Information Warfare Rising (Part I):

Characterizing Threats in the Information Environment

Capt Katelynne Baier

Air University Advanced Research

16 December 2020

"Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of the Air University, the United States Air Force, the Department of Defense, or any other US government agency.

Virtual In-Residence Squadron Officer School

Maxwell AFB, Alabama

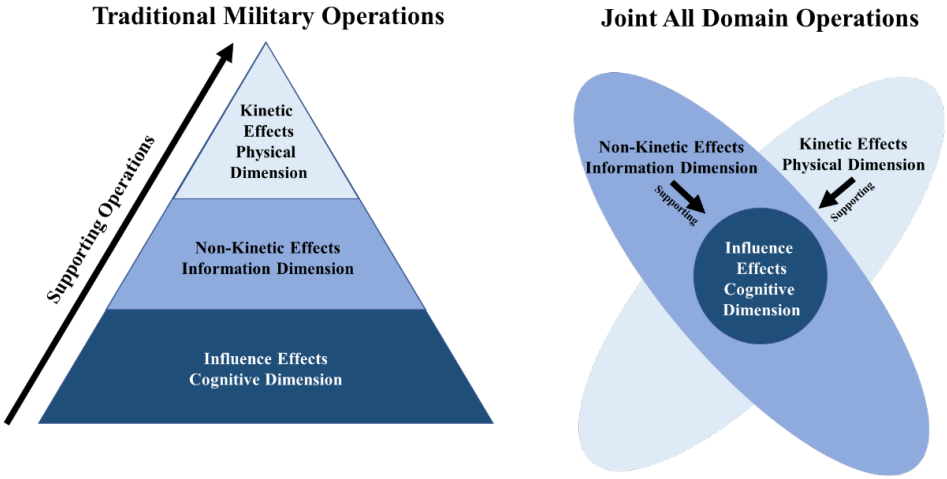
Abstract

Information Advantage (IA) within the information environment (IE) is one of the most critical focal points of Joint All Domain Operations (JADO)[i]. China and Russia recognize this and are prioritizing Information Warfare (IW) to counter US strengths and military might. These adversaries are focusing on effects in the information environment, specifically the information and cognitive dimensions with physical actions to support, posing a direct threat to US, allied, and partner forces[ii] [iii]. Identifying and characterizing threats to JADO in the information environment is a difficult process. How do we evaluate adversary capabilities, intent, and historical actions to create adversary courses of action? How do we identify these threats at the strategic, operational, and tactical levels? This paper will propose a new comprehensive analytical framework for IW specialties within the Air Force to holistically evaluate threats in the information environment at the strategic, operational, and tactical levels.

Gen Charles Q. Brown Jr., current Chief of Staff of the Air Force, cast a vision of an Air Force that needs to "accelerate change or lose" to prepare for a future fight[iv]. This future fight will be defined by the joint force's ability to embrace Joint All Domain Operations (JADO). Gen (ret) David Goldfein once stated this about JADO:

> *"The goal is producing multiple dilemmas for our adversaries in a way that will overwhelm them…. An even better outcome…is to refine [JADO] to the point where it produces so many dilemmas for our adversaries that they choose not to take us on in the first place.[v]"*

Gen (ret) Goldfein is describing leveraging JADO to influence the adversary to create end states and desired effects within the information environment, defined in Joint Publication 5-0 "Joint Planning" as a combination of the physical, information, and cognitive dimensions[vi]. The goal of JADO, as outlined by Goldfein, is to shift the dominant focus from the physical dimension and "platform-based" thinking to a holistic approach that includes the information and cognitive dimensions and "effects-based" thinking. JADO is primarily used to influence adversary decision-making, behavior, and actions, all of which are characterized within the information environment. We achieve these influencing effects by leveraging all domains in a synchronized manner to achieve Information Advantage (IA), which ultimately enables all other aspects of JADO[vii].



