



**E-BOOK:**

# **Technologies for 21st Century Security**

**SPONSORED BY:**

**LOCKHEED MARTIN** 

# Note from the Editor

Perhaps no technology captured the public's imagination in 2023 like artificial intelligence, with firms like OpenAI grabbing headlines – both good and bad. The Pentagon and defense industry were no different, with top leaders quick to espouse the potential benefits of the technology, even while admitting they don't really have a handle on it yet.

Though less splashy, Pentagon leaders also spent chunks of the year studying the potential applications of quantum technology – something that a decade ago seemed unlikely to ever really come to fruition, but which experts now believe is closer to a reality, at least in some applications.

In this four-part series, Breaking Defense contributing editor Sydney Freedberg takes a step back from the hype for both technologies and asks not just how the Pentagon could apply such capabilities, but whether it actually makes sense. It's a question DoD leaders don't always ask as they chase the latest buzzword, but it's a vital thread to pull for both defense planners and industry executives who hope to cash in on these new capabilities. I trust you will find this collection of stories illustrative and thought provoking. At the very least, we promise it will be more interesting than something written by an AI.

Thanks for reading,

Aaron Mehta  
Editor in Chief, Breaking Defense



# Table of Contents

[Gen Z gamers help Army race towards robotic future force](#) 4

**Sponsored By: LOCKHEED MARTIN** 

[Modernizing our supply chain is a national security imperative](#) 6

[‘All systems need to be hardened’: Officials, industry sound the alarm on quantum threat to encryption](#) 8

[Beyond ChatGPT: Experts say generative AI should write – but not execute – battle plans](#) 11

**Sponsored By: LOCKHEED MARTIN** 

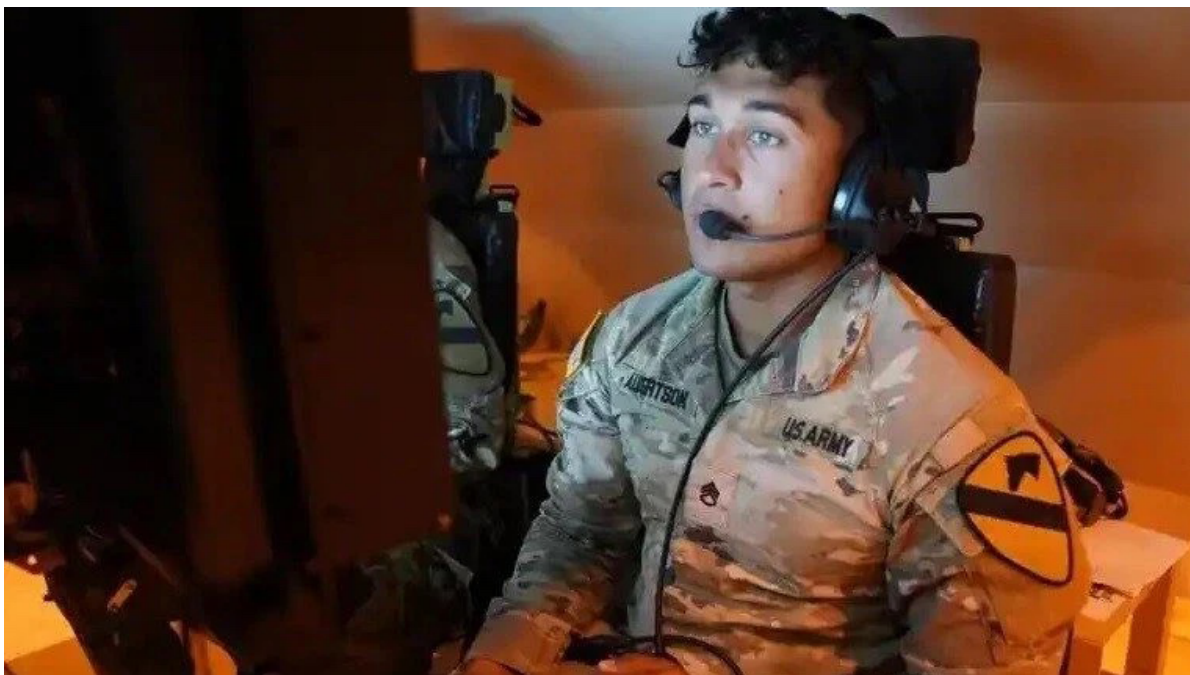
[Rapidly evolving threats demand 21st Century Security solutions](#) 14

[Quantum clocks could revolutionize precision warfare within a decade: experts](#) 17

[3 ways DARPA aims to tame ‘strategic chaos’ with AI](#) 19

# Gen Z gamers help Army race towards robotic future force

With the Robotic Combat Vehicle Light set to enter service in 2028, young soldiers are providing vital feedback on prototypes, tactics and user-friendly interfaces.



An Army soldier remote-controls an experimental Robotic Combat Vehicle (RCV) Medium during field tests at Fort Cavazos (then Hood) in July, 2022. (Eric Franklin/US Army)

By SYDNEY J. FREEDBERG JR. - October 16, 2023

AUSA 2023 — “Keep It Simple, Stupid.” It’s an age-old military maxim, but KISS still applies even to the dawning age of high-tech combat robots. As the Army puts experimental [Robotic Combat Vehicles](#) through field tests in anticipation of a contract award in 2024 and a First Unit Equipped in 2028, young soldiers are providing vital feedback on how to streamline awkward interfaces and complex controls to a robust system they might actually trust their lives to in combat.

To take one very tangible example, “we’ve tried a number of different controllers and gotten really great feedback ... that was a little surprising,” said Brig. Gen. [Geoffrey Norman](#), director of the Next Generation Combat Vehicles team at Army Futures Command, during a Warriors’ Corner panel at the Association of the United States Army conference. “Really elegant Formula 1-style controllers ... were actually less popular than a simple laptop-keyboard-mouse set up that the gamers might be more familiar with.”

Some of that feedback from an experiment at the Army’s [National Training Center](#) at Fort Irwin, Calif., recalled [Michael Cadieux](#), director of the Ground Vehicle Systems Center at Combat Capabilities Development Command: “The operator at NTC [National Training Center] said, ‘you know what, I don’t need this kind of steering wheel that looks like an F1 steering wheel. [Just] give me a mouse and a keyboard, because I have like 29 hours of [War Thunder](#) every day, and I can absolutely control multiple robots and their payloads from a mouse and a keyboard.’”

“A lot of our young people are digital natives and are very comfortable employing this type of technology,” said Maj. Gen. [Curtis Buzzard](#), head of the armor and infantry “schoolhouse” at Fort Moore (formally, the [Maneuver Center of Excellence](#)). That means they may be less vulnerable to information overload than their elders, he explained: “Cognitive overload — sometimes I think we may be overemphasizing that with young people because, again they’re using to doing things and watching multiple things at a time.”

At Fort Moore, Buzzard noted, “we run the small UAS [Unmanned Aerial System] master-trainer course, and we’ve got to go through and train folks on a bunch of legal requirements” — for example, safe operation in domestic airspace — “but we know a young person can grab a UAS and fly it within an hour.”

