13th ICCRTS: C2 for Complex Endeavors

"Prioritization Taxonomy and Logic for Network-Centric Operations"

Collaborative Technologies for Network-Centric Operations

Brian P. Donnelly

Scott M. Galster

Point of Contact:
Brian P. Donnelly
Air Force Research Laboratory
2255 H Street
Wright-Patterson Air Force Base, OH USA
937.255.7400
brian.donnelly@wpafb.af.mil

Paper cleared for Public Release by the US Air Force Office for Security Review (SAF/PAX). Disposition Date: 2/4/2008. Document Number WPAFB 08-0013.

Prioritization Taxonomy and Logic for Network-Centric Operations

Abstract

The effects of network-centric operations would be degraded if not for inherent human or machine sensemaking capabilities. Without knowing the situation or understanding the actors and their disposition and intent, deciding and executing the most appropriate response is a futile activity. Collecting data and creating track information to resolve the intent and disposition of disparate actors is only possible by having an integrated intelligence, surveillance, and reconnaissance (ISR) network of humans and supporting systems. While ISR networks in the military context are becoming increasingly elaborate and more tightly 'networked' to perform their roles for a commander, so, too, must the underlying logic be developed to impart commander's intent on the ISR network such that it functions with the agility needed to keep pace with the dynamic environment. Dynamic networks rely on a foundation of interoperability standards, among which should be a prioritization taxonomy that baselines priorities of actors in the situation and dynamically allocates the ISR resources accordingly to achieve the desired effects. This paper examines the required characteristics of a prioritization taxonomy and proposes a sample framework for implementation.

Keywords: automation, target priority, decision support, taxonomy

Introduction

"Effective C2 demands that commanders and staffs ***collaborate*** *in planning (e.g. determining the mission, operational objectives, desired effects, and tasks), preparing for, executing, and assessing joint operations.* ***Commander's critical information requirements*** *(i.e. priority intelligence requirements and friendly force information requirements) are a key information management tool for the commander…"* (JP 3-0, 2006, p. xvii, see Figure 1)

No matter the type of military operation (i.e. major operations, homeland defense, civil support, etc), or its scale (crisis response through campaigns), the commander's critical information requirements are going to determine the baseline performance of the supporting intelligence, surveillance, and reconnaissance (ISR) network of systems. The success of every operation depends on timely and accurate sharing of information and intelligence such that all parties involved share a common understanding of all actors in the operational environment. Whereas in the past the difficulty was tracking the multitude of military forces, both friendly and enemy, in defined theaters of operations, future conflicts may be less conventional and more irregular, disruptive, or catastrophic. In other words, the problem has shifted from one of tracking capacity (quantity) to one of finding needles in haystacks (quality).

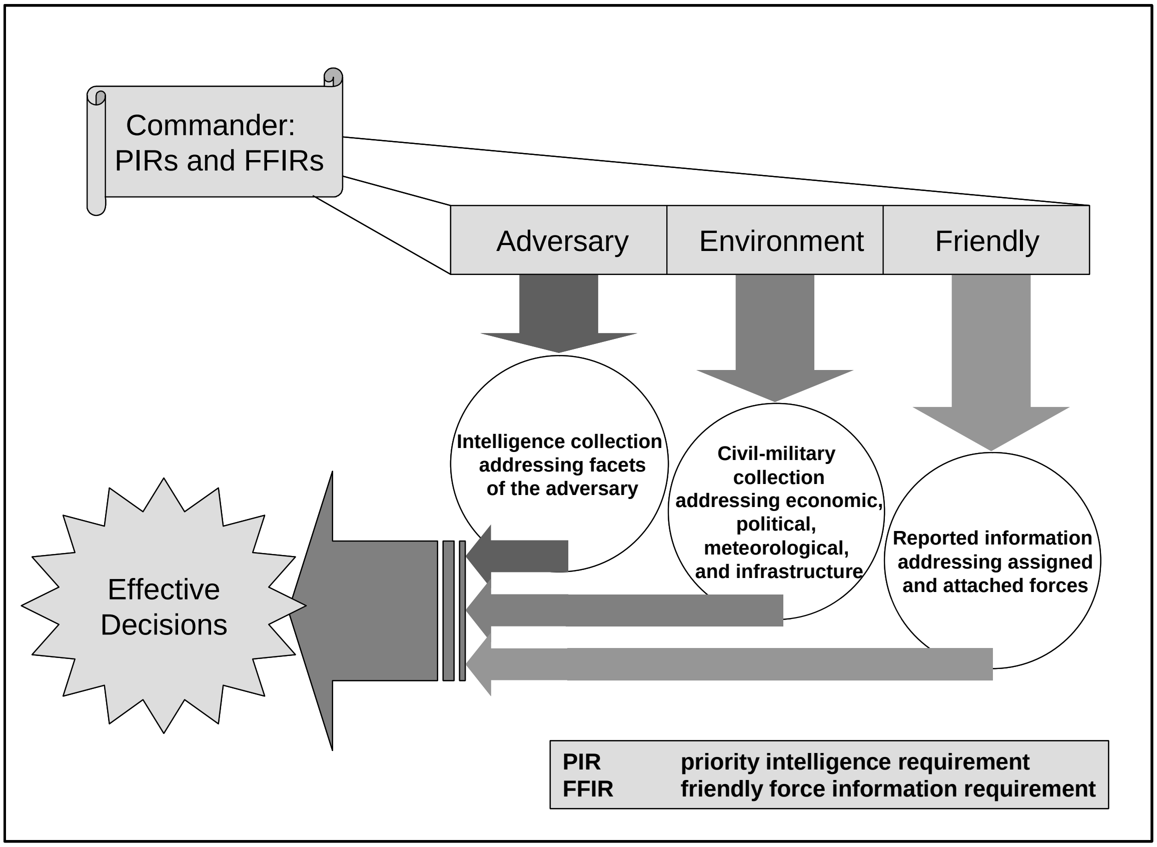

Commander:
PIRs and FFIRs
Adversary
Environment
Friendly
Intelligence collection addressing facets of the adversary
Civil-military collection addressing economic, political, meteorological, and infrastructure
Reported information addressing assigned and attached forces
Effective Decisions
PIR priority intelligence requirement
FFIR friendly force information requirement

Figure 1. Information Requirements Categories (JP 3-0, 2006, Fig. III-3).

The challenge for the network, and indeed the challenge for network-centric operations in general, regardless of the type of conflict, is to process validated information from a multitude of sources, and maintain tracking and identification (ID) continuity on actors that matter. Because resources are limited, a balance must be struck between searching for, and maintaining awareness of, important actors. Optimizing ISR resource allocation over tens, hundreds, or thousands of networked systems would be impossible without a common method to determine actor priority. The current targeting process assigns a static priority to specific targets before the air tasking order (ATO) is flown, and that priority changes when the target is damaged or destroyed. Some individual systems have means of employing their sensor resources according to priority, but only on an individual system basis. What is required, however, is a ubiquitous, common means of assigning *dynamic* priorities to objects/actors in the operational environment. This will both allow resource optimization to occur at the speed of electrons, and also enable command and control (C2) forces to focus on battle management instead of system management. A common, dynamic prioritization taxonomy is at the heart of network-centric operations requirements.

