Intelligence Support to Joint All Domain Command and Control Network Vulnerabilities

By

Captain Natalie L. Howie (USAF)

Air University Advanced Research Group - JADC2

07 August 2020

eSchool of Graduate PME

Maxwell AFB, Alabama

ABSTRACT

This Air University Advanced Research paper focuses on intelligence support to units employing Joint All Domain Command and Control (JADC2) networks that are exposed to an adversary's non-lethally employed exploitation effects in contested environments. A 2020 RAND corporation study defines JADC2 as "connecting distributed sensors, shooters and data from and in all domains to all forces to enable distributed mission command at the scale, tempo, and level to accomplish commander's intent - agnostic to domains, platforms, and functional lanes".[1] Non-lethally employed effects are those identified as executed through cyber, space, influence operations, and/or electronic warfare enabled methods to deny, degrade, disrupt, destroy and/or manipulate the data integrity or function of forward deployed devices. The current JADC2 network employed in contested environments potentially leaves communications equipment vulnerable to adversary exploitation means, and/or subjects mission data traversing the network to exposure. This paper highlights requirements for: 1) centralized databasing of adversary non-lethal threats (both assessed and confirmed capabilities or methods), 2) compiled threat trend analysis reporting based on threats observed, 3) advanced research conducted on intelligence gaps present in intelligence requirement(s) submitted by supported units (threat database relevance maintained), and 4) use of the intelligence threat data acquired to implement technical solutions, mitigation techniques, and/or changes to how equipment and connections are established in contested environments.

Intelligence Support to JADC2 Network Vulnerabilities

For non-lethally employed threats in an identified Area of Responsibility (AOR), local supported units lack a dedicated staff level intelligence support function to perform the following: 1) identify threat(s) associated to identified JADC2 network enabling device(s), 2) analyze non-lethally employed threats to perform trend analysis, 3) establish a centralized database or repository on assessed or confirmed reporting of adversary's non-lethally employed effects observed in an AOR, 4) maintain threat data (ensure relevance intelligence refresh rate is occurring) between staff level and support units, and 5) establish a dedicated liaison function in translating classified data to a medium in which the larger consumer-based audience can utilize.

Currently, analysts produce intelligence reports yielding an 'assessed capability' (not confirmed or observed) of an adversary's capabilities or methods with varying confidence levels ("low", "medium", or "high"). The assessed confidence level is driven by the ability to observe non-lethally employed capabilities occurring on network enabling devices. As the information arms race continues in multi-domain operations, the adversary's capabilities will be harder to detect, collect on, and assess confidently. As a result, military forces will lose the opportunity to confirm adversaries are employing non-lethal threats against JADC2 networks. As military detection and attribution capabilities decline, assessed confidence levels will also decrease in future observations of non-lethally employed threats against JADC2 networks in contested environments. The threat of losing ISR confirmed or "high" confidence reporting on non-lethally employed adversary threats against JADC2 networks, will inhibit the military's ability to implement mitigation techniques to counter them. This will result in an undetected threat, which will inherently blind the operator to the associated vulnerability level of the device – critical information in a contested environment.

The recommended process for ensuring JADC2 networks are operational and secure in future contested environments include the following: 1) employment of JADC2 network enabling equipment in contested environments, 2) ISR overhead in collecting threat data on observed or assessed adversary capabilities against JADC2 network enabling devices utilized, 3) adequate centralized databasing of those threats at COCOM levels with intelligence threat data refresh rate maintained, 4) persistent ISR support in translating the threat data to supported units to enable 5) implementation of required actions to mitigate risks associated with JADC2 network enabling devices (reference image 1).