Robust, easy-to-use controls — like those popularized for gamers and hobbyists — have become a major focus for the Army, Buzzard said. That requires settling on standardized handled devices and software interfaces across a whole future fleet of unmanned systems. That will include multiple types of aerial drones and ground robots, equipped with a wide range of possible payloads, from machine guns and Javelin missiles, to long-range sensors or medical supplies, and operating alongside humans as part of multiple different units, from heavy armored brigades to light infantry.

“What we don’t want,” Buzzard said, “[is] we’ve got five different things we want to employ, so we’ve got to carry five different controllers and five different batteries that require five different types of training.”

“The key thing,” added Norman, “is regardless of what the physical construct is, that the software that’s running behind them is common and that the interface allows the soldier to go from one platform to another to another to another without having to learn a new software system.”

The foundation of that hoped-for future commonality is a set of software standards known as GCIA, intended to apply across the Army’s entire future ground force of manned and unmanned vehicles. (It’s a nested acronym for GCS (Ground Combat System) Common Infrastructure Architecture). GCIA compliance is mandatory not only for companies working on RCV but for those competing to build the [Optionally Manned Fighting Vehicle](#), the replacement for the M2 Bradley troop carrier.



QinetiQ’s proposal for the Robotic Combat Vehicle – Light (RCV-L) (QinetiQ photo)

GCIA, in turn, is an Army ground force implementation of a wider philosophy called [Modular Open Systems Architecture](#), which aims to establish a strict baseline of technical standards but then allow plugging in a wide variety of software packages, or modules, from any company, as long as the software complies with the standard. The hope is this can break the all too common “vendor lock” monopolies, where one large prime contractor develops bespoke software that only it can modify for the rest of a system’s service life.

“The intent there is to have an open system, where we are able to partner ... with industry, best of breed athletes, that understand how to bring very unique and capable software modules into the platform,” said Cadieux. “[There are] probably greater than 50 different industry partners we’ve been collaborating with.”

Another way the Army is trying to get simpler, more flexible and more compatible systems is to separate software development from the work on the various unmanned vehicles. The Robotic Combat Vehicle Light, for instance, is “actually two programs,” explained Norman: “a platform program to [develop the robotic vehicle itself](#)” — with four companies competing — and “a [Software Acquisition Pathway](#) [for] modular system architecture.”

That kind of split is increasingly seen as a more flexible alternative to old-school megacontracts in which one traditional prime contractor does everything. The Pentagon has historically struggled to manage information technology programs — a problem that it’s intent to overcome in an era of warfare where [software, not hardware, becomes ever more decisive](#).

# Modernizing our supply chain is a national security imperative

presented by **LOCKHEED MARTIN**

Closing supply chain gaps in innovating technology will reposition the industrial base to be a strategic source of value.



Photo courtesy of Lockheed Martin.

By BREAKING DEFENSE - April 24, 2024

The U.S. defense industrial base must undergo generational change to keep pace with adversaries and stay ahead of emerging threats. That's what the Pentagon determined in its first [National Defense Industrial Strategy](#) (NDIS) released this year. The report is underscored by a volatile geopolitical environment. The United States is supporting critical partners in Europe, the Middle East and Asia – while still facing the challenge of supply chain fragility exposed by the COVID-19 pandemic.

## *A fully capable, 21st-Century industry*

The NDIS calls for industry to transform into a “robust, resilient, fully capable 21st century defense industrial ecosystem.” Industry must close gaps in the U.S. supply chain's ability to innovate advanced technology integrated systems while simultaneously delivering conventional weaponry for tactical operations.

Prime contractors are developing their own strategies to deliver advanced solutions and surge capability. [Lockheed Martin](#) anticipated the Pentagon's needs and is already operationalizing an enterprise-wide vision for 21st Century Security.

“Our supply chain transformation is repositioning the industrial base to be a strategic source of value,” Lockheed Martin Senior Vice President of Operations Mark Stewart said. “We are creating digitally-connected factories of the future with intelligent, AI-enabled systems, advanced manufacturing technologies, and a high-velocity supply chain for enhanced quality, agility, and readiness to support our customers' missions.”

### **Lockheed Martin: Delivering innovation through supply chain resiliency**

Lockheed Martin has developed its own plan to improve resiliency through a connected, multi-tier supply chain, aligned to the Pentagon's priorities.

"Better understanding risks and opportunities throughout the supply chain allows us to manage our supply more comprehensively," Stewart said. "It's about leveraging where we are common, regardless of where we operate or what we make. A washer can offer the same fit, form and function on an airplane as it does on a missile. If that's the case, we should purchase these in a similar way, minimizing transactions while maximizing buying power and capacity."

Lockheed Martin is focusing on three pillars to deliver manufacturing innovation.

#### **Intelligent Factory Framework**

Lockheed Martin's factories of the future are already improving resiliency and operations to support increased demand. The Intelligent Factory framework allows machines across the enterprise to automatically report their status and utilization using application programming interfaces, machine learning, and software-defined networking.

According to Stewart, the environment currently has more than one-thousand machine connections and tools secured, collecting more than 100 terabytes of data in real time from connected machines – all improving operational efficiency via automation and machine optimization.

"The data from these machines gives our production team visibility into predictive maintenance, dynamic work scheduling, and smart tools," Stewart said.



Photo courtesy of Lockheed Martin.

#### **Additive Manufacturing**

In 2022, the White House launched Additive Manufacturing Forward (AM Forward), a voluntary compact between large manufacturers and their smaller U.S.-based suppliers. Prime contractors, including Lockheed Martin, are working with small and medium enterprise suppliers to help transform shop floors across the country by bringing in new technologies like 3D printing.

The industrial base is also bolstering technical education and training opportunities for additive workforce development.

"Lockheed Martin is supporting AM Forward goals by purchasing additively produced parts from smaller U.S.-based suppliers, training suppliers on new technologies, providing technical assistance to support suppliers' adoption of new capabilities to include new materials, and engaging in common standards development and certification for additive products," Stewart said.