Our adversaries also recognize the importance of IA. Russia has long relied on misinformation and propaganda to influence target audiences and undermine their adversary interests[viii]. Col General Arkadiy Bakhin, Russian Federation Air Force, is quoted saying:

> *"It is our profound conviction that victory in a future war will belong not to whoever has the most sophisticated tank or the fastest and most maneuverable fighter and most powerful missile, but to whoever is able, with the greatest effectiveness and coordination, to command and control the entire array of his own—albeit not even the most advanced—land, air, sea, and space-based information armaments.[ix]"*

Similarly, China is making significant progress as a "global data powerhouse" and is on track to surpass US information capabilities in several critical areas, including electronic warfare, quantum computing and communications, and BeiDou position, navigation, and timing (PNT) services[x]. These adversaries can successfully deny and degrade US advantages in military might and achieve their own desired effects by focusing on the cognitive and information dimensions with physical operations in a supporting role.

To holistically characterize the information environment and achieve Information Advantage (IA) for JADO, the first step is to identify and define threats[xi]. What are the threats to Information Advantage (IA) and our desired effects? How do we identify these threats at the strategic, operational, and tactical levels? How do we evaluate adversary capabilities, intent, and historical actions to create adversary courses of action? This paper will propose an analytical framework for Information Warfare (IW) specialties within the Air Force to holistically evaluate threats in the information environment at the strategic, operational, and tactical levels.

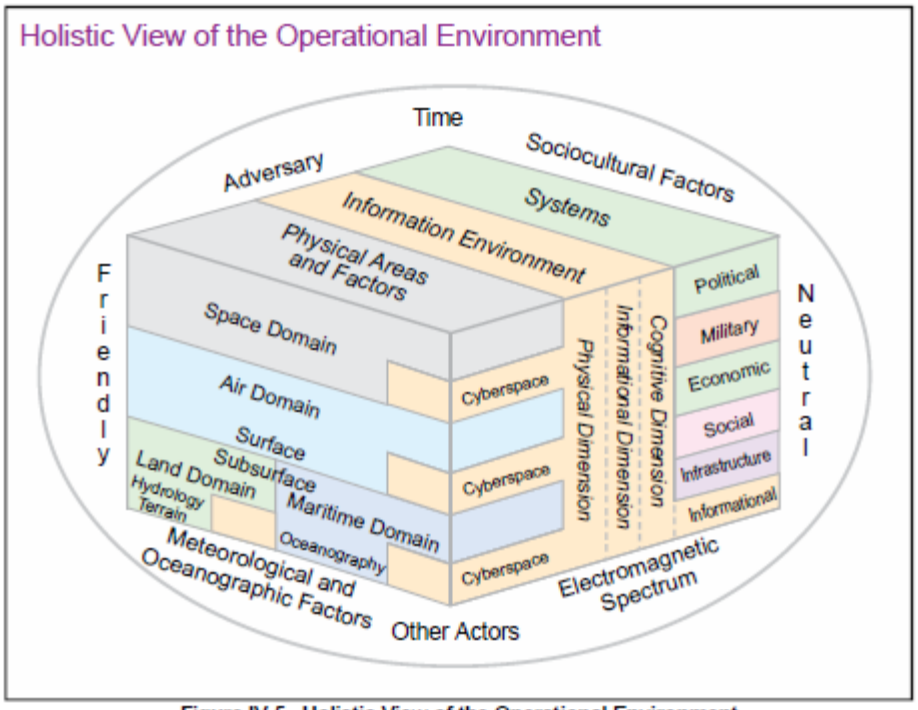
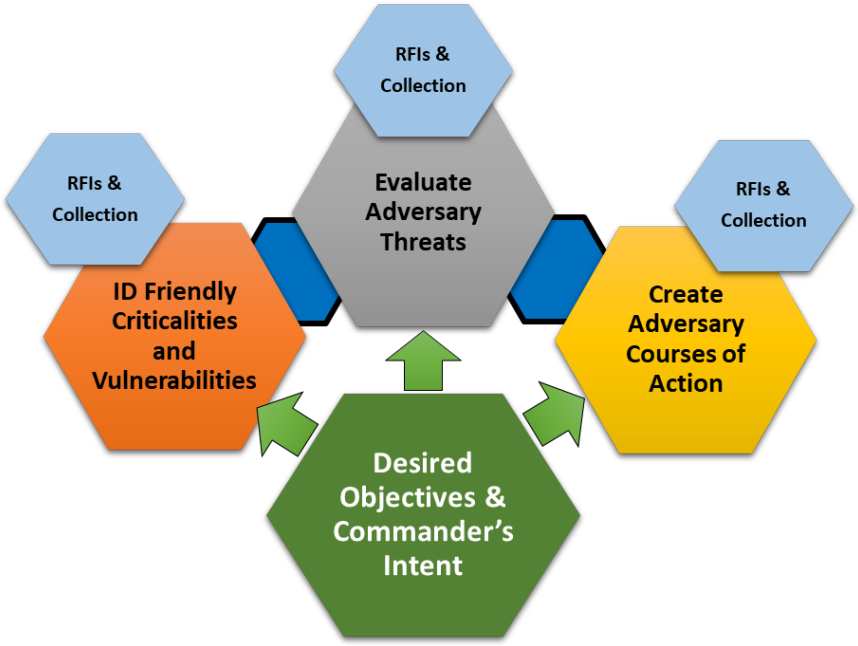