Just as operators are constantly sifting through data and information to gather what they need to make decisions, so, too, should the network-centric systems supporting them. Battle management is a combination of risk management and resource management applied to achieving objectives in a conflict. As there are never enough resources to reduce risk to zero, the Joint Force Commander (JFC) sets priorities for the operation, and from those priorities a dynamic prioritization taxonomy can be defined for managing ISR resources, re-supply resources, etc., and for finding, fixing, tracking, targeting, engaging, and assessing (F2T2EA) targets.

This paper expands on earlier concepts outlined in various forums within the international C2 community (Donnelly, Bolia, & Wampler, 2007; Donnelly & Galster, in press, 2008). The focus here is to describe in greater detail 1) how to define a dynamic prioritization taxonomy, 2) how such a taxonomy would be used to manage an ISR network (using future military challenges in example scenarios), and, finally, 3) how common prioritization promotes concerted action by aligning individual system priorities with common network priorities.

The Dynamic Prioritization Taxonomy

When you walk into a crowded room, you see and hear information that allows you to recognize people you may already know, take note of those you don't know, and recall information that gives a rudimentary priority to those with whom you may want to interact. People within your social network may introduce you to people whom they want you to meet for whatever reason, complicating your individual set of priorities and causing you to accumulate information on people new to you. Before you arrived at the party or gathering, you likely had some idea of who would be there, what the context for gathering was, etc, and that likely set your expectations for your social interaction. In a similar way, intelligence precedes every military operation and sets initial expectations as to who the actors are in the operational environment and how they may interact. Intelligence continues to shape the commander's intent for what must be done once an operation is initiated. The commander has a vested interest in keeping track of all relevant actors in the area of responsibility (AOR), no matter in which domain they are "acting" —physical space or cyberspace. For clarity, an "actor" is defined here as a thinking human/machine system, which includes humans operating manned and unmanned vehicles, humans controlling remote systems (e.g. satellites), or simply humans themselves. Uncontrolled objects, such as minefields, ordnance in flight, etc, are not considered actors for this discussion (the authors recognize there are grey areas in this definition). An actor's priority is a function of: 1) identification (or combat ID (CID), for non-friendly forces), 2) location, or more precisely, proximity to other non-affiliated actors, 3) health/inherent capability (including changes, e.g. from a battle damage assessment), and 4) engagement status. Since those contributing factors can change over time, priority is dynamic. In a generic sense, priority results from determining who/what the actor is, where the actor is in relation to others, how capable the actor is in conducting its mission, and how readily it might be stopped. It should be clear that an Intercontinental Ballistic Missile (ICBM) weapons system has a high priority, and that priority increases once it is put on alert. So if network-centric operations are to support the commander, it might seem obvious to ask: "How does one convert those four factors into a taxonomy that machines can understand and support through automation? In other words, how does the priority get calculated? And at what point does it get recalculated? The relative weight behind each factor is also a point for consideration. What follows will highlight some aspects of the prioritization taxonomy concept, but does not attempt to prescribe the methodology so much as to foster discussion and point out the need for further research and development, and for vetting the concept with the war fighting community.

Of the four contributing factors, an actor's identification is the most important for calculating priority. For this discussion, ID is simply a categorization of an actor as: Friendly, Neutral/Assumed Friendly, Unknown, Suspect/Assumed Enemy, or Hostile (Note: This last category, Hostile, results from the CID process which is "an accurate characterization of detected objects in the operational environment sufficient to support an engagement decision" (JP 3-0, p. GL-10), typically by applying rules of engagement, the details of which are not discussed here.). ID is determined by accumulating and sharing information on an actor via ISR networks, and using the aggregate to make the characterization. At the moment an actor is detected, it is an "Unknown" to any unit monitoring the operational environment. When enough data has been accumulated and correlated with an Unknown to refine its ID, that ID is updated to reflect the characterization. For Friendly actors and others that cooperate with the ISR network to 'publish' their ID, this can be an extremely fast process. For Suspects, Hostiles, and other actors unwilling or unaware of the need to distinguish their ID, the ISR network collaborates to 'build the picture,' which takes time.

ID is actually the coarse measure from which the other three factors are refinements in determining priority, as will be explained. Location, health/inherent capability, and engagement status are interrelated, and will modify the coarse priority in interrelated ways. As a starting point, suffice it to say that close proximity is "good" if the actor is Friendly, and "bad" if the actor is Suspect or Hostile. So bad actors in close proximity to good actors will have higher priority than those further away. For actors in cyberspace, proximity equates more to the ability to affect other actors versus proximity in a physical sense (a better descriptor for "proximity" in cyberspace might be "degrees of separation," with 'quarantined' at one extreme and 'unabated' at the other). Similarly, bad actors that are healthy, or more capable, will have a higher priority than those who are incapable of creating effects, either because of inability to act (i.e. lost health) or reduced effectiveness of the weapon (lost capability). Finally, if good actors are in the process of acting upon, or neutralizing (i.e. "are engaged with") bad actors, their priority will change automatically to match the higher enemy priority which will alert the network that they need support (i.e. in the form of an accurate picture as well as monitoring for mission success).

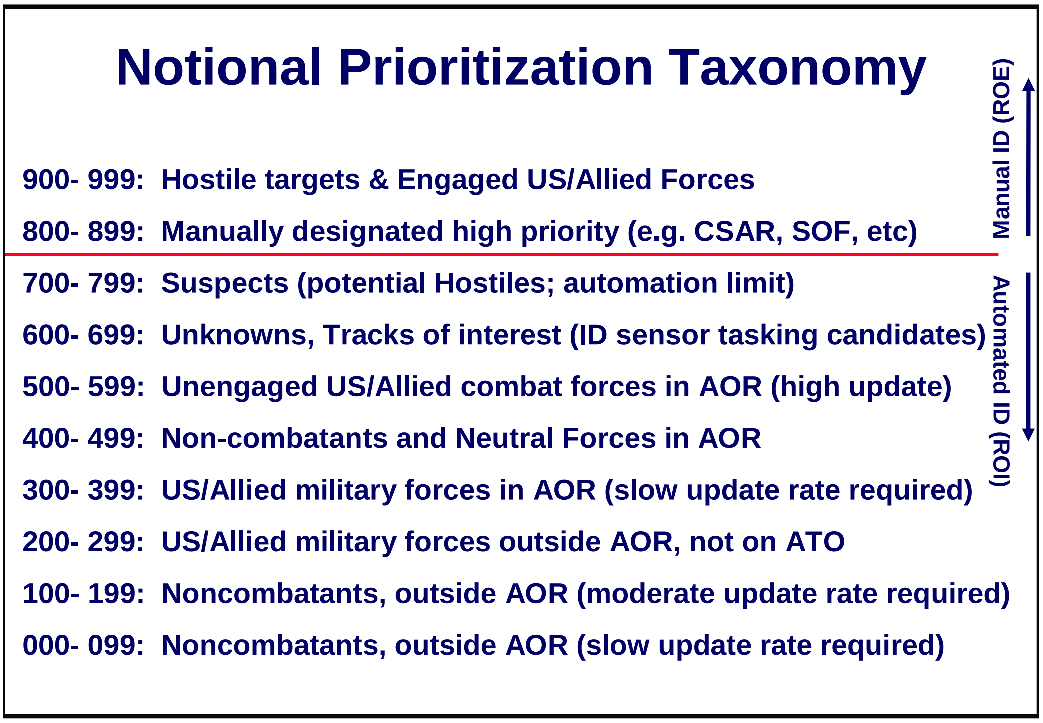
Before examining a notional taxonomy in detail, it is important to reiterate the purpose priorities serve in network-centric operations. First, priorities represent thresholds in value to the commander that enable machines capable of processing millions of value comparisons per second to allocate resources appropriately (within limitations) based on the commander's intent. Second, priorities can act as tripwires for where information is lacking or is projected to be lacking, and therefore trigger resources to be allocated to reduce or prevent gaps in data or to corroborate data where needed. In other words, resources would be expended to preserve continuity of information based upon priority. This includes coordination between sensor resources (machine to machine) that have either different vantages or capabilities to maintain tracking and ID continuity. Finally, a common prioritization taxonomy can benefit distributed teams of operators by leveling information between networked systems that collect/produce data. By auditing logged changes in priority, operators throughout the network can examine where data is being corroborated as well as help reveal sources of corrupt data.