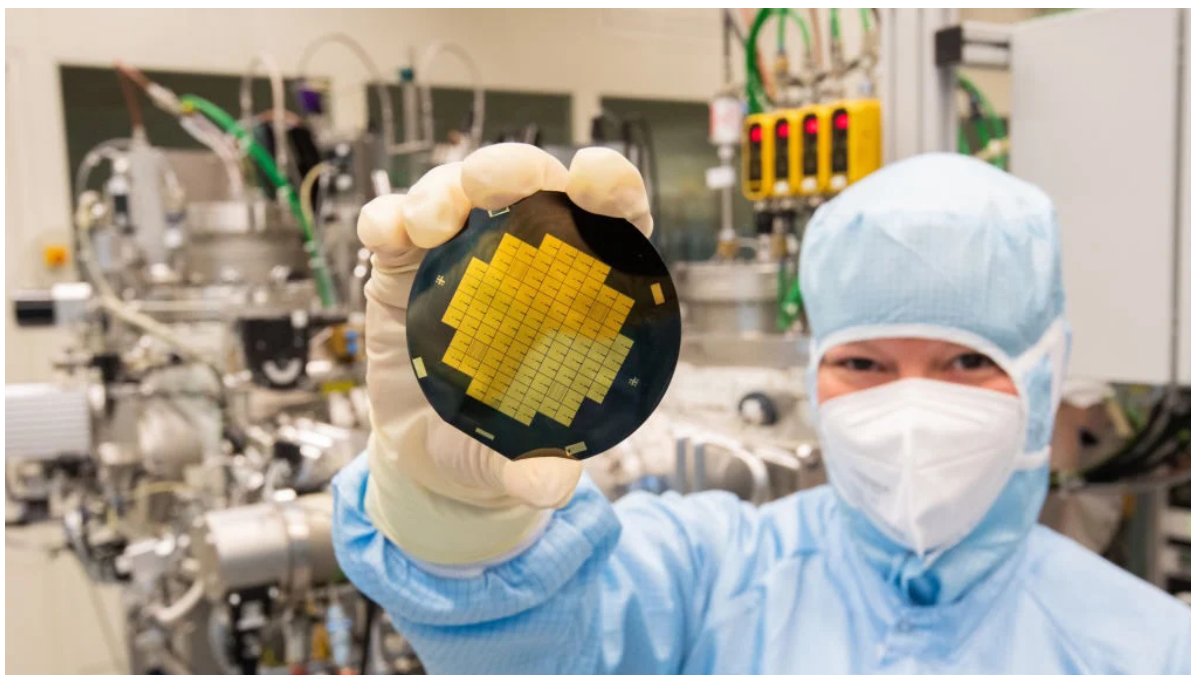
#### **Supply Chain Transformation**

Lockheed Martin's supply chain transformation is repositioning the industrial base to be a greater source of value and to empower supply chain professionals with advanced processes, smart tools, and training to boost skills, enhance agility, and drive value.

"Transforming our supply chain and investing in advanced manufacturing technologies will support our singular focus on our customers and the missions they face today and in the future," Stewart said.

# 'All systems need to be hardened': Officials, industry sound the alarm on quantum threat to encryption

New “quantum resistant” encryption standards won’t be finalized until next year, but officials and experts say agencies and industry should start hunting vulnerabilities hidden in their software and hardware, including embedded chips critical to US weapons.



Friederike Giebel, research associate, shows microchips for quantum processors in a clean room laboratory at the Physikalisch-Technische Bundesanstalt PTB. (Photo by Julian Stratenschulte/picture alliance via Getty Images)

By SYDNEY J. FREEDBERG JR. - September 29, 2023

WASHINGTON — Here at only the second-ever [Quantum World Congress](#), there’s excitement in the air about the prospects for everything from [picosecond-precise timing](#) to [unhackable communications](#) using entangled particles. But a shadow looms on the horizon: the potential for quantum computers to crack the current encryption algorithms that safeguard everything from bank transactions to weapons systems.

“It is important to us to make sure we are investing in both sides — to make sure that we are protecting ourselves [from quantum attacks] while we are also seeking to figure out ... how to leverage quantum technology” for America’s own use, said [Stacey Dixon](#), Principal Deputy Director of National Intelligence, in a Q&A with conference attendees. “All systems need to be hardened.”

This is not a problem for the distant future but today, said [James Kushmerick](#), director of the Physical Measurement Laboratory at the [National Institute of Standards and Technology](#), which is finalizing new “[quantum-resistant](#)” encryption standards. “The sooner we get this out,” he told the conference, “the better off we’ll be whenever a cryptographically relevant quantum computer is developed.”

Such an all-conquering computer doesn’t actually exist yet. But there lies the paradox of what’s called quantum-resistant or “post-quantum” encryption: You don’t need a quantum computer to start laying the foundations for a quantum-powered hack — or, fortunately, to start building a defense.

## *'All systems need to be hardened': Officials, industry sound the alarm on quantum threat to encryption*

The threat is a tactic called “collect now, decrypt later.” Well-heeled foreign intelligence agencies (and the American NSA) already scoop up terabytes of encrypted communication. Whatever they can't crack today can just go into long-term storage, waiting for quantum computers to get powerful enough to break them.

Of course, some secrets will be irrelevant by then, such as the positions and immediate orders of military units: It doesn't help much to decode “Attack Pearl Harbor Dec. 7” on Dec. 8. But other data remains relevant for decades, because that's how long the US military keeps many systems in service. Data like design details and test data from X-35 development in the late 1990s, for instance, will be of interest to adversaries until the [F-35](#) retires circa [2070](#). And even out-of-date information on past operations could be fed into an artificial intelligence that looks for repeated patterns that might predict a future move.

“There's a long tail of how valuable information may be if it's collected now and decrypted later,” Kushmerick told the conference, what the government has described as data with a [“long secrecy lifetime.”](#)

How much “later” will someone get a quantum computer able to break existing codes? While the public can't know what's happening in secret government labs, IBM unveiled a [127-qubit](#) (quantum bit) computer in 2021, hit [433 qubits](#) in 2022, aims to reach [1,121 qubits](#) this year, and has talked of breaking [4,000 qubits](#) by 2025 — what [some experts](#) (but [hardly all](#)) say is a critical threshold for codebreaking. By [one company's estimate](#), a 4,000-qubit computer could to decrypt the widely used RSA encryption — which would take today's supercomputers “millions of years” to crack — “in a matter of hours”; [another company](#) says 10 seconds.

So while widespread quantum computing remains many years away, cutting-edge intelligence agencies could apply it to high-priority targets much sooner.

“You want to do ChatGPT on quantum computers, that will require it to become commonplace... That's 10 years away, no doubt about it,” said [Neeraj Paliwal](#), general manager at Rambus, a company developing quantum-resistant chips. “[But] all they need, at the state level, is four or five functioning quantum computers, even if it is at the cost of \$200 million.”

“That's why NSA and government are all over it,” he told Breaking Defense.

The good news, according to Paliwal and others in the field: You don't need a quantum computer to stop a quantum computer, just better encryption algorithms. And those new algorithms should be able to run on today's computers, although a lot of lower-power devices will need to be upgraded or replaced.

“It's not all that different from how we're doing it now,” said [Michael Vermeer](#), a senior scientist at RAND, in an interview with Breaking Defense. “It's just a new algorithm, [using] a different area of mathematics.”

“You don't need a quantum computer to fight a quantum computer,” agreed [Rebecca Krauthamer](#), co-founder of QuSecure, which develops quantum-resistant software. “It's not a quantum algorithm we're using to encrypt things,” she told Breaking Defense. “It's still classical math, it's just math that's really hard for a quantum computer to solve.”

That said, she warned, “You can't say anything is ‘quantum-proof’ because everything is always changing.... It's going to evolve in ways we can't foresee.”