Figure IV-5. Holistic View of the Operational Environment [xii]

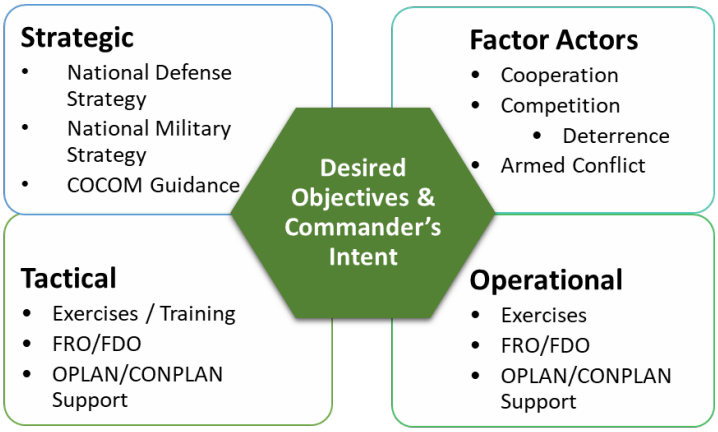
JP5-0 "Joint Planning" provides a comprehensive depiction of the information environment's intertwined nature, as it is comprised of physical, informational, and cognitive dimensions. When identifying and evaluating threats, it is critical to examine them holistically. No one system operates in an isolated dimension; increased interconnectedness and interdependencies between the physical, informational, and cognitive systems open the door to increased vulnerabilities to adversary attack[xiii]. Historically, threat characterization and enemy courses of action are the primary outputs of the Joint Intelligence Preparation of the Operational Environment (JIPOE) process[xiv]. During this four-step process, analysts define the operational environment (OE), describe impacts of the OE on key players (friendly, neutral, adversary), evaluate adversary capabilities, and create most likely and most dangerous courses of action. As it is currently written, traditional JIPOE focuses on "order of battle" and physical targets, treating the information environment as a secondary consideration and not a central focus or mission[xv].

To characterize threats within the information environment, this paper will selectively adopt aspects of the JIPOE process to craft a new analytical process focused on the critical aspects necessary for planning and execution. While it is loosely adopted from JIPOE, this analytic process is not "one and done" but needs to be constantly revisited to adapt with the rapidly changing information environment[xvi]. Additionally, for this process to be effective, it cannot be accomplished solely by intelligence analysts but rather is a tool to be used by all Information Warfare (IW) specialties. It requires a "whole of IW effort," whether it is an IW cell at a wing or IW division at an Air Operations Center or a 16th Air Force strategic IW unit. Finally, unlike traditional JIPOE, every step of the analytic framework requires constant inputs and updates; therefore, submitting Requests for Information (RFIs) or collection requests is a persistent requirement and not limited to a specific step.



Adapting JIPOE to the information environment requires the elimination of a couple steps that no longer apply. Examples of this are the typical "define the operational environment" and "describe the impact on the operational environment" steps. The traditional physical

operational environment does not translate to the information environment. While a specific military operation may be bounded in the physical dimension, those examining threats still need to maintain global awareness. Globalization, interconnectedness, and interdependencies between the physical, informational, and cognitive systems open the door to increased vulnerabilities to adversary attack to a global scale[xvii]. How, then, does an IW cell scope their analysis and the problem set? The solution is to begin with heavy focus on defining and understanding commander's intent as well as desired objectives or effects.



