E-BOOK:

2023: Year In Review / 2024: The Look Ahead
With one deadly war already raging in Europe, the international community was stunned to see another open in the Middle East in late 2023. And while the conflicts may be very different, they both continue to reverberate the world over, prompting protests in the streets, heated arguments in the halls of government and strain at major defense industrial firms.

At the same time, the US and other militaries are racing to modernize the way they fight, from submarines to satellites to software, upgrading decade-old vehicle fleets and playing with bleeding edge artificial intelligence.

In this eBook, you’ll see that in 2023, Breaking Defense covered all the major developments in the defense world and, at the end of the year, took a peek into the crystal ball for what 2024 may hold.

Whether the predictions turn out correct or not, you can keep up with key news and analysis in 2024, as always, at BreakingDefense.com.

Thanks for reading,

Lee Ferran

Managing Editor, Breaking Defense
<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Saving Schrödinger’s Cat: Getting serious about post-quantum encryption in 2024</td>
<td>5</td>
</tr>
<tr>
<td>Turning 4, the Space Force’s favorite word is ‘more’: 2024 Preview</td>
<td>7</td>
</tr>
<tr>
<td>In 2024, will the Navy again reassess increasing demands on the surface force?</td>
<td>10</td>
</tr>
<tr>
<td>In 2023, the Navy’s ‘silent service’ started making noise</td>
<td>12</td>
</tr>
<tr>
<td>Ethical Terminators, or how DoD learned to stop worrying and love AI: 2023 Year in Review</td>
<td>14</td>
</tr>
<tr>
<td>Getting to zero trust: The Pentagon’s effort to put data security first in 2023</td>
<td>18</td>
</tr>
<tr>
<td>Gaza war, increased production and unmanned proliferation: Middle East 2023 in review</td>
<td>20</td>
</tr>
<tr>
<td>From a door-related conundrum to Russians with Javelins: 5 Army stories from 2023</td>
<td>22</td>
</tr>
<tr>
<td>High-tech trench warfare: 5 hard-won lessons-learned for the US from Ukraine</td>
<td>24</td>
</tr>
<tr>
<td>From Russians in Abu Dhabi to the Navy’s nuclear conundrum: Top 10 stories from 2023</td>
<td>27</td>
</tr>
</tbody>
</table>
WASHINGTON – For decades, most digital communication has relied on an algorithm called RSA, invented in 1977 to allow two parties to communicate securely without having to exchange secret codes beforehand. Starting in 2024, that’s going to have to change.

Specifically, government agencies and private companies need to begin combing through countless lines of software code to find every instance of RSA and other long-standard protocols, so they can ultimately replace them with Post-Quantum Cryptography (PQC), a new set of algorithms designed to resist rapidly advancing quantum computers which could, in theory, crack any existing encryption.

The issue is urgent for agencies and companies have data that’s both highly sensitive and likely to remain relevant for many years, like performance and design specs for military vehicles and weapons systems. That’s the kind of encrypted data a well-heeled intelligence agency, like China’s Ministry of State Security, might spend the resources to scoop up now, even though they can’t decrypt it yet, and then store it until the long-awaited RSA-killing quantum computer arrives — a strategy known as “harvest now, decrypt later.”

If someone’s already run a “harvest” operation against you, one attendee at a recent ATARC webinar asked, what can you do to protect yourself? Not much, said Bill Newhouse, a senior cybersecurity engineer at the National Institute of Standards & Technology: “Unfortunately, that data’s out.”

What makes quantum computing such a game-changer? Every digital device in widespread use today — from baby monitors and microwave ovens to smartphones and smart missiles — uses thousands of tiny integrated circuits to store and manipulate information. If the circuit is holding enough electrical charge, it’s “on” and counts as a “1” in binary logic; if it’s not charged, it’s “off” and counts as “0.” Every function a digital device can perform boils down to adding and subtracting 1s and 0s over and over and over at superhuman speed.

This works great for a surprising range of applications, from the obviously mathematical, like tax prep software and encrypted messaging, to the seemingly creative, like generative AI making songs and videos. But the 1s and 0s struggle with computations that involve a huge number of different variables, like simulating how a new enzyme might behave or breaking an enemy code.
Quantum computers get around that problem by using “quantum bits,” or qubits, which exploit the ambiguous nature of subatomic particles to **embody every possible value between 0 and 1**. It’s a practical application of *Schrödinger's Cat*, the famous thought experiment where a trapped animal is neither alive nor dead, but both and neither and all states in-between. While “macroscopic” objects such as cats don’t actually behave this way, subatomic objects do, which means quantum computers can carry out calculations far too complex for classical computers — which, in time, will probably include including breaking RSA.

Late last month, NIST formally closed the public comment period for three PQC algorithms it plans to finalize for widespread use next year. But NIST finalizing algorithms doesn't solve the problem: That takes everybody implementing them.

“This is huge,” said Newhouse. “This migration [to PQC] should be the biggest one ever undertaken,” he told the ATARC webinar, at least since software began using RSA and other **public key encryption** in the first place decades ago.

A crucial caveat: That doesn't mean everyone should leap to install the new algorithms now. In fact, you’re not supposed to until they’re finalized. Technically, Newhouse said, “you could use them, but you’d be in violation of some rules, [because] you have to have a [FIPS] [Federal Information Processing Standard] validated product and that’s not there yet.”

“Those three drafts are just finished receiving comments,” he noted at the Dec. 5 webinar. “[NIST] will be adjudicating those comments, making the final publication even better because people submitted things they noticed.” And NIST takes outside input seriously: It had originally planned to release four new algorithms until independent testing revealed fatal flaws in one of them just last year.

“These open standards and these validation processes mean you’re getting a lot of eyes on this technology before you’re equipped with it,” Newhouse said at a **Defense Scoop event** on the same day.

Once NIST finalizes the PQC standards, however, there are yet more steps before anyone can use them. Software companies have to implement the new cryptography algorithms in actual code a computer can run — and that code should go back to NIST for **Cryptographic Module Validation** to ensure it actually works. That can take “months or years,” Newhouse acknowledged.

But that doesn't mean agencies and companies should just sit around waiting for their favorite cybersecurity vendor to come up with a PQC implementation, Newhouse and other experts emphasize. Far from it: Firms should already be taking inventory of the software your organization uses, so you can find where it uses RSA and other soon-to-be-superseded encryption protocols that will have to be replaced with the new PQC algorithms. And because RSA can crop up in all sorts of unexpected places — basically every time one computer wants to communicate something securely with another — it can take a long, long time to find every instance.

“It impacts everything we do, from switches to routers to our most prized possessions, our critical weapons systems,” said **Wanda Jones-Heath**, principal cyber advisor for the Air Force, speaking at the Scoop News event. “If we had not started this two years ago, we would be even further behind.”

