

Jeffrey Thomas

Professor Mark Wegge

Module 4: Joint Capabilities

05 January 2025

DBF 4.6: INTEL, INFO & CYBER

Response

QUESTION: *The cohort will be divided into two groups—a BLUE group and a GOLD group. The BLUE group must answer the BLUE question below and the GOLD group must answer the GOLD question below. (minimum of 250 words)*

- **BLUE:** (INTEL) *Intelligence, Information Operations and Cyber warfare are often put in the category of “force multipliers.” How can the capabilities associated with each be most effectively integrated into a military operation? (Ensure the distinctions between the three are highlighted.*
- **GOLD:** (INFO & CYBER) *What is the difference between information operations and cyber operations? Provide examples from our historical cases or recent operations on how both can be incorporated to enhance military operations and explain the expected results from their use.*

Primary Gold Post (by January 5, 2026)

Information operations (IO) shape how audiences interpret events and choose, while cyberspace operations (CO) create technical effects in and through networks. The advantage comes when commanders synchronize both so cyber actions reinforce the narrative they need accepted.

Joint doctrine stresses that “all activities have inherent informational aspects” (Chairman of the Joint Chiefs of Staff [CJCS], 2022, p. I-1) and frames the information joint function as applying information “to change or maintain perceptions, attitudes, and other drivers of behavior” (CJCS,

2022, p. II-6). CO is “the employment of cyberspace capabilities where the primary purpose is to achieve objectives in or through cyberspace” (CJCS, 2018, p. I-1). IO targets perception and decision-making, whereas CO targets the systems that enable or constrain those choices.

Stuxnet is a useful illustration of why that distinction must collapse in practice. As Crowell explains, the malware used code to physically alter and damage Iranian nuclear processing equipment while simultaneously sending deceptive “signals (content) to the human operators that all was working well” (Crowell, 2019, p. 7). In other words, the technical effect only mattered because it shaped what humans believed and therefore how they acted.

Operation Glowing Symphony illustrates the same IO and CO synergy at the operational level. U.S. Cyber Command (USCYBERCOM) sought to “deny, degrade and disrupt them in cyberspace” and leaders assessed a “psychological component” that punctured the Islamic State of Iraq and Syria’s (ISIS’s) image of competence (Temple-Raston, 2019).

These gains endure only if IO begins with audience analysis. As Reilly argues, “Successful information operations understand the target audience” before developing objectives and means (Reilly, 2013, p. 2). Expected results include slower propaganda throughput, degraded command confidence, and reduced recruitment resonance.

Friendly advantage collapses if the joint force cannot communicate and coordinate under attack. Fahrenkrug notes, “An integrated defense begins by first trying to avoid the attack by actively dispersing the networks” (Fahrenkrug, 2021, p. 197). Resilience preserves command and control (C2) and credibility, keeping messaging and cyber effects coherent.

In summary, CO changes what systems can do, but IO shapes what people conclude.

Synchronized use turns disruption into behavior change.

References

Chairman of the Joint Chiefs of Staff. (2018). Joint Publication 3-12: Cyberspace Operations. Washington, DC: Department of Defense.

Chairman of the Joint Chiefs of Staff. (2022). Joint Publication 3-04: Information in Joint Operations. Washington, DC: Department of Defense.

Crowell, R. M. (2019). War in the information age: A primer for information operations and cyberspace operations in 21st century warfare (5th ed.). U.S. Naval War College.

Fahrenkrug, D. T. (2012). Countering the offensive advantage in cyberspace: An integrated defensive strategy.

Reilly, R. R. (2013). Information operations: Successes and failures (NWC 2163). Newport, RI: U.S. Naval War College, Joint Military Operations Department.

Temple-Raston, D. (2019, September 26). How the U.S. hacked ISIS. NPR. Retrieved from <https://www.npr.org/2019/09/26/763545811/how-the-u-s-hacked-isis>

Secondary Post #1 (*by January 8, 2025*)

QUESTION (Suzy): BLUE (*minimum of 150 words*)

Suzy, strong breakdown of the three lanes. One addition from the professor's office hours is that integration must start with commander decision points: well-written priority intelligence requirements (PIRs) are few, urgent, and the answer "triggers a sequence of actions". Intelligence leads by building Joint Intelligence Preparation of the Operational Environment (JIPOE) and describing the operational environment's physical, informational, and human aspects, then translating gaps into collection and analysis that "inform the commander" and enable decision advantage (Chairman of the Joint Chiefs of Staff, 2022, p. xii). That foundation also cues cyber target selection and frames how information effects will be assessed.

From there, information operations (IO) should specify the desired behavior change and target audiences, while cyber operations (CO) provide timed technical effects in and through cyberspace and preserve friendly command and control (C2) resilience.

Stuxnet shows the interplay: intelligence-enabled targeting of industrial control systems produced real physical effects, and the malware simultaneously fed "signals (content) to human operators that all was working," showing how technical disruption and perception management converge and why attribution and escalation control shape the strategic payoff (Crowell, 2019, p. 7).

References

Chairman of the Joint Chiefs of Staff. (2022, May 26). Joint Publication 2-0: Joint intelligence. Washington, DC: Department of Defense.

Crowell, R. M. (2019). War in the information age: A primer for information operations and cyberspace operations in 21st century warfare (5th ed.). U.S. Naval War College.

Secondary Post # 2 (*by November 26, 2025*)

QUESTION (Will): GOLD (minimum of 150 words)

Hi Will, your definitions and cases are on point. One nuance from the professor's office-hours slides is that information operations focus on influencing decision-making and behavior in the information environment, while cyber operations focus on creating effects in or through cyberspace, including protecting friendly networks and, when authorized, acting against adversary systems. They are distinct, but they can be used together to compound effects.

Your Russia example fits well: information operations help shape perceptions and legitimize action, while cyber operations can disrupt or control the channels that carry information, degrade adversary command and control, or protect friendly communications from interference. A historical case is Operation Glowing Symphony: U.S. cyber actions disrupted the Islamic State of Iraq and Syria's media pipeline while aiming for psychological impact. Expected results included slower propaganda production, reduced credibility, and degraded recruitment reach.

Stuxnet reinforces the relationship: cyber activity caused physical disruption while feeding deceptive signals to human operators, showing how technical effects can be paired with influence on what people believe and how they respond.

References

N/A

Professor Feedback

Jeff,

Meets expectations. Good examples (Stuxnet, Glowing Symphony), good summary too. Keep in mind bringing Intel (typically already there), IO and cyber in at the planning stages is the key to successful operational integration. Excellent DBF!