### **DoD trying to prepare industry**

At first glance, the government timeline to deploy the new quantum-resistant algorithms looks outright stately. [Last year](#), the NSA set an official target of 2035, over a decade away, for all “national security systems” across the US government to migrate to quantum-resistant encryption.

The [National Institute of Standards & Technology](#) released draft standards for the first three algorithms [last month](#) and will take comments on them until Nov. 22 before finalizing them next year. At that point, Kushmerick told the QWC conference, it'll be up to “industry [to] deploy into a product.”

## *'All systems need to be hardened': Officials, industry sound the alarm on quantum threat to encryption*

But that doesn't mean companies and agencies should sit on their hands until 2024, experts emphasized.

"The government... especially DoD, has been doing a lot on trying to prepare the defense industrial base and elsewhere in the government to transition as quickly as possible to the new standard," said RAND scientist Vermeer.

In August NIST, the NSA and and Homeland Security's [CISA published a factsheet](#) urging industry, especially those who support critical infrastructure, to "begin preparing now" to migrate to post-quantum defense.

The message was, in essence, "We haven't fully signed off on the algorithms, so be careful, but you need to start today, [because] it's a really hard problem," said [Kaniah Konkoly-Thege](#), head of government affairs at the quantum computing firm Quantinuum. "Take that basic step of inventorying your data, inventorying your assets, [and] putting in proper policies for retention of data. You also should start testing aggressively, she told Breaking Defense: "Break your system and figure out what doesn't work."

"When we move some aspects of our infrastructure to the new standard, it's going to break things," agreed Vermeer. That's something Google, Amazon, and other major companies have already found in trial runs with prototype post-quantum encryption, he said. "The point of these tests was to figure out where things fail, [but even so] they were surprised – things broke in places that they weren't expecting."

"There is a lot of software that needs to be patched," he said. "We don't know where all of it is right now."

Many applications that use RSA and other [reportedly](#) quantum-vulnerable algorithms are obvious, from online shopping to military communications. But other uses of encryption are hidden deep in complex systems, sometimes in obscure subroutines that need to communicate securely, sometimes in functions embedded on individual chips.

The military has a particularly tricky hardware problem because a lot of its secure technology is not in laptops, desktops, or centralized data centers, but built into all sorts of weapons systems. Much of this "embedded" microelectronics is tailored for specialized military purposes and — because of its age, cost-cutting, or both — has little margin to run the new and more complex quantum-resistant algorithms.

"If you have some hardware that is deployed... and it cannot handle the new algorithm, you cannot fix that, a lot of the time, without ripping it out and replacing it, which is a big problem," Vermeer said. "Part of the urgency for national security systems [is] trying to make sure that what we are deploying now is going to be able to be updated in the field — because most of the time, it can't be."

# Beyond ChatGPT: Experts say generative AI should write — but not execute — battle plans

Training artificial intelligence on military-specific doctrine and intelligence to come up with operational plans is an “active area of experimentation right now,” according to a Special Competitive Studies Project analyst.



What role could AI play in war planning? (Graphic by Breaking Defense, original images via Getty and DVIDS)

By SYDNEY J. FREEDBERG JR. - September 19, 2023

WASHINGTON — Chatbots can now invent new recipes (with [mixed success](#)), [plan vacations](#), or write a [budget-conscious grocery list](#). So what’s stopping them from summarizing secret intelligence or drafting detailed military operations orders?

Nothing, in theory, said AI experts from the independent [Special Competitive Studies Project](#). The Defense Department should definitely explore those possibilities, SCSP argues, lest China or some other unscrupulous competitor get there first. In practice, however, the project’s analysts emphasized in interviews with Breaking Defense, it’ll take a lot of careful prep work, as laid out in a [recently released SCSP study](#).

And, they warned, you’ll always want at least one well-trained human checking the AI’s plan before you act on it, let alone wire the AI directly to a swarm of lethal drones.

“Right now you can go on ChatGPT and say, you know, ‘Build for me a schedule for my kids’ lunch boxes for like the next five days,’” said [Ylber Bajraktari](#), a veteran Defense Department staffer now serving as a senior advisor to SCSP. With a little more programming, he added, “it could connect to Instacart or whatever [and] can order all of those instantaneously, and that will get shipped to you.”

“The technology is there,” Bajraktari said. “The question is plugging those in.”

Plugging in intelligence databases and military command systems, of course, will take a higher standard of engineering than automating menus.

“Specific military tasks [require] a much greater degree of specificity than, you know, creating a great Chicken Parmesan,” said [Justin Lynch](#), a former Army officer and Hill staffer who heads SCSP’s defense studies. “[It] would require better tuning for the LLM [Large Language Model]. It needs to be something that’s more specifically created” for military purposes, he explained: trained on such data as military intelligence, official doctrine, and other verified sources, rather than [scraping text from Reddit posts](#) and other public websites as OpenAI did for ChatGPT.

“That is an active area for experimentation right now,” he told Breaking Defense.

If the generative AI could generate a complete military operational plan, could it then also execute that plan, perhaps by transmitting orders directly to a swarm of combat drones? That’s technologically conceivable but a terrible idea, Lynch said, and it’s not at all what SCSP is recommending.

“Everything we’re talking about is very firmly within [3000.09 \[PDF\]](#),” he emphasized, citing the [recently updated DoD directive](#) that [mandates \(with major loopholes\) human control of lethal force](#).

“We strictly limited ourselves to what I would characterize as sort of a ‘cognitive copilot,’” Bajraktari said. “It’s all about like enhancing *human* decision-making, planning, information intake, information processing, rather than execution of the missions... The technology is not there [for] automated execution.”

You obviously don’t want the SkyNet problem from the *Terminator* movies, where a rogue military AI decides humanity itself is the enemy and launches nuclear missiles. More subtly, Lynch said, you don’t want “the Thomas Beckett problem,” where an agent (human or AI) misunderstands instructions and does something counterproductive while sincerely trying to help.

That’s a reference to the [1170 murder of Saint Thomas Beckett](#), Archbishop of Canterbury, in his cathedral by knights loyal to King Henry II. The king, fed up with years of political wrangling between church and state, is said to have exclaimed “Who will rid me of this troublesome priest?” — only to have some well-armed henchmen take him a little too literally. Now remember AI can be more literal-minded than any human and imagine someone making a poorly worded request to “eliminate” or “remove” a problem.

You always want a knowledgeable human double-checking the AI-generated plan to catch any errors, the SCSP experts emphasized, just as any human writer needs an editor. [Editor’s Note: Correct.] While that slows the pace somewhat compared to pure automation, they acknowledged, it takes a lot less time for a human to check an existing draft than to generate it from scratch, so it should still save significant time over today’s manual and labor-intensive staff processes.