The taxonomy described below is purely notional. Reaching agreement on a common taxonomy for network automation among a coalition of nations will require intense involvement of, and development with, the operational communities involved. The 000-999 scale was chosen because it allows enough flexibility to capture the different sub-elements of prioritization. It is important to note that, given only 1000 discrete priorities, there will be many tracked entities with the same priority. In an area of interest (AOI) of, say, a city block in Manhattan where the network of systems system is trying to track a single person of interest who is trying to employ a weapon of mass destruction (WMD), one can imagine there being thousands of 001-priority civilians walking through the streets, shopping in stores, or riding elevators in buildings. When the person of interest is positively identified as a terrorist with a biological weapon, however, his priority would automatically rise to 799 before again rising to 999 when an operator manually sets the priority to match the ID (applying rules set by the commander). This distinction between an automatic and a manual ID (and subsequently the priority value resulting) points out a key aspect of the taxonomy: the distinction between Rules of Identification (ROI) and Rules of Engagement (ROE).

ROI is best described as the logic by which an actor in the operational environment can be characterized and identified. Automating ROI requires that specific rules (e.g. an ID matrix) or logic be encoded for continual, dynamic evaluation by the network, allowing authorized operators to override the results, as necessary. As sensor data is accumulated and correlated to a particular actor, the ID is refined, but this ID can regress back to Unknown should there be any ambiguity (e.g. the white van with the terrorists under surveillance enters a tunnel; unless the ISR network can continue to track the van and its passengers in the tunnel). Ambiguities occur when two or more actors become indistinguishable by proximity (their locations are within a single resolution cell of the sensor network), or when tracking continuity is lost (the object cannot be tracked by the sensor network for a threshold amount of time). It should be obvious that the best sensors, and networks of sensors, are those that can resolve objects' IDs and locations quickly, and maintain that resolution under a variety of challenging conditions. While more costly in terms of resources consumed, positive ID (i.e. identification confirmed to the satisfaction of the commander or delegated ID authority) is a prerequisite for any weapons employment.

ROE, on the other hand, involves human reasoning that isn't easily captured in machine logic (e.g., legal limits that may apply to some forces and not others, or combinations of rules, some of which may change from day to day). Unlike ROI, with the focus on establishing and maintaining ID, ROE seeks to determine intent (friendly or hostile), and can lead to weapons employment. Because weapons should never be employed without a human operator making the decision, for both moral and legal reasons, the prioritization taxonomy below assumes network-centric operations that limit automatic IDs to "Friend," "Neutral/Assumed Friend," "Unknown," or "Suspect" (i.e. dynamic priorities of 799 or less), which is below the threshold for engagement. Priorities above 799 are reserved for manual input only.

As a starting point to the detailed description of the taxonomy, Figure 2 outlines the top-level discrimination between priority classes.



Notional Prioritization Taxonomy

900- 999:	Hostile targets & Engaged US/Allied Forces
800- 899:	Manually designated high priority (e.g. CSAR, SOF, etc)
700- 799:	Suspects (potential Hostiles; automation limit)
600- 699:	Unknowns, Tracks of interest (ID sensor tasking candidates)
500- 599:	Unengaged US/Allied combat forces in AOR (high update)
400- 499:	Non-combatants and Neutral Forces in AOR
300- 399:	US/Allied military forces in AOR (slow update rate required)
200- 299:	US/Allied military forces outside AOR, not on ATO
100- 199:	Noncombatants, outside AOR (moderate update rate required)
000- 099:	Noncombatants, outside AOR (slow update rate required)

Figure 2. Notional Prioritization Taxonomy for Network-Centric Operations.

There have been some refinements in the taxonomy since earlier publications, but the key points to draw from Figure 2 are reiterated as follows:

1) ***The ID process can only be automated to a point.*** At that point, operators manually apply rules of engagement based upon their training and experience to determine which actors meet the criteria to be designated Hostile. Automating the integrated C2 and ISR network of systems to produce and maintain IDs should therefore be limited, and that limit is the threshold between ROI and ROE (depicted here by the line between Suspect and Manually-designated priority classes). No weapons should ever be employed based on a system-only ID without an authorized operator making that determination (i.e. applying ROE and manually changing the ID to Hostile).
2) ***The manually designated class (i.e. 800s) is reserved as a special class*** of actors with an operator-assigned high priority. This class of priority might include unengaged battle-damaged US/allied forces returning to base, special operations forces (SOF), combat search and rescue (CSAR) forces, forces on alert, special payload missions, etc.
3) ***New actors to the network, or "Unknowns," enter with a reasonably high priority (600s).*** This triggers the ISR network to accumulate data and correlate information to assign an ID (e.g. Friend, Assumed Friend, Unknown, and Suspect are the automatic ID categories; Hostile designation is reserved for operators with ID authority). It is important to keep the number of Unknowns to a minimum, especially in a high-threat environment where weapons are actively being employed. This class will usually be the primary focus of ISR assets' network collaboration, as establishing ID is critical.

4) This taxonomy is based on the earlier referenced concept that ***priority is a function of ID (or CID), location/proximity, organic health/capability, and engagement status***. Further explanation within taxonomy classes follows below.

5) ***When US/Allies forces engage, or are engaged by an enemy (Hostile), their priority automatically rises to match that enemy's priority.*** This insures that required tracking accuracy and continuity are maintained on both the Friendly and Hostile actors throughout the engagement: a) to insure mission success; and b) to provide other support as quickly as possible (e.g. in the event search and rescue is required). For kinetic operations, accurate histories are critical for relief and/or recovery. For both kinetic and nonkinetic operations, accurate histories of actors are critical for archival.

