

BREAKING  
**DEFENSE** / *GAME CHANGER*

# Internet Operations Management Is Well Suited To Military Networks

*U.S. Marines with the Special Purpose Marine Air Ground Task Force 19.2 Crisis Response Command Element prepare field condition crisis response center networks in Kuwait. (U.S. Marine Corps photo by Sgt. Robert Gavaldon).*

Sponsored by





# Internet Operations Management will enable Joint Force Headquarters-DoD Information Network to gain real-time visibility over all DoD networks.

By Barry Rosenberg, *Breaking Defense*

As data proliferates and attack surfaces expand, the Defense Department continues to have a fundamental need to discover, understand, track, and manage its assets and devices that are exposed on the internet.

The House Armed Services Committee noted the need to manage this process in an integrated end-to-end capability in its markup of the National Defense Authorization Act (NDAA) for Fiscal Year 2021.

“The Department of Defense (DoD) lacks a similar comprehensive understanding of the internet-connected assets and attack surface across the DoD enterprise; the committee notes in this regard that the DoD only recently discovered that it has twice as many managed connections to the internet as it thought it did—connections established and maintained by components that were not protected like the other sanctioned Internet Access Points managed by the Defense Information Systems Agency.

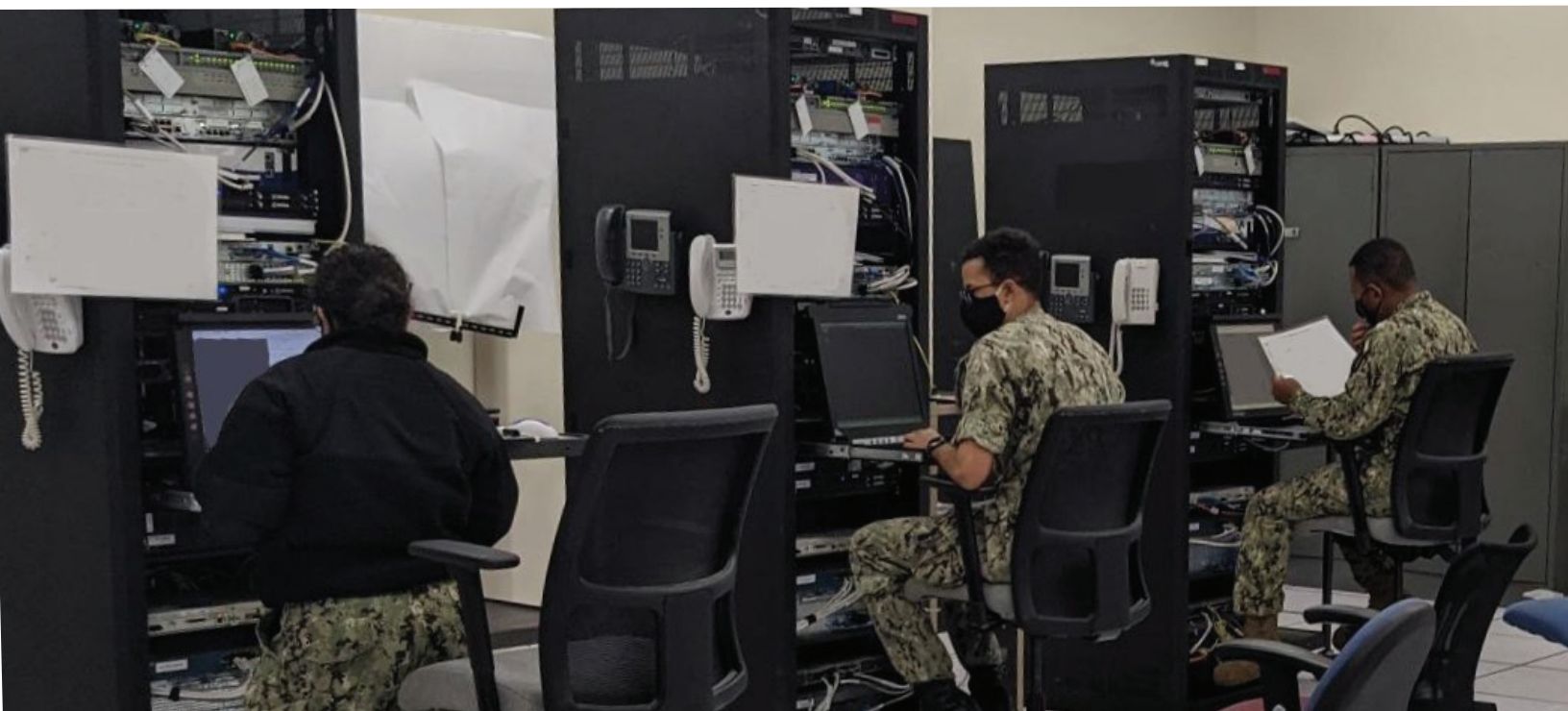
“Despite strides made by Joint Force Headquarters Department of Defense Information Network (JFHQ DODIN) in improving its enterprise-wide visibility of DoD networks, DoD networks are controlled by individual components, with JFHQ-DODIN deriving most of its situational awareness from component reporting. The committee believes that it is critical that JFHQ-DODIN achieve real-time visibility over all DoD networks.”