The key to understanding desired objectives, effects, and commander's intent within JADO includes understanding the difference between cooperation, competition below armed conflict, or armed conflict regions as is defined by Joint Doctrine Note 1-19 "Competition Continuum[xviii]." The US could be engaged in cooperation, competition, and even armed conflict within the same geographic combatant command, and it is essential to define clear objectives and desired effects for each aspect of this dynamic. This effects all other steps within the analytic framework, as factor friendly critical functions or vulnerabilities as well as potential threats will vary drastically depending on what the unit is tasked to support: a threat to "cooperation" efforts will look vastly different than one

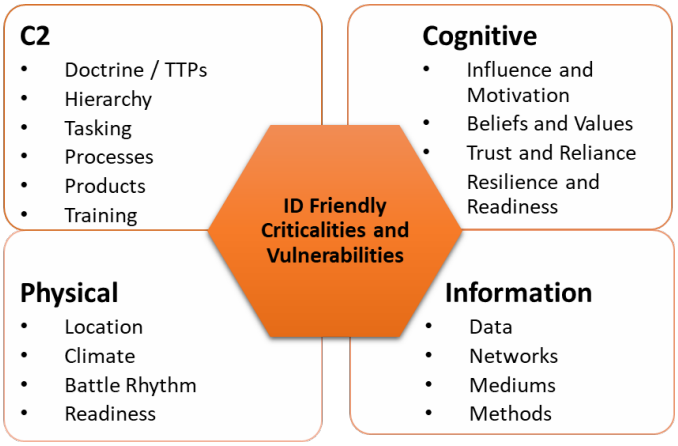
- **Cooperation**: Mutually beneficial relationships with compatible interests.
- **Competition**: Relationships with incompatible interests–none seeking to escalate to armed conflict.
- **Armed conflict**: A situation in which combat is the primary means to satisfy interests.

for “competition” or “armed conflict.” The table below provides examples of how the Department of the Air Force looks at supporting these different regions within the continuum.

JADO Across the Competition Continuum	
Continuum region	**Joint all-domain operations, activities, and investments**
Cooperation	✪ Improve materiel and non-materiel partner nation interoperability. ✪ Obtain and maintain air and cyberspace domain access enabling global reach and rapid projection of military power. ✪ Establish cooperative sharing agreements improving mutual support in crisis response.
Competition	✪ Incorporate all-domain approaches into flexible deterrent options. ✪ Expose and counter malign influence. ✪ Maintain freedom of access and maneuver in the global commons.
Conflict	✪ Gaining information advantage. ✪ Projecting global combat power. ✪ Synchronizing action in, from, or through all domains to gain and maintain theater access. ✪ Overmatching adversary forces at decisive points. ✪ Preserve combat capability to conduct future operations

JADO Across the Competition Continuum

As of now, we are in a state of competition with global players such as Russia and China[xix]. Potential operations, activities, and investments of the competition region are flexible deterrence options, countering malign influence, and maintaining freedom of access and maneuver in the Area of Operations (AO). These activities are inherently all-domain; no singular military branch or set of military capabilities can achieve these objectives. Identifying and countering PRC and Russian threats to US objectives under this competition region is the current challenge for the US joint and coalition force.

