion, Russia's military has indeed wrought physical devastation in Ukraine but has not achieved its objectives—in part because Moscow's parallel cyber and influence operations have largely failed.

https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf

PSYOP Veterans Association | 117 Bernal Road, Suite 70-338, San Jose, CA 95119 408-270-1800

[Unsubscribe spawrtan@wideopenwest.com](mailto:spawrtan@wideopenwest.com)

[Update Profile](#) | [Constant Contact Data Notice](#)

Sent by dietz.pova@gmail.com powered by



Try email marketing for free today!