9th International Command and Control Research and Technology Symposium Coalition Transformation: An Evolution of People, Processes, and Technology to Enhance Interoperability

Topic: Operational Requirements to Network Centric Applications

Operational Trust: A New Look at the Human Requirement in Network Centric Warfare

Author: Major Nicole Blatt, USAF

Naval Postgraduate School, Monterey, CA
Student Paper

21 May 2004

815B Oceanview Blvd
Pacific Grove, CA 93950
Telephone: (831) 647-1883
Email: niblatt@nps.edu

Introduction

Everyone agrees that the new information technology systems affect the way we fight wars. Advocates from the President of the United States[1] to NATO leaders even recognize the information revolution in military affairs (RMA) and prescribe the need for major operational changes. However, the opinions of *how* the command and control operations should change are often diametrically opposed. Leading civilian authorities in network centric warfare profess a decentralized control system called self-synchronization. Meanwhile, the U.S. military leadership sponsors new technology experiments that often centralize control and increase micromanagement. Could these differences stem from a different assessment of operational trust?

An enduring principle for increasing efficiency and effectiveness of command and control has always been "centralized command, decentralized execution." In network centric warfare, this can be optimized through an approach called self-synchronization. However, certain necessary conditions must first be met for self-synchronization to succeed. The authors of the book, *Power To The Edge*, state that these conditions include "Trust in the information, subordinates, superiors, peers, and equipment"[2] Can this condition be met?

Meeting this condition asks a lot from military leaders, decision-makers, operators, effectors, managers, industry – basically, everyone who is in some way involved with network centric operations. Everyone knows that teams that work together can be more efficient, and a key aspect to working as a team is trusting one another. But trust is not something that can be ordered. You cannot expect people to trust each other just because someone directs them or it is part of the doctrine. Yet many people that discuss trust just expect it to be readily available regardless of its earned value. Instead, trust needs to be examined from a realist's perspective. By examining the nature of trust, we can determine the factors it relies on. Perhaps, by concentrating on improving those factors in a network centric environment, we may be able to increase the level of trust among entities. This, in turn, will allow for more effective and efficient operations in network centric applications such as those involving self-synchronization.

This paper tackles the requirement to trust in network centric warfare. After a short summary of network centric warfare and self-synchronization, this paper will explain a new definition of *Trust* and introduce a new concept, called *Operational Trust*. I will then explain why there is a need for trust, and follow with factors to make it easier to trust. Finally, I will give a real-world example of how the decision-making process involving trust demonstrates our need to develop systems, practices, and concepts of operations keeping in mind the need to trust.

Network Centric Warfare and Self-Synchronization

Before delving into the nature of trust, it is important to ensure we have a common understanding of network centric warfare and self-synchronization. It is from this basis that we will later apply the factors of trust.

Network Centric Warfare (NCW) is a new approach to warfare that strives to build shared battlespace awareness and knowledge across geographically dispersed forces. Conceived from technical advances associated with the information revolution in military affairs (RMA), NCW provides the catalyst for military transformation, exercising new processes of command and control. Warfighters at all levels from the lowest echelon gunner to the Chief of Staff can access a common operating picture of the battlespace and have superior situation awareness (SA). When put into practice, these information systems affect the way we fight wars.

According to the U.S. Office of the Secretary of Defense C2ISR Center, network centric warfare is defined as the concept of organizing and distributing critical, tactical information, via high-speed data links and networking software, to increase efficiency and effectiveness of military command and control.[3] This awareness and knowledge is then leveraged to increase the efficiency and effectiveness of actions. NCW is more than just advanced data links systems – it requires the co-evolution of doctrine, concepts of operations, force structure, and tactics. Advocates predict it will improve combat power by increasing the speed of command, tempo of operations, lethality, and survivability. Experts in NCW list three key concepts that should be emphasized when explaining the idea : 1) forces can be geographically dispersed; 2) troops are more knowledgeable; and 3) one can achieve effective linking among entities.[4]

Self-synchronization is an approach to command and control that exploits the key concepts of NCW to provide the most efficient and effective results. Self-synchronization, also called self-coordination, is an effort to "increase freedom of low level forces to operate near-autonomously and re-task themselves through the exploitation of shared awareness and commander's intent."[5]

How self-synchronization works can best be explained by examining a decision process. Command and control has been based on decision loops such as John Boyd's famous OODA loop – observe, orient, decide, act. The speed at which this cycle occurs affects the speed of command and ultimately the tempo of operations. The speed of command increases by applying the philosophy "centralized command, decentralized execution." As technology improves, the cycle-time of the decision loop also shrinks accordingly. With the goal of reducing the decision cycle time even further, self-synchronization comes into play. In self-synchronization, the knowledge is shared across the battlespace allowing organization on the edge of the command to be responsible for their own areas. Actors at the edge of the organizations work with a shared knowledge, which provides them the ability to make proper decisions. By increasing the number of decision-makers, multiple OODA loops can occur in parallel. Command and control becomes less like a giant circle and more like layers of small loops as all steps occur

simultaneously in parallel. The gained efficiency in speed of command is the ultimate benefit of self-synchronization.