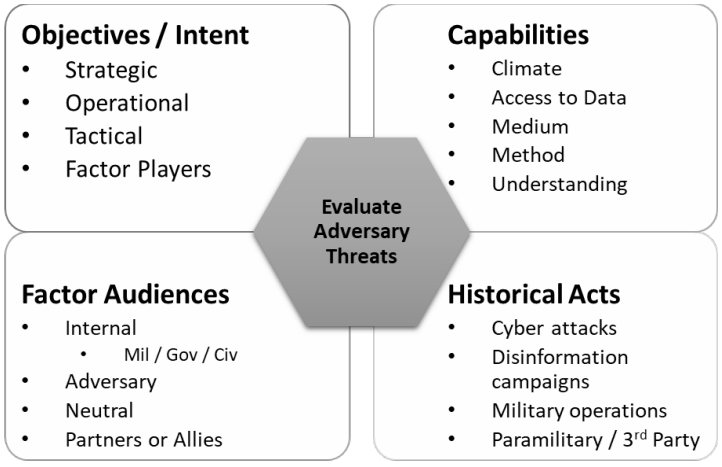


With commander's intent in hand, the next step of the analytical process is friendly force criticalities and vulnerabilities. This is another point where the IW analytical framework departs from traditional JIPOE; before threats can be identified and characterized, there must first be a thorough and comprehensive review of the "friendly forces" aka. US, allied, and partner forces. Joint Publication 3-60 Joint Targeting outlines how to evaluate a target through physical, functional, cognitive, and environmental characteristics[xx]. Replace "target" with "friendly" forces and the same model can be used to identify key characteristics. An alternative model to consider is called the CARVER model, which stands for Criticality, Accessibility, Recuperability, Vulnerability, Effect and Recognizability[xxi]. This US military model provides in depth analysis on the "target" characteristics listed above to evaluate which components of a system to attack. While currently the CARVER model is used to evaluate potential targets and "target system analysis," turning the model towards friendly force evaluation could also be effective[xxii]. At a minimum, friendly force evaluation needs to include these four categories: 1) cognitive, 2) information, 3) physical, and 4) command and control (C^2).

Consequently, this is where it is essential to involve all disciplines under the Information Warfare category. No one specialty can conduct this friendly force analysis on their own. For example, Information Operations provides insights into the cognitive and C^2 realms to answer questions such as friendly sources of motivation, patterns of behavior, biases and dogmas, levels of trust in systems or organizations, and even unit readiness through resilience[xxiii]. Cyber understands the connections between the cognitive and information dimensions as well as the technology that supports C^2 processes. Public Affairs and Operations Research can provide insights into the social and political "climates" in the information environment that could affect friendly objectives, and Public Affairs and Information Operations can identify and characterize

key audiences essential to achieving friendly force desired effects[xxiv]. This step truly sets this analytic framework apart from any other: it forces us to understand our own audiences and organizations, our own dogmas and biases, as well as our norms and patterns. The answers to these questions need to be tailored based on the level of the organization: strategic, operational, or tactical. Recognizing the need for comprehensive IW analysis and teamwork will ultimately drive new training and organization requirements.

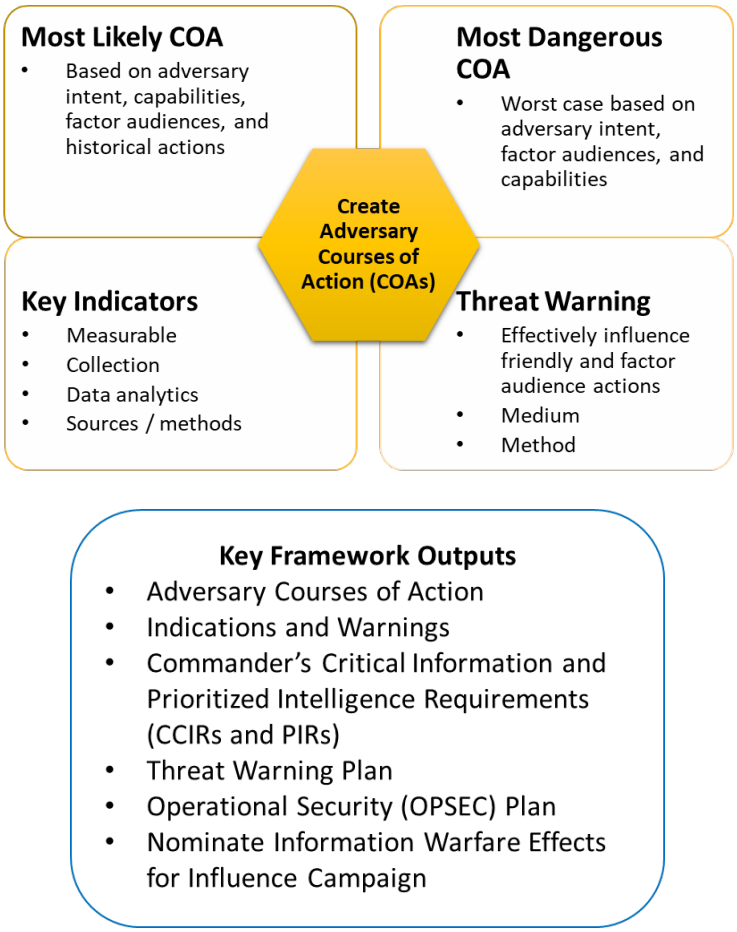
As these questions are answered, critical nodes within these organizations and processes will reveal areas of weakness and vulnerabilities[xxv]. The goal is to define friendly force Centers of Gravity (CoGs) which could be single points of failure, critical people, organizations, and processes to achieving commander objectives and intent, and potential vulnerabilities to adversary influence or manipulation. Other impacts examined in this step include events, activities, or dynamics that drive positive or negative impacts to the stated commander's intent that are not a result of adversary action. Examples of this are the impacts of weather, geographical distance, news coverage, and domestic or regional political climate. These can be captured as vulnerabilities to friendly forces.