6) ***Priorities are associated with every actor in the operational environment (geo- and cyberspace), not just targeted systems.*** Priority is a dynamic measure of an actor's relevance in the operational environment, whether that be for targeting, collecting intelligence, and monitoring (i.e. against Suspect/Hostile units), or for providing ISR support, rescue/recovery operations, and coordinating mutual protection (i.e. for Friendly units). For clarification, inanimate targets (i.e. not human-machine systems as defined by 'actor') also are assigned priorities within the targeting process independent of the dynamic priority discussed here used for ISR management.

7) Finally, ***higher priority actors require more resources to either positively ID them, maintain their tracking continuity, or both.*** Should the network performance ever degrade (e.g. in a cyber attack), the lowest priority actors' data should be the first to suffer, and the network should be alerted in all cases where degradation occurs. Typically, the network is going to require more accuracy on high priority actors.

The Devil's in the Details

Although some questions may arise when first confronted with the information presented in Figure 2, the logic behind the basic classes of priority should be clear, as they generally follow ID as the primary determinant. As stated earlier, proximity/location, health/capability, and engagement status are interrelated, and factor somewhat differently depending on the class within the taxonomy to which they are applied.

1. Hostiles (900-999): Once an actor has met the ROE criteria and been determined to be Hostile by an operator with ID authority, the next most important factor is whether it is engaged by Friendly forces or has been requested to be engaged (e.g. by a Friendly in self-defense). Those that are cleared to be engaged or currently being engaged, assume a 950-999 priority, with the tens digit (5-9) signifying the relative capability of the hostile to affect friendly forces (i.e. a combination of health and organic capability). A Cessna aircraft being used as a weapon would have a lower priority than a Boeing 757 over New York City, for example. A Cessna aircraft carrying a dirty bomb (i.e. greater capability than just a fueled aircraft) might have a greater priority still. The ones digit is reserved as an indicator to the ISR network of the tracking and ID accuracies required to complete the engagement. A "9" might indicate very high precision required to prevent collateral damage, whereas a "0" might indicate low precision is acceptable. Again, once a Friendly is engaged with a Hostile, either offensively or defensively, both priorities reflect the Hostile priority to alert the ISR network to support the engagement, as required. Hostiles not cleared to be engaged would assume 900-949 priorities, and the tens and ones digits would parallel those of the 950-999 set. A variety of circumstances might prevent a commander from clearing a Hostile for engagement, including unconfirmed intelligence showing the target has been destroyed or neutralized, a desire to monitor the Hostile to gain further intelligence, or an engagement proximity that would result in poor Friendly resource management. Typically, a lot of effort and resources have been used to reach a positive Hostile ID, so it's imperative that both tracking and ID continuity be maintained. Thus, Hostiles and those Friendly forces engaging them are the highest priority actors.

2. *Manually-designated High Priority actors (800-899):* This priority class does not correlate with an ID category, per se, but is a placeholder for any of a number of special missions (i.e. Friendly or Assumed Friendly) as well as any mission that may require more from the network's ISR resources. As the title implies, actors are given this priority manually, and instances where this might occur include: Friendly forces experiencing non-combat related emergencies, alert forces, high value platforms, forces available to support time-sensitive missions, etc. Specific network-centric support could be assigned to given priorities within this class, but that is left out of this discussion. As this is a class reserved for Friendly actors, it is conceivable that rules to semi-automate, or recommend, ID changes to this class could be created. The notion is that some Friendly actors will need to be manually made distinct in the network, and this is the placeholder class. By making such a distinction, everyone in the network could quickly recognize where high priority Friendly actors are.

3. *Suspects, potential Hostiles (700-799):* Once the ISR network has accumulated and correlated enough information about an Unknown to meet ROI criteria for Suspect, the priority automatically changes to 700-799 with the ID change, and, just as specified in the 900s, those not within proximity to be monitored directly would fall within 700-749, while those to whom US/Allied forces are directed to investigate, shadow, or otherwise intercede would be 750-799. Suspects would closely parallel the categorization of Hostiles, just without the application of ROE, and subsequently the lower priority. The tens digit again would be used to show levels of health/capability and the ones digit reserved to show required tracking and ID accuracies required from the network. As an example, in the Cold War, the Tu-95 Bear bombers surveilling the US coastal defenses would have a priority of 79X once identified (required accuracy left to be determined in this example). The F-15Cs, or other aircraft flying the intercept mission, would also have priority 79X when scrambled and while shadowing the bomber. Just as in the case for Hostile actors, significant resources have typically been expended to reach a Suspect ID characterization; their priority reflects the desire to maintain tracking and ID continuity.

4. *Unknowns, tracks of interest (TOIs) (600-699):* Any new actor awaiting additional data accumulation and correlation falls into this category, as do all actors that have become ambiguous to the network, through either active or passive means. Similarly to Suspects (700s) and Hostiles (900s), engagement status defines the break between 600-649 and 650-699. Also like Suspects and Hostiles, the tens digit might signify a developing ID as to health and capability (e.g. a fast moving ground vehicle approaching a checkpoint (65X), a facility possibly dedicated to cyber attack (68X), or a white van with unconfirmed intelligence that it contains an armed group of terrorists in a European city (69X)). Unlike the Suspects and Hostiles, however, an Unknown characterization causes the network to quickly accumulate and correlate data to resolve its ID while maintaining tracking continuity, which places a greater burden on the ISR

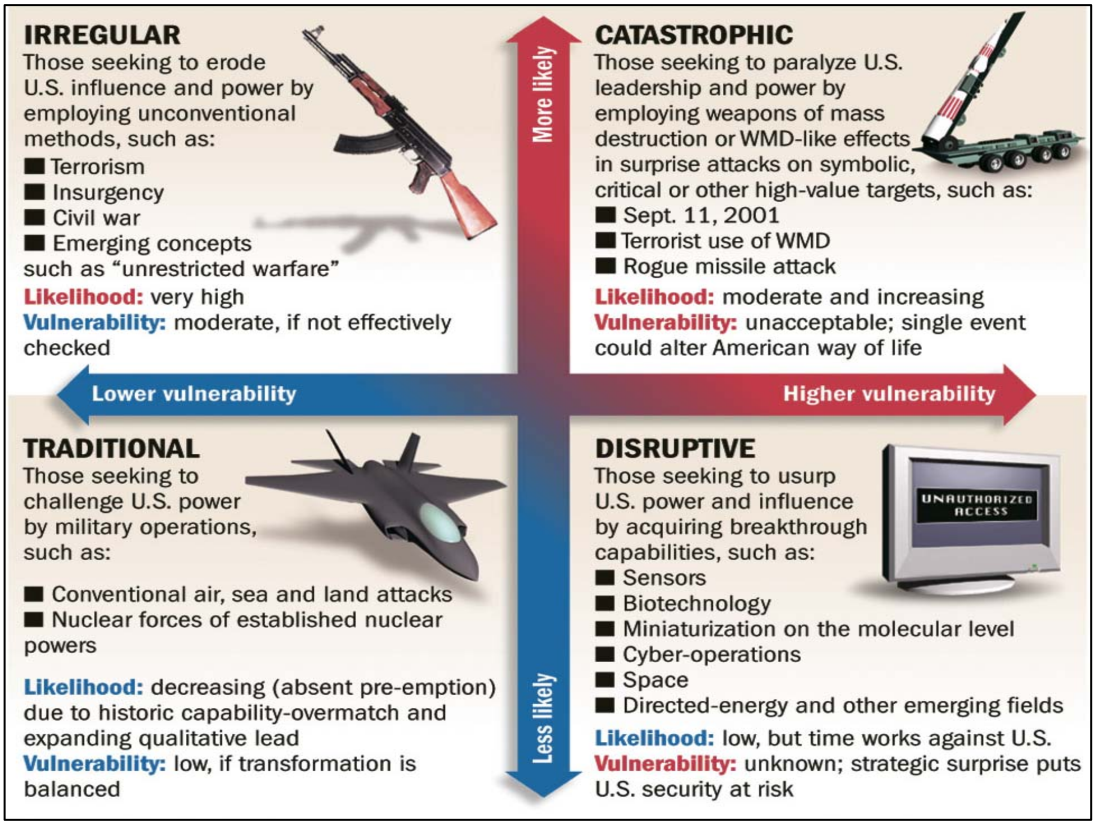
network. Because of this, and the desire to minimize Unknowns in the operational environment, it is important that the network resolve Unknown IDs quickly and efficiently. This class will therefore require the greatest degree of sensor-to-sensor collaboration (i.e. automation), typified by technology like the Network-Centric Collaborative Targeting advanced concept technology demonstration (NCCT ACTD; Carson, 2004). For Unknowns, the ones digit in the priority might represent different sensor requests to trigger unscripted forms of machine to machine collaboration versus required collaboration to maintain tracking and ID already established.

