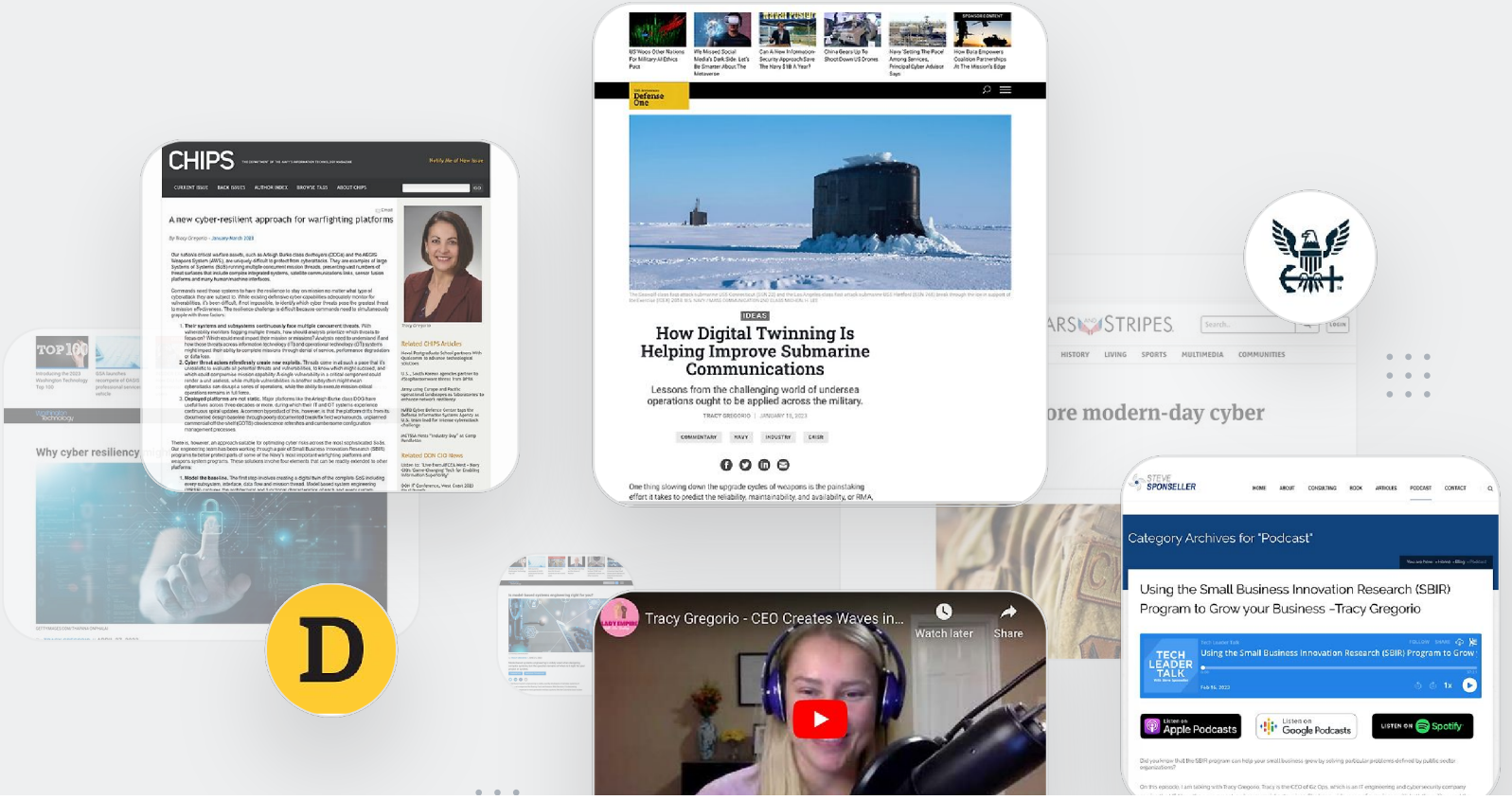
WAYNE HENNINGER
COMMUNICATIONS

YVONNE TOCQUIGNY
BRANDING GROUP

# G2 Ops Press Hits



# Contents

**Summary** ..... 3

**Highlights** ..... 5

**Byline articles** ..... 8

# Summary

# 34

## Pieces of Coverage

Total number of online and social clips

# 32.9K

## Estimated Views

Prediction of lifetime views of coverage, based on audience reach & engagement rate on social

# 3.87M

## Audience

Combined total of publication-wide audience figures for all outlets featuring coverage

# 209

## Engagements

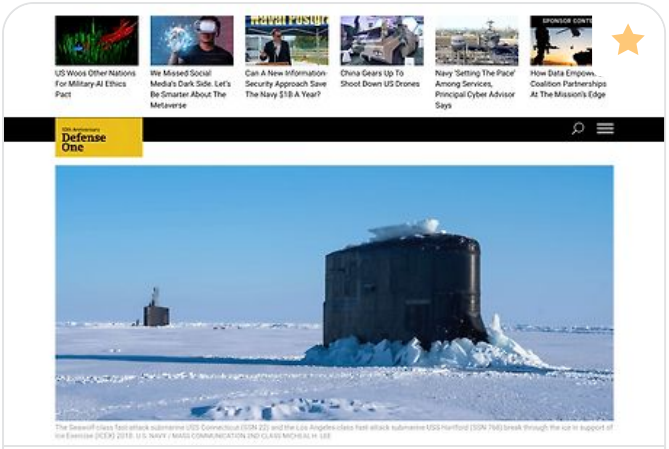
Combined total of likes, comments and shares on social media platforms

# 55

## Avg. Domain Authority

A 0-100 measure of the authority of the site coverage appears on. Provided by Moz

# Highlights




### Defense One

How Digital Twinning Is Helping Improve Submarine Communications

3.92K 693K 49


### CHIPS

A new cyber-resilient approach for warfighting platforms

47 13.5K 0


### Tech Leader podcast by Steve Spo...

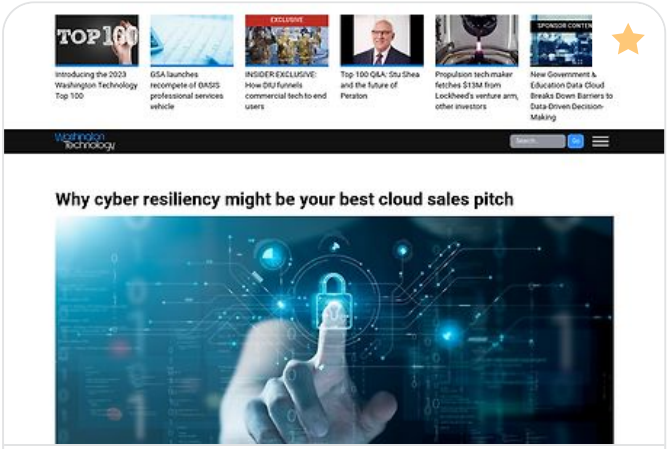
Using the small business innovation research program (SBIR) to grow your...

0


### Lady Empire Podcast

Tracy Gregorio - CEO Creates Waves in Cybersecurity

1 9 -




### Washington Technology

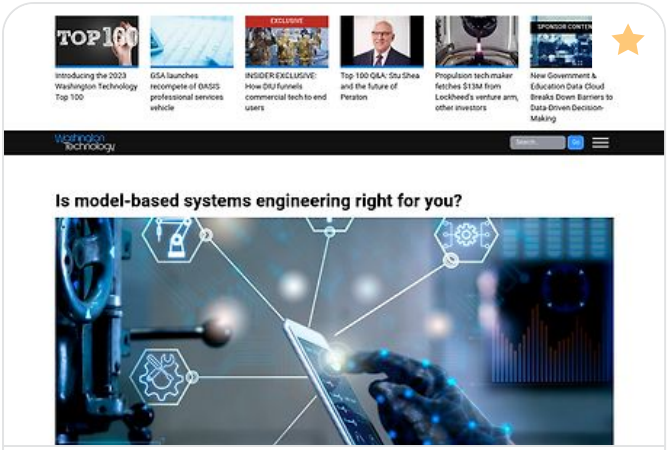
Why cyber resiliency might be your best cloud sales pitch

397 42.8K 3


### Stars and Stripes

The need for more modern-day cyber warriors

3.48K 838K 0




## Washington Technology

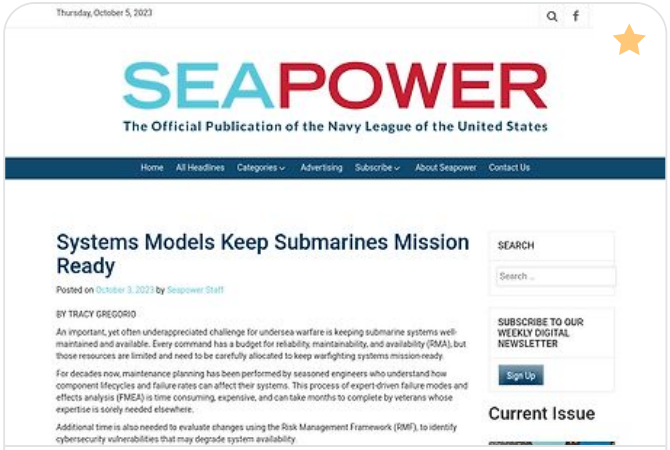
Is model-based systems engineering right for you?

404 42.8K 9


## NavySTP Transitions Newsletter

Build-Test-Build Iterative Design Improves Development

542 981 0




## Seapower

Systems Models Keep Submarines Mission Ready

244 23.5K 0

# Byline articles

Exclusive bylines featuring Tracy Gregorio thought leadership.

17 pieces

## GovTech

Government Technology has IT articles for state, local and city government. Find government news...

**81**
Domain Authority
Provided by MOZ

**172K**
Unique Visits
Provided by SimilarWeb

government technology

CONTINUE TO SITE

OPINION

### Digital Twins Key to Cyber Resilient Infrastructure

Attack vectors in critical infrastructure are always changing, and agencies must move beyond just preventing cyber attacks and toward resiliency. Digital twin modeling can help governments prepare to work through any scenario.

December 16, 2022 • Tracy Gregorio, G2 Ops

Shutterstock/Yurchanka Siarhei

Deploying systems fully designed to sustain operations during and after a cyber attack is quickly becoming the most realistic method for keeping critical infrastructure online.

Critical infrastructures often comprise complex systems of systems (SoS) running through interrelated IT platforms, applications, operational technologies (OT) and human/machine interfaces. We depend on systems of systems to orchestrate transportation networks, protect citizens from terrorist attacks and sustain utility grids. The increasing convergence of IT and OT systems creates opportunities for exploitation that can have catastrophic consequences.

Most state and local government IT managers have recognized these vulnerabilities and responded by

December 16, 2022 • ONLINE

# Digital Twins Key to Cyber Resilient Infrastructure

govtech.com/opinion/digital-twins-key-to-...

Estimated Views **635**

Estimated views calculated based on audience size and socia...