The next step is to identify all possible adversary threats to commander's intent and target friendly vulnerabilities. This threat analysis is similar to traditional JIPOE that examines

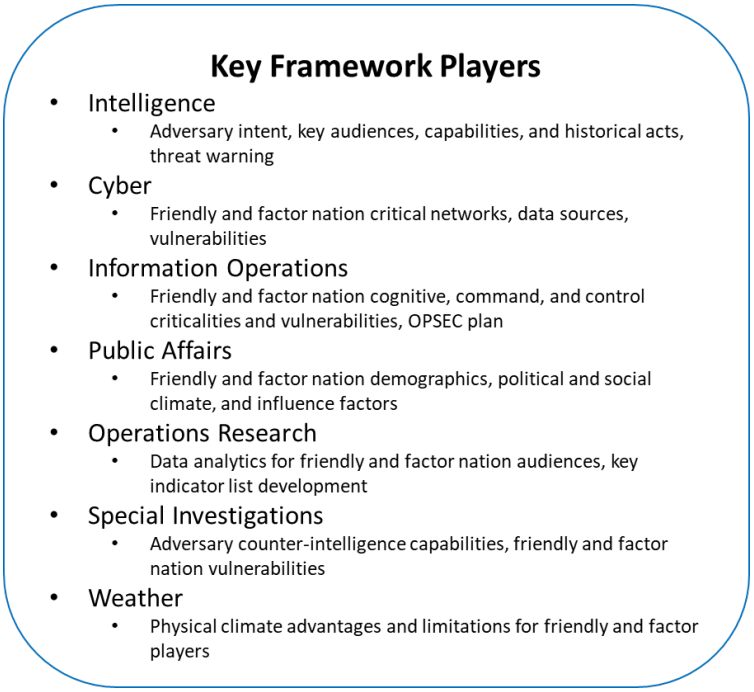
adversary intent and objectives, their demonstrated and future all-domain capabilities, and historical actions[xxvi]. However, unlike JIPOE that heavily emphasizes physical order of battle and the capabilities and limitations of the weapon systems, this framework examines the equivalent players that are the factor audiences necessary to achieve adversary desired effects or objectives. While this may connect to some physical order of battle in relation to military units involved with operations, the primary focus is characterizing cognitive and information Centers of Gravity (CoGs)[xxvii]. A comprehensive analytical model that could be loosely adopted for this step is a commercial organization evaluation tool known as SIPOC, which stands for Supplier (adversary intent, objectives, and doctrine), Inputs (data mediums or methods, personnel, and collection), Processes (computer networks and information flow diagrams), Outputs (specific messages or themes), and Customers (or target audiences)[xxviii].

This kind of intelligence analysis marks a significant departure from traditional "intelligence support to operations," especially for those intelligence professionals working within an operational or tactical unit. It will require additional training, authorities, and networks accesses for units to use Publicly Available Information (PAI) to conduct open-source intelligence (OSINT), human intelligence (HUMINT) tasking and reporting, and signals intelligence (SIGINT) combined with cyber reporting to answer these non-traditional analysis questions. While this is in line with the 2019 Air Force ISR Flight Plan, there is a long way to go to produce trained analysts to support this process[xxix].