Advocates of self-synchronization believe that with increased knowledge and awareness by all entities, there is less need for a hierarchical command and control structure. As long as the commander's intent is well understood, lower echelon warfighters will make the decisions and act accordingly. Empowering the edge organizations to make decisions and act will free up the General's time so he can focus on higher-level strategic issues. However, for this to be achievable, the elements of trust must be examined and incorporated.

A New Definition of Trust

Research into trust studies has proven one certainty: Nobody can agree on a single definition of trust. From my perspective, this allows me to derive a definition that best suits the needs of operational missions. This is my definition of trust:

> ***Trust is a bet that those entities, which you cannot control, will act in a predictable manner that is favorable to your cause.***

Breaking down this definition, "trust is a bet" means that the person who must give trust – called the "trustor" – makes a speculation on whether his prediction will pay off. The trustor is always a person. Trust is a human behavior. Alice can trust that Bob will drive her safely to school. Bob can trust that his car will not breakdown. But the car cannot trust that Alice or Bob will not spill their drinks on the seats. The car is not capable of trust.

The aspect of the "bet" comes from Piotr Stompka's definition of social trust.[6] When you trust someone, you are placing a bet as to how he will act. If that person or entity acts correctly (in your perception) then you have won your bet. Trust paid off.

"Entities" refers to the object in which you place your trust—the "trustee." This can be another person. It can also be an object such as a computer, radio, vehicle, any hardware, etc. Information can also be the object of your trust. "I trust the information to be relevant, accurate, and timely" is a valid (perhaps far-fetched) statement. The trustee can also be a system or concept such as network centric warfare, democracy, America, or God. Receivers of trust are not required to be human.

"…which you cannot control…" is critical in defining trust. If you have complete control over the trustee, then there is no requirement to trust him. A sure bet is not really a bet; it is a guarantee. Trust happens when you cannot completely control the outcome. If there are areas that allow you to reduce the amount of uncertainty, then the bet will be easier to make. Hence, it becomes easier to trust. However, eliminating the uncertainty completely means there is no longer a requirement for trust.

The next section of the definition is "…will act in a predictable manner…" Trust is a bet on the future. Based on your current assessment, you predict the future outcome of events around you. "Based on my assessment that I always receive mail on weekdays and today is a weekday, I predict that the mailman will deliver my mail today." I do not have control over the mailman, but I have come to expect mail delivery, which makes it easy to predict that he will stop by today. By allowing business associates to send correspondence to me, I am now placing trust in the postal service that they will deliver the mail. In other words, I place a bet that the mailman will deliver. It is an easy bet to make since he reliably delivers the mail every weekday, thus making the prediction fairly simple. If my prediction of the future turns out to be false, then I wrongly placed trust in the mailman, lost my bet, and will not receive that promised check in the mail.

This brings us to the final part of the definition: "…that is favorable to your cause." Just because you can predict an outcome does not make it the future you want. Trust is necessary for people to work towards a common goal. Results must be favorable. If your prediction of the future action is not the outcome you want, your expectation of its occurrence is not trust. It is just something you must recognize and tackle. For example, Alice can expect that if Bob drives her to school at 8:00am, there will be traffic. Alice does not trust in the traffic, she predicts that it will be there and leaves a few minutes earlier to compensate for it. As another example, my sister has never arrived to anything on time in her entire life. If I trusted her to be on time to dinner, I would most likely be disappointed and eat cold food. But, I don't say that I put trust in my sister to let me down. I just predict it (and can even bet on it!). For this reason, trust requires predictions that will help your cause, not hinder it.

Finally, the resulting action of the trustee is either "cooperation" or "defection." If you place trust in a trustee, and he lives up to your expectations, then he has cooperated with you. Even if he performed those actions because it was in his best interest, that is still cooperation since it matched your needs in a favorable way. If he fails to meet your predictions that you used when placing the trust, for whatever reason, then he has defected and broken your trust.[7]

What is Operational Trust?

Now that we have spent the time looking at the definition of Trust, I want to develop a new concept – *Operational Trust*. What is it and why is it important?

