

BREAKING

DEFENSE

/ GAME CHANGER

Cyber and full-spectrum operations push the Great Power conflict left of boom

Sponsored by





Unlike a weapon that can be tested, validated, and put on a shelf knowing that it will work when needed, deployed information warfare and cyber capabilities have to be continually tuned and optimized in order to be relevant to the warfighter.

As the United States and its allies move from almost a quarter century of focus on the Global War on Terrorism, and shift to the new realities as specified in the current National Defense Authorization Act (NDAA) — which authorizes funding levels and provides authorities for the U.S. military and other critical defense priorities — so too must technology and capability adapt and align to the new operational environment. Cyber and information warfare will take greater precedence than ever before as the NDAA outlines the threat environment.

How then can cyberspace operation (CO) and information warfare (IW) capabilities best align to support and enable multi-domain operations across a wide spectrum of threats, while at the same time ensuring safety and security of critical infrastructure and assets? On one hand, CO and IW must operate in a Phase 0, or “left of boom” non-kinetic environment to help shape, deter, defend, and inform, while at the same time posturing to ensure combatant commander and National Command Authority (NCA) freedom of maneuver in cyberspace while denying adversaries the same, should hostilities begin.

Full spectrum CO and IW contain numerous supporting efforts, to include cyber or computer network operations (CNO), signals intelligence (SIGINT), information operations (IO), electronic warfare (EW), as well as other various supporting disciplines such as machine learning and artificial intelligence, big data and data science, and the use of publicly available information (PAI). All combine to ensure information advantage and decision dominance for the commander within the Joint Information Environment (JIE) and across the traditional operational maneuver domains of air, land, sea, space, and cyber. The really interesting challenge, then, is to fuse all of this immense stand-alone capability in time to be relevant and deliver effects as needed.

To ensure commander freedom of maneuver in the JIE and drive information advantage and decision dominance, Army Cyber Command has created new capability and capacity in the form of unique new units and commands; this is in addition to the already established Cyber Mission Force. A recent example is the 915th Cyberwarfare Battalion — the first organic, scalable expeditionary

Cyber Electromagnetic Activities (CEMA) capability — which is providing commanders a new tactical tool with the ability to deny, degrade, disrupt, destroy, deceive, influence, shape, and manipulate the capabilities and decisions of adversaries.

“Whether it be deterrence in the early competition phase or dominance throughout conflict, the invisible, complex, and congested electromagnetic spectrum will be where future battles are won or lost,” states the Cybersecurity and Information Systems Information Analysis Center (CSIAC), a component of the Defense Department’s Information Analysis Center enterprise.

Our adversaries are no longer “just” terrorist cells in the desert operating off of a pay phone or an Internet cafe. Rather, U.S. forces need to be prepared for much higher sophistication and maturity of cyber and EW capabilities.



Jack Koons, senior principal solutions architect for Cyberwarfare and Information Warfare within HII.

“I wasn’t worried about ISIL breaking into this conversation and listening to us talking, but I do have to worry about peer and near-peer adversaries having the capability to do just that,” said Jack Koons, senior principal solutions architect for Cyberwarfare and Information Warfare within [HII \(better known until recently as Huntington Ingalls Industries\)](#), the largest shipbuilder in the U.S. and the builder of the under-construction Ford-class aircraft carriers that are the first to be fully digitally designed.).

“You now have to operate with an ‘assume breach’ mentality, that any platform that you’re using for communications or for network access is potentially compromised at the very least, exploited at the worst. I may have to work in degraded operations or constrained environments, or lose primary access. So you need to have B, C, and D fallback plans to cover gaps, extend operational reach and access, and ensure freedom of maneuver for the combatant commander in the information environment.” In a word, cyber must provide options.



Ron Fodor, operations manager for HII's Cyber, EW & Space business.

The challenge faced by U.S. and allied forces has been on full display in Ukraine. Prior to Russian forces mounting their kinetic attack, they unleashed a slew of cyberattacks to weaken Ukraine's posture and take its focus off of the mounting physical forces that were about to cross the border.

"In the case of Ukraine, General Paul Nakasone (U.S. Cyber Command commander and NSA director) has said that we have deployed expeditionary cyber warfare elements into theater to support

them," observed Ron Fodor, operations manager for HII's Cyber, EW & Space business. "What's interesting is that we're seeing the convergence of the cognitive, the physical, and the virtual space."

Challenges for the warfighter and for industry

Of the five previously mentioned operational domains, cyberspace is unique in that it exists in an artificial world. Air, land, sea, and space are all naturally occurring environments. As such, certain challenges arise when one considers the operational considerations associated with offensive, defensive, and maneuver operations in cyberspace.

"We literally have to build the transport mechanisms and infrastructure to get from point A to point B. And then, in a peer-to-peer environment, or 2+3 strategy, this is fully contested every step of the way. You're under attack while you're building this transport mechanism and spectrum. You may lose pieces or linkage, and then you have to adjust. Cyberspace is a living, breathing thing," said Koons.