In outline, the SCSP experts envision three tiers of military and intelligence uses for generative AI, from the simplest near-term applications to the most ambitious ones requiring years of careful prep work and experimentation:

1. **Content generation:** SCSP starts with the kind of work that chatbots already do, only custom-tailored for tasks like summarizing secret intelligence reports or military logistics inventories. The more accurate and specific the datasets the AI is trained on, the more accurate and actionable its answers, in contrast the “jack of all trades, master of none” approach adopted by ChatGPT and other consumer AIs. Most military users would want especially strong safeguards in place against AI “hallucinations” that output falsehoods; but, CIA alumnus and SCSP intelligence expert [Chip Usher](#) said, the Agency could use AI’s predilection for fiction to create detailed fake backgrounds for its agents, potentially including years of convincing social-media posts.
2. **Automated orchestration:** At the next level, instead of just drawing on a single dataset, however large, the AI could “call up information from a large set of databases or tools,” Lynch explained. “I’ve spent a lot of time working in Tactical Operations Centers, and usually you have access to hundreds of databases and tools, and time to become familiar with a much smaller number of them.... A large language model can do automated orchestration of [those] and then pull up the most relevant data sets, the most relevant analytic tools for you.”
3. **Agentic AI:** This is where the AI might go from *recommending* tasks to *executing* them, albeit under strict controls. The SCSP experts envision the generative AI tasking subordinate AIs to gather information to fill in gaps in its data, for example, or to organize supply convoys — not to launch autonomous lethal swarms.

The higher levels in this framework build on generative AI's ability to take a broad, plain-English request — from “plan my kids’ meals for next week” to “come up with a logistics plan for my battalion” — and turn it into a detailed checklist of specific tasks. The AI doesn’t actually *understand* the tasks, Lynch emphasized, but it has seen enough human-written checklists to generate its own, similar ones when asked.

Likewise, the AI doesn’t really “understand” what its human masters are asking it to do. It has no awareness of external reality, only of statistical correlations among words and parts of words (“tokens” in the jargon). But LLMs have gotten really good at turning human-language input into machine-readable 1s and 0s and then turning their output into intelligible words. That allows them to act as intermediaries between humans — even untrained humans — and ever-more-sophisticated algorithms.

“What’s different with ChatGPT, suddenly you have this interface, [where] using the English language, you can ask it questions,” the former director of the Pentagon’s Joint AI Center, retired three-star general [Michael Groen](#), [told Breaking Defense](#) this past spring. “It democratizes AI [for] large communities of people.”

“Many of the tools we are seeing emerge have natural language interfaces that dramatically increase accessibility and lower barriers to operating in certain sectors without years of intense training or education,” SCSP’s Bajraktari said. The downside is that it’s easier than ever for a few ill-intentioned individuals to mass-produce misinformation, malware, or even lethal weapons like homemade bombs or poison gas. The upside is a tremendous potential for people without intensive technical training in AI to take advantage of powerful new AI technologies.

In fact, between the rise of AI and the rise of China, the SCSP report argues, humanity is facing a combination of technological change and geopolitical instability with an unnerving “resemblance to the era before World War I.” That’s less than reassuring, but with some expert (human and maybe non-human) advice, perhaps the world can navigate the turmoil better this time.

# Rapidly evolving threats demand 21st Century Security solutions

presented by **LOCKHEED MARTIN** 

Innovative, interoperable capabilities networked seamlessly across all domains will be required to maintain the edge and deter future conflict.



Lockheed Martin JADO from space. Photo courtesy of Lockheed Martin.

By **BREAKING DEFENSE** - December 6, 2023

In this Q&A with Lockheed Martin vice president and Chief Technology Officer Steve Walker, we discuss the company's vision for urgent technology innovation called [21st Century Security \(21CS\)](#), how it is transforming to support customers' missions in a more complex battlespace, and why it is partnering with commercial industry to drive advanced capabilities for the defense industry.

## **Breaking Defense: What is Lockheed Martin's 21CS vision?**

**Walker:** We all know that the world is increasingly complex and threatening with issues across the globe. From a security standpoint, the pacing challenge we measure ourselves against is China, which has resources and massive investments in advanced technology. That means the U.S. must get a lot better at multi-domain operations and Joint All Domain Command and Control (JADC2).

When I first came to Lockheed Martin from DARPA about four years ago, I identified capabilities that we need to accelerate as a country and a strategy for how Lockheed Martin could deliver advanced, mission-focused technologies while leveraging emerging ones across multiple domains that would give us the edge and help deter war in the future.

That strategy accelerated when Jim Taiclet was named CEO a few months later. He understands that evolving threats require new ways of doing business and has been my biggest advocate in building research partnerships and integrating commercial investments to drive innovative capabilities for the best mission effects.

Those capabilities are laid out in our 21CS vision and include technologies such as AI, machine learning, autonomy and crewed-uncrewed teaming, and the 5G.MIL Unified Network Solutions (UNS) tactical mesh network. We just successfully demonstrated this hybrid 5G-tactical mesh network live in a multi-domain environment.

Lockheed Martin makes the best physical platforms in the world across land, air, sea, space and cyber. Through our 21CS strategy, we are collaborating to harness the best of commercial technology to drive capabilities that give military forces more range, speed, agility and a decision-making advantage.

**Breaking Defense: Tell us some details about those capabilities you just mentioned.**

**Walker:** 5G.MIL and advanced comms are about resilient communications, and being able to combine the low latency and high bandwidth advantages of 5G with our military advanced tactical data links that are highly secure to give our customers the best of both worlds.

If we can do that, we'll have a resilient comms capability that can network our satellites, airplanes, and weapons systems across space, air, and maritime domains. That's a critical technology for connecting the dots.

We think that AI and machine learning are such important areas that my team stood up the Lockheed Martin AI Center to help promulgate that technology across the company. We've built up a capability in-house to do the compute, the algorithm development, and to harness the algorithms that are out there and apply them to military applications using our ethical AI framework; all knowledge that we then share across Lockheed Martin.

So how does AI and machine learning play into the big picture? When we think about AI and machine learning, we don't really think about machines making decisions. We think about machines helping humans make more informed decisions faster.

We also have significant investments in autonomy and crewed-uncrewed teaming. This is about building 5G.MIL, AI, machine learning, and communications technologies into some of our platforms so they can understand and communicate with each other in order to accomplish missions with one understanding.

This would produce what we're referring to as 'autonomy-enhanced JADC2' that works across multiple domains and produces capabilities that are hard to defeat.

Another area is microelectronics or edge computing. If you're going to have an autonomy-enhanced JADC2 system, you're going to need edge processing. That means processing on platforms – not necessarily big platforms but smaller ones operating at the edge of the battlefield.

The processor in that edge device has to do the compute, processing, and in some cases the AI/machine learning. Another technology that's critical to all of this is the processing or the microelectronics that go into these systems.

All those technologies are going to have to come together to help us enable JADC2.

**Breaking Defense: What milestones have you reached in the execution of the 21CS vision to support DOD priorities, especially as a participant in exercises like Northern Edge?**

**Walker:** We participated in Northern Edge '23 in Alaska this summer, the first true joint force, multinational synchronization demonstrated at this scale across all services, operation levels, and domains. One of the things we demonstrated was our battle management command and control (BMC2) planning tools called DIAMONDShield. This is an important product for multi-domain battlespace management that helps with more centralized, upfront planning of a battle than we've done it in the past. Think about all the services coming together and using DIAMONDShield to produce a battle plan for a C2-type operation.