Engagements **13**

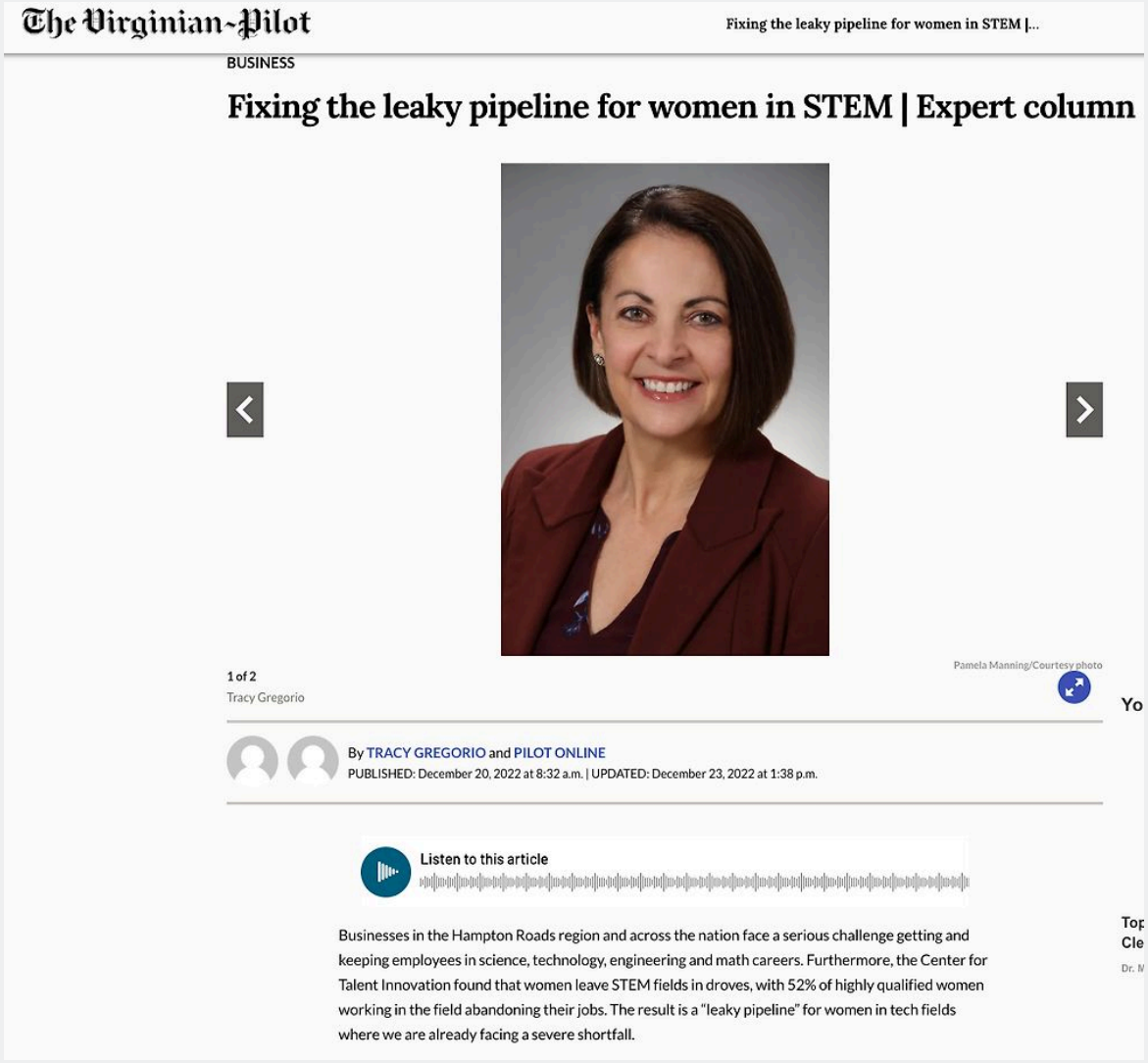
Total number of social engagements

## The Virginian-Pilot

The Virginian-Pilot: Your source for Virginia breaking news, sports, business, entertainment, weather an...

**76**
Domain Authority
Provided by MOZ

**823K**
Unique Visits
Provided by SimilarWeb




December 20, 2022 • ONLINE

# Fixing the leaky pipeline for women in STEM | Expert column

pilotonline.com/2022/12/20/fixing-the-lea...

Estimated Views

**5.02K**

Estimated views calculated based on audience size and socia...

Engagements

**0**

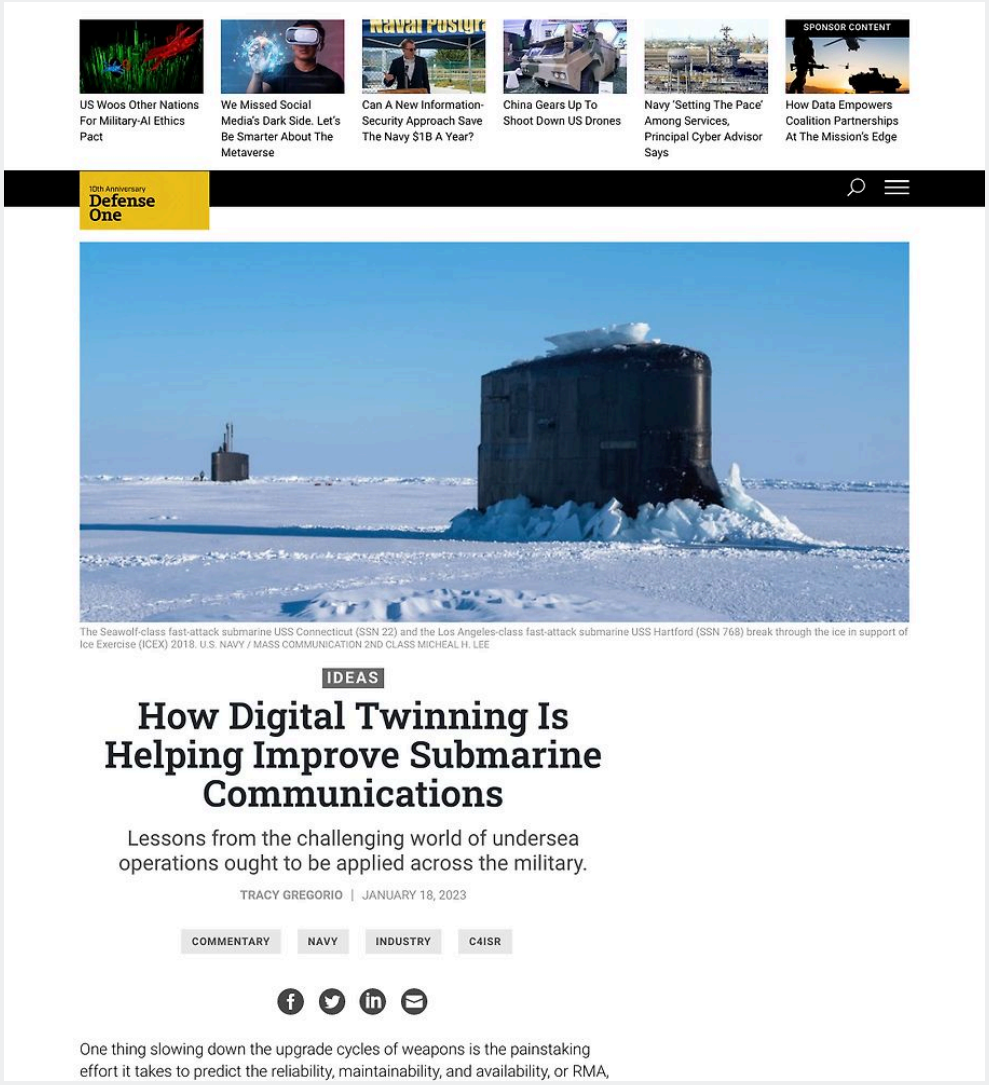
Total number of social engagements

# Defense One

Defense One provides news, analysis, and ideas about the future of national security to defense an...

**75**
Domain Authority
Provided by MOZ

**693K**
Unique Visits
Provided by SimilarWeb




January 18, 2023 • ONLINE

## How Digital Twinning Is Helping Improve Submarine...

defenseone.com/ideas/2023/01/how-digit...

Estimated Views

**3.92K**

Estimated views calculated based on audience size and socia...

Engagements

**49**

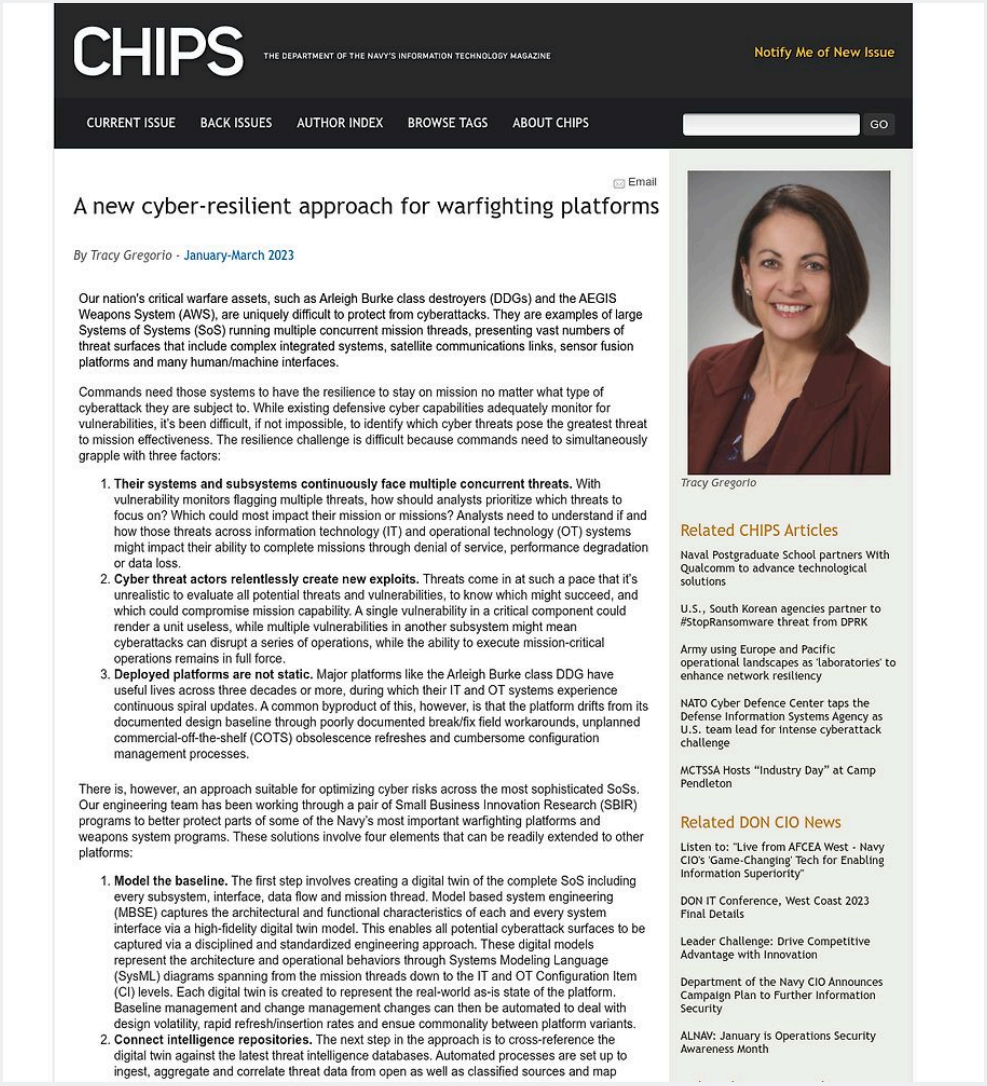
Total number of social engagements

## CHIPS

CHIPS is an official U.S. Navy website sponsored by the Department of the Navy (DON) Chief Informati...