5. Unengaged US/Allied forces in the AOR (500-599): In the future, most if not all of those combat forces considered Friendly will have a means of quickly confirming their ID to the network. Until that is true, there are a host of cooperative means of identification for Friendly forces (via interrogation/response or datalink methods) with varying degrees of accuracy. Although these forces are not engaged, their priority is higher amongst most Friendly/Assumed Friend classes because of their potential for combat and requirement for a higher update rate to maintain tracking and ID continuity. Those actors with a self-reporting capability would fall into the 500-549 window, those without would be in the 550-599 band, with the tens and ones digits being used to signify either system capability or other distinguishing characteristics for network resource management. As a cyberspace example, a critical information node might have a priority of 549, or be manually assigned 899. Once attacked and defensive, the same node might be 999, pending the source and capability of the attacker.

6. Remaining classes (000-499): The principal logic behind the remaining classes is one of ISR update rate required, because they are either Friendly, Neutral, or have no potential for combat. The highest priority class is the noncombatants and neutral forces (e.g. UN or Red Cross units) in the AOR, as they have the highest likelihood of either being misidentified, attacked by Hostile forces, or otherwise threatened. The next class (300-399) represents those US/Allied forces in the AOR that require a lower update rate, as their location or status may change less frequently, requiring less effort from the ISR resources. Those that could report their own position/status might have the lower band, 300-349, just as in the case for the combat forces in the AOR (500-549). Below a priority of 300 are actors not considered in the AOR, and their priority should be self-evident. It is worth pointing out that in a conflict with terrorists, where there is no defined AOR, a parallel method of defining priority classes might be to use the Threat Conditions (i.e. have areas designated as High condition (Orange) equate to "within the AOR") outlined in Homeland Security Presidential Directive 3 (The White House, 2002).

Applying the Taxonomy to 21st Century Military Challenges

"Although U.S. military forces maintain their predominance in traditional warfare, they must also be improved to address the non-traditional, asymmetric challenges of this new century. These challenges include irregular warfare (conflicts in which enemy combatants are not regular military forces of nation-states); catastrophic terrorism employing weapons of mass destruction (WMD); and disruptive threats to the United States' ability to maintain its qualitative edge and to project power." (DoD QDR, 2006, p. 3, see Figure 3)



IRREGULAR
Those seeking to erode U.S. influence and power by employing unconventional methods, such as:
- Terrorism
- Insurgency
- Civil war
- Emerging concepts such as "unrestricted warfare"

Likelihood: very high
Vulnerability: moderate, if not effectively checked

CATASTROPHIC
Those seeking to paralyze U.S. leadership and power by employing weapons of mass destruction or WMD-like effects in surprise attacks on symbolic, critical or other high-value targets, such as:
- Sept. 11, 2001
- Terrorist use of WMD
- Rogue missile attack

Likelihood: moderate and increasing
Vulnerability: unacceptable; single event could alter American way of life

TRADITIONAL
Those seeking to challenge U.S. power by military operations, such as:
- Conventional air, sea and land attacks
- Nuclear forces of established nuclear powers

Likelihood: decreasing (absent pre-emption) due to historic capability-overmatch and expanding qualitative lead
Vulnerability: low, if transformation is balanced

DISRUPTIVE
Those seeking to usurp U.S. power and influence by acquiring breakthrough capabilities, such as:
- Sensors
- Biotechnology
- Miniaturization on the molecular level
- Cyber-operations
- Space
- Directed-energy and other emerging fields

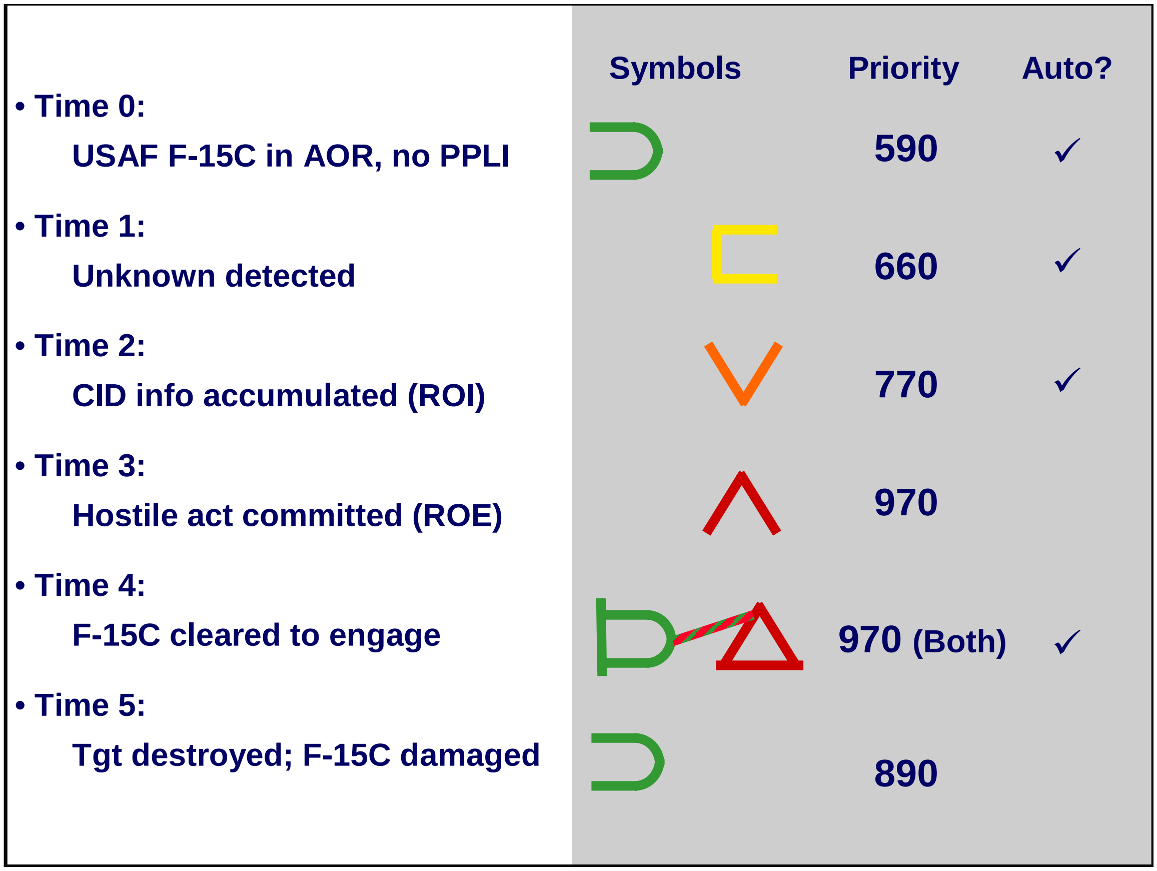
Likelihood: low, but time works against U.S.
Vulnerability: unknown; strategic surprise puts U.S. security at risk