As hard as hunting out instances of RSA can be for private companies, it’s even more complicated for government organizations, both military and civilian, which tend to use a patchwork of technologies of varying ages. “Federal networks are weird,” said Nick Polk, senior advisor to the **Federal Chief Information Systems Officer** in the Executive Officer of the President. “We have legacy IT from the seventies out there still … [and] encryption is everywhere.”

Software companies are already offering automated "discovery" tools, designed to inspect code and find instances of encryption that will need to be replaced. But there’s still no easy fix, so both finding the problem and fixing it will be the work of years.

With that laborious timeline in mind, a White House **National Security Memorandum** issued last year gave federal agencies until 2035 to complete their migration to post-quantum encryption. But that deadline assumed it would take many years for today’s experimental quantum computers to evolve into “cryptographically relevant” machines able to break RSA, an assumption challenged by a recent breakthrough by a DARPA-funded, Harvard-led research team.

That advance — a quantum leap in quantum computing — could bring the end of RSA and other long-used encryption years closer for everyone.
WASHINGTON — Over the last six months, there has been no mistaking a louder and louder drumbeat in favor of growing the Space Force — from its mission set to its budget to its end strength. So, perhaps the key question for the service as it enters its fourth year will be: how much growth?

With the concerns of lawmakers about costs firmly in mind, the Air Force’s original planning document for standing up the newest military service provided to Congress in February 2020 promised: “The Space Force will be lean, agile, and mission-focused.”

And since then, those words have been the mantra for service leaders, both civilian and those in uniform. But lately, a slight reinterpretation seems to be underway that opens the door to a bigger Space Force — one with more money and more people to take on what many in the service hope to be a greatly expanded set of missions, including operations in cislunar space around the Moon.

While noting that he wasn’t “at the head of the table” when the Defense Department, the Air Force and Congress were negotiating on the creation of the Space Force, Chief of Space Operations Gen. Chance Saltzman told reporters on Dec. 13 that the key issue was minimizing administrative bureaucracy.

“The idea was lean, agile headquarters. They didn’t want a lot of bureaucracy. They didn’t want a lot of support. They wanted us to be very mission-focused. And so they didn’t want us to have cops, they wanted the Air Force to do it. They didn’t want us to have our own big [HQ] staff. They wanted us to rely on other staffs,” he told reporters in Orlando at the Space Force Association’s inaugural conference.

“And so I think, as you see new missions come on, you can presume that that means more Guardians to perform those missions, and we’ll have to adjust the strength going up,” said CSO Gen. Chance Saltzman.
Turning 4, the Space Force’s favorite word is ‘more’: 2024 Preview

“But being mission-focused, as new missions are coming on, there’s growth in the missions. And there is wide support that says, ‘Hey, where the missions are going to grow, we understand you’re going to need to grow.’ And so as long as it’s focused on operations, there is an appetite for the kind of growth that we would expect,” Saltzman said.

“And so I think, as you see new missions come on, you can presume that that means more Guardians to perform those missions, and we’ll have to adjust the strength going up,” he added.

Saltzman did not specify what new missions he had in mind; nor did he quantify the increase of personnel, or the budget necessary to support them.

More Missions?

There are a couple areas where the Space Force’s ambitions to grow are clear.

The first is **intelligence, surveillance and reconnaissance (ISR)** — an arena where the service has spent much of the past year negotiating with the Intelligence Community about who is supposed to be doing what. To that end, the Space Force has come up with a new term of art to define what it considers its basket of those operations: “tactical surveillance, reconnaissance and tracking.” (Note that the word ‘intelligence’ has been stricken.)

“The new missionary we’re excited about is tactical surveillance, reconnaissance and tracking,” Col. Robert Davis, program executive officer for space sensing at Space Systems Command, told the Orlando conference on Dec. 13. “We’re very excited about how we leverage commercial analytics, overhead data and capabilities to get after provide information to combatant commanders and take care of their business out there in the field.”

Davis said that the command soon will issue its first solicitations for commercial imagery and/or data sources, as well as commercial data analytics to support to launch a pilot project to “help out to figure out how we can contribute to the fight.”

The Space Force already is working with the National Reconnaissance Office on new ISR satellites optimized to track moving targets on the ground in close to real-time, and the service is considering whether space-based sensors should be developed for doing the same for airborne targets.

The other future mission area on the lips of Space Force brass over the past year is **dynamic space operations** — that is, operations requiring highly mobile spacecraft such as closely following adversary satellites to watch out for threatening behavior, jinking out of the path of anti-satellite weapons or potentially even chasing down adversary birds to disable them with jamming or lasing.

Such missions would require improved satellite maneuvering, as methods for extending their lifetimes on-orbit such as in-space refueling. Those same sorts of operations and technologies would be needed even more if the Space Force begins to orbit systems near the Moon to keep an eye on China’s activities there.
The service’s first request for industry input in this arena focuses on “Combat Space Mobility,” seeking “to identify potential capabilities/technologies/services,” including “rapid delivery to space,” the development of spacecraft that can “routinely” maneuver, and in-space refueling. The goal is to generate budgetary requirements by March 2024 to insert into for the fiscal 2026 budget process. Companies have until Jan. 30 to respond.

More Self-Support?

For his part, despite the “lean” messaging, Saltzman did not even rule out some growth within the Space Force for it to take over more of its own support functions — especially given that the just-passed fiscal 2024 National Defense Authorization Act approved a separate Space Force legislative liaison, and that there is a push for the service to get its own public affairs officers. Separating some functions from the Air Force would bring the benefit of “focus and attention,” he said.

“I think it’s going to be an evolution and it’s hard to figure out exactly when you hit that tipping point of saying now we need a separate capability. I’m extremely happy with the level of support we’re getting. But, imagine as we grow in complexity, there will come a time we have to start talking about [growth] not just in the headquarters staff, but out in the field,” Saltzman elaborated.

He noted that airmen currently are undertaking a number of tasks that are critical, involving the day-to-day running of weapon systems. The question is whether that still will be feasible as the Air Force starts “optimizing for great power competition” and is “under stress.”

“Those are the kinds of things that that [Air Force Secretary Frank Kendall] is asking us to ask. Let’s ask now and make some decisions before we’re actually put into in extremis environment and we have to sort it out then,” Saltzman said.

More Money?

Of course, growth in missions and personnel will require growth in dollars to support them. The Space Force’s budget requests have been climbing at a steep angle since its inception, with Congress seemingly happy to indulge up until now — but there are signs the days of open checkbooks may be waning.

The service asked for a whopping $30 billion in FY24, focused primarily on research and development but also for increasing its launch tempo. However, Senate appropriators in their July-passed funding bill cut about $1 billion from the request, as did their counterparts in the House. In fact, the House Appropriations Committee for the second year in a row chided the service for not budgeting realistically over DoD’s five-year planning cycle.