**88**
Domain Authority
Provided by MOZ

**13.5K**
Unique Visits
Provided by SimilarWeb



CHIPS
THE DEPARTMENT OF THE NAVY'S INFORMATION TECHNOLOGY MAGAZINE
Notify Me of New Issue

CURRENT ISSUE | BACK ISSUES | AUTHOR INDEX | BROWSE TAGS | ABOUT CHIPS | GO

Email

A new cyber-resilient approach for warfighting platforms

*By Tracy Gregorio* · January-March 2023

Our nation's critical warfare assets, such as Arleigh Burke class destroyers (DDGs) and the AEGIS Weapons System (AWS), are uniquely difficult to protect from cyberattacks. They are examples of large Systems of Systems (SoS) running multiple concurrent mission threads, presenting vast numbers of threat surfaces that include complex integrated systems, satellite communications links, sensor fusion platforms and many human/machine interfaces.

Commands need those systems to have the resilience to stay on mission no matter what type of cyberattack they are subject to. While existing defensive cyber capabilities adequately monitor for vulnerabilities, it's been difficult, if not impossible, to identify which cyber threats pose the greatest threat to mission effectiveness. The resilience challenge is difficult because commands need to simultaneously grapple with three factors:

1. **Their systems and subsystems continuously face multiple concurrent threats.** With vulnerability monitors flagging multiple threats, how should analysts prioritize which threats to focus on? Which could most impact their mission or missions? Analysts need to understand if and how those threats across information technology (IT) and operational technology (OT) systems might impact their ability to complete missions through denial of service, performance degradation or data loss.
2. **Cyber threat actors relentlessly create new exploits.** Threats come in at such a pace that it's unrealistic to evaluate all potential threats and vulnerabilities, to know which might succeed, and which could compromise mission capability. A single vulnerability in a critical component could render a unit useless, while multiple vulnerabilities in another subsystem might mean cyberattacks can disrupt a series of operations, while the ability to execute mission-critical operations remains in full force.
3. **Deployed platforms are not static.** Major platforms like the Arleigh Burke class DDG have useful lives across three decades or more, during which their IT and OT systems experience continuous spiral updates. A common byproduct of this, however, is that the platform drifts from its documented design baseline through poorly documented break/fix field workarounds, unplanned commercial-off-the-shelf (COTS) obsolescence refreshes and cumbersome configuration management processes.

There is, however, an approach suitable for optimizing cyber risks across the most sophisticated SoSs. Our engineering team has been working through a pair of Small Business Innovation Research (SBIR) programs to better protect parts of some of the Navy's most important warfighting platforms and weapons system programs. These solutions involve four elements that can be readily extended to other platforms:

1. **Model the baseline.** The first step involves creating a digital twin of the complete SoS including every subsystem, interface, data flow and mission thread. Model based system engineering (MBSE) captures the architectural and functional characteristics of each and every system interface via a high-fidelity digital twin model. This enables all potential cyberattack surfaces to be captured via a disciplined and standardized engineering approach. These digital models represent the architecture and operational behaviors through Systems Modeling Language (SysML) diagrams spanning from the mission threads down to the IT and OT Configuration Item (CI) levels. Each digital twin is created to represent the real-world as-is state of the platform. Baseline management and change management changes can then be automated to deal with design volatility, rapid refresh/insertion rates and ensue commonality between platform variants.
2. **Connect intelligence repositories.** The next step in the approach is to cross-reference the digital twin against the latest threat intelligence databases. Automated processes are set up to ingest, aggregate and correlate threat data from open as well as classified sources and map



*Tracy Gregorio*

Related CHIPS Articles

Naval Postgraduate School partners With Qualcomm to advance technological solutions

U.S., South Korean agencies partner to #StopRansomware threat from DPRK

Army using Europe and Pacific operational landscapes as 'laboratories' to enhance network resiliency

NATO Cyber Defence Center taps the Defense Information Systems Agency as U.S. team lead for intense cyberattack challenge

MCTSSA Hosts "Industry Day" at Camp Pendleton

Related DON CIO News

Listen to: "Live from AFCEA West - Navy CIO's 'Game-Changing' Tech for Enabling Information Superiority"

DON IT Conference, West Coast 2023 Final Details

Leader Challenge: Drive Competitive Advantage with Innovation

Department of the Navy CIO Announces Campaign Plan to Further Information Security

ALNAV: January is Operations Security Awareness Month

January 20, 2024 • ONLINE

# A new cyber-resilient approach for warfighting platforms

doncio.navy.mil/chips/ArticleDetails.aspx?...

Estimated Views **47**

Estimated views calculated based on audience size and socia...

Engagements **0**

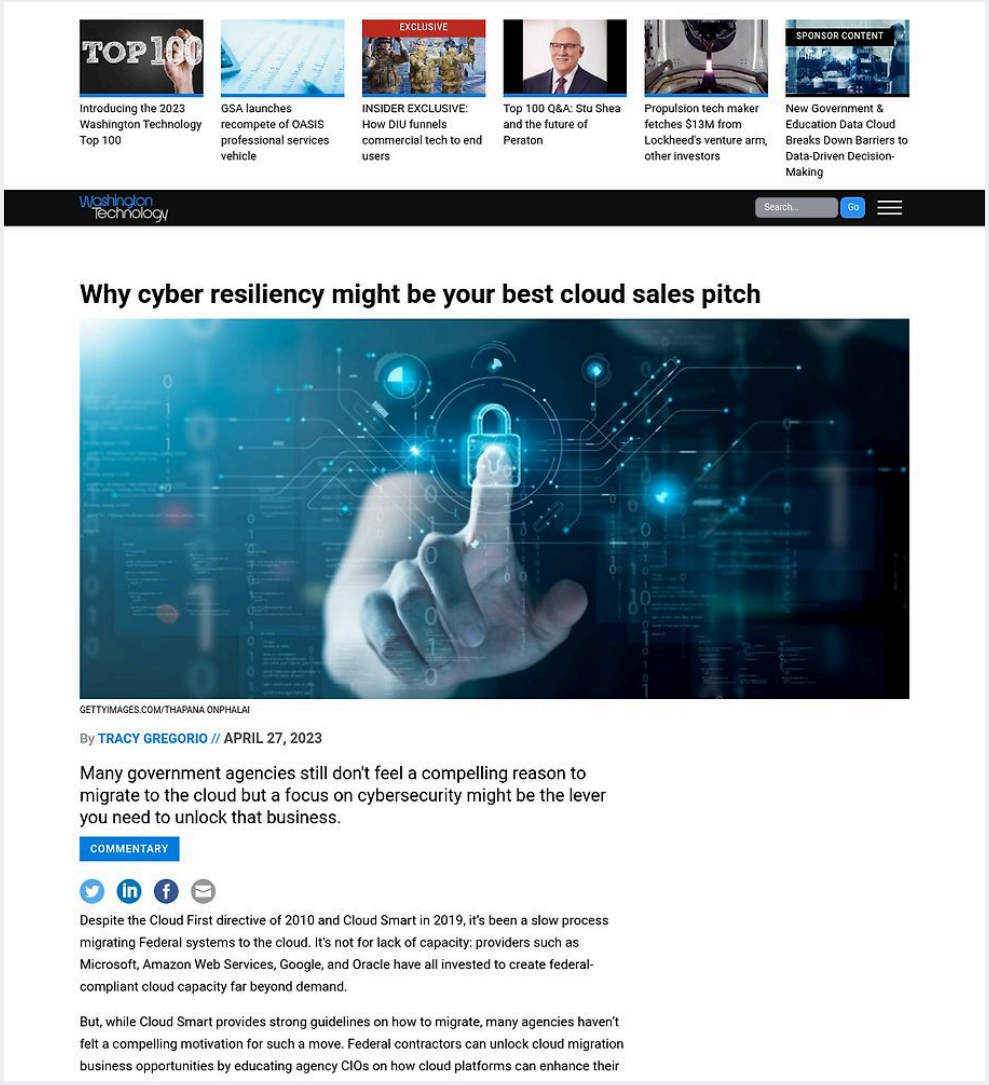
Total number of social engagements

## Washington Technology

Latest news and information on the business of delivering technology and services to government...

**59**
Domain Authority
Provided by MOZ

**42.8K**
Unique Visits
Provided by SimilarWeb




April 27, 2023 • ONLINE

# Why cyber resiliency might be your best cloud sales pitch

washingtontechnology.com/opinion/2023...

Estimated Views **397**

Estimated views calculated based on audience size and socia...

Engagements **3**

Total number of social engagements

## Stars and Stripes

U.S. military news organization providing independent news and information to the military...

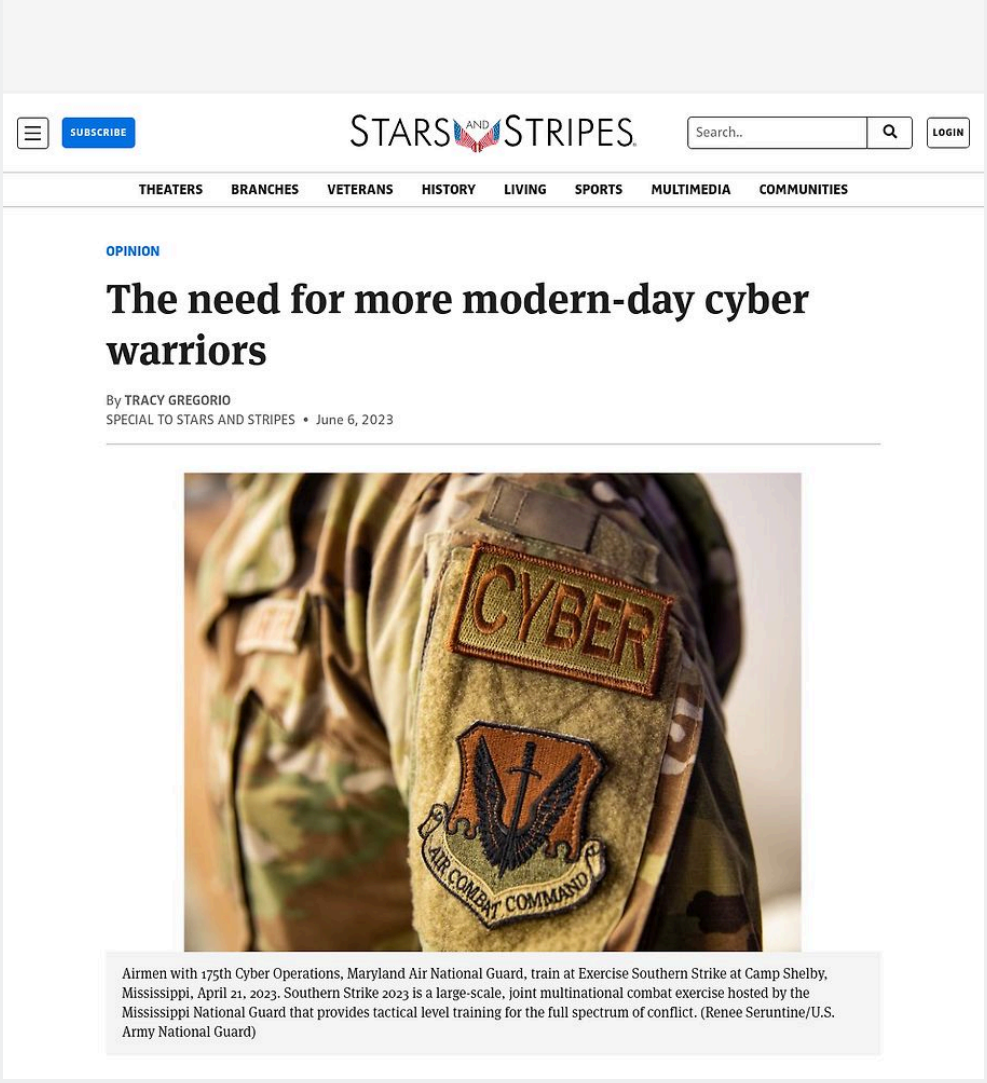
**80**
Domain Authority
Provided by MOZ

**838K**
Unique Visits
Provided by SimilarWeb

June 06, 2023 • ONLINE

# The need for more modern-day cyber warriors

stripes.com/opinion/2023-06-06/modern-...