Operational trust is the trust that is required from every person and earned from every entity to accomplish an endeavor. Complex operations involve several entities that require a level of interdependence. Each relationship requires a level of trust in order to complete the entire mission. By sharing knowledge and dividing workload, we become more efficient at accomplishing the mission.

However, the more we interlink and share knowledge to accomplish a task, the more dependent we become on entities we do not necessarily control. As operations become more complex, no single person or even small team can accomplish all tasks

required of a mission. At this point, trust is not only desired, but required to complete the mission.

Operational trust comes from a variety of perspectives. Warfighters must trust their peers, commanders must trust subordinates, and subordinates must trust their commanders. Operators must trust the equipment, and all players must trust in the tactics, techniques, and procedures. Moreover, the leaders of the overall operation must trust in the players to accomplish the endeavor. In other words, a person has no choice but to give a level of trust to certain entities (people, objects, systems) in order to complete his mission.

An example of operational trust can be illustrated using the objective of the transportation system. Alice must drive in order to get to work. For her to be willing to get in the car, she must trust in the infrastructure – that the roads are well-paved; the traffic lights are correctly timed; the lines are painted on the ground. She must also trust in the equipment – her car is reliable; the tires hold air; the brakes can stop the car. She must trust the other drivers on the road – they will obey traffic laws; they will stay on their side of the road; they will avoid hitting her. She must trust in the doctrine and training system – everyone driving has learned the same set of rules as she.

If she does not extend trust to these entities over which she has no control, then she can choose not to drive. However, if she needs to drive to get to work to pay the mortgage to have a place to live, then she has to drive and she has to trust.

Her task in the overall mission is to drive to work and support herself. The Dept of Transportation's task is to build the roads and establish the policy so individuals can collectively support the economy. Congress appropriates funding for the national highway system to support commerce which supports the economy. The Dept of Motor Vehicles task is to ensure drivers are properly trained so they can safely drive to work and collectively support the economy. The task of the highway patrol is to ensure everyone is following the rules so that everyone can drive to work safely and support the economy. On and on, you get the idea.

Every entity has a piece of the overarching operation. By successfully accomplishing each individual portion of the mission, they collectively accomplish the big picture endeavor. However, as entities interact during their individual tasks, they are affected by each other's actions. Therefore, they become required to extend a certain level of trust in order to carry out the mission. Alice could not drive to work (her role in supporting the economy) if she was not willing to trust the other drivers, roads, vehicles, law enforcement, etc.

The key difference in operational trust compared to other types is that this level of trust is required, not just desired. Otherwise, the mission success is either not achievable or, at best, completely inefficient. This is trust from a realist perspective. I do not expect that by simply advocating that everyone should trust each other, that operations will become more efficient. The reason to extend trust is because you require it to accomplish

your goals in an efficient manner. However, by discovering ways to make trust assessments more precise, we can make decision-making easier and more correct. This will, in turn, make it possible to further increase the efficiency and effectiveness of the overall operations.

How Operational Trust Factors In – Why Is It Important to Network Centric Warfare

Because NCW is based on the concept of interdependency to gain a shared knowledge, Operational Trust is critical to the success of the NCW mission. Linking information from multiple sources adds another degree of complexity to an already complex mission. The more entities that are involved with sharing information and dividing tasks, the more the requirement for trust grows. Operational Trust is the lynchpin in all networked operations.

In light of the changing events after September 11th and the war on terrorism, the U.S. Department of Defense has redefined its strategic posture from a threat-based response strategy to a capabilities-based all-encompassing strategy. Due to the uncertainties of near-future threats, we need to be prepared to fight any enemy, anywhere, at any level of conflict, from enforcing sanctions and capturing terrorists, to full-scale theater operations and nuclear war. We require agile, adaptable command and control to respond to any given situation. This will require the synergy inherent in NCW to provide the accuracy, relevance, and timeliness of the target information under an increased operations tempo.

Unfortunately, many understand a need for trust, but do not address how to develop it. Advocating grandiose statements like "Everybody should just trust each other more and we will all work together better," conjures images of flower children dancing in green fields. However, trust is not something that you can expect everyone to just give freely. Face it, if we all easily trusted everyone and everyone was trustworthy, communism would have worked. The rest of this paper focuses on determining the requirement to trust and how to make it easier to extend trust.