In the final step of this IW framework, the objective is to create most likely and most dangerous adversary courses of action (COAs). The most likely COA is crafted using a combination of adversary intent, capabilities, and known or historical actions. The most dangerous COA assesses the worst possible case based primarily off adversary intent and capabilities. As they are developed, these courses of action include a comprehensive "indications and warnings" (I&W), a list of measurable, specific adversary actions that point towards the most likely, most dangerous, or even an unassessed alternative COA. This I&W list drives follow-on collection, data analytics and monitoring within the information environment, as well as updates to commander's critical information requirements (CCIRs) and prioritized intelligence requirements (PIRs). The I&W list should be a product created in combination with intelligence,

IO, PA, and operations research analyst inputs so that not only are the indicators identified but the methodology and notification process for those indicators is also clearly developed.



After the COAs, I&W list, and CCIRs or PIRs are updated, IO and OSI analysts should nominate additional changes to OPSEC or INFOSEC plans based on assess friendly force vulnerabilities and adversary COAs. Public affairs main task is to work with intelligence, IO, and operations research to develop a "threat warning" plan. This plan is not simply about notification of a growing threat, but it also includes friendly force analysis that identifies how to effectively communicate the threat in a way it is received and internalized. Message sent does not always mean message received, and it is vital to understand the friendly force and how to influence behavior and thought in a way that supports the defense and wellbeing of the unit. Example recommendations could be revealing security issues with a certain social media platform, changes in policy for personal cellphone or other device use at work, the need to change patterns of behavior on or off base, etc. Communicating the threat in a way so that the youngest, most technological savvy Airman to the oldest senior NCO in the unit both understand and embrace

the changes is a significant challenge that requires a "whole of IW" effort. This includes influencing the actions and behaviors of our joint partners as well as our coalition allies and partners. Once again, these products need to be tailored based on the level of organization in which the IW cell operates, whether that is strategic, operational, or tactical. It will require multiple new skillsets from several IW specialties to support this unprecedented, combined effort.

This framework is just the first step in a series of efforts to gain and maintain information advantage in support of JADO. Now that we have identified the steps necessary to defend US desired objectives and commander's intent, the next step is to go on the offensive. We must now utilize "information firepower" to weaponize our knowledge of the adversary that comes from this IW threat analysis framework. In Part II of this "Information Warfare Rising" series of papers, Capt Jun Hong explains exactly how this ought to be accomplished. Finally, it is not enough to simply admire the current barriers within the Information Warfare community or the military at large to accomplishing real change within our culture to allow this new "influence focus" thinking to be adopted. To make these new processes and organizations a reality, it is going to require a major shift in the predominant mindset tied to traditional, kinetic-focused military operations to effects-based or influence operations. In Part III of the "Information Warfare Rising" series, Capt Reid Hottel discusses how to make this change in culture a reality. Ultimately, we must "accelerate change or lose," recognizing the need to adopt these changes as quickly as possible to successfully implement JADO and ultimately fight and win against peer and near-peer competition or armed conflict[xxxxxxi].

[i] Haugh
[ii] China
[iii] Russian
[iv] Brown
[v]
[vi]
[vii]
[viii] Russian Information Warfare: A Reality That Needs a Response | RAND
[ix] Russian
[x] https://asia.nikkei.com/Spotlight/Century-of-Data
[xi]
[xii] JP5-0
[xiii] Tagarev
[xiv]
[xv] Haugh
[xvi] Ibid
[xvii] Tagarev
[xviii]
[xix] NDS?
[xx] JP3-60
[xxi] https://sofrep.com/gear/green-berets-and-the-carver-matrix/, Mr. Grant Holt Interview
[xxii] Holt
[xxiii] Interview with Sheri
[xxiv] Interview with Sheri
[xxv] 3-60 TSA
[xxvi] JIPOE
[xxvii] JP3-60
[xxviii] https://www.toolshero.com/quality-management/sipoc-model/ , Holt
[xxix] ISR Flight Plan
[xxx] Brown
[xxxi] Continuum