SUBSCRIBE STARS AND STRIPES Search.. LOGIN

THEATERS BRANCHES VETERANS HISTORY LIVING SPORTS MULTIMEDIA COMMUNITIES

OPINION

**The need for more modern-day cyber warriors**

By TRACY GREGORIO
SPECIAL TO STARS AND STRIPES • June 6, 2023




Airmen with 175th Cyber Operations, Maryland Air National Guard, train at Exercise Southern Strike at Camp Shelby, Mississippi, April 21, 2023. Southern Strike 2023 is a large-scale, joint multinational combat exercise hosted by the Mississippi National Guard that provides tactical level training for the full spectrum of conflict. (Renee Seruntine/U.S. Army National Guard)

Estimated Views **3.48K**

Estimated views calculated based on audience size and socia...

Engagements **0**

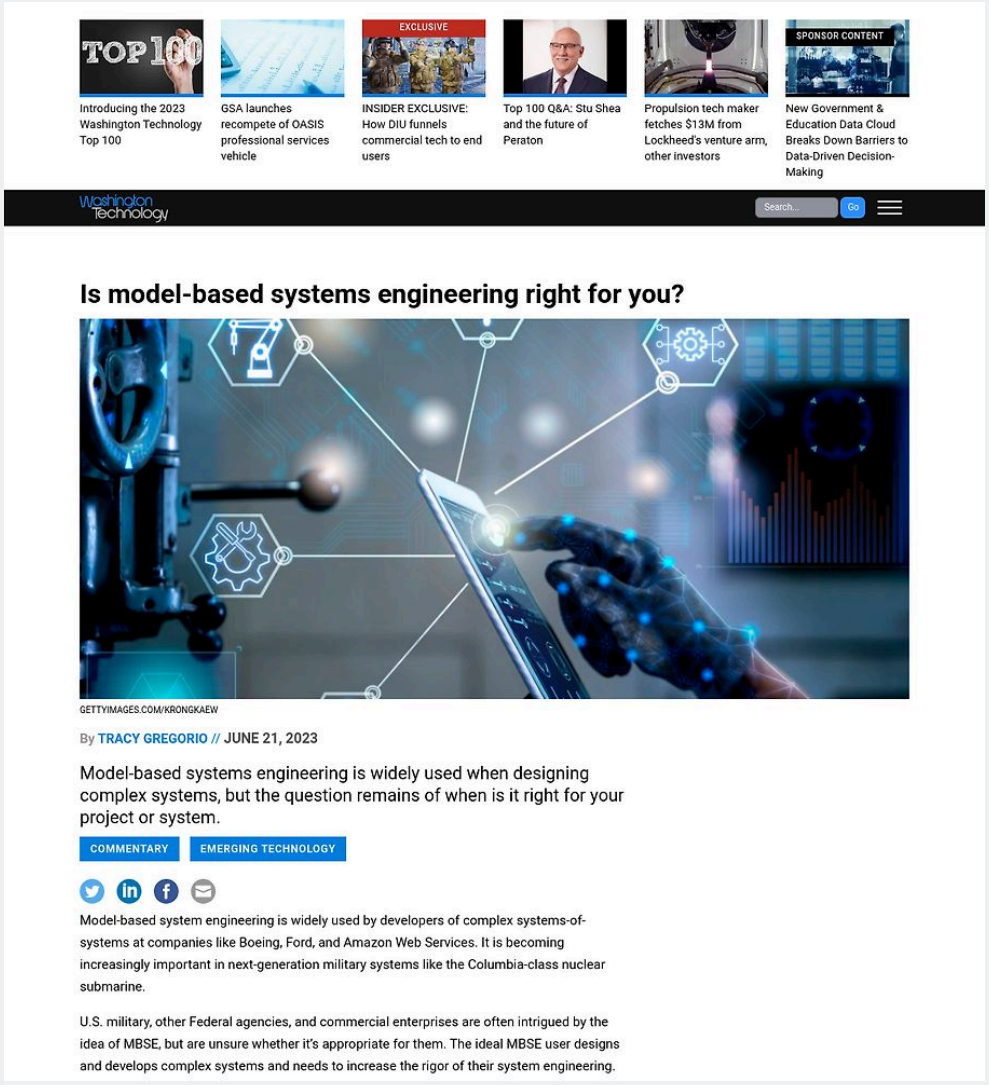
Total number of social engagements

## Washington Technology

Latest news and information on the business of delivering technology and services to government...

**59**
Domain Authority
Provided by MOZ

**42.8K**
Unique Visits
Provided by SimilarWeb




June 21, 2023 • ONLINE

# Is model-based systems engineering right for you?

washingtontechnology.com/opinion/2023...

Estimated Views **404**

Estimated views calculated based on audience size and socia...

Engagements **9**

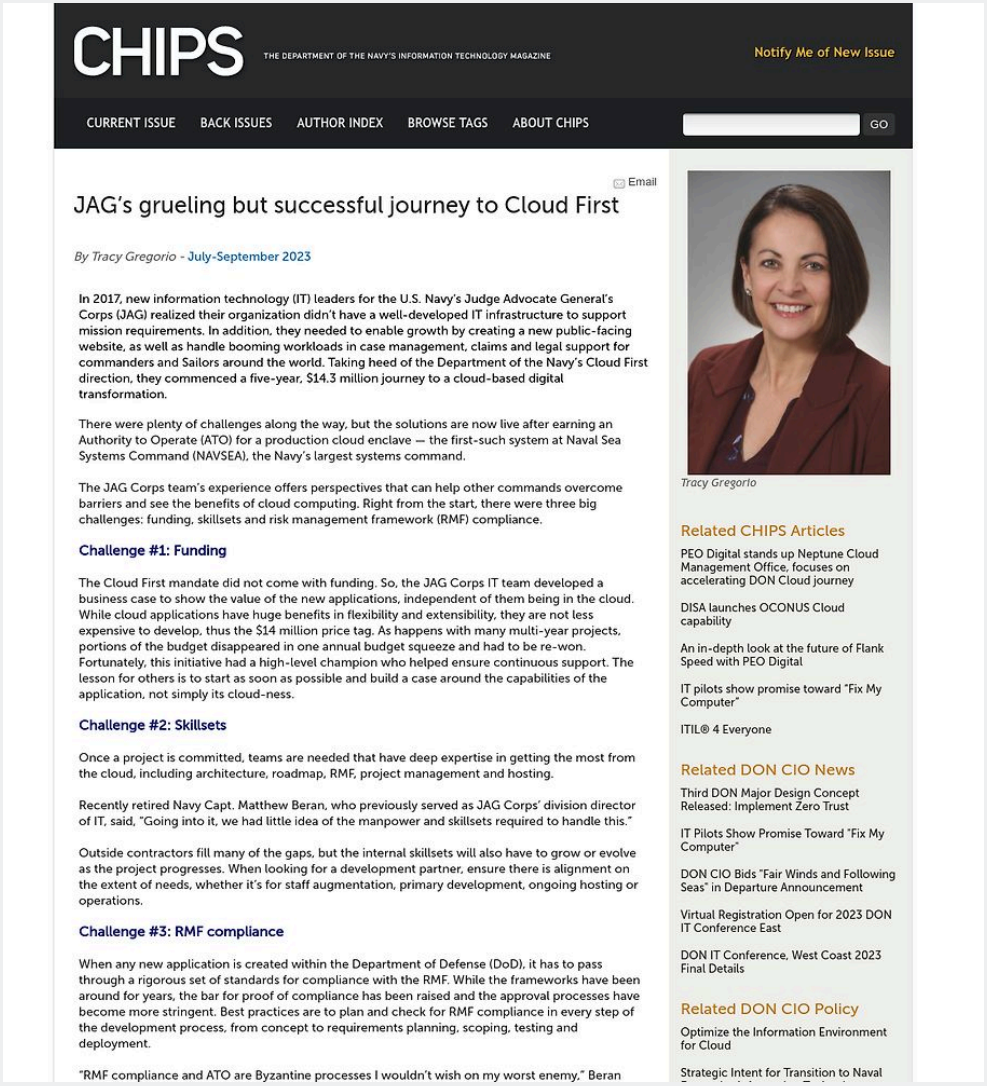
Total number of social engagements

## CHIPS

CHIPS is an official U.S. Navy website sponsored by the Department of the Navy (DON) Chief Informati...

**88**
Domain Authority
Provided by MOZ

**33.9K**
Unique Visits
Provided by SimilarWeb



CHIPS
THE DEPARTMENT OF THE NAVY'S INFORMATION TECHNOLOGY MAGAZINE
Notify Me of New Issue

CURRENT ISSUE | BACK ISSUES | AUTHOR INDEX | BROWSE TAGS | ABOUT CHIPS | GO

Email

JAG's grueling but successful journey to Cloud First

*By Tracy Gregorio - July-September 2023*

In 2017, new information technology (IT) leaders for the U.S. Navy's Judge Advocate General's Corps (JAG) realized their organization didn't have a well-developed IT infrastructure to support mission requirements. In addition, they needed to enable growth by creating a new public-facing website, as well as handle booming workloads in case management, claims and legal support for commanders and Sailors around the world. Taking heed of the Department of the Navy's Cloud First direction, they commenced a five-year, $14.3 million journey to a cloud-based digital transformation.

There were plenty of challenges along the way, but the solutions are now live after earning an Authority to Operate (ATO) for a production cloud enclave — the first-such system at Naval Sea Systems Command (NAVSEA), the Navy's largest systems command.

The JAG Corps team's experience offers perspectives that can help other commands overcome barriers and see the benefits of cloud computing. Right from the start, there were three big challenges: funding, skillsets and risk management framework (RMF) compliance.