Understanding the Need to Trust

When determining the need to trust, two main questions come to the mind of the trustor: 1) Do I have to trust?; and 2) What are the risks involved? To help explain these questions, I have created an example scenario that uses typical network centric application threads, Time Critical Targeting (TCT) with Blue Force Situation Awareness (Blue Force SA). In this scenario, the Blue Force fighter aircraft must eliminate a mobile surface-to-air missile (SAM) site as quickly as possible in order to maintain air superiority. This will, in turn, allow the flight to continue with close air support (CAS) missions supporting dispersed Army special teams on the ground. In this case, I am taking the perspective of "Thud" the lead F-16 fighter pilot of a flight of four aircraft carrying high-speed anti-radiation missiles (HARMS) and precision guided munitions. However, to fully understand operational trust, the same process must be applied from

the perspective of the Army teams, the air-C2 node, the ground forward air controller (FAC), the combined air operations center (CAOC), the regional combatant commander, and any other player involved in the mission.

Step 1. Determining the Need to Trust: *Do I have to make a bet.* Three factors play a role in determining the need to trust:

a) Importance of my task – This first step before extending trust is determining how critical my own task is in the overall success of the operation. How much are others depending on me to successfully complete my task? This is where having clear understanding of the commander's intent is so crucial. Every player must understand what the commander's intent is to be able to properly assess the importance of his task in the overall mission and to understand how other tasks are depending on his success. In our scenario, Thud and his wingman need to destroy the mobile SAM site so that the other element of his flight will be able to provide CAS without being shot down. The Army teams are depending on the F-16's weapons for support against enemy fire. The other aircraft in the area, such as JSTARS, AWACS, and tankers, need Thud to destroy the SAM so they can continue their missions controlling the fighters. Failure to successfully complete the mission could have consequences across the spectrum from personal (getting shot down) to tactical (losing aircraft) to operational (inability to provide CAS to Army troops) to strategic (the Army unable to achieve their objective on the ground due to lack of air support) to political (CNN films the Coalition army absorbing huge casualties). Thud's mission is, therefore, very important.

b) Necessity of dependency – Do I need help to accomplish my tasking? Whom do I need to depend on for the information necessary to complete my mission? Thud cannot find this SAM site on his own without risking being shot down. He needs the support of sensor platforms such as JSTARS and satellites to pinpoint the location of the threat. He needs the target analysts to provide an accurate assessment of the location and lethality of the threat. Their assessment is critical to his attack on the target. There must also be a reliable process in place to convey the target information to the pilot. Furthermore, Thud needs his wingman to protect him from immediate enemy fire while finding and destroying the target.

c) Amount of dependency – How critical is each of these dependencies? Do I have alternatives? Before the advent of radios, commanders had to convey detailed rigid plans in advance, hope his men fully understood the orders, and trust they would carry them out. Mid-course corrections required messengers running to the front line – if they made it. There were few alternatives. Changes in technology and tactics enable contingencies and alternate methods more readily. This means there can be less dependency on certain entities with redundant capabilities. In this case, the choice of options may be prioritized to achieve efficiency or convenience.
Returning to our net centric example, Thud depends on the network data link to provide the information into his cockpit for rapid targeting. However, if the data link fails, he has an alternate, but slower, way to receive the information (e.g. voice communications). Therefore, depending on the urgency of the situation, the data link

may or may not be critical for his success. Is the data link a convenience that makes him operate more efficiently, or will it increase the safety of the mission? How often has he practiced the alternate methods? As the alternative approaches become less practiced, his dependency on the data link network increases. This will factor in to how much trust in the data-linked information he is required to give in the future.

Step 2. Assessing the Risk: *What are the stakes of the bet?* At this point, you have decided whether you need to extend trust. Now comes the question of assessing the risk. Determining the amount of risk can be accomplished though the use of a risk assessment matrix, multiplying severity by probability:

    a) <u>Severity of Negative Consequences</u> – This step addresses the severity of the consequences if the entity in which you placed your trust defects. In other words, if the trustee fails to meet your needs, how will that inhibit your ability to accomplish the mission successfully? Thud is trusting that the data link will display the correct SAM information in his cockpit for quick efficient targeting. If the information does not come through, then he must get on the radios and go through the lengthy process of passing coordinates and target information by voice. This will delay his attack on the SAM. The delay may also allow time for the SAM to fire at the Blue Force aircraft. Or the delay could cause him to be too low on fuel by the time he gets the information confirmed that he is no longer able to service the target. If there are multiple SAM targets in the area, the slower communications mean he may be able to engage only one target during his sortie.

        A potentially more dangerous scenario is that the data link information that arrives in his cockpit is wrong. If he does not recognize the "defection of the trustee" – the data link providing inaccurate information – then Thud may continue on the wrong target run-in, and fly directly over friendly troops. Wrong information is often more lethal than missing information because it might not be recognized that the information is wrong.