Figure 3. Military Challenges for the 21st Century (derived from DoD QDR, 2006, p.19).

As stated earlier, priority is a dynamic measure of an actor's relevance to the operational environment, whether that is for targeting, collecting intelligence information, monitoring, or some other purpose. Because priority is derived from Commander's Intent, it should be relatively independent of the type of military challenge faced. To illustrate this, two of the challenges highlighted in the National Defense Strategy of 2005 (DoD NDS, 2005) and reiterated in the Quadrennial Defense Review (QDR) of 2006 (DoD QDR, 2006) will be considered with examples highlighting the taxonomy in practice.

Traditional Challenges

In traditional warfare, achieving air superiority is critical to dominating the battlespace, establishing the operations tempo, and maintaining the initiative. The following example illustrates the prioritization taxonomy for network-centric operations in an air-to-air engagement scenario. Note that some of the dynamic prioritization is automatic, while some is operator-driven. Figure 4 outlines the scenario's progression over time. The symbols themselves would appear on a geospatial display, moving on the display as detected and reported by the ISR network. The priorities are attributes of each entity, and that information may or may not be displayed by the operator, but would factor into the network's automation of sensor resources to maintain tracking and CID continuity (the ones digit is not used in this example for any purpose).



	Symbols	Priority	Auto?
• Time 0: USAF F-15C in AOR, no PPLI		590	✓
• Time 1: Unknown detected		660	✓
• Time 2: CID info accumulated (ROI)		770	✓
• Time 3: Hostile act committed (ROE)		970	
• Time 4: F-15C cleared to engage		970 (Both)	✓
• Time 5: Tgt destroyed; F-15C damaged		890	

Figure 4. Dynamic prioritization in an air-to-air scenario.

The scenario unfolds as follows:

1) At **Time 0**, a USAF F-15C on a combat air patrol (CAP) mission is searching the Area of Responsibility (AOR) with its radar, and is not reporting its own position via the data-link (i.e. no precise position location information (PPLI)). The Blue force 4-ship has an automatic priority 590, based on CID, location, weapon system capability, and engagement status.

2) At some point during the mission, **Time 1**, an unknown airborne object is detected and automatically given priority 660, triggering the ISR network to rapidly accumulate data to better the ID. The flight on CAP is alerted to the Unknown via datalink.

3) When specific information is correlated to the track, **Time 2**, the system automatically generates a new ID of Suspect based on the ID matrix encoded into the system in accordance with the daily instructions. The priority for a Suspect at that location is 770, and the category change focuses surveillance operators' attention to apply training and expertise and watch for ROE determinants to be met.

4) At **Time 3**, the Suspect track commits a hostile act, noted by ISR operators in the network, who then recommend to the ID authority that the ID be changed manually to Hostile. By manually changing the ID, the priority automatically rises to 970 (again, based on CID, location, capability, etc).

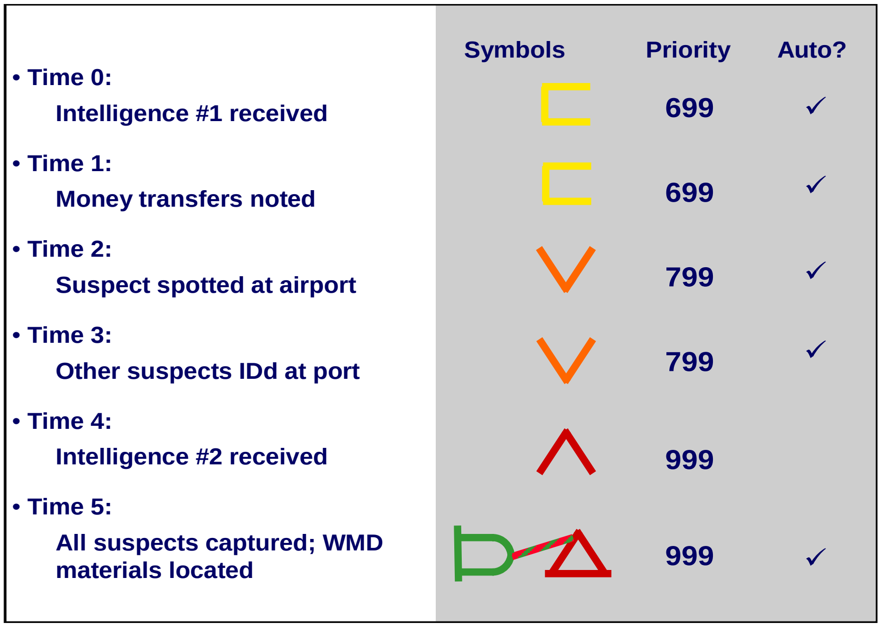
5) According to the ROE, this ID change also triggers the F-15C on CAP to engage the Hostile, now at **Time 4**, and the F-15C's priority automatically rises to 970 as well once the pilot has begun the engagement (triggered by an event in system employment such as an engagement radar mode or datalink message declaring the engagement).

6) Finally, at **Time 5**, the engagement is over with the target destroyed, but the F-15C flight has one battle-damaged aircraft. They communicate this to the C2 operator who manually sets the track priority to 890 until the aircraft is recovered safely at its base. This higher priority insures the ISR network keeps the track quality high in case the damaged aircraft is lost and search and rescue efforts are needed. It also alerts the CSAR crews to the potential for a mission or to increase their state of alert.