**Challenge #1: Funding**

The Cloud First mandate did not come with funding. So, the JAG Corps IT team developed a business case to show the value of the new applications, independent of them being in the cloud. While cloud applications have huge benefits in flexibility and extensibility, they are not less expensive to develop, thus the $14 million price tag. As happens with many multi-year projects, portions of the budget disappeared in one annual budget squeeze and had to be re-won. Fortunately, this initiative had a high-level champion who helped ensure continuous support. The lesson for others is to start as soon as possible and build a case around the capabilities of the application, not simply its cloud-ness.

**Challenge #2: Skillsets**

Once a project is committed, teams are needed that have deep expertise in getting the most from the cloud, including architecture, roadmap, RMF, project management and hosting.

Recently retired Navy Capt. Matthew Beran, who previously served as JAG Corps' division director of IT, said, "Going into it, we had little idea of the manpower and skillsets required to handle this."

Outside contractors fill many of the gaps, but the internal skillsets will also have to grow or evolve as the project progresses. When looking for a development partner, ensure there is alignment on the extent of needs, whether it's for staff augmentation, primary development, ongoing hosting or operations.

**Challenge #3: RMF compliance**

When any new application is created within the Department of Defense (DoD), it has to pass through a rigorous set of standards for compliance with the RMF. While the frameworks have been around for years, the bar for proof of compliance has been raised and the approval processes have become more stringent. Best practices are to plan and check for RMF compliance in every step of the development process, from concept to requirements planning, scoping, testing and deployment.

"RMF compliance and ATO are Byzantine processes I wouldn't wish on my worst enemy," Beran



*Tracy Gregorio*

Related CHIPS Articles

PEO Digital stands up Neptune Cloud Management Office, focuses on accelerating DON Cloud journey

DISA launches OCONUS Cloud capability

An in-depth look at the future of Flank Speed with PEO Digital

IT pilots show promise toward "Fix My Computer"

ITIL® 4 Everyone

Related DON CIO News

Third DON Major Design Concept Released: Implement Zero Trust

IT Pilots Show Promise Toward "Fix My Computer"

DON CIO Bids "Fair Winds and Following Seas" in Departure Announcement

Virtual Registration Open for 2023 DON IT Conference East

DON IT Conference, West Coast 2023 Final Details

Related DON CIO Policy

Optimize the Information Environment for Cloud

Strategic Intent for Transition to Naval

August 01, 2023 • ONLINE

# JAG's grueling but successful journey to Cloud First

doncio.navy.mil/CHIPS/ArticleDetails.aspx...

Estimated Views **95**

Estimated views calculated based on audience size and socia...

Engagements **0**

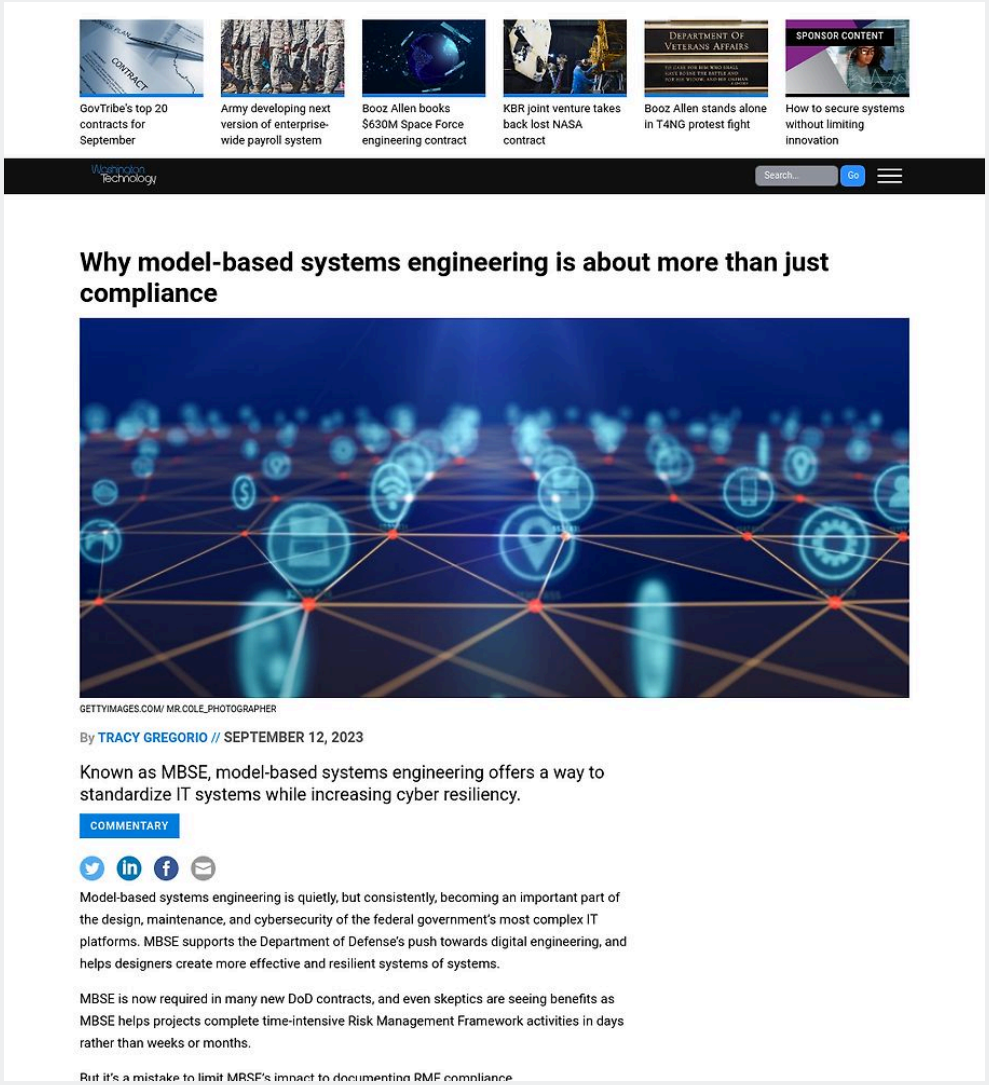
Total number of social engagements

## Washington Technology

Latest news and information on the business of delivering technology and services to government...

**59**
Domain Authority
Provided by MOZ

**29.4K**
Unique Visits
Provided by SimilarWeb




September 12, 2023 • ONLINE

# Why model-based systems engineering is about more than...

washingtontechnology.com/opinion/2023...

Estimated Views **242**

Estimated views calculated based on audience size and socia...

Engagements **1**

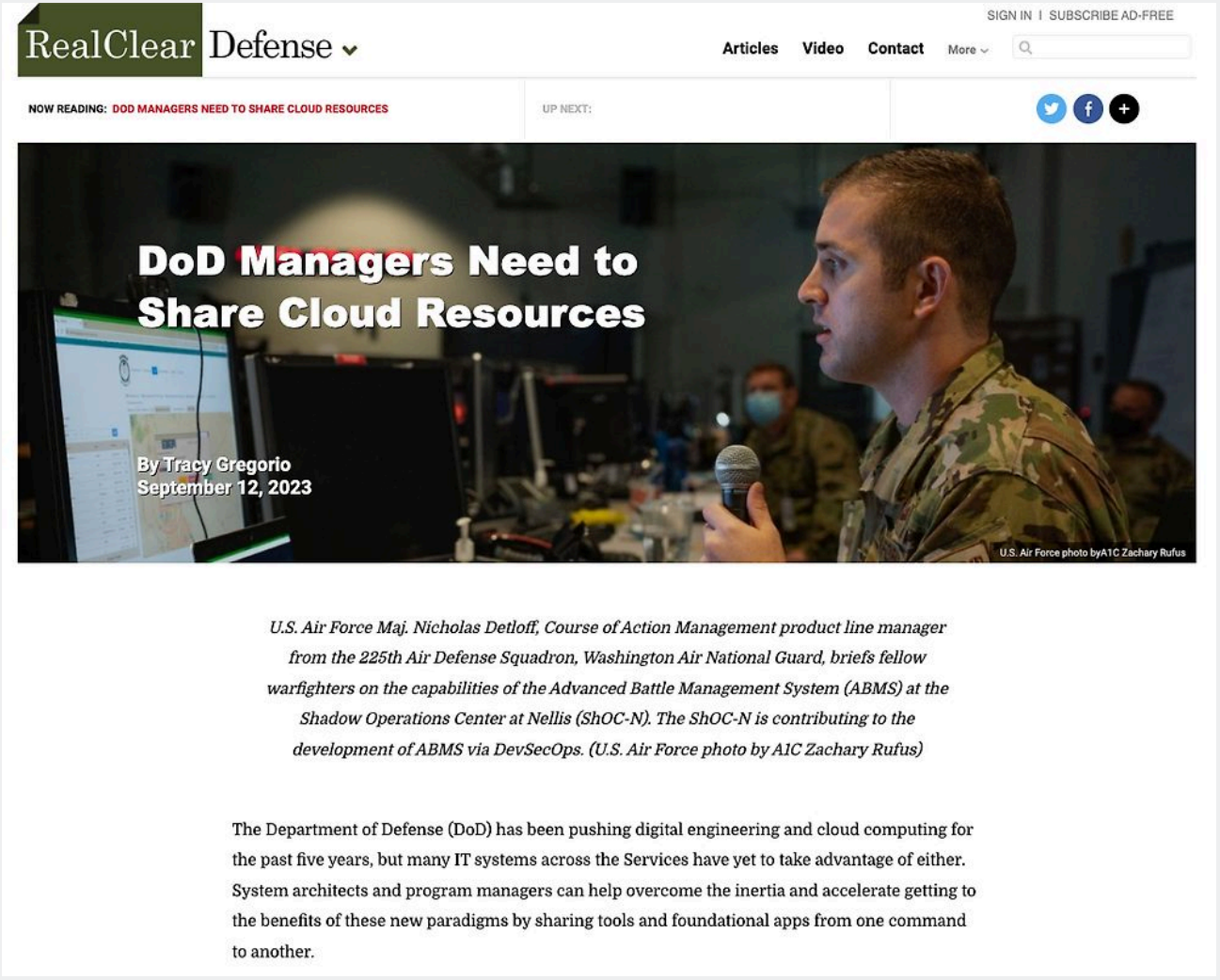
Total number of social engagements

## RealClearDefense

RealClearDefense (RCD) was created at the request of the Pentagon and Hill staff on the House Armed...

**63**
Domain Authority
Provided by MOZ

**214K**
Unique Visits
Provided by SimilarWeb




*U.S. Air Force Maj. Nicholas Detloff, Course of Action Management product line manager from the 225th Air Defense Squadron, Washington Air National Guard, briefs fellow warfighters on the capabilities of the Advanced Battle Management System (ABMS) at the Shadow Operations Center at Nellis (ShOC-N). The ShOC-N is contributing to the development of ABMS via DevSecOps. (U.S. Air Force photo by A1C Zachary Rufus)*

The Department of Defense (DoD) has been pushing digital engineering and cloud computing for the past five years, but many IT systems across the Services have yet to take advantage of either. System architects and program managers can help overcome the inertia and accelerate getting to the benefits of these new paradigms by sharing tools and foundational apps from one command to another.

September 14, 2023 • ONLINE

# DoD Managers Need to Share Cloud Resources

realcleardefense.com/articles/2023/09/12...