        However, missing information that goes unrecognized, for example, Blue Force friendly positions not appearing, can also be lethal. What if the data-linked information displayed the location of the target, but not the location of the friendly Special Forces team that was also on the ground destroying it at the same time. Thud and his wingman could easily deploy their weapons without knowing that friendlies were in the area. Depending on how coordinated the targeting data was when the analysts were consolidating the information, they may be unaware of the additional Special Forces team that is already in place destroying the SAM. If Thud unquestioningly trusted the data link target information provided by the analysts in the CAOC without receiving the Blue Force SA, he runs the risk of causing a fratricide incident. The higher the risk, the higher the stakes are to trust.

    b) <u>Probability of occurrence</u> – Addressing the second part of the risk matrix, you must determine the likelihood that your trustee will fail in his part of supporting your mission. What is the probability that the entity in which you place your trust defects? This can be based on several factors. How difficult is the trustee's task? How much experience does the trustee have in accomplishing this task? How trustworthy is the

trustee? How much does the trustee need to depend on others to complete his tasking? How many steps along the way need to take place correctly for the end to be successful? What are his other requirements that may conflict with your needs? These issues need to be properly assessed to understand the stakes, or likelihood, of the trust bet ending in your favor.

Returning to our scenario, Thud needs to trust his wingman. Properly assessing his wingman's capabilities, attitude, and primary mission will help Thud determine the likelihood of his wingman living up to Thud's expectations or not (in other words, will he cooperate or defect). In this scenario, Thud's wingman is carrying the high-speed anti-radiation missiles (HARMs) needed to suppress the SAM, which will enable Thud to get in close enough to the threat to be able to destroy it with his precision guided bomb. We have already determined this is a necessary role for the overall accomplishment of the mission. Since Thud is not carrying his own HARMs, he must rely on his wingman to accomplish his tasking before Thud can safely complete his. Luckily, Thud has been training with his wingman for several months and knows he is a competent pilot and trusted friend (which came from drinking beers together in the squadron bar).

If his wingman were new to the mission, he may not be able to achieve his objectives under the stress of enemy fire. In other words, the probability of defection increases even if the wingman intended to achieve his portion of the mission, but still does not complete his task. However, Thud is only able to make an adequate judgment on his wingman's capabilities because he knows him personally, has trained with him in the past, and has prior knowledge of his wingman's capabilities.

Turning Thud's trust towards another recipient, we will look at the controller who passes the targeting information through the data link network to Thud. The controller's tasking is complex in that it depends on several correct correlation processes happening in the CAOC for the target information to reach him correctly. He must correctly interpret the data and match up the best aircraft suited for the mission (in this case, Thud's flight) in addition to assessing the situation in the airspace. Thud has never met the controller directing his attack, but he estimates that most of them are young airmen with little experience. Thud does not know this individual's level of training but has to trust that the training system has brought him up to an adequate level. Can Thud make a good assessment about the trustworthiness of his controller? In addition, Thud is expected to trust the data link itself. If the information just appears on his screen without some sort of verbal confirmation from the controller, then Thud does not know if the information is really intended for him or if it is just a glitch in the system. Since the network design is an extremely complex process, the data link could easily send accidental data flowing to the wrong place until all the bugs are worked out. In other words, the probability of any new network breaking your trust is generally high. Without prior knowledge and experience with the people on the other end of the computer network, Thud will generally be conservative in his risk assessment. Therefore, Thud will most likely assess the risk as high until he has collected some past experience with the controller and the specific network design. Thud's ability to develop a good assessment of the probability of defection occurring is necessary to adequately evaluate the risk of trusting.

Finding Ways To Make It Easier To Trust

Now that we know we have to trust certain entities and we have assessed the risk associated with that trust, we can start to look for ways to mitigate the risk. This starts by making a better prediction of the trustee's actions. By knowing what to expect, it is easier to identify if and when a defection is beginning. The trustor also has more of an opportunity to reduce the severity of the defection by identifying alternatives sooner, correcting the situation, or beginning damage control. By reducing the risk, it makes trust easier to accept. Facilitating trust will lead to better operational decision-making, which will, in turn, lead to more efficient and effective operations.