Further, the service’s new(ish) Comprehensive Plan shows a downward trend through FY26, but a big jump back up to above the FY24 top line in FY27 and FY28.

So it may be that any real growth is yet a ways away.
In 2024, will the Navy again reassess increasing demands on the surface force?

The conflict in Gaza has drawn the US Navy's surface forces into an extended missile and drone defense mission to support the Israeli Defense Forces.

By JUSTIN KATZ - December 28th, 2023

WASHINGTON — In 2017, the US Navy was forced to reckon with the demands put on its surface ship crews following the tragic and fatal collisions involving the destroyers John S. McCain (DDG-56) and Fitzgerald (DDG-62). Seven years later, I think the Navy in 2024 may once again have to confront its operational tempo requirements.

The impetus for that examination could come from the unexpected obligations the fleet now faces in the Mediterranean and Red Seas. The crews of the Carney (DDG-64), Mason (DDG-87) and Thomas Hudner (DDG-116), all of which are being supported by other American ships in the region, in recent weeks have shot down or intercepted dozens of drones and missiles suspected of being deployed by enemies of Israel, which finds itself in a vicious ground conflict with Hamas.

Whether the United States is officially a party to the war in Gaza is a question best left to others. But here's what is plainly clear: US Navy warships are actively protecting Israeli forces by being on station, and if the service can’t maintain its presence in the region's waters, for readiness reasons or otherwise, it will only stand to benefit Israel's adversaries.

This pressure, in turn, could serve as a catalyst to test whether the Navy truly embraced the lessons from the 2017 ship collisions, both in terms of individual sailor readiness and more broadly, ship maintenance.

One of the root causes for the 2017 collisions was the Navy's surface force being regularly worked to exhaustion, which in turn led to numerous errors on the crews’ parts that cascaded into tragedy. That so many sailors lost their lives as a result was nothing short of tragic. And those were ships that weren't in active combat zones.

Now, in Mediterranean and Red Seas, US Navy ships have engaged at least five drones or missiles thought to be deployed by Iran-backed Houthi rebels in a single day. In other words, these ships and their crews are not just present, but very much in harm's way. And it's not just the crews' well-being that will be cause for concern as the conflict drags on.
In 2024, will the Navy again reassess increasing demands on the surface force?

Steve Wills, of the Center for Maritime Strategy, told me if the Navy hopes to stay on station in the Middle East to continue fending off missiles and drones bound for Israel, that mission will require “regular rotations of ships.”

“Those missions have an impact on overall Navy readiness for other potential zones of conflict like the Indo-Pacific,” he added.

The Navy’s issues with timely ship maintenance are well documented by organizations such as the Government Accountability Office. But the need to help protect the country’s biggest ally in the Middle East will bring new urgency to ensuring new ships and crews are ready to depart the US when the time comes for Ford, Carney, Mason and others to return home.

As the war in Ukraine has demonstrated, it is nearly impossible to predict how long conflicts like these will last. Prior to Russia’s invasion, the lion’s share of defense analysts seemed convinced Kyiv would not withstand a Russian onslaught for more than a few days. Now, here we are, more than two years later with no clear end to that war in sight.

How the Navy copes with the normal demands of ship maintenance, the extended deployments that the conflict in Gaza brings while the Navy maintains its presence in the Indo-Pacific will all be on this reporter’s watch list for the new year.
The advent of AUKUS has brought the Navy’s submarine community into the national spotlight and that has led it to breakaway from its historical silence.

By JUSTIN KATZ - December 22nd, 2023

WASHINGTON — "We all need some more yellow submarines, yellow submarines," famously sang The Beatles.

Alright, that is not how the song goes. But 2023 has arguably been the year of the submarine for the US Navy. The raft of new details the public learned about the trilateral security pact AUKUS in March is in turn bringing more public attention to the various issues plaguing both the US Navy’s submarine inventory and its shipyards’ woes.

In this reporter’s opinion, 2023 was the year that the Navy’s “silent service” began to seriously grapple with that moniker in the interest of both ensuring the fleet’s readiness as well as demonstrating to the public at large why its mission matters to the country, America’s allies and to AUKUS.

First, a step back. The title “silent service” stems largely from the need for submarines to be as quiet as possible when operating in the interest of stealth. But it has a double meaning: The submarine community is notoriously news shy. That’s not just the opinion of a reporter whose interview requests were scorned; the Navy itself acknowledges that fact.

Like it or not though, AUKUS has shoved this inherently quiet community into the national and international spotlight, and their struggles — be it on maintenance, production or otherwise — will now take on new scrutiny as those faults have the potential to publicly ripple across the world’s oceans and directly impact underwater allies.

The best example of a slightly-less-silent service at work is the $3.4 billion in supplemental funding the president submitted to Congress in October. Top submarine leadership subsequently went to Capitol Hill and publicly testified about why that money is needed to shore up the service’s shipyard infrastructure, which has been historically overburdened and backlogged by in-service submarine maintenance.
In 2023, the Navy’s ‘silent service’ started making noise

The Navy officials also expressed to lawmakers, and the American public, the exponential increase in workload that AUKUS will bring and why the industrial base must be strengthened. Due to the impacts of the coronavirus pandemic, the Navy was already struggling to meet its prior goal of building one Columbia-class and two Virginia-class submarines annually. With AUKUS in motion, there will be additional work to do to help allies as well as added pressure to not let the Virginia class fall behind, given that three, or potentially five, will leave American hands in the 2030s.

While testifying on Capitol Hill may be a mandatory event for the Navy’s leadership given the cash they’d receive from the supplemental, there are other clues that the silent service reckoned with its name.

Matt Sermon, a senior Navy civilian overseeing submarine production, recently told reporters the Navy had spent more than $200 million contracting with BlueForge Alliance, a Texas-based non-profit company that is assisting the Pentagon with reaching out to the American public in an effort to cultivate a larger industrial base workforce.

Another example of that kind of public outreach is the website, buildsubmarines.com.

“The Navy is on a once-in-a-generation journey to completely transform its nuclear-powered submarine fleet and maintain its critical undersea advantage,” the website states. “However, this military mandate will require the addition of more than 100,000 skilled workers with the training and commitment to ensure success. And there’s not a moment to spare.”

In May, not long after the formal AUKUS rollout in San Diego, Breaking Defense’s Robbin Laird spoke to Rear Adm. Jeffrey Jablon, who at the time was one of the service’s most senior operational submariners. Jablon himself had been rethinking the moniker and whether it was serving the Navy’s — and the country’s — best interests.

“I would no longer characterize ourselves as a silent service,” said Jablon. “Deterrence is a major mission for the submarine force. You can’t have a credible deterrent without communicating your capabilities; if the adversary doesn’t know anything about that specific deterrent, it’s not a deterrent.”