Estimated Views **2.57K**

Estimated views calculated based on audience size and socia...

Engagements **7**

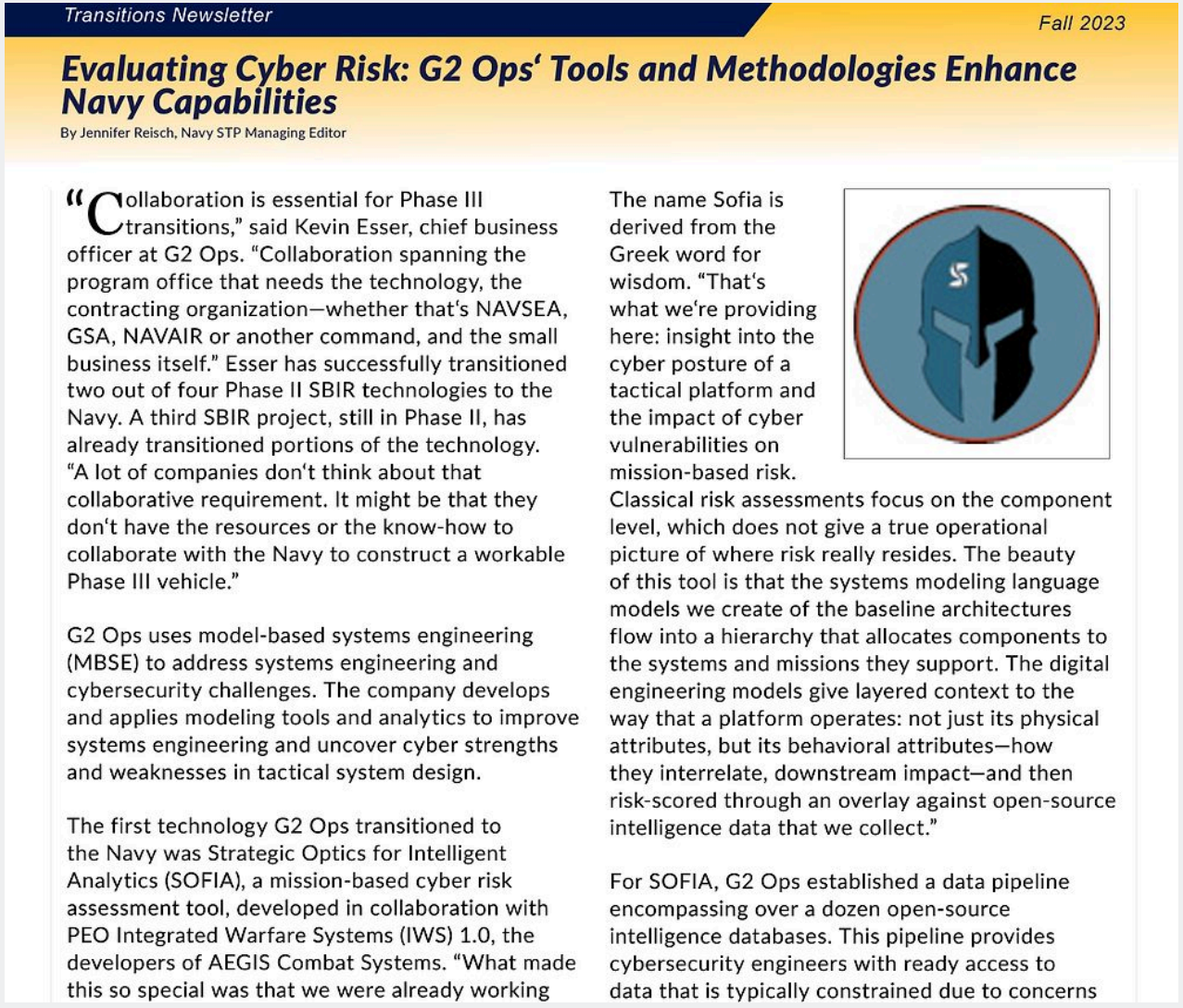
Total number of social engagements

## NavySTP Transitions Newsletter

Now in its 23rd year, the Navy STP (SBIR/STTR Transition Program) has been a long-standing vehicle for connecting...

**12**
Domain Authority
Provided by MOZ

**717**
Unique Visits
Provided by SimilarWeb



*Transitions Newsletter* *Fall 2023*

### *Evaluating Cyber Risk: G2 Ops' Tools and Methodologies Enhance Navy Capabilities*

By Jennifer Reisch, Navy STP Managing Editor

"Collaboration is essential for Phase III transitions," said Kevin Esser, chief business officer at G2 Ops. "Collaboration spanning the program office that needs the technology, the contracting organization—whether that's NAVSEA, GSA, NAVAIR or another command, and the small business itself." Esser has successfully transitioned two out of four Phase II SBIR technologies to the Navy. A third SBIR project, still in Phase II, has already transitioned portions of the technology. "A lot of companies don't think about that collaborative requirement. It might be that they don't have the resources or the know-how to collaborate with the Navy to construct a workable Phase III vehicle."

G2 Ops uses model-based systems engineering (MBSE) to address systems engineering and cybersecurity challenges. The company develops and applies modeling tools and analytics to improve systems engineering and uncover cyber strengths and weaknesses in tactical system design.

The first technology G2 Ops transitioned to the Navy was Strategic Optics for Intelligent Analytics (SOFIA), a mission-based cyber risk assessment tool, developed in collaboration with PEO Integrated Warfare Systems (IWS) 1.0, the developers of AEGIS Combat Systems. "What made this so special was that we were already working

The name Sofia is derived from the Greek word for wisdom. "That's what we're providing here: insight into the cyber posture of a tactical platform and the impact of cyber vulnerabilities on mission-based risk. Classical risk assessments focus on the component level, which does not give a true operational picture of where risk really resides. The beauty of this tool is that the systems modeling language models we create of the baseline architectures flow into a hierarchy that allocates components to the systems and missions they support. The digital engineering models give layered context to the way that a platform operates: not just its physical attributes, but its behavioral attributes—how they interrelate, downstream impact—and then risk-scored through an overlay against open-source intelligence data that we collect."

For SOFIA, G2 Ops established a data pipeline encompassing over a dozen open-source intelligence databases. This pipeline provides cybersecurity engineers with ready access to data that is typically constrained due to concerns

September 14, 2023 • ONLINE

# Evaluating Cyber Risk: G2 Ops' Tools & Methodologies...

navystp.com/wp-content/uploads/2023/0...

Estimated Views **224**

Estimated views calculated based on audience size and socia...

Engagements **0**

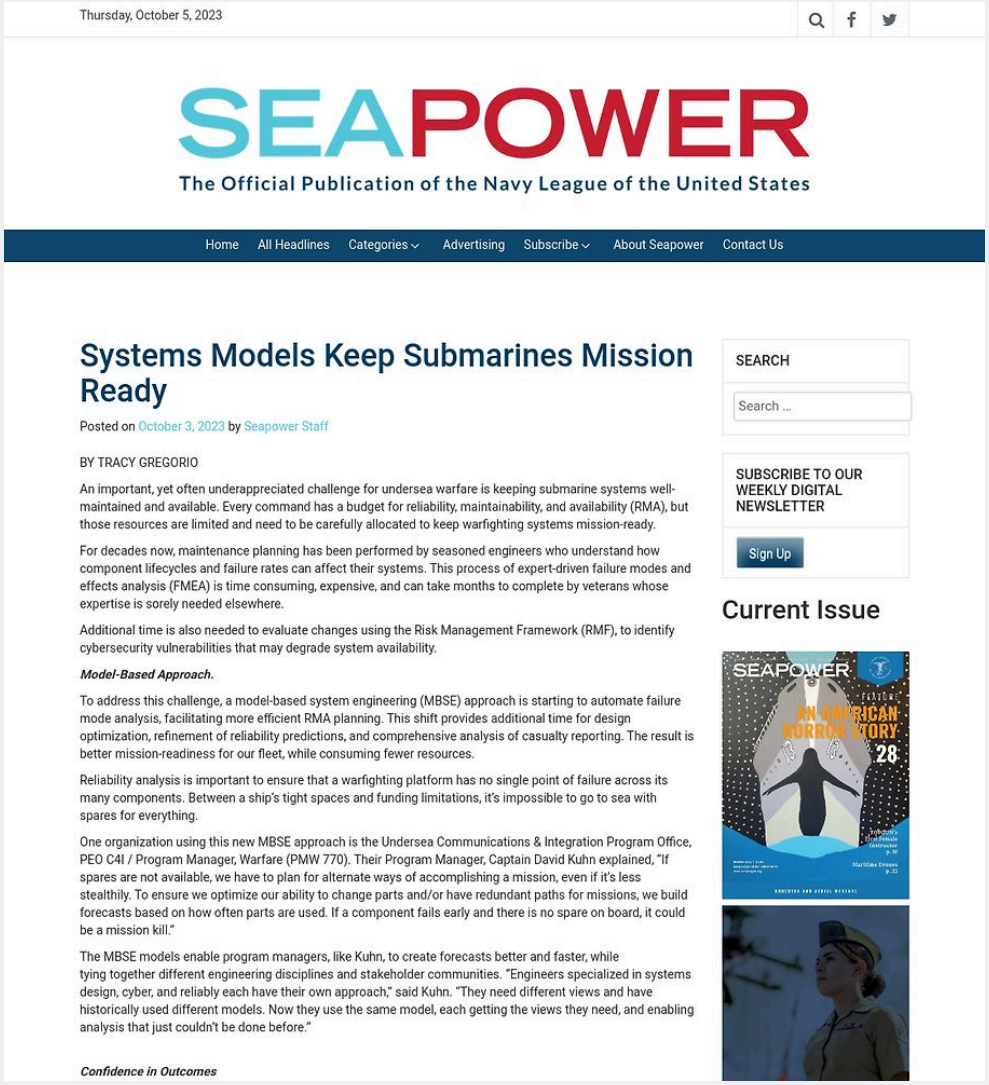
Total number of social engagements

## Seapower

Educating Congress and the American people about the activities, requirements and...

**58**
Domain Authority
Provided by MOZ

**23.5K**
Unique Visits
Provided by SimilarWeb



Thursday, October 5, 2023

SEAPOWER

The Official Publication of the Navy League of the United States

Home | All Headlines | Categories | Advertising | Subscribe | About Seapower | Contact Us

### Systems Models Keep Submarines Mission Ready

Posted on October 3, 2023 by Seapower Staff

BY TRACY GREGORIO

An important, yet often underappreciated challenge for undersea warfare is keeping submarine systems well-maintained and available. Every command has a budget for reliability, maintainability, and availability (RMA), but those resources are limited and need to be carefully allocated to keep warfighting systems mission-ready.

For decades now, maintenance planning has been performed by seasoned engineers who understand how component lifecycles and failure rates can affect their systems. This process of expert-driven failure modes and effects analysis (FMEA) is time consuming, expensive, and can take months to complete by veterans whose expertise is sorely needed elsewhere.

Additional time is also needed to evaluate changes using the Risk Management Framework (RMF), to identify cybersecurity vulnerabilities that may degrade system availability.