Step 3. Changing the Odds: *Can I make a better prediction?* The next six areas figure in to making a better prediction by reducing the uncertainty. This will make it easier to trust, which correlates to faster, more efficient decision-making:

a) <u>Situation Awareness (SA)</u> – SA is a trust enabler because it greatly figures into your ability to make predictions about trust. Situation awareness is "the knowledge, cognition, and anticipation of events, factors and variables affecting the safe, expedient and effective conduct of the mission."[8] It is developed through the continuous integration of new observations into recurring mental assessments. This is the stage of the OODA loop where you orient yourself to everything going on around you. The analogy of trust and SA is if trust represents the future, then SA is the equivalent for the present.

By having a good mental picture, I can better predict the next set of events around me. For example, as I am driving my car, I like to know what vehicles are around me and their relative speeds. By knowing the placement of the other cars, if an unexpected dog jumps in front of my car, I know which direction I can swerve while still avoiding crashing. This also requires knowing the maneuverability of my car and the conditions of the road to avoid skidding. If I am driving in an unfamiliar rental car and it is snowing, I may have more attention focused on just driving and be less aware of the traffic around me. Being less prepared for the unexpected puts me in a more dangerous position due to lack of SA.

Good SA will greatly increase Thud's ability to predict future actions or recognize when events are not working out as planned. This is where the data link has proven to be truly invaluable. By having near real-time information of the friendly ground and aircraft positions, Thud is much more able to accomplish his mission without a fratricide incident. Sharing this information among his flight gives them a common picture. Therefore, he can be more certain about his wingman's level of SA also.

However, bad data can cause a decrease in SA. For example, data-linked position information is actually where the object (aircraft, vehicle, person) *was* when the radio transmitted it. Depending on how fast they are moving or the update rate, the data could be anywhere from several seconds to several minutes stale. There also may be no indication to the pilot how stale the data points are. During the final run-in stage of attacking a target, it is critical to have not "near real-time," but actual real-time information on the friendly positions in the area. This is especially true for CAS missions where ground troops are always in close proximity to the targets.

Our pilot, Thud, uses his SA to predict how events will unfold and recognize quickly when they are not as expected. For example, if he sees that his wingman is flying out of position, he may be alerted that his wingman's SA has dropped (perhaps due to an avionics restart in his aircraft) and needs some time to rebuild his mental picture. Thud's SA can also help him predict the accuracy of the AWACS surveillance information, such as a neutral aircraft, as it appears on his display. If he believes there are errors in the position being reported, he could point his radar in the direction of the neutral aircraft and refine the data coming to him through the data link. When he receives bad data into his cockpit, such as a hostile aircraft at his location, if his SA is high, he can determine that there is an error in the information and he is being incorrectly displayed to others as the enemy. This adds to his experience base when evaluating how much trust the AWACS crew deserves from him.

Situation awareness is key to developing good predictions, which are required to be able to trust other entities. The better your SA, the easier it is to extend trust because you will be able to quickly recognize if events are transpiring as predicted or not. By maintaining a more complete understanding of the situation around you, you will be better able to predict follow-on actions, even those you cannot control. This will allow you to extend trust more easily.

b) Verification (both during and after) – Part of building a good mental picture is being able to distinguish good information from bad. Having an ability to verify the information is a simple way to accomplish this. Tools that allow you to crosscheck information will help you quickly ascertain the accuracy and sometimes even the relevance of the information. This verification process can also help correlate multiple pieces of information in order to decrease the error in all of them. For example, a global positioning system (GPS) receiver works in this manner to determine its precise location.

One of the major benefits of network centric warfare is its ability to link information to gain a shared awareness of the battlespace. In 20th century warfare, verification of information was accomplished through a hierarchical chain of command. This approval process provided the checks and balances required to feel confident in committing to action. With self-synchronization, the players at the edge need to have their own system of verification in order to know the information they are receiving is valid. Thud is an example of an edge player who needs to be able to confidently assess new information to build and maintain his SA, and consequently be able to trust the other players he depends on.

In network centric warfare, multiple sensor types in different parts of the electromagnetic spectrum can be used to verify the location and targeting information of the SAM. By collecting and crosschecking this information with each sensor, the analyst that fuses all of the observations can feel very confident predicting the target's exact location. However, if all that information is consolidated in the CAOC and then only the final answer is sent to the fighter, then the fighter has limited capability to verify the target information in his own cockpit. This may reduce his trust or at least cause him to believe the stakes are higher in granting trust. This is a problem for self-synchronization. His SA has effectively been reduced by not having the ability to see some of the information that led to concluding the target was valid.