Steve Walker vice president and Chief Technology Officer, Lockheed Martin.

We were also able to use that tool and combine it with something we call the ‘Virtualized Aegis Weapon System’ that extended this planning capability out to the edge. It demonstrated a superior planning capability both centrally for more strategic operational use, and then also when connected to edge platforms through the virtual Aegis system.

That combination is something that can help INDOPACOM with their joint fires network. I commend INDOPACOM for pursuing JFN and, in my mind, being the first instantiation of something close to JADC2. I’m proud that Lockheed Martin, through our tech developments and 21CS solutions, is a full partner in that work with INDOPACOM.

**Breaking Defense: Earlier you described some of the capabilities you’re looking for from commercial sector partners. Tell us about some of those collaborations.**

**Walker:** Part of our 21CS strategy is collaboration with commercial companies who have made significant investments in many of these tech areas such as AI and communications. We have quite an array of large and small partners, some that we’ve announced and some that we haven’t, with whom we are focused on applying advanced technologies to military problems.

One example would be a recent demonstration we did with IBM Red Hat to determine how to get a processor onto an edge device like a small unmanned aerial vehicle and then have the ability to control this UAV — or multiple UAVs — in real time as the mission changes on the battlefield.

We worked with IBM Red Hat on what was needed in terms of size, weight, and power for the processor that we wanted to install, and they did it. We’ve shown great success in being able to modify the mission set that a series of UAVs would perform in real-time based on dynamic battlefield scenarios.

I’ll also mention our collaborations with GlobalFoundries and Intel on microelectronics, a critical technology that basically goes into everything we do. The partnership with Global Foundries that we announced in June is already paying off for both companies as we work to understand how microelectronics affect defense applications. We are on several of the government’s Tech Hubs around the country and are winning resources to pursue microelectronics development for national security.

These win-win collaborations help the microelectronics companies that have not traditionally been involved in the national security space better understand the market as they work with us on developing advanced capabilities. Those companies will then spin that knowledge and experience back into the commercial world where the security of microelectronics and chips is becoming increasingly important.

**Breaking Defense: AI is not a new capability for Lockheed Martin. How do you ensure the ethical use of AI for national security?**

**Walker:** We quickly embraced the Pentagon’s five principles of AI ethics – responsible, equitable, traceable, reliable, and governable – and developed an internal policy based on those five principles.

Our governance process includes an AI executive steering committee with an AI ethics subcommittee that regularly meets to understand and assess our AI work and ensure it abides by those five principles.

We’re also working on technologies that help the user understand what the AI is doing. Emphasizing the explainability of AI or explaining to the user why the AI is making its decisions, is critical.

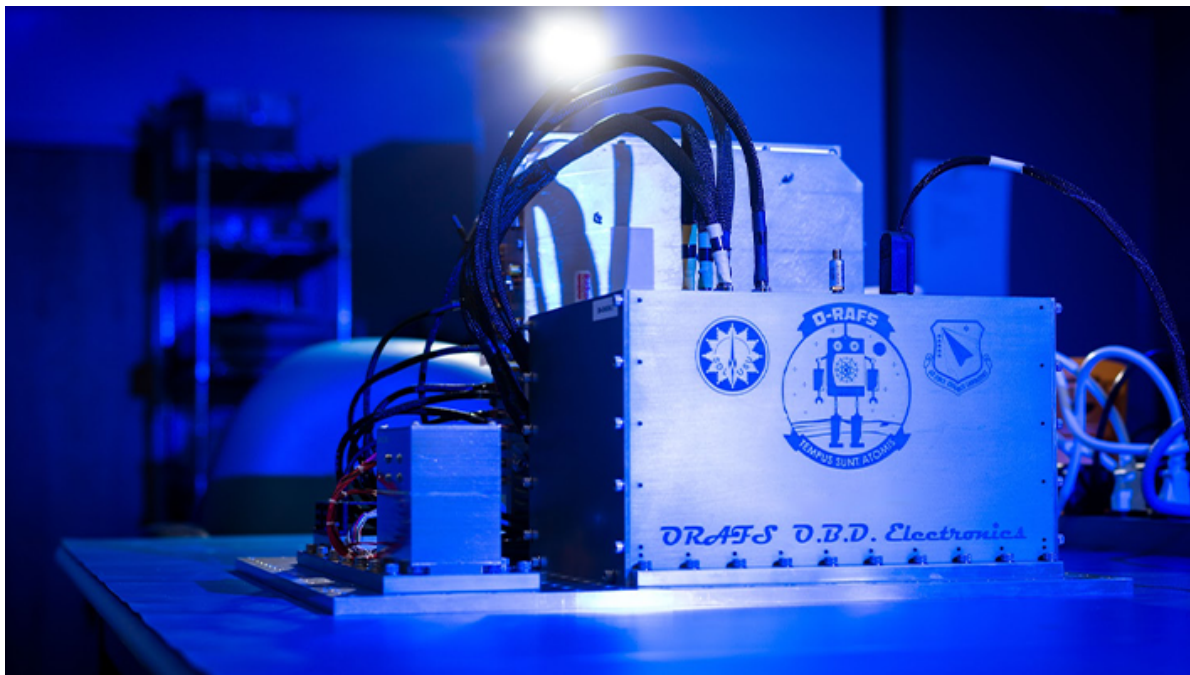
Also important is coming up with a way to test and verify systems that are autonomous and might be using AI and machine learning to make decisions. Part of our investment in autonomy and crewed-uncrewed teaming is how we test these systems and validate/verify what they’re going to decide and what they’re going to do.

My overall view of AI and the ethics associated with it, especially in warfighting, is that AI shouldn’t be making the final decisions, humans should. However, AI can enable humans to receive and process data faster and more accurately than we could do on our own, for improved decision making.

It’s more about human-machine partnership than just machine understanding on its own what to do.

# Quantum clocks could revolutionize precision warfare within a decade: experts

Within five to 10 years, clocks “a million times” more precise than GPS could improve accuracy, communications, and electronic warfare – without relying on an easily jammed satellite signal.



AFRL's Quantum Sensing & Timing (QST) group looks into the development of advanced atomic clocks to further improve time measurements and investigates ways to use and distribute the precise time. (AFRL)

By SYDNEY J. FREEDBERG JR. - September 12, 2023

NATIONAL HARBOR, Md. — What difference does a nanosecond make? If you're using your phone's GPS to find the nearest Starbucks, not much. But for satellites zipping along in [low orbit](#) at five miles per second, radio waves moving at the speed of light, or AI chips doing billions of calculations per second, being off by one billionth of a second actually matters.

That's why the US military wants to move beyond the GPS timing signal — which is accurate to less than 30 nanoseconds, and which enemies can jam — to compact “quantum clocks,” small enough to fit in a missile warhead or small drone and accurate to the picosecond (one thousandth of a nanosecond) or beyond.