Jablon was clearly not the only one who felt that way because in early November, the Pentagon publicly announced the arrival of a guided-missile submarine in the Middle East. The revelation made headlines, even at major TV news networks.

Operational submarine locations are highly classified, and the Defense Department does not point them out to the public arbitrarily. Vice Adm. Bill Houston, the Navy’s top operational submariner, told reporters in the weeks that follow that, indeed, the silent service was intentionally making some noise.

“Part of the messaging is, as submariners, we operate everywhere that we’re allowed to operate across the globe,” he said, comparing it to another event in July when an American boat surfaced at a South Korean port, a first in decades.

And, in the spirit of what Jablon said about letting the adversary know about the deterrent, Houston continued by warning that although other boats may not be announced, they are certainly still out there.

“And just like I wouldn’t answer [a previous] question [about] where my submarines that I haven’t reported are — nobody will know where my submarines that I haven’t reported are, because that’s our asymmetric advantage,” he continued.
Ethical Terminators, or how DoD learned to stop worrying and love AI: 2023 Year in Review

Over the last 11 months, the US has made major progress in defining “Responsible Military Use of Artificial Intelligence” and even getting other nations to sign on the idea – without ever actually precluding the kind of automated “killer robots” activists want to ban.

By SYDNEY J. FREEDBERG JR.

WASHINGTON — When pundits talk about military use of artificial intelligence, the phrase “human in the loop” is almost certain to come up. But a “human in the loop” isn’t defined in the official Pentagon policy, even after the policy was revised and expanded in January, nor in the months of internal refinement and international talks that followed.

Still in 2023 — the year ChatGPT rocketed AI into the international spotlight — the US government make a full-court push to define “responsible” military use of the technology on its own terms, and sell that concept to both the American public and world opinion.

The Pentagon wants to keep its options open, in part, because many systems already in use have had a fully automated option, which takes the human out of the loop, for decades — like the Army’s Patriot, the Navy’s Aegis and similar missile defenses in service around the world. It may also be because the US military has no desire to unilaterally disarm itself if a highly automated system proves lethally superior, at least in some scenarios, to one slowed down by a human decision-maker — as years of simulations and experiments with AI-controlled fighter jets already suggest.

“I just got briefed by DARPA on some work that they’re doing on man versus unmanned combat [with] fighters,” said Frank Kendall, the Secretary of the Air Force, said at the Reagan National Defense Forum on Dec. 2. “The AI wins routinely, [because] the best pilot you’re ever going to find is going to take a few tenths of a second to do something — the AI is gonna do it in a microsecond.”

“You can have human supervision,” he said. “You can watch over what the AI is doing. [But] if the human being is in the loop, you will lose.”
Yet Kendall isn't some cackling Doctor Strangelove seeking to unleash the Terminator on the puny humans. He's a human rights lawyer who's served on the boards of Amnesty International and Human Rights First.

"I care a lot about civil society and the rule of law, including laws of armed conflict, and our policies are written around compliance with those laws," he told the Reagan Forum. "[But] you don't enforce laws against machines: You enforce them against people. And I think our challenge is not to somehow limit what we can do with AI, but it's to find a way to hold people accountable for what the AI does."

Kendall's remarks aren't just important because they show what the Secretary of the Air Force thinks. They also embody, with his distinctive bluntness, the fine line the entire US military is trying to walk between imposing ethical limits on the responsible use of AI and exploiting its war-winning potential to the fullest.

Walking A Fine Line in 2023

Kendall and his Pentagon colleagues were hardly unique in spending much of 2023 wrestling with the ethical and practical consequences of AI.

The European Union's AI Act passed in early December, while President Joe Biden published an unprecedented executive order — the longest and most detailed EO in history — in October. But the Biden order focused on commercial and civil service AI, with relatively few provisions for the Pentagon and many provisions that actually applied defense innovations to other agencies, like having a designated chief AI officer and a formal AI strategy. That's probably because the Defense Department was a leading agency on "responsible AI" and had worked hard on its own AI framework all year, with a significant assist from the State Department in signing up allied support.

The roots of this effort go back to the Trump administration. In 2019, the semi-independent Defense Innovation Advisory Board issued ten pages of "AI Principles [for] the Ethical Use of Artificial Intelligence by the Department of Defense," emphasizing that military AI must be "responsible," "equitable," "traceable," "reliable" and "governable," the last meaning both human oversight and AI self-diagnostics to stop the system running amok. A few weeks later, a bipartisan Congressional commission argued that autonomous weapons could be deployed in accordance military ethics and the law of war, declaring that "ethics and strategic necessity are compatible with one another." Early the following year, then-Defense Secretary Mark Esper adopted many of these ideas in a formal set of ethical principles, with DoD later inviting over a dozen friendly nations to discuss them.

But it took until 2023 for the DoD to expand these principles into a comprehensive policy and implementation plan. What's more, that policy carefully and deliberately left a pathway open for fully autonomous weapons, even as State managed to co-opt a UN resolution introduced by activists seeking a binding legal ban on such weapons.

The crucial step came in late January, with the long-awaited revision of the governing DoD Directive on Autonomy in Weapons Systems, DoDD 3000.09. While much longer and more detailed than the 2012 original, with a strong emphasis on implementing the 2020 ethical principles, the new 3000.09 retained a crucial provision allowing the deputy secretary to waive all its restrictions "in cases of urgent military need."

The new 3000.09 also exempted "operator-supervised autonomous weapon systems used to select and engage materiel targets for local defense to intercept attempted time-critical or saturation attacks." That section is written to cover defenses that require superhuman reaction speeds to shoot down fast and/or numerous incoming threats, from a Navy Aegis cruiser to an Army tank's anti-antitank missile system.

Aegis, Patriot, and similar air defense systems like it have actually had a fully autonomous mode for decades, because Cold War commanders feared the Soviets would unleash too many bombers and missiles for humans to track, a fear now revived by China's build up. While such autonomous defenses are focused on destroying missiles, they're perfectly capable of shooting down manned aircraft as well. In fact, they've actually killed friendly aircrew by accident. — for example, in 2003, when Patriot batteries were mistakenly switched to their Cold War fully automatic mode, twice.

It's worth noting that not one of these systems is "artificial intelligence" in the modern sense of the word. They don't use machine learning and neural nets to digest masses of data and then modify their own algorithms. They're straightforward, deterministic IF-THEN codes of the kind in use since the days of punch cards and vacuum tubes.
"As lieutenant, I was operating a HAWK air defense unit in Europe," Kendall recalled. "I had a switch on my console, it said 'automatic,' and I could have put the switch in that position and just sat there and watched this shoot down airplanes."

"The data inputs that were necessary to enable that were pretty straightforward," he said. "Which direction is the airplane that your radar's tracking going in? How fast is it going? What altitude is it at, and is it sending any IFF, Identification Friend or Foe, signal? … That was in 1973. We are infinitely better than that now."