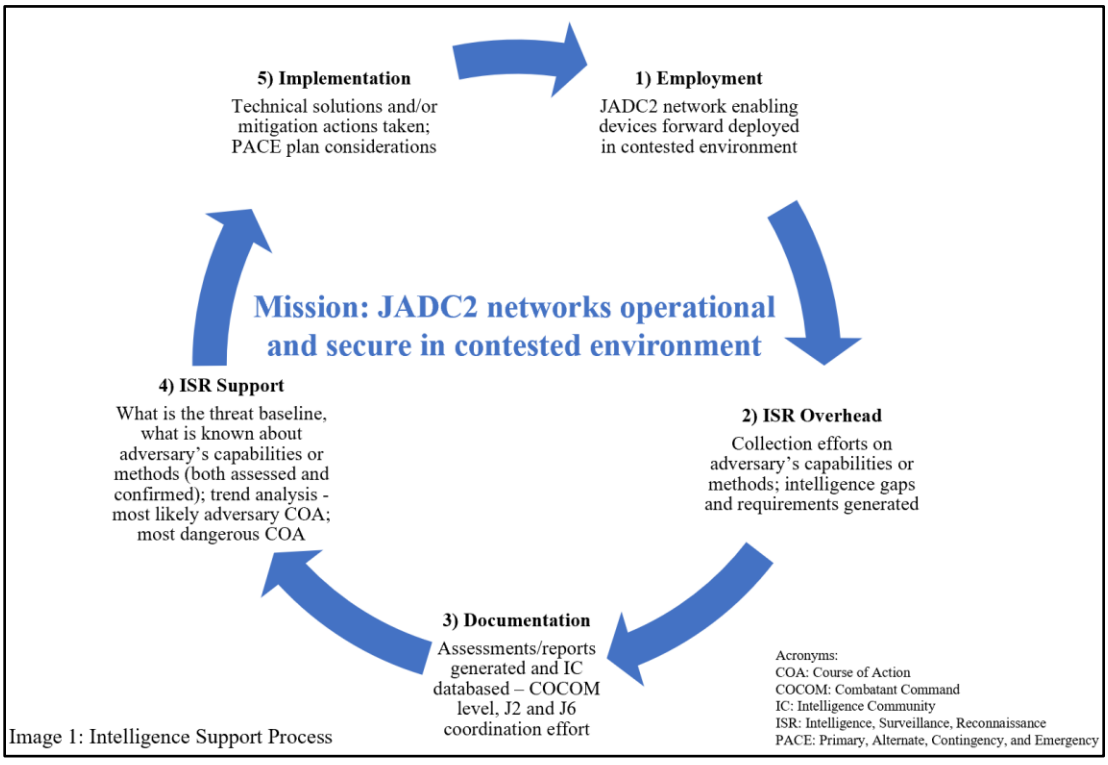

Image 1: Intelligence Support Process

When the threats are known, properly documented, and distributed to consumer base that enables JADC2 networks, intelligence can be utilized to implement technical solutions and mitigation techniques to minimize associated vulnerability levels in a contested environment. Sixteenth Air Force leadership confirmed this assessment in a 2020 report advocating for the requirement to employ processes that are relevant to the speed of the information environment;

the report additionally states that "effective information warfare operations in a peer conflict will require tight synchronization among ISR, Cyber, electronic warfare, and information operations, as well as seamless integration into combatant command operational process."[2] The intelligence data gained can contribute to changes in military employed tactics, techniques, and procedures in a contested environment. As an example, a network operator may not want to rely on a device that enables a command and control (C2) connection because of the known threat intelligence associated with the device; that network operator may then establish an alternate connection that enables the same C2 function but at a lower risk level against the known adversary threat.