Irregular Challenges and the Possibility of Catastrophe

Defeating terrorist networks and preventing non-state actors from acquiring WMD are two of the four priorities described as the focus of the 2006 QDR. Because terrorists seek to hide within populations, and because they use publicly accessible tools like the internet for some of their communication, surveillance and reconnaissance efforts take on a different shape than in the case of traditional warfare with state-sponsored militaries. Intelligence efforts are heavily reliant on human intelligence (HUMINT) to find these bad actors which are humans, for the most part, or teams of humans as opposed to aircraft, ships or columns of tanks being operated by humans. The prioritization taxonomy is just as applicable, if not more critical, in Irregular Warfare scenarios as it is in traditional scenarios. The ISR network supporting the tracking and identification in terrorist scenarios is quite a bit more saturated with data as the Hostiles are intentionally trying to hide (i.e. remain ambiguous to the ISR network), and they do not follow any conventions of warfare, either legal or ethical, and seek to attack noncombatants. Terrorists also exhibit what most consider irrational behavior by using suicidal attacks as a primary method of weapons employment. So not only is the ISR network stretched to its limits trying to find "needles in a haystack," but it is constrained by time as well. These Hostiles, once found, tend to be very time sensitive, employing their weapons indiscriminately to preserve their human network and future operations.

In the case of a terrorist looking to employ a WMD (the upper right quadrant of Figure 3), ID and location relevance should be clear. The terrorist's location with respect to a population center will establish how much time a commander has to decide and act, as well as the magnitude of the alerting and or disaster recovery operations required. Again, the difficulty is in the identification and tracking processes to prevent the opportunity for weapons employment at all. In this scenario, once the terrorist has an armed weapon, the contest is probably over. It then becomes a question of limiting the damage and damage response, which can be automated to a certain extent based on the capability of the weapon and its employer. Inherent capability includes both the capability of the weapon, and the capability of the transporting system (in this case, the terrorist himself, and whether he's healthy, wounded, capable of employing/detonating the weapon, etc). Engagement status includes whether the terrorist is being prosecuted as a target already, and the need to support the friendly forces conducting the mission which might include efforts to quarantine the area where the damage is expected. One can imagine that a healthy terrorist with an armed WMD within a population center would have a high, if not the highest, priority among the Hostiles in the network. The priority would trigger continuous cross-cueing among sensors for tracking and ID continuity, and would also alert the varying responders as well as others within the zones of anticipated damage. Losing such a target in a crowd would be unthinkable and potentially devastating, and relaying accurate information on target location and ID would be critical to engaging forces as well as other ISR elements in the network that can maintain the tracking. Once a target is lost to Unknown status, the area to be searched grows with time relative to the capability of the actor to move. It is much more efficient to maintain track on a very high priority target once IDed than to try to reacquire that target in a large population after even a few minutes of ambiguity.



	Symbols	Priority	Auto?
• Time 0: Intelligence #1 received	⊏	699	✓
• Time 1: Money transfers noted	⊏	699	✓
• Time 2: Suspect spotted at airport	∨	799	✓
• Time 3: Other suspects IDd at port	∨	799	✓
• Time 4: Intelligence #2 received	∧	999	
• Time 5: All suspects captured; WMD materials located	⊐–△	999	✓

Figure 5. Dynamic prioritization in a Terrorist/WMD scenario.

In this scenario there are both similarities and distinct differences with the traditional combat scenario. Figure 5 outlines the scenario's progression over time. This is how the scenario unfolds:

1) At **Time 0, intelligence is received** that a specific person with no criminal record is connected to a terrorist network and will be traveling to the US to join a group planning a WMD event for a coastal US city. The individual's location is not currently known, and so the network generates an Unknown with most likely position, cueing ISR elements to search for him. Multiple agencies are alerted as to his probable location and potential mode of travel.
2) According to the intelligence received at Time 0, specific electronic money transfers would potentially identify subjects that the first individual would be meeting in the US. At **Time 1, those transfers are noted** and lead to more individuals being tracked, with other affiliations that cause them to be IDed as Suspects. Agencies are alerted to monitor all individuals 24/7.
3) At **Time 2, the first Suspect is identified** at a customs desk at a US airport, triggering elements from different agencies to act. The ISR network tracks the individual to a port.

4) At **Time 3, other individuals associated with the financial transfer are IDed** and tracked; all individuals come together in a private facility at the port.
5) At **Time 4, updated intelligence is received** that the individuals have received some components of a WMD device and will be traveling to another port location for the rest.
6) At **Time 5, all individuals are apprehended** and taken to a detention center awaiting sentencing.

While this scenario seems more like a police action than a military scenario, it shows the integration of agencies and cross-cueing required to prevent a catastrophic event. Although simplified as an example, this scenario would include military and nonmilitary government agencies as various jurisdictions, ISR systems, and methods would be involved. The bottom line requirement, however, is to prevent fabrication and employment of a WMD, and by employing the common prioritization taxonomy, ISR systems (including HUMINT, in this case) work together to support locating and apprehending the terrorists (i.e. create the effects desired by the commander).

Allocating Resources and Leveling Information

"The QDR…reflects the thinking of the senior civilian and military leaders of the Department of Defense: [Including the] *Need to "find, fix and finish" combat operations against new and elusive foes."* (DoD QDR, 2006, p. vi)

Finding, fixing, and finishing elusive foes in the operational environment requires sifting through data for what's relevant, maintaining and expanding on what has been found of relevance, and resolving discrepancies to prevent errors in the finishing phase. ISR resources are limited, and therefore prioritization helps establish where the 'budget' is expended fixing and finishing beyond the 'sunk cost' of finding. Elusive foes are going to require more resources both in finding as well as fixing—it simply takes more sensing to find and maintain track on non-cooperative actors. On that note, there are certain expectations for the difficulty of performing an ID on any actor, and those that remain elusive beyond what is considered normal actually trigger increased surveillance response. Similarly, once a priority actor is being tracked, the ISR network needs to monitor its own ability to maintain tracking and ID continuity, resulting in close coordination between sensor systems. As an example, an unmanned aerial vehicle (UAV) with an electro-optical sensor is tracking a suspected terrorist, but the vehicle the terrorist is traveling in is about to go into a tunnel. ISR network operations would include cross-cueing the Transportation Department sensors in the tunnel to maintain positive track on the vehicle and occupants until the UAV can reacquire on the far side. Additionally, if those sensors provide a better image of the suspect's face, cross-cueing the intelligence networks with the image might expedite the ID that could lead to apprehension.

Not every sensor or intelligence system in the ISR network is going to have the same capabilities. All will have some capability to track and/or perform identifications on actors. Because there are these differences in capabilities, vantage points, and duty cycles, information within any one system is a subset of the network information. At any point in time, a given ISR system should have not one but three IDs on any actor in the network: (1) the ID communicated and held in the network by the ID authority, (2) the ID achieved by the organic capability of the individual system, and (3) the ID that operators working with that individual system believe is correct based on their training, experience, and information (i.e. acquired outside of the network, and/or not yet recognized by, and approved for, the network). If information throughout the network is congruent or "level," these 3 IDs would all be the same—ID harmony. More typical are situations where some percentage of the total network information is in conflict as a result of correlating correct with incorrect ID information, or accurate with inaccurate position information. The notion of information leveling is that, over time these conflicts will be identified and corrected, improving network operations for all systems. Using common priorities, information on the highest priority actors would be addressed and corrected first, as resources to correct errors would be allocated according to priority. The difficulty is that this assumes an uncompromised network (i.e. all the data is from trusted sources). If network data is corrupt, having a common priority taxonomy could actually work against efficient ISR management, allocating resources to falsely high priority actors. Conversely, by automatically or manually auditing logged changes in actors' priorities, operators throughout the network can examine where data is being corroborated as well as help reveal sources of corrupt data. This is why it is important to maintain both the organic ID from the individual system (which, if found to be corrupt, is more readily quarantined from the network; if not found to be corrupt, may help redress the network ID) and the ID held by the network (as approved by the commander's designated ID authority). Because of the potential for either incorrect or corrupt data influencing what network operations automatically produce, operators should always have the ability to manually change an actor's ID and/or priority, if they have reason and authority to do so.