This complexity makes DoD networks particularly ripe for the application of technology known as Internet Operations Management (IOM). IOM capabilities enable organizations to:

- Understand what their on-premise and cloud-hosted attack surfaces look like in near-real time, how elements of their networks behave externally; and
- Detect previously unknown compromises, unsanctioned connections, misconfigurations, vulnerabilities, and threat activity.

“Internet Operations Management capabilities are a foundation for defensive cyber operations not just for the military but also for federal agencies and commercial customers,” said Joseph Lin, Vice President of Product Management at Palo Alto Networks. “All of these organizations have fundamental challenges around cyber situational awareness regarding their Internet-facing assets and devices.”

*Sailors training with the Automated Digital Network System course at Information Warfare Training Command, San Diego. (U.S. Navy photo by Electronics Technician 1st Class Christopher Yoshida)*





An IOM platform aggregates all of this data about Internet assets and devices into a single, secure data lake, and uses machine learning algorithms and analytics to attribute them to military services and government agencies, discover anomalies, and derive insights. Decisionmakers can then use this information to make, enforce, and verify IT and security policies and orders in an actionable, scalable, and automated way across the entire enterprise.

### IOM Is Well Suited to Military Networks

Military networks are, generally speaking, very large. They can be highly federated and diverse in nature, which makes managing all of their internet-facing assets that much more difficult.

Because of the large, distributed, highly federated, and sometimes expeditionary nature of government networks, managing their internet-facing assets is difficult and complex. For example:

**1. Self-reporting compliance:** In most cases, cyber security leaders lack an independent way to verify compliance across their network. They rely on reports from their sub-components and agencies, which can contain erroneous information.

#### 2. Lack of an accurate and shared source of truth:

Cyber security leaders and their agencies/commands often do not have a shared understanding of which IP ranges and internet assets belong to which sub-components and agencies. Existing inventory databases that should be the comprehensive source of truth for the enterprise's IP ranges are often outdated and incomplete. If vulnerabilities exist in IP space that no organization is directly responsible for, they may never appear in an asset inventory.

### 3. Multicloud and third-party hosting as extended attack surfaces:

Enterprise assets hosted by commercial Cloud Service Providers and Internet Service Providers are assumed to be secure but are in fact often insufficiently monitored or entirely unmanaged. While the risks posed by these assets vary, a meaningful subset of this attack surface periodically includes Controlled Unclassified Information (CUI) or other potentially high-value enterprise assets.

### 4. Unclear asset and device attribution and ownership:

For even those portions of the network that both the security and network operation centers are monitoring, determining who is specifically responsible for a given asset or device can be challenging. This affects how quickly vulnerabilities can be patched and mitigated.

### IOM Addresses Those Issues

It is these challenges that are driving the need for enterprise-wide security transformation among militaries around the world.

Cybersecurity and IT operations are most effective when there is centralized visibility and operational control over the entire network. The DoD owns some of the world's largest and most complex networks, with hundreds of millions of IP addresses and endpoints in multi-tiered enclaves. DoD organizations and service members require best in-breed IOM technologies to centralize and manage their security and network operations. The good news is that these technologies already exist commercially and are widely deployed across legacy networks, especially in the private sector and government agencies.



"A major part of managing legacy network systems is that they are properly secured behind firewalls and not exposed on the public internet because of vulnerabilities associated with their software that are simply unpatched, or are no longer supported by their original manufacturer," said Lin. "Because these vulnerabilities can be easily exploitable by adversaries, it's that much more important to ensure that they're properly secured."

"What IOM enables owners of legacy systems to do is, first and foremost, ensure that they're not exposed on the public internet, that they're not discoverable by adversaries, and that they're properly configured and secured."

## Conclusion

U.S. government cyber defense, detection, response, and recovery capabilities remain inadequate.

IOM products like Palo Alto Networks' Cortex suite of systems, including Xpanse and XSOAR, enable JFHQ-DODIN to meet the requirements detailed by the FY21 NDAA through the deployment of IOM capabilities that provide JFHQ-DODIN real-time visibility over all DoD networks.

Situational awareness is a basic requirement in all forms of conflict, and with Cortex IOM, the Defense Department can continuously discover, manage, and monitor all globally deployed DoD internet assets.