***Model-Based Approach.***

To address this challenge, a model-based system engineering (MBSE) approach is starting to automate failure mode analysis, facilitating more efficient RMA planning. This shift provides additional time for design optimization, refinement of reliability predictions, and comprehensive analysis of casualty reporting. The result is better mission-readiness for our fleet, while consuming fewer resources.

Reliability analysis is important to ensure that a warfighting platform has no single point of failure across its many components. Between a ship's tight spaces and funding limitations, it's impossible to go to sea with spares for everything.

One organization using this new MBSE approach is the Undersea Communications & Integration Program Office, PEO C4I / Program Manager, Warfare (PMW 770). Their Program Manager, Captain David Kuhn explained, "If spares are not available, we have to plan for alternate ways of accomplishing a mission, even if it's less stealthily. To ensure we optimize our ability to change parts and/or have redundant paths for missions, we build forecasts based on how often parts are used. If a component fails early and there is no spare on board, it could be a mission kill."

The MBSE models enable program managers, like Kuhn, to create forecasts better and faster, while tying together different engineering disciplines and stakeholder communities. "Engineers specialized in systems design, cyber, and reliably each have their own approach," said Kuhn. "They need different views and have historically used different models. Now they use the same model, each getting the views they need, and enabling analysis that just couldn't be done before."

***Confidence in Outcomes***

SEARCH

Search ...

SUBSCRIBE TO OUR WEEKLY DIGITAL NEWSLETTER

Sign Up

Current Issue

October 03, 2023 • ONLINE

# Systems Models Keep Submarines Mission Ready

seapowermagazine.org/systems-models-...

Estimated Views **244**

Estimated views calculated based on audience size and socia...

Engagements **0**

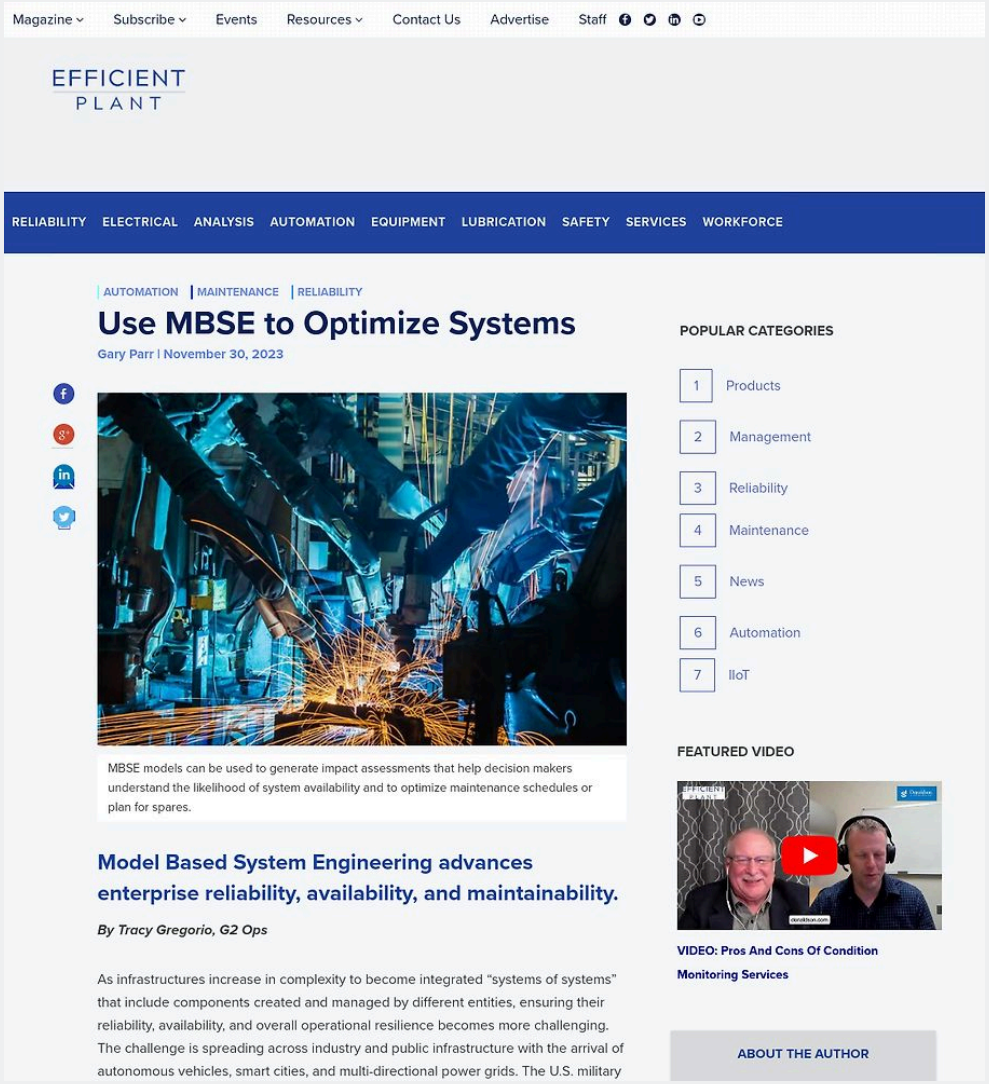
Total number of social engagements

## Efficient Plant

The Source For Reliability Solutions

**39**
Domain Authority
Provided by MOZ

**5.84K**
Unique Visits
Provided by SimilarWeb




November 30, 2023 • ONLINE

# Use MBSE to Optimize Systems

e cientplantmag.com/2023/11/use-mbse-...

Estimated Views **913**

Estimated views calculated based on audience size and socia...

Engagements **1**

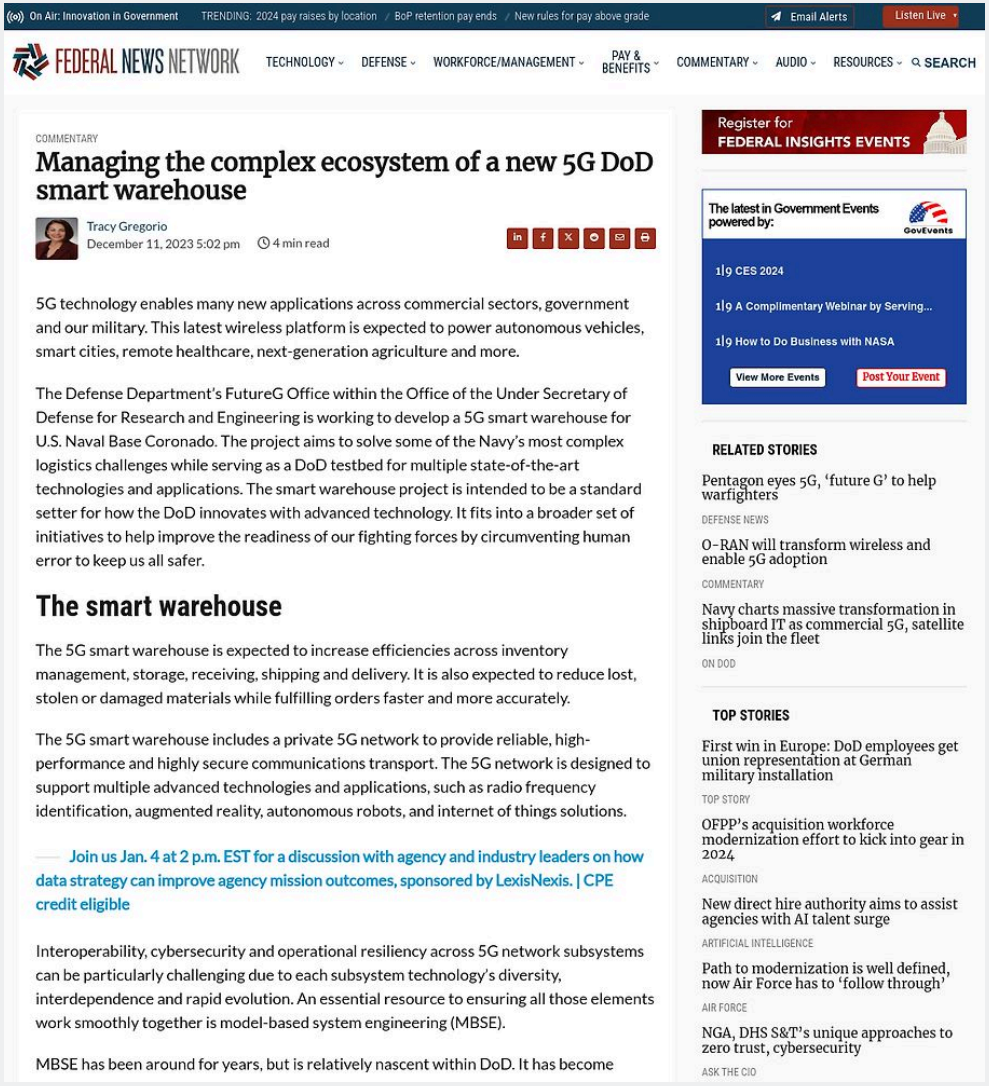
Total number of social engagements

# Federal News Network

Federal News Network covers the latest issues and breaking stories within the U.S. government that...

**68**
Domain Authority
Provided by MOZ

**439K**
Unique Visits
Provided by SimilarWeb


On Air: Innovation in Government TRENDING: 2024 pay raises by location / BoP retention pay ends / New rules for pay above grade Email Alerts Listen Live

FEDERAL NEWS NETWORK TECHNOLOGY DEFENSE WORKFORCE/MANAGEMENT PAY & BENEFITS COMMENTARY AUDIO RESOURCES SEARCH

COMMENTARY

## Managing the complex ecosystem of a new 5G DoD smart warehouse

Tracy Gregorio
December 11, 2023 5:02 pm 4 min read

5G technology enables many new applications across commercial sectors, government and our military. This latest wireless platform is expected to power autonomous vehicles, smart cities, remote healthcare, next-generation agriculture and more.

The Defense Department's FutureG Office within the Office of the Under Secretary of Defense for Research and Engineering is working to develop a 5G smart warehouse for U.S. Naval Base Coronado. The project aims to solve some of the Navy's most complex logistics challenges while serving as a DoD testbed for multiple state-of-the-art technologies and applications. The smart warehouse project is intended to be a standard setter for how the DoD innovates with advanced technology. It fits into a broader set of initiatives to help improve the readiness of our fighting forces by circumventing human error to keep us all safer.

### The smart warehouse

The 5G smart warehouse is expected to increase efficiencies across inventory management, storage, receiving, shipping and delivery. It is also expected to reduce lost, stolen or damaged materials while fulfilling orders faster and more accurately.

The 5G smart warehouse includes a private 5G network to provide reliable, high-performance and highly secure communications transport. The 5G network is designed to support multiple advanced technologies and applications, such as radio frequency identification, augmented reality, autonomous robots, and internet of things solutions.

Join us Jan. 4 at 2 p.m. EST for a discussion with agency and industry leaders on how data strategy can improve agency mission outcomes, sponsored by LexisNexis. | CPE credit eligible

Interoperability, cybersecurity and operational resiliency across 5G network subsystems can be particularly challenging due to each subsystem technology's diversity, interdependence and rapid evolution. An essential resource to ensuring all those elements work smoothly together is model-based system engineering (MBSE).