[Last year](#), the Air Force Research Laboratory, the US Navy, and foreign partners from the ultrasensitive Five Eyes alliance collaborated to test quantum tech at sea during the annual [Rim of the Pacific](#) exercises, AFRL official Michael Hayduk said this morning. That included tests of quantum sensors and navigation systems — both of which rely on precision timing — as well quantum clocks, he said. The goal was take bulky experimental systems from the lab — “very large, lots of lasers” — and shrink them down to fit aboard a ship, while making them rugged enough to preserve their atomic-scale accuracy despite the constant motion of the ocean, he told the [Air Force Association conference](#) outside DC.

“We were kind of surprised how good some of the results were,” Hayduk said. “We’re going to go back [to the lab] and continue to tweak.”

So how close are quantum clocks to militarily relevant reality, given all the often-overheated quantum hype? Consider that full-scale quantum computers, capable of breaking any existing encryption, are generally considered to be more than a decade away. Last year, the NSA officially set a deadline for defense contractors to implement new quantum-proof algorithms by 2035 [[PDF](#)].

But a quantum clock is a much simpler piece of hardware, and there have been major advances in crucial underlying technologies, especially the ultra-precise lasers used to measure and manipulate individual atoms oscillating billions of times per second.

“When we look at quantum capabilities that could be near-term relevant in five to 10 years... something we can shove in any old aircraft... it really comes down to timing — clocks that are millions of times better than today’s atomic clocks,” said [Heather “Lucky” Penney](#), a former [fighter pilot](#) now at AFA’s [Mitchell Institute](#). Of all the potential applications of quantum tech, she told the AFA conference, “that is probably the nearest term capability.”

Clocks with “a million times” greater precision are “the nearest term” application of quantum tech, agreed Chester Kennedy, who oversees research and security applications at [ColdQuanta](#).

Today’s atomic clocks are bulky and expensive, which means they can be accommodated aboard a small number of bulky, expensive platforms, like GPS satellites. But, Kennedy told Breaking Defense after the AFA panel, quantum clocks are not only exponentially more accurate, improvements in miniaturization mean it should soon be possible to shrink them to the size of a water bottle.

That means you could accommodate quantum timing aboard a modestly sized drone, or in an electronic warfare pod on a jet fighter, or in the targeting systems of a hypersonic missile, instead of relying on a GPS timing signal that enemy [electronic warfare](#) units could jam. And with exponentially more precise timing, quantum-equipped forces could hop frequencies more frequently to avoid enemy jamming, transmit more devilishly complex jamming themselves, and deliver precision ordnance more accurately.

Of course, all this depends on getting today’s accurate but bulky quantum clocks small and tough enough to work on the frontline. That’s not a challenge the commercial sector or academia have much incentive to solve, warned several of the panelists, so the Pentagon has to lead the way on miniaturization R&D — and pay for it.

“The people that are doing the quantum information science R&D are not experts in mission-level sensing or mission-level timing,” said Tanner Crowder, a quantum expert at the White House [Office of Science & Technology Policy](#). “They don’t know necessarily what it takes to take something that’s sprawled out on a 4×8 optics breadboard and ... make it go on a ship or on a plane.”

# 3 ways DARPA aims to tame 'strategic chaos' with AI

Combat is too complicated and chaotic for existing AI to analyze, and DARPA is trying to figure out the best way to combine algorithms with human expertise.



While AI is improving all the time, playing chess is small fry compared to actual war scenarios. (Westend61/Getty Images)

By SYDNEY J. FREEDBERG JR. - September 5, 2023

WASHINGTON — Chess is the world's oldest wargame, and computers mastered it in 1997. Real war is vastly more complex, and machines still struggle to make sense of it. So while the machine-learning techniques that power today's AI can crunch the numbers to win at chess — two identical armies of 16 pieces fighting over 64 squares — they cannot grapple with the ambiguity and chaos of actual combat.

That's a problem for the Pentagon, which wants AI-driven "battle management" aides to help human commanders coordinate [Joint All Domain Operations](#) with dozens of ships, hundreds of aircraft, and thousands of troops maneuvering across land, sea, air, space, and cyberspace. So the Defense Department's official agency for long-shot, high-payoff research, DARPA, contracted earlier this year with three companies to push past machine-learning to next generation of AI — something that could, at least in theory, help bring order to what DARPA calls "strategic chaos."

"JADC2 [[Joint All Domain Command & Control](#)] does require a lot of planning," said [Aaron Kofford](#), a DARPA program manager. "That's what SCEPTER's all about."

SCEPTER is short for the Strategic Chaos Engine for Planning, Tactics, Experimentation and Resiliency, where "Engine" is a deliberate nod to the game-playing programs known as [chess engines](#), Kofford explained in an interview with Breaking Defense.

"I'm a chess player," Kofford said, and there's a lot to learn from chess AI. Modern chess engines can not only beat human players, he emphasizes, they can also help them by analyzing their games, commentating, and advising on better moves. Similar AI tools for warfare help commanders and their staffs to plan a military operation.

"This is not replacing humans," he emphasized. "This is a tool for humans." (That's in keeping with longstanding Pentagon policy and strategic culture that prefers a [symbiosis between human and machine](#), rather than a SkyNet-style AI that controls everything like, well, pawns). "We are trying to improve the tools that humans have to help them evaluate situations."

"Trying" is very much the operative word. "We're still in the 'can this possibly work?' step," Kofford admitted freely. "This is a pretty crazy idea."

Why? Games like chess are amenable to computers because they are, as Kofford puts it, "well-bounded." While the total number of possible positions is practically infinite, the available choices for each player on each turn are starkly limited and clearly defined. So algorithms can explore potential pathways step-by-step, then calculate which branching paths likely to lead to victory and which branches lead to loss and should be trimmed. (The technical term is "[Monte Carlo tree search](#)").

But for a military force about to enter battle, or just leaving its home base for the front, the number of possible "next moves" is much larger and less precisely measurable than on an 8 by 8 grid. Even for an ordinary civilian getting up in the morning, there are incalculably many options, some trivial and some radical, from "make coffee, then go to work" to "go to work, then get coffee" to "quit my job, sell all my belongings, and go join a commune in Nepal."

"There is an infinite number of things I could do next," Kofford said, which requires cutting down the infinite possibilities to something the machine can manage.

To do that, it turns out, you need to revive an idea that predates machine learning, going back to what DARPA calls "[first wave AI](#)": so-called expert systems, still used today for everything from tax preparation to medical diagnosis. Instead of unleashing the algorithm on a mass of data and have it trial-and-error through in search of correlations, you start with knowledgeable humans — experts — defining a set of options and rules for the machine to follow.

"I do think we can apply some expert knowledge to search some of the more important spaces and search them quickly," Kofford said "faster than any individual human mind or any collective human council."

The goal is to get the best of both worlds, a synergy of human understanding of the universe (as in old-school expert systems) and computer speed at processing big data (as in modern machine learning). But just like with the decision tree in combat, there are multiple ideas for how to get to that end result, and DARPA is open to different approaches. So the agency has awarded three contracts for SCEPTER — to research firm [Charles River Analytics](#), non-profit Parallax Advanced Research, and behemoth [BAE Systems](#) — to explore three different paths.