Common vs. Individual Priorities and the Need for Self-defense

A concern with any team arrangement (i.e. where some independence is relinquished by the individual as a means of better supporting a "team") is that individual needs will not be satisfied as a result of team membership. As an example in combat operations, that might equate to a combat air controller having to call in strike coordinates from a position that increases his/her own potential for becoming a casualty. In this instance, the controller might be assigned a priority of 899 to prevent a fratricide. The intent of having a common set of priorities for actors in the operational environment is to better manage ISR resources and not impede self-defense or individual mission management. Instead, by knowing where the priority actors are across the network, individual members of the network can better contribute their resources and capabilities when the network needs their help. For instance, a cyber attack creates a failure within a portion of the network preventing key C2 nodes from transmitting information to defense units to counter the strike. Designated reserve units monitoring the attack could step into primary roles to respond offensively and defensively until the affected C2 nodes are back online. On the kinetic side, a strike has occurred at a remote location and the scheduled ISR asset for performing battle damage assessment (BDA) unexpectedly cannot fulfill its mission. Other non-traditional ISR assets in the immediate area (e.g. a SOF team) could recognize the unfulfilled request on the high priority target and either perform the BDA without being directed, or publish to the network their ability to perform the BDA, if requested/required. In the first example, the C2 nodes under attack would automatically pick up a high priority to match the attacker, and the network would compensate to support the attacked units. In the second example, scheduled information that might affect a high priority target is not filled on time, cueing the network to fill the requirement with available capacity. In both cases, assets conducting their primary missions are affected, and because they are of high enough priority to warrant immediate support, secondary or reserve units in the network recognize the need and offer assistance. In neither case is self-defense sacrificed to support the "team," conscious decisions are made based on priority and capacity to support, and network operations are more efficient as a result.

Alternatively, with common priorities across the network, individual systems can anticipate where their capabilities might be needed as the plan unfolds. As contingencies occur, friendly actors can volunteer support where none had been pre-planned. As an example, a terrorist manages to escape from being killed in a situation where unacceptable collateral damage would have occurred, but in the process of escape moves into an area where other friendly actors not assigned to the mission can complete it. As long as the ISR network can either maintain the track, or rapidly reacquire and ID the Hostile actor, the "team" can support the individuals assigned primary roles in the mission. Every actor, Friendly or Hostile, has the ability to influence some area around them with their capabilities. Common priorities across the big picture allow individuals to act within their "spheres of influence" and recognize or anticipate when to look beyond their intended role or offer support when it is needed.

Conclusion

> *"It will not be enough to implement network-centric capabilities, conduct network-centric operations (NCO), and test the theory of NCW only in a "critical mass of the joint force" or in certain high priority units. Instead, the capabilities must be developed and the theory applied enterprise wide, i.e., throughout the DoD."* (OSD, 2005, p.11)

It would be foolish to think that warfare in the future will be fought using outdated methods of the past. With the advent of the Information Age has come the ability and requirement to manage networks of surveillance and reconnaissance assets with both greater speed and greater accuracy. If given the choice, and were it possible, the JFC would want his subordinate commanders to share a true picture of the operational environment at all times. It is difficult enough synchronizing efforts and maintaining the initiative knowing all relevant information accurately. It can be impossible to do either if the picture is inaccurate or presented with so much latency as to be irrelevant. A notional prioritization taxonomy was presented here as a first step in defining network-centric operations (i.e. where to focus, and where to trigger coordinated actions) that allow ISR resources to perform some functions automatically at the speed of electrons.

An actor's priority is a function of CID, proximity to other actors, health/capability, and engagement status. It is important to interrelate who the actor is with where he is relative to his ability to create effects, and then correlate that with allied forces that might be able to affect his plans. Those factors change over time, and as a result priority is dynamic. Whether the US and its allies are faced with a large conventional force, or a small group of terrorists seeking to employ WMD, the concept of dynamic priority applies. As a nation, we have to manage resources and risk simultaneously to defend against the spectrum of future threats, whether they are near peers in a war of attrition or needles in haystacks that seek to go unnoticed until it is too late. Without collaboration between systems in network-centric operations, resources will not be managed efficiently, and missing a single high-priority target could have devastating results.

In managing ISR resources, the goal is effectively to have a truth “window” on the world, but given resource limitations, it becomes important to find, fix, and finish relevant, higher priority actors while being cognizant of lower priority actors all at requisite levels of accuracy for a consistent less-than-truth picture. The process of finding and fixing becomes infinitely faster when automatic sensor-to-sensor coordination is enabled, while preserving the operator’s ability both to focus on the results of the automation and manually apply ROE, as well as to override those results manually when necessary. Tracking and ID continuity are critically important, as breaks in either result in further consumption of ISR resources and potentially mission failure. Dynamically assigning priority helps the ISR network resolve conflicts, focus resources, and establish IDs faster, all in concert with the commander’s intent, allowing operators to manage the network itself and respond to the resulting picture produced.

Common ubiquitous priorities harmonize network-centric operations. While not every actor can affect every other actor at any given moment, being aware of other actors considered high priority in the commander’s eyes opens the door to creating effects when opportunities present themselves. At the very least, common prioritization will facilitate mutual support and communication, self-defense, and mission success. At best, the network of US and allied actors in the operational environment will find, fix, and finish Hostile actors in marked symphony, and will have new metrics to measure how efficiently they balanced risk against resource consumption in achieving the commander’s intent.

References

Carson, B. (2004). Networked sensors aid targeting. *Military Aerospace Technology, Online Ed.* 3:3 (November 15, 2004).

Donnelly, B.D. and Galster, S.M. (2008, in press). Designing net-centric interfaces to capture commander’s intent. DDRC Press, Toronto, Canada..

Donnelly, B.D., Bolia, R.S., and Wampler, J. (2007). Capturing commander’s intent in user interfaces for network-centric operations. *Proceedings of the 12th International Command and Control Research and Technology Symposium, June, 2007, Track 4, Paper 050.*

Office of the Secretary of Defense. (2005). *The Implementation of Network-centric Warfare*. DoD, 5 January 2005,Washington, DC: Author.

The White House. (2002). *Homeland Security Presidential Directive 3*. The White House, March 2002, Washington DC: Author.

Joint Publication 3-0, *Joint Operations*, US Government Printing Office, 17 September 2006 (p. III-10). Washington, DC: Author.

U.S. Department of Defense. *The National Defense Strategy of the United States of America*. DoD, March 2005,Washington, DC: Author.

U.S. Department of Defense. *Quadrennial Defense Review Report.* DoD, 2006,Washington, DC: Author.