In this case, Thud may have to just accept the higher risk in trust – call it blind trust – where he has no choice but to trust and no way to reduce the risk. However, if he is able to use his own onboard sensors, such as his radar or targeting pod, to correlate the coordinates, then he can verify the target appears to be in line with other information. A key difference between simple network centric operations and self-synchronization is that, with the latter, the effectors – the guys actually dropping the bombs – must have the ability to assess the trustworthiness of the data. It cannot be left up to the CAOC or other C2 platforms to just issue a "Trust Me" card. Everybody is responsible and accountable for self-synchronization to work.

    c) <u>Past experience or indirect reputation of trustee</u> – Another way to improve your prediction is to have past experience with the trustee. The more you get to know how someone responds to different situations, the more likely you will be able to predict how he will respond in future interaction. The same logic goes with equipment. The more familiar you are with a system, the more you understand its capabilities and limitations. When these systems become critical to your mission, you will already have experience with them and know how well they work. While this seems obvious, it underscores the need to train together. By practicing the mission with the same team of people, the same equipment, and the same procedures, everyone will be better prepared to trust each other and accomplish the real mission just as they have trained.

The US Air Force has put new emphasis on effects-based operations. Yet training still focuses on small pieces of the mission. Aircraft squadrons train together to practice their specific tactics required to target a SAM, but rarely train with the operators and controllers that they will undoubtedly be linked with during real operations. Large joint and combined exercises are difficult to plan and coordinate, and expensive to budget. However, if we do not train jointly, then how do we develop the past experience together to build trust in each other's capabilities? Since one of the key concepts to network centric warfare is that entities can be geographically dispersed, then maybe it is possible to plan for more training opportunities across elements of a mission without the cost of training deployments. In addition, if bases took the initiative to plan low-level training exercises with nearby posts, relationships could form allowing each unit to find the other more trustworthy. As these relationships form into packaged mission sets, then it would be beneficial to deploy the joint package together to meet real operational requirements.

Another option if personal experience is not possible is having indirect knowledge of the reputation of the entity. The Army ground FAC may not know Thud personally, but he may have had several occasions working with Thud's squadron. If he develops an opinion of the squadron that the people in it are competent and trustworthy, then he can extend this level of trust to the squadron members he has yet to work with. By sharing experience bases of a group with individuals, the Army FAC can make a prediction of the competency of Thud's flight. The indirect reputation to show trustworthiness can also come from Thud working with another trusted member of the Army team who vouches for Thud. While indirect reputation does not provide as good a prediction as direct experience, it can still make it easier to extend trust.

    d) <u>Amount of control</u> – How much control do I have over the actions of other entities? As flight lead, I have a measurable level of control over my wingmen, since I

direct their actions in the mission. Based on our training and experience together, I can assess how much control over the flight I have. For example, if a new, inexperienced pilot is flying with me, he may be more likely to act unpredictably due to lack of training. This equates to having worse odds in the trust bet. The more control over the situation, the less risk I have to take. This equates to making it easier to trust. I am more willing to make that bet.

How easy is it to control people through a data link without face-to-face contact? That depends on how well you know them or how much you have worked with them. It might also depend on how closely they follow the planned tactics, technique, and procedures. Again, it is based on past experience that will determine your assessment of control you have over the situation.

The amount of control an operator has over a given piece of equipment is directly related to the human factors design of the system. For example, some radios, such as a survival radio may be designed to be foolproof and have very few switches that can be adjusted. But in so doing that, it limits the capabilities of the radio and leaves the survivor with less control. On the other hand, the combat search and rescue team has better control over the survivor because they know he cannot change the frequency or try to do something with the survival radio that it was not designed to do.

e) <u>Finding a common cause/objective with the trustee</u> – Another way to reduce the uncertainty in a trustee's actions is to assess whether you and he have a common objective. If you are both working toward the same cause, then he will be more likely to be trustworthy. While he achieves his objectives, he also helps you achieve yours, and you have a win-win situation.

With NCW and especially self-synchronization, one of the necessary conditions for successful operations is having clear command intent. This will ensure that people understand their role in the overall mission. It will also help ensure that both you and your trustee realize that you are both working for the same mission. This will allow both of you to extend trust more easily. In other words, the best way every player can feel easier about extending trust is for everyone to clearly understand the overall mission and their role in it. This is best accomplished by having a clear commander's intent.

f) <u>Likelihood of future interactions</u> – Finally, the last factor to make it easier to trust is by assessing the likelihood of future interactions with the same trustee. Future interactions are sometimes needed to keep people trustworthy. If they expect or fear reciprocal treatment, then they will be more likely to do what is expected of them. If there is no chance of future interaction, then the trustee has no fear of reprisal, and he is free to act in a less favorable manner. For example, if Bob stops at a his hometown cafe for breakfast, receives good services, and then does not tip the waitress, there is a possibility that she will remember him next time and provide bad service. In this case, the waitress placed trust that Bob would follow custom if he received good service. The likelihood of a future interaction between Bob and the waitress ensures that Bob will meet her prediction. On the other hand, if Bob stopped at a truck-stop diner that he never intends to visit again, he could easily save his money by not tipping and get away with it. However, just because there is no future interaction does not mean that Bob cannot be

trustworthy; it only means that future relationships can act as a warranty for Bob to live up to the trust bestowed upon him.