MBSE has been around for years, but is relatively nascent within DoD. It has become

Register for FEDERAL INSIGHTS EVENTS

The latest in Government Events powered by: GovEvents

1|9 CES 2024
1|9 A Complimentary Webinar by Serving...
1|9 How to Do Business with NASA
View More Events Post Your Event

RELATED STORIES

Pentagon eyes 5G, 'future G' to help warfighters
DEFENSE NEWS

O-RAN will transform wireless and enable 5G adoption
COMMENTARY

Navy charts massive transformation in shipboard IT as commercial 5G, satellite links join the fleet
ON DOD

TOP STORIES

First win in Europe: DoD employees get union representation at German military installation
TOP STORY

OFPP's acquisition workforce modernization effort to kick into gear in 2024
ACQUISITION

New direct hire authority aims to assist agencies with AI talent surge
ARTIFICIAL INTELLIGENCE

Path to modernization is well defined, now Air Force has to 'follow through'
AIR FORCE

NGA, DHS S&T's unique approaches to zero trust, cybersecurity
ASK THE CIO

December 11, 2023 • ONLINE

# Managing the complex ecosystem of a new 5G DoD smar...

federalnewsnetwork.com/commentary/2...

Estimated Views **3.13K**

Estimated views calculated based on audience size and socia...

Engagements **15**

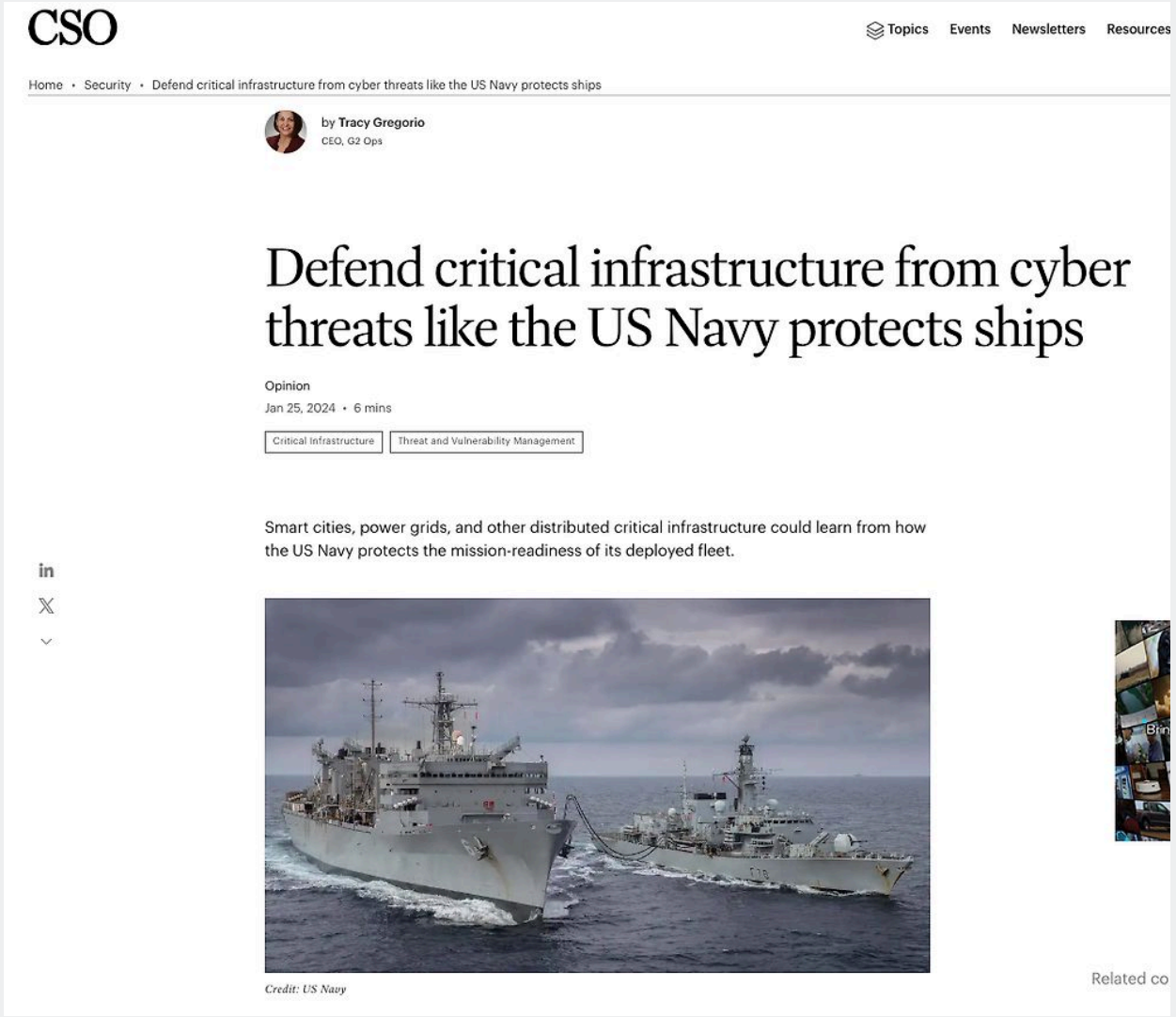
Total number of social engagements

## CSO Online

CSO delivers the critical information about trends, practices, and products enterprise security leaders...

**85**
Domain Authority
Provided by MOZ

**509K**
Unique Visits
Provided by SimilarWeb



CSO

Topics Events Newsletters Resources

Home • Security • Defend critical infrastructure from cyber threats like the US Navy protects ships

by Tracy Gregorio
CEO, G2 Ops

# Defend critical infrastructure from cyber threats like the US Navy protects ships

Opinion
Jan 25, 2024 • 6 mins

Critical Infrastructure | Threat and Vulnerability Management

Smart cities, power grids, and other distributed critical infrastructure could learn from how the US Navy protects the mission-readiness of its deployed fleet.

*Credit: US Navy*

Related co

January 23, 2024 • ONLINE

# Defend critical infrastructure from cyber threats like th...

csoonline.com/article/1297773/defend-cri...

Estimated Views **1.86K**

Estimated views calculated based on audience size and socia...

Engagements **16**

Total number of social engagements

## Contract Management

The starting point for all things NCMA, the community for contract management, procuremen...

**52**
Domain Authority
Provided by MOZ

**13.5K**
Unique Visits
Provided by SimilarWeb


January 11, 2024 • ONLINE

# Leveraging the Small Business Innovation Research Program

ncmahq.org/Web/Web/Resources/Contra...

Estimated Views **184**

Estimated views calculated based on audience size and socia...

Engagements **1**

Total number of social engagements

## RealClearDefense

RealClearDefense (RCD) was created at the request of the Pentagon and Hill staff on the House Armed...

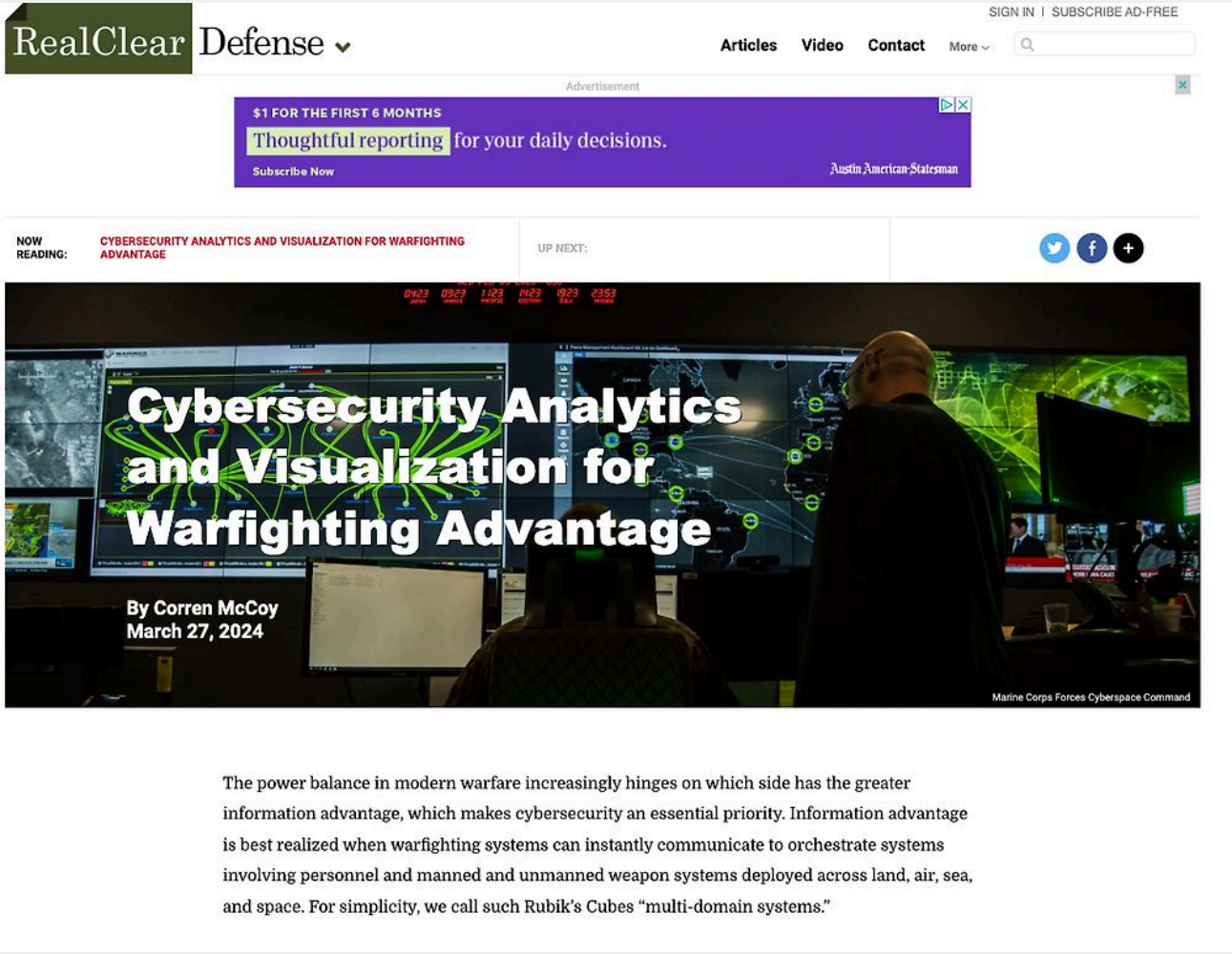
**63**
Domain Authority
Provided by MOZ

**133K**
Unique Visits
Provided by SimilarWeb

March 27, 2024 • ONLINE

# Cybersecurity Analytics and Visualization for...

realcleardefense.com/articles/2024/03/2...




The power balance in modern warfare increasingly hinges on which side has the greater information advantage, which makes cybersecurity an essential priority. Information advantage is best realized when warfighting systems can instantly communicate to orchestrate systems involving personnel and manned and unmanned weapon systems deployed across land, air, sea, and space. For simplicity, we call such Rubik's Cubes "multi-domain systems."

Estimated Views **1.84K**

Estimated views calculated based on audience size and socia...

Engagements **31**

Total number of social engagements