Modern machine-learning AI can sort through much larger and more complicated datasets, which makes it increasingly possible for an automated system to target not just missiles and jets in the empty air, but ground vehicles partially hidden by terrain, or even human beings under cover. The most plausible nightmare scenario of the arms control activists and AI doomsayers is not some bipedal killbot with an Austrian accent, but a swarm of kamikaze mini-drones, each with just enough intelligence — and explosives — to track down an individual human. But UN arms control negotiations in Geneva have been stalled for almost a decade over how to define such "lethal autonomous weapons systems."

In February, the State Department’s ambassador at large for arms control, Bonnie Jenkins, went to an international conference on military AI in the Hague and issued a formal Political Declaration on Responsible Military Use of Artificial Intelligence and Autonomy. Largely derived from the DoD policies released in January, the US Political Declaration has won official endorsement from 46 other nations, from core allies like Australia, Britain, France, Germany and Japan to minor neutrals like Malta, Montenegro and Morocco.
In the following months, while State racked up more countries’ endorsements of the Political Declaration, DoD kept developing its policy. June saw a conference of over a hundred senior officials and outside experts and the release of an in-depth Responsible AI Strategy & Implementation Pathway [PDF] detailing 64 “lines of effort,” which were then encapsulated in a handy online guide to help baffled bureaucrats actually execute it. Biden even got China to agree to vaguely defined discussions on “risk and safety issues associated with artificial intelligence” at his November summit with Xi Jinping, with experts suggesting the first top would be ensuring human control of the highly sensitive command-and-control systems for nuclear weapons.

But even a ban on AI control of nukes — like the SkyNet nightmare straight out of the Terminator movies — would not restrict other applications of military AI, from personnel management to intelligence analysis to “lethal autonomous weapons systems.” The Pentagon strategy has been to codify how to make responsible and ethical use of AI across all those applications — not just the narrow use case of “killer robots” — while still keeping all its options open.

“I don’t see, any time soon, the Terminator or… the rogue robot that goes out there and runs around and shoots everything in sight indiscriminately,” Kendall said. “I think we can prevent that — but we are still going to have to find a way to manage this technology, manage its application, that holds human beings accountable for when it doesn’t comply with the rules that we already have.”
Getting to zero trust: The Pentagon’s effort to put data security first in 2023

Defense Department Chief Information Officer John Sherman set the tone early in the year by telling Breaking Defense a major focus over 2023 would be aiming for baseline, targeted zero trust within four years.

By JASPREEET GILL - December 22nd, 2023

WASHINGTON — With the leak of hundreds of classified documents and a new zero trust strategy, the Pentagon became laser focused on getting the implementation of the security concept right this year.

Zero trust means rather than letting users who pass security checks have free reign over a network, there would be continual checks to make sure each user is allowed to access different information. Essentially, under zero trust, networks are always assumed to be compromised.

The Pentagon released a zero trust strategy and roadmap in 2022 that painted a concerning picture for the Defense Department’s information enterprise, which is “under wide-scale and persistent attack from known and unknown malicious actors,” and specifically China. The strategy outlined what it would take to get the department to both a “targeted” and “advanced” level of zero trust.

Defense Department Chief Information Officer John Sherman set the tone early in the year by telling Breaking Defense that a major focus over 2023 would be starting to implement zero trust with a full baseline version of the strategy by fiscal 2027.

And while it remains unclear if a full implementation of the security concept earlier could have prevented the leaking of national security documents in what became known as the Discord leaks, Sherman in May said, “it sure as heck would’ve made it a lot more likely” that DoD could’ve prevented it.
But the path to zero trust may not be so simple. In June, Randy Resnick, director of DoD’s zero trust portfolio management office, said his office was finding it “hard to orchestrate” each individual military service’s zero trust efforts into something cohesive. As a result, DoD started doing weekly “huddles” and quarterly meetings with the services and “communities of interest” in an effort to educate them on how to execute the vision outlined in DoD’s zero trust strategy.

The military services and DoD components submitted their own zero trust implementation plans by October, Signal Media reported. In September, Sherman said DoD was getting ready to review those plans and the assessments would be led by Resnick’s team, who’d make sure the plans align with the department’s fielding of targeted zero trust.

And industry seemed to align to DoD’s ambitions. Amy Gilliland, president of General Dynamics Information Technology, told Breaking Defense in June that the company was pouring more money towards areas DoD deemed critical, including zero trust.

Gilliland said GDIT was increasing its investment this year by 50 percent in areas that mirror DoD’s increased investments: zero trust, 5G, multi-cloud management, software factories, automation for IT operations and artificial intelligence and machine learning. The company, she said, was also working to increase investments in quantum computing and defensive cyber operations.

One major zero trust program hailed out of the Defense Information Systems Agency finally reached a milestone this year. Booz Allen Hamilton in July was awarded a production agreement worth up to $1.86 billion for Thunderdome, DISA’s zero trust network architecture program. The contract was a follow-on production award for the company as DISA transitioned Thunderdome from prototyping to production.

Overall, it seems that DoD is taking steps down the path toward true zero trust, but there’s a ways to go.
Gaza war, increased production and unmanned proliferation: Middle East 2023 in review

From tectonic geopolitical shifts to billion-dollar-defense deals, here's just some of the key events in the Middle East in 2023.

Rockets fired by Palestinian militants from Gaza City are intercepted by the Israeli Iron Dome defence missile system in the early hours of October 8, 2023. (Photo by EYAD BABA / AFP) (Photo by EYAD BABA/AFP via Getty Images)

By AGNES HELOU - December 21st, 2023

BEIRUT — In my first year as a full-time reporter at Breaking Defense, there was no shortage of news in the Middle East. Then, before the year could end, the region was set ablaze with Oct. 7 Gaza attack which resulted in a war, dwarfing any other defense efforts and development in the region.

As the war reaches the three-month mark, the conflict has reverberated throughout the region, the fear of the violence spreading to south Lebanon, where the Lebanese armed group Hezbollah has fought in several skirmishes, or further.

The conflict put a pause on one of the biggest stories of the year, the approaching normalization of relations between Israel and Saudi Arabia, though analysts told Breaking Defense in the early days of the Israel-Gaza war that normalization would likely continue after things die down.

Digging deeply into the Kingdom of Saudi Arabi's other strategic moves in 2023, one thing that can be said is: Opposites attract. From a surprising agreement to restore diplomatic relationships with Iran, to taking command of two US-led Task Forces, to the lifting of an Italian embargo on defense exports to Riyadh, and finally to defense rapprochement with Turkey, KSA is maintaining relationships with as many countries as it can, even those historically at odds with each other.

On the technological level, Riyadh this year pushed its defense industry heavily to indigenous production, with an ambitious plan for Saudi Arabia Military Industries to become a top 25 defense firm, and a large deal to produce Turkish Baykar Akinci drones in the Kingdom.