By flying together Thud and his wingman have a common mission even with different roles. The next time they fly, their roles may be switched. Either way they will mutually support each other as they have learned to do on every mission they fly together.

A Real-World Example of Trust in the Decision Process

Finally, to tie the factors regarding operational trust to network centric operations and self-synchronization, I would like to close this paper with a real world example that demonstrates the aspects discussed above. In some ways it worked well, in others it did not. While it shows how trust affects the decision process, it also shows how far we need to come to co-evolve technology, tactics, conops, and training with operational trust in mind.

During Operation Iraqi Freedom (OIF), I witnessed a close-call in a potential fratricide incident. The problem began when a computer restarted at a location geographically separated from the point where the incident was unfolding, but still linked through the network. When the computer restarted, it opened its transmit filters, and at the same time, began transmitting stale targeting data over data link network. The location that the data pointed to was of a target that had been destroyed days earlier and a Special Forces team was already working in that vicinity. However, the stale data passed machine-to-machine through an air control squadron, which automatically transmitted the false data over the air. At this point, the target information then took on the reputation of the air control squadron transmitting it. What the fighter aircraft received in his cockpit was target information of a hostile target coming from an authoritative control element.

What saved this from becoming a terrible situation was the pilot making a proper assessment of trust while, at the same time, flying his mission over enemy territory. Because of the nature of the operation, he knew the importance of his mission and the need for the data link to provide timely, accurate, relevant information to him. He also recognized the potential consequences of acting on incorrect information over the link. Luckily, this was an experienced pilot with very high SA at the time. He had also witnessed, in the past, glitches with the network. While the data link was putting out false targeting information, it also had Blue Force friendly positions in the vicinity being displayed correctly. Because the pilot's SA was high, he was able to notice that the two sets of overlaying data did not correlate. It did not make sense to have friendlies and hostiles at the same location. Since the data link in his aircraft was a relatively new system and the network in OIF was extremely complex, he did not place a high level of trust in the system. Through voice communications, he was able to verify which piece of information was correct. He was also able to inspect the target with on-board sensors to further verify that the operators had also made a correct assessment of the ambiguous information being displayed. In this case, the fratricide was avoided.

However, due to the urgent nature of destroying time sensitive targets, a pilot with less SA might have engaged the target based on the direction from the data link. If this occurred, what would the mishap investigation discover? Who would be held accountable for the lethal error? Could the pilot who would have dropped the bomb been feel guilt-free because he was following the direction of the computer? Would the air control squadron be held accountable since the target information had their computer stamp on it? What about the designers of the computers that attach to the network? The bottom line is that accountability of information on a network must be traceable and verifiable not only during post-event investigations, but also real-time. Where the data truly originates from is a critical factor in deciding the level of trust in the data. People mentally assess the timeliness, accuracy, and relevance based on who is transmitting it. Any operator on the net deserves to know the source.

Conclusion

While this last example demonstrates a failure in the networked system, it also demonstrates the successful decision making process associated with assessing trust. This example is here to show everyone how far we have come in network centric warfare, but at the same time, how much farther we need to go to get it right. Operational Trust is the lynchpin in all networked operations.

By taking into account the process people go through to develop and extend trust, perhaps we will be able plan for these factors. Networked systems need to be designed with the components of trust in mind. But it is not just about the design of the data link systems. Network centric warfare requires the co-evolution of doctrine, concepts of operations, force structure, and tactics. These, too, must incorporate the human element of trust in decision-making during development, operations, and training.

Network centric warfare and self-synchronization are, no doubt, the direction the latest technology will take us. But, we must develop it smartly with operational trust in mind. Facilitating trust will support better operational decision-making, which will lead to more efficient and effective operations.

---

[1] In a speech to the U.S. Naval Academy, President George W. Bush stated: "We must build forces that draw upon the revolutionary advances in the technology of war…one that relies more heavily on stealth, precision, and information technologies." 25 May 2001.

[2] The Office of the Secretary of Defense C2ISR Center sponsored the book by Richard Hayes and David Alberts. *Power to the Edge.* C4ISR Cooperative Research Program (CCRP), Washington, D.