#### **Symbolic Reasoning: What Would Humans Do?**

How do ordinary people cope with the everyday, real-world messiness that baffles the smartest machines? "What makes these problems solvable, for humans at least, is that humans are always applying a big bag of what you might call heuristics or approximations," Charles River scientist [Michael Harradon](#) told Breaking Defense. "I don't have to consider every possible thing."

When you're driving and deciding where to turn, for instance, you don't calculate every possible angle from zero degrees to 180, you generally just choose left/right/straight. When tax prep software generates your return, Harradon explained, it doesn't randomly allocate all possible numbers to all possible lines of Form 1040 and then apply machine learning to figure out which combinations are less likely to get you audited; It follows strict rules pre-programmed by human experts.

"Any time you are deducing something logically, any time you are producing a checklist, any time you're making a plan," Harradon explained, "those are all really forms of symbolic reasoning." Computers may have a harder time coming up with checklists, but once it's made they can check it off much faster than a human — or even than a machine learning algorithm trying to calculate every possibility.

So how do you create a big enough checklist to plan a battle? That's where it gets tricky, Harradon admits. Instead of only using heuristics or only using machine learning, he says, you "take the best of both" and combine them, each feeding back to improve the other. In some areas, humans can input heuristics to tame a mass of data; in others, the algorithm can crunch the data, find correlations, and deduce its own rules of thumb.

"This field, it's very much in its infancy," Harradon acknowledges, "[but] there are a number of really good demonstrations" – including some in-house studies that Charles River isn't ready to share.

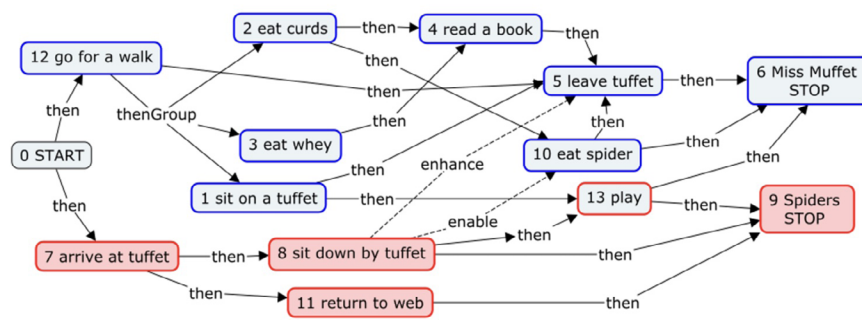


Fig. 11: Causal Event Graph for Miss Muffet

From H. Van Dyke Parunak, "How to Turn an MAS [multi-agent system] into a Graphical Causal Model."

### Causal Networks: Little Miss Muffet Sat Down On A Tuffet

In contrast to Charles River's straightforward method of combining human expertise with computer calculation, Parallax's approach is almost whimsical: It has people tell the AI stories, in flowchart form.

Consider Miss Muffet of nursery rhyme fame, Parallax scientist [Van Parunak](#) said in an interview. If she's sitting on her tuffet, eating her iconic curds and whey ([a form of cottage cheese](#)), and along comes a spider... does she run away? Keep eating? Smush the spider? Eat the spider? (That last option first occurred to Parunak in 5th grade). While Miss Muffet theoretically has infinite options — far too many for even a computer to analyze — in practice there's a finite number of plausible, relevant responses to the situation.

Each of those responses leads in turn to a new situation, where there are new possible options — maybe now the spider tries to run away? — which lead to yet more situations with more options. By linking all these relatively simple options, step by step by step, you end up with a sophisticated map of possibilities, formally called a "causal network."

Computer programmers already use this kind of story flowchart all the time: It's the basic skeleton of many [roleplaying games](#). Instead of analyzing every possible option, Parunak says, you simplify the problem to "When the player is in one particular state, what can you do next?"

"It has huge potential for military people who aren't computer programmers, but they love to draw boxes and arrows," he went on. "I met with many people in the IC [[intelligence community](#)] and whenever they wanted to explain a scenario, the first thing they would do is pullout a piece of paper or walk to a whiteboard and start drawing boxes and arrows."

Of course, these flowcharts of options are more complicated than Miss Muffet's and require more expertise to draw. One of Parallax's military scenarios — which they can't share with the public — was drafted by a retired Air Force master sergeant and includes almost a thousand discrete events.

The good news? Such military experts don't need to learn to code in order to draw flowcharts. Even better? The AI doesn't need to understand the story of the flowchart to analyze it, just understand that event A has options A1, A2, A3, etc. that lead to situations B1, B2, B3, and so on. Add positive and negative values to each situation, so the computer knows which ones to seek out and which to avoid, then set the algorithm loose to explore the possibilities over and over, learning optimal paths that might be apparent to a human looking at the flowchart.

"It's a very simple decision process," Parunak said, "which lets it run extremely fast," over and over until the AI has enough data to make correlations.

#### **Tailorable Abstraction: Simulating The Simulations**

One lesson of chess engines is that if you let an AI play a game over and over enough times, it can learn to play as well as, or better than, a human. An while chess is too simple to be a realistic wargame, BAE scientist [Marco Pravia](#) told Breaking Defense, there are lots of better simulations available — many of them developed specifically for the Defense Department using detailed (often classified) data on real-world weapons systems.

"There is already a huge library of simulations that people have spent decades, in many cases, refining, [and] that planners already find already find useful," Pravia said in an interview. So instead of running simulated chess games to train a chess bot how to win, you're running the military-specific simulators over and over until the AI can start to see what patterns of choices lead to success.

Of course, Pravia acknowledged, there's a catch: These military simulations are a lot more complex than chess, so they require a lot more computing power to run. While you can teach an AI to play chess through brute force trial and error, running millions of simulated chess games until it learns the statistical correlations between certain moves and checkmate, you can't do that with military-specific simulations.

So BAE is taking a shortcut: Essentially, they're simulating the simulations. Running a military simulator creates data that an AI can analyze. Give the AI enough of that data, and it can create a simplified version of the original simulation that captures the essential dynamics but abstracts away minor details. That simplified simulation-of-a-simulation — what BAE calls a "tailorable abstraction" — takes much less computing power to run, so you can run it over and over and over again, creating enough data for machine learning algorithms to analyze that output in turn.

But, when you're simplifying the original simulation into the "tailorable abstraction," how do you know you're only getting rid of trivial details, not essential ones? That's a judgment call, Pravia acknowledged, one that must be made by expert humans.

In essence, it's a layer cake of AI and human expertise: Humans create the underlying simulations, AI generates the simulations of the simulations, and humans tune those tailorable abstractions to meet specific purposes.

And how will DARPA evaluate if any of these three approaches works? By feeding the results back to human beings.

"We're having [military] planning experts look at the outputs and say, 'actually, that was kind of useful'" — or not, Kofford said: "Ultimately, it's going to be up to planners to let us know if we're wasting time or helping them."