Saudi's neighbor, the United Arab Emirates, this year continued its trend steadily on the expansion plans of its defense conglomerate EDGE Group, not least of which the large budge to buy stakes in already established European firms and crossing the Atlantic Ocean to Latin America, with Brazil's market taking central stage of EDGE's attention.
In line with its localization plans, UAE cancelled an approximately one billion dollar deal with French Airbus, and is looking elsewhere for better technology transfer offers. The country announced plans to establish the first MBDA missile center outside Europe. Additionally, EDGE Group, the UAE's sprawling defense conglomerate, turned four years old in 2023, and had the lion's share of announcements in the two large shows it hosts: Dubai Airshow and IDEX. The firm is also intertwining its tech with those of its international partners, integrating its missiles with the US-made MQ-9B drone, and French Rafale and Indian HAL Tejas fighter jets.

Turkey, one of the most advanced defense producers in the Middle East surpassed drone production to developing its fifth generation fighter, naval vessel production and submarine production. This was evident on the IDEF 2023 show floor.

Ankara's defense exports, mainly led by land systems, increased in 2023. One gap, however, remains for Turkey to fill — new fourth generation fighter jets to fly before the fifth-gen KAAN to see light.

On the opposite side of the Arabian Gulf, Iran reached its own milestones in defense procurement and production. Tehran remains the biggest concern of the US and its allies in the region. In the second rank of concern, comes China's relationship with Middle East countries.

Meanwhile, Iraq in 2023 prioritized air defense systems in its procurement list, and Qatar announced plans to boost its naval capabilities with a multi-billion-dollar deal with Italian shipbuilder Fincantieri.

Last but not least, Lebanon with its modest defense spending has been struggling not only with what is happening on its southern border with Israel, but also economic crisis and corruption. But small rays of hope were always present in 2023, from new vessels received as part of the US military aid, to Resolute Union drills and the rebuilding Beirut naval base that was destructed during the Port Explosion is still on the military's dream list.
From a door-related conundrum to Russians with Javelins: 5 Army stories from 2023

In 2023, the US Army eyed ways to better support troops in the Indo-Pacific region, and ways to restructure its formations for the future.

By ASHLEY ROQUE - December 18th, 2023

WASHINGTON — US Army plans to refill weapon stockpiles and weapon modernization milestones may have dominated our service-related news this year, but Breaking Defense also carved out time to chase down a few offbeat stories too.

Here are my five top Army stories from the past 12 months (a few with crucial assists) that range from an Australian-bug-logistics challenge and Russians playing with a Javelin in Abu Dhabi, to way too much time spent talking about “occlusion” and doors.

1. Russians playing with Javelins: US Army, Russia display weapons yards apart in the desert

In 2023, in the shadow of Russia’s invasion of Ukraine and America’s stalwart support of Kyiv, what happens when Russian defense companies set up shop at one of the world’s largest weapons shows in Abu Dhabi, United Arab Emirates? The US Army pops up a simple tent with a white canvas sign, devoid of any US military insignia, just a few yards down.

In it, and next to it, American soldiers donning 116th Cavalry Brigade unit patches, show off a Javelin and an operational Patriot launcher, while fielding curious passersby’ questions about the weapons.

Outside IDEX 2023 this year, Russians were among those guests peering through the Javelin’s viewfinder. One US Army soldier billed the mood as so jovial (my word, not his) and even said he traded patches with one Russian.
2. Army's pricey IVAS goggles meet a training obstacle: Doors

The Army and Microsoft's quest to develop a combat-suitable, heads-up display for soldiers continued on this year, and the service even began fielding a small batch of the initial Integrated Visual Augmentation System (IVAS) configuration to schoolhouses. However, the Army also wants to use the device as the centerpiece of a mixed-reality training system that it dubs the Squad Immersive Virtual Trainer (SiVT) program.

Breaking Defense spoke with more than a half dozen current and former service officials and industry sources about dynamic occlusion limitations with that program — the lack of ability to hide a virtual object behind a real one — that could limit how soldiers use IVAS to train in mixed-reality scenarios.

While the service previously acknowledged that it faces challenges using IVAS outdoors for mixed-reality training due, in part, to ever-changing light conditions, those occlusion limitations also inhibit how soldiers train indoors too. For example, they are not able to open a real door and then suddenly see the virtual objects, like enemies, that had been virtually placed behind the real-world objects. The Army, and entire mixed-reality industry, is working on the broader issue but there is not a single, easy fix.

3. From petroleum pipes to pest problems, what a US Army two-star learned from Talisman Sabre 23

"Every plan you do does not survive the first day," 8th Theater Sustainment Command Maj. Gen. Jered Helwig told Breaking Defense this year following Exercise Talisman Sabre 23 in Australia. "We had to make some quick changes, and having the combined joint theater sustainment component, which was a mix of us and Australian partners, really helped us get after those things."

While the first part of his remarks may have been echoing the famous maxim by a Prussian general (or heavyweight boxer Mike Tyson), neither spent time wrestling with contested logistics hurdles in the Indo-Pacific at a time when Washington is preparing for a possible military incursion there.

From agricultural inspections for bugs to laying three miles of pipe to move fuel from the waterline up to an airfield inland, Helwig and the service are looking for ways to up their game and better prepare to work with regional allies and partners.

4. Shooting for the moon: Army's 2025 budget to reflect artillery revamp

If the wars between Ukraine and Russia, and Israel and Hamas have shown Army leaders one thing, it's the importance of maintaining a deep magazine to stay in the fight. While that sentiment extends beyond the artillery world and 155-millimeter production, the service is studying which artillery capabilities its future arsenal needs ahead of its fiscal 2025 budget request.

5. 'Good, healthy debate': Eyeing the Indo-Pacific, Army leaders grapple with force structure shake up

Yes, 2023 ushered in a host of well-documented senior leaders changes across the services. For the Army, that meant saying goodbye to Chief of Staff Gen. James McConville and hello to Gen. Randy George.

The new top uniformed leader wasted little time, discussing potential force structure and training changes to better prepare the service to fight a modern war. And this fall George — along Army Futures Command Gen. James Rainey and Army Pacific commander Gen. Charles Flynn — provided a peak at what this could mean for the service.

The verdict: Nothing is decided, but some of the Army's formations are simply too heavy, and the service needs to think through the roles of some of its newer teams like the multi-domain task force and security force assistance brigade.
High-tech trench warfare: 5 hard-won lessons-learned for the US from Ukraine

From expendable drones, to ad hoc battle networks, to hacker “armies” of volunteers, the war in Ukraine has shown the big-spending US military new ways to fight in the Information Age.