That means speed to market for cybersecurity capabilities and technologies is critical. It's not like a weapon that can be tested, validated, and put on a shelf knowing that it will work when needed. When a cyber capability is deployed, it has to change as the network changes.

"You never get to come off the gas pedal with this capability," said Koons, a retired Army cyberwarfare officer with 25 years working cyber issues with U.S. national intelligence, Special Operations, and cyber communities. "Once it's deployed, it has to be continually tuned and optimized in order to be relevant to the warfighter."

Another difference in the cyber domain that doesn't exist in the other warfighting domains is that the pace of operations is much faster because it's all computer and network based.

"We're talking nanoseconds to microseconds to seconds, whereas in the kinetic world it's days, weeks, months, and years," said Fodor, a former officer in the U.S. Air Force. "Look at the Ukraine crisis; it started in February and it's still happening today. A cyber operation goes off in an instant. Enemies find access to your system, exploit your systems, position an implant, and exfiltrate data within the matter of minutes."

Nearly \$1 billion in recent contracts supporting DoD cyber

With more than 100 facilities worldwide, Virginia-based HII has become a trusted DoD partner developing integrated solutions that address the challenges just described while enabling today's



HII's expertise ranges from building aircraft carriers and developing unmanned systems and advanced C5ISR solutions to conducting full-spectrum cyber operations. (Image courtesy of HII.)

connected, all-domain force. Capabilities include: C5ISR systems and operations; the application of AI and machine learning to battlefield decisions; defensive and offensive cyberspace operations; electronic warfare; space systems; unmanned autonomous systems; live, virtual, and constructive simulation; as well as the naval construction/overhaul/modernization and critical nuclear operations that HII is so well known for.

Those capabilities will play important roles in helping HII execute two recent contracts with the government. Under the \$826 million Decisive Mission Actions and Technology Services (DMATS) task order awarded by the General Services Administration in August, HII will provide threat and specialized analysis and analytics support, as well as operations integration and operational effects support. It will benefit all DoD service components, component research labs, components of the DoD Fourth Estate, national intelligence agencies, and combatant commands.

Also in August, HII was awarded a \$127 million task order to support the Defense Security Cooperation Agency to perform research, development, test and evaluation of emerging technologies. Under the task order, HII will enhance the functionality and capability of systems integration through the development of software and hardware capabilities, systems engineering, research and analysis. That support will develop and create new knowledge for the enhancement of the Defense Technical Information Center repository, as well as the R&D and science and technology communities

In recent years, HII has embarked on a program of acquisitions that have bolstered its portfolio of capabilities within its Mission Technologies division in targeted areas of importance to the DoD. This includes:

- The acquisition in 2021 of Alion Science and Technology, which provides advanced engineering and R&D services in the areas of ISR, military training and simulation, and cyber and data analytics;
- Commonwealth Technology Innovation, an HII company that has advanced engineering tools and prototyping labs where integrated product development teams can evaluate concepts and quickly deliver solutions to the field, including intelligence solutions, integrated sensing, and SIGINT technology; and
- Enlighten, another HII company, is a subject matter expert on the Big Data Platform (BDP) and big data analytics.



Under the \$826 million Decisive Mission Actions and Technology Services task order, HII will provide threat and specialized analysis and analytics support, as well as operations integration and operational effects support. (Image courtesy of HII.)

"None of the cybersecurity and EW challenges that the DoD is facing are new to HII," said Koons. "We understand the rigorous process that goes into building exquisite technologies. I would argue that we build the most complex, technically advanced, most powerful systems on the face of the Earth.

"And, perhaps, the most sophisticated and sensitive piece of technology on an aircraft carrier or an attack submarine is the nuclear, electronics, and cyber systems. Not only do those systems have to be built to rigorous government standards, they have to be done in a very small form factor. There are very few organizations that can do all that organically and do it on a daily basis."

HII Moves the Needle

With expertise that ranges from building aircraft carriers and developing unmanned systems and advanced C5ISR solutions to conducting full-spectrum cyber operations, HII is a company of companies.

"It comes down to three things," said Koons, "people, processes, and technologies. We have an entire workforce that is heavily weighted on military veterans so many of us come from the community. Then we have depth and breadth across all engineering disciplines, and across program and project-management disciplines to build and deploy systems fast."

It goes back to HII's philosophy of putting technology professionals in positions of responsibility and leadership within the company to drive investment so that it's ready for what comes next.

"We see the way that the domain, the science, and the technology are changing, and we position ourselves by investing in technologies that we think are going to be relevant to the future of cyber warfare and information operations," said Fodor. "We're moving away from the days of the Global War on Terrorism and effects-based cyber operations to more sophisticated, holistic, and fused operational environments to produce an effect on an adversary — whether that effect is kinetic or not."

The goal of most military organizations is not to be forced to deploy forces and use kinetic weapons. The goal is to avoid that, going back to a Sun Tzu military strategy on the importance of deterrence that is doubly true today: "The supreme art of war is to subdue the enemy without fighting."

Wars are sometimes won long before they're fought, and helping to make that true for the DoD through the use of cyber and the electromagnetic spectrum operations is a key part of what drives HII today.