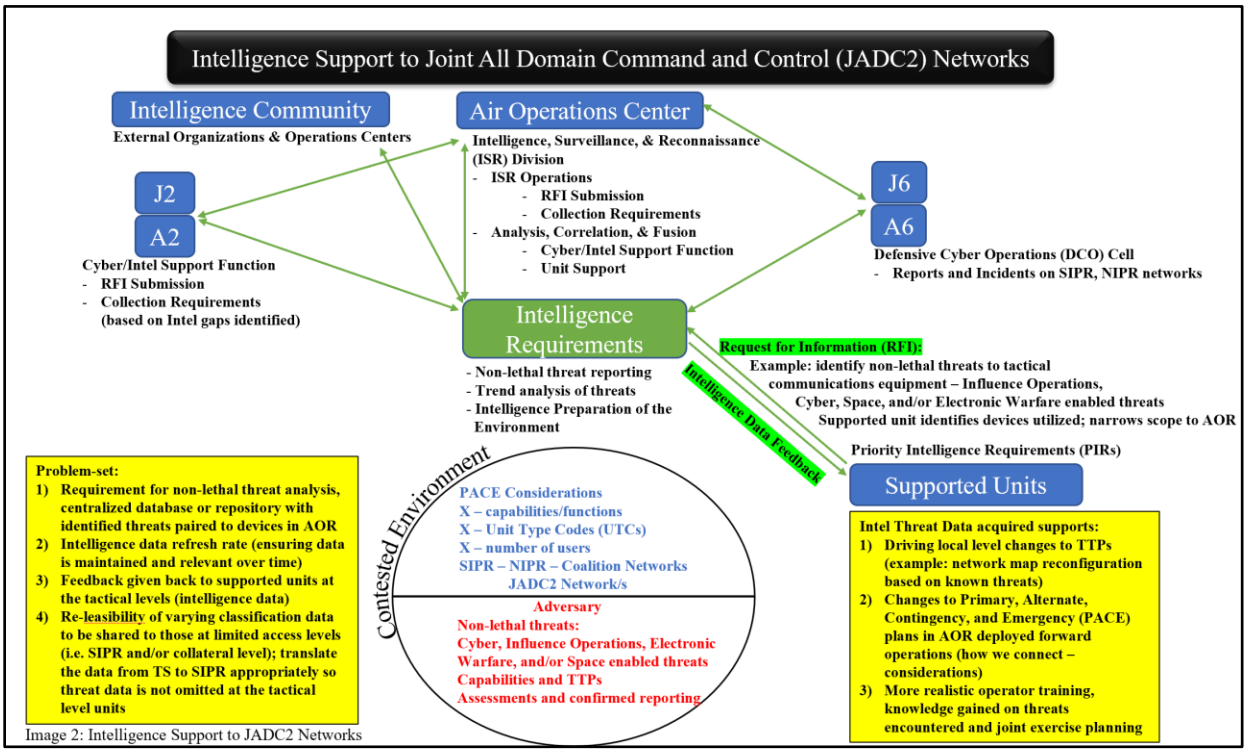

Image 2: Intelligence Support to JADC2 Networks

CONCLUSION

In order to ensure JADC2 networks are operational, the DoD should: 1) increase priority on identifying non-lethally employed effects to forward deployed JADC2 network enabling devices, 2) document the non-lethal threats to JADC2 networks at COCOM staff levels, at different classification levels (tear lines, as appropriate to ensure releasibility to consumer base), and 3) prioritize efforts to ensure technical solutions and mitigation actions are implemented at a remediation rate acceptable for meeting operational demand as adversary's capabilities and methods become known. This recommended approach identifies military network dependencies in a contested environment, with intent to fortify the JADC2 networks against adversary non-lethally employed threats. The ability to articulate the full threat picture and implement operational planning considerations that counter near-peer adversaries' anticipated capabilities and methods, as they are still in development, will be key in the next generation conflict.

REFERENCES

1. RAND Corporation, “Joint All-Domain Command and Control for Modern Warfare: An Analytical Framework for Identifying and Developing Artificial Intelligence Applications”, 2020, https://community.apan.org/wg/aucoi/multi-domain-operations-in-education /w/wiki/ 25779/joint-all-domain-command-and-control-jadc2/.

2. Lieutenant General Timothy D. Haugh, Lieutenant General Nicholas J. Hall, Major Eugene H. Fan, “The Cyber Defense Review: 16 Air Force and Convergence for the Information War”, Summer 2020, 8, https://cyberdefensereview.army.mil/Portals/6/Documents/CDR% 20Journal% 20Articles/Haugh_Hall_Fan_CDR%20V5N2%20Summer%202020.pdf?ver=2020-07-27-053232-357.

3. Department of Defense, “Joint Publication 3-12: Cyberspace Operations”, Washington DC: Department of Defense, 2013, 25-26, https://fas.org/irp/doddir/dod/jp3_12r.pdf

4. Department of Defense, “Joint Publication 3-13: Information Operations”, Washington DC: Department of Defense, 2014, 34-35, https://www.jcs.mil/Portals/36/Documents /Doctrine/pubs/jp3_13.pdf.

5. Department of Defense, “Joint Publication 2-0: Joint Intelligence”, Washington DC: Department of Defense, 2013, 49-60, 71, https://www.jcs.mil/Portals/36/Documents /Doctrine/pubs/jp2_0.pdf.

6. Department of Defense, “Joint Publication 6-0: Joint Communications System”, Washington DC: Department of Defense, 2019, 33-34, https://fas.org/irp/doddir/dod/jp6_0.pdf.

Author's Note:

This research paper was written from the perspective of a Network Operations (17DXA) and Intelligence (14N) dual-Air Force Specialty Coded officer. The core focus of this research paper derives from an effort currently being worked at staff level by the author in support of a tactical communications group and is working towards codifying what non-lethal requirements submitted on behalf of tactical level units should look like to 16th Air Force moving forward.

Senior mentors contributing to research topic (July 2020):

Mr. Grant Holt, 17th Intelligence Squadron, Senior Intelligence Analyst

Major Neale Linge (USAF), Air University Advanced Research Group Facilitator

Major Jahmil Edwards (USAF), Air Education and Training Command

Major Van De Water (USAF), LeMay Center Mentor