Ukrainians train with handheld drones. (Photo by Sean Gallup/Getty Images)

By SYDNEY J. FREEDBERG JR. - December 19th, 2023

WASHINGTON – What high-tech weapons really work? What tactics make the difference between victory and death? There's no test like the test of battle, and the US military has been watching the war in Ukraine with a keen and anxious eye. It's another question whether the Pentagon bureaucracy is learning the right lessons about cheap drones, real-time intelligence-sharing and the weaponization of the Internet.

The dramatic defeats and victories of 2022 have settled in 2023 into a slow-motion meatgrinder, a conflict where cutting-edge technology combines with brutal battles of attrition over minefields and trench lines. Like the Malayan Emergency before Vietnam, the Spanish Civil War before World War II or the Russo-Japanese War before World War I, Putin's bloody debacle in Ukraine is full of warnings for the next big conflict we all hope won't ever come. But if it does come, the US had better have heeded at least these five lessons:

1. **The cloud, fiber optics and hiding in basements:** Army races to adapt to new command post threats

   Over more than a decade of guerrilla warfare in Afghanistan and Iraq, American commanders got used to large, lavishly equipped Forward Operating Bases blessed with everything from Burger Kings to live video feeds from surveillance drones. As early as 2016, then-Chief of Army Staff Gen. Mark Milley warned such big, static targets would not last long against a well-armed foe with their own scout drones and long-range artillery. But it took Russia's 2022 invasion of western Ukraine to drive the point home. Battlefield lessons began informing official Army doctrine and driving decisions on procurement of command, control, and communications gear.
High-tech trench warfare: 5 hard-won lessons-learned for the US from Ukraine

This past May, the three-star chief of the Combined Arms Center, Lt. Gen. Milford Beagle, and two of his subordinates published a Military Review article that grimly called Ukraine “The Graveyard of Command Posts.” I talked to Beagle and his team for more about their dark vision of the future battlefield and how to survive it. Their ideas ranged from cutting-edge technology, like moving non-essential data from bulky “tactical servers” to the cloud, to old-school soldiering tricks, like hiding your command post in the basement of a rubbled building.

“This is something I think all armies are going to wrestle with,” Beagle told Breaking Defense. “The US Army certainly has. [But] we can better protect ourselves, reduce risk, even with the technologies that are emerging out there currently.”

2. Dumb and cheap: When facing electronic warfare in Ukraine, small drones’ quantity is quality

High tech doesn’t always mean high cost. One of the most striking developments in Ukraine — popularized by propaganda videos from both sides — is the ubiquity of drones. But as anti-aircraft defenses and electronic warfare units adapted to the threat, both sides moved away from the larger drones like the Turkish Bayraktar TB2, with its 40-foot-wingspan, towards smaller drones, even Chinese DJI Mavics less than 10 inches wide, that were both harder to target and cheaper to replace. One report estimated that Ukraine alone was losing up to 10,000 drones a month, mostly to Russian jammers disrupting their remote control links.

Even so, five independent experts agreed that it was still more cost-effective to buy cheap drones in bulk and treat them as essentially disposable, rather than try to upgrade them with better defenses against electronic warfare, let alone physical gunfire. “Commercial quadcopter and FPV [First Person View] drones are treated as expendable munitions,” said Samuel Bendett of CNA. “It’s not cost-effective to proof them against EW.”

That’s a hard lesson for the US procurement bureaucracy to learn. “We are losing out on the requirement to get these systems into the hands of soldiers at every echelon,” said retired US Army two-star Patrick Donahoe. “It’s got to be expendable.”

3. Ukraine War: Vast hacker ‘militias’ do little damage – but can rally mass support, says study

How did so much video of Ukrainian battles get into all our social media feeds in the first place? In large part because both sides crowdsourced propaganda — once the business of state bureaucracies and government-friendly corporate giants — by mustering millions of supporters online to edit, distribute and hype up their combat footage. Just as ubiquitous, cheap drones played a major role in collecting unprecedented quantities of video from the war zone, ubiquitous, cheap internet access (and video editing tools) played a major role in distributing it.

So the internet has become a major tool of wartime mass mobilization in the 21st century, just as then-novel media like radio and newsreels were in World War II. But mass mobilization has its limits, then and now. It’s a lot easier to make people feel like they’re participating in the great crusade than to turn their well-intentioned efforts in practical impacts on the battlefield. That said, sometimes people’s feelings are the point: Public morale has been a make-or-break-it factor in conflicts as different as World War I and Vietnam.

In May, the Center for Strategic & International Studies released a 64-page report bundling research from US and European scholars that delved deep into Ukrainian and Russian efforts to raise “IT armies” and hacker militias. While these groups’ hacks have been technically crude and dubiously effective, contributor Erica Lonergan wrote, “the act of collectively conducting relatively simple cyberattacks thus builds and reinforces community, providing something around which to rally and energize supporters.”

4. Ukraine and industry show how Europe can jump ahead on JADC2, ex-generals say

Joint All-Domain Command & Control, or JADC2 — occasionally seen with a “C” at the beginning to add “Combined”— is the Defense Department’s all-encompassing acronym for a future communications system linking all the armed services and, when “combined,” US allies. Aided by artificial intelligence, JADC2 would let units across land, sea, air, outer space and cyberspace (the five “domains”) share targeting data and coordinate strikes in near-real-time.
Actually building such a meta-network has proven a tremendous technical and organizational challenge, although the Air Force, Space Force, Army and (most secretly) the Navy all have conducted intriguing experiments. Yet it’s Ukraine that has actually implemented, in combat, the rapid digital sharing of targeting data from “sensor to shooter,” from a surveillance drone or human observer to an artillery battery or missile launcher. The role of Elon Musk’s Starlink satellites in relaying this kind of targeting data is well known. But, the Ukrainians also get at least some guidance from Western intelligence agencies, drawing on their own vast networks of air and space surveillance assets, and Ukraine routinely uses Western software, much of it provided free or bought “off the shelf” from friendly firms.

In some ways, Ukraine’s lack of established “legacy” equipment has given it an advantage over the US, argued the former vice-chairman of the Joint Chiefs, retired Gen. James “Hoss” Cartwright. “We have a legacy force that needs to be brought forward,” he said. “You can’t just say, you know, wave your hand and it’s all of a sudden digital. It doesn’t work that way. That is tens of billions of dollars [and] probably ten years to do it effectively.”

5. Cyber lessons from Ukraine: Prepare for prolonged conflict, not a knockout blow

Putin is far from the first head of state seduced by the siren of a short, victorious war won with a swift knockout blow. Men marched off to World War I boasting they’d be “home by Christmas.” But it wasn’t just Russian paratroopers and tanks that fell fatally short of their objectives in early 2022: It was Moscow’s vaunted cyber/electronic warfare forces as well.

In 2007, Russian hackers took much of Estonia offline, while in 2014, Russian electronic-warfare troops shut down Ukrainian military radios. The fear among many cyber pundits and US officials was of a “Cyber Pearl Harbor,” where Russia, China or some other sophisticated threat would hack into American or allied networks and bring both government agencies and critical infrastructure to a crashing halt.

Yet Ukraine proved it had learned from its own and others’ painful experiences with Russia and armored its digital backbone with extensive help from Western governments and tech firms. Putin’s hackers tried for a knockout blow but found themselves in a protracted slugging match with Ukrainian cyber warriors. In the words of Illia Vitiuk, cybersecurity chief for the Ukrainian Security Service (SBU): “If you have 12 rounds in a boxing match … we are in probably round eight now.”

“There’s been sort of this assumption … that there’s just going to be this massive, disruptive, decisive round of disruptions,” said Michael Martelle, a scholar at the National Security Archive. “The term ‘cyber Pearl Harbor’ just won’t die, even though it really needs to.”
WASHINGTON — As the new year beckons, over the past couple weeks Breaking Defense turned its analytical eye on the tectonic shifts in geopolitics and the defense industry across every domain that took place in 2023.

As a trade publication with a dedicated, loyal readership that includes policymakers, practitioners and game-changers in the defense world around the globe, we’re lucky we don’t live and die by clicks and views, but by the quality and insightfulness of each report all through the year.

That doesn’t mean, however, that we’re above enjoying the occasions in which our stories leap out of the defense stream to make a splash with a more general audience.

Therefore, it’s my pleasure to present Breaking Defense’s top 10 most read stories of 2023. If you’re reading this — in which case you may have already read a few of the articles below — thank you for your time and attention. We’ll see you in 2024 with the most important defense news and analysis from our team on the ground.

**UK reveals capture of Russian equipment, instructs industry to develop counter-measures**

The comments may have been a big vague, but a senior United Kingdom Ministry of Defence official was among the first to reveal that Western militaries had captured Russian equipment during the conflict in Ukraine and were actively working to figure out ways to counter them.
As Breaking Defense's Tim Martin reported from the International Armoured Vehicles conference in London in January 2023, the official said that being able to “undermine the credibility” of the Russian systems will lead to the creation of market opportunities for “alternative solutions,” a clear hint that industry has been instructed to interrogate the Russian equipment and design superior countermeasures. The UK, the official said, is also ensuring Ukrainians benefit from the newfound knowledge.

**UK minister: Iran made ‘big mistake’ in giving drones to Russia for Ukraine war**

Also in January 2023, just a few days before the IAV conference, another senior UK official questioned the wisdom of Iran allegedly providing scores of unmanned systems to Russia for its invasion of Ukraine for much the same reason.

Writing for Breaking Defense, Riad Kahwaji quoted UK Minister of State for Armed Forces James Heappey during a visit to the Middle East as saying that “Russia’s extensive use of Iranian drones” has enabled the Ukrainians and their Western allies “to detect the weaknesses within the Iranian technology and provide effective solutions to counter them.”

**Russians playing with Javelins: US Army, Russia display weapons yards apart in the desert**

Breaking Defense had a team on the ground in Abu Dhabi for this year’s International Defence Exposition and Conference (IDEX) 2023 and so was on hand to walk by and raise an eyebrow at the placement of a Russian arms pavilion literally yards away from a US Army tent.

That would be odd enough, but the US Army tent was specifically showing off a Javelin anti-tank weapon and the Patriot missile system — two platforms used extensively by Ukraine in its defense against Russia’s ongoing invasion. That didn’t stop a few Russians from wandering over and checking out the Javelin, according to a couple American soldiers manning the booth who spoke with Breaking Defense's Ashley Roque. Such is the odd nature of international defense shows.

**Millimeters cost millions: UK still to decide who ‘should cough up’ for $31M aircraft carrier repair bill**

Building defense systems can be an exact science, so exact that if something is off by just a hair, it’s a massive problem. That’s what the United Kingdom learned after it discovered a seemingly tiny — measured by the millimeter — issue with a new aircraft carrier, as Tim Martin reported.

**Uncharted waters: Navy navigating first-ever dismantling of nuclear-powered carrier**

In this report, Breaking Defense's Justin Katz took a deep dive into a novel but long-term problem facing the US Navy: how to dismantle a formerly nuclear-powered aircraft carrier. While the Navy has dismantled nuclear-powered subs before, aircraft carriers present a host of new problems, and the service is only now gingerly approaching the best way to solve them, including a new reliance on industry.

And their first decisions carry weight: Other carriers are in line for dismantling, so whatever the Navy does now could set the template for decades to come.

**Naval Intelligence admiral: ‘Naive’ American public has ‘China blindness’ problem**

The words may sound harsh, but they clearly resonated with readers. In February, a week after a Chinese balloon floated leisurely across the US, Justin Katz reported that the head of Naval Intelligence, Rear Adm. Mike Studeman, was very worried about how Americans viewed Beijing.

“It’s disturbing how ill-informed and naive the average American is on China. I chalk this up, if I could summarize, into a China blindness. We face a knowledge crisis and a China blindness problem,” he said at the West 2023 conference in San Diego.

**Navy begins long haul to inactivate second nuclear-powered carrier Nimitz**
Back on the topic of nuclear-powered carrier dismantling — a surprise hit with readers, apparently — this April report from Justin Katz followed the Navy’s first steps in determining how to deactivate the Nimitz, the second ship scheduled to be broken down after the Enterprise. The Nimitz will actually keep operating until 2026, the Navy said then, but the service had to start planning in 2023 for the massive undertaking.

**Weapons tracing shows Russia firing new cruise missiles at Ukraine just weeks after production**

As the war in Ukraine continued through 2023, all eyes turned to the production capacity not just of the West to keep Kyiv in the fight, but to Russia’s domestic arms war machine. In this May report, Tim Martin followed new analysis that showed Russia was using cruise missiles in combat just weeks after they had been produced, a potential sign that existing stockpiles may be low.

**Russia’s Air Force ‘eating into’ aircraft lifespans, with no easy solution**

Along the same theme, it appears Russia’s ability to keep some of its aircraft in the air is running up against its own problems. In this story, frequent Breaking Defense contributor Reuben Johnson reported that Moscow’s air force was suffering from availability problems, brought on by a combination of over-use and poor maintenance.

“When it comes to the Russian VKS all you can say sometimes is ‘thank God for shoddy maintenance,’” a NATO-nation military aviation analyst said.

**Stop being ‘foolish’: To improve recruitment, Marine Corps takes aim at outdated rules**

All of the military services are struggling with recruitment, so its little surprise the Marine Corps is trying to update its requirements to draw in young applicants and retain the servicemembers they have. Still, it was a bit jarring to hear then-Assistant Commandant Gen. Eric Smith, who’s now in charge of the service, admit that some of the personnel strategies the Marines had been using were “foolish,” as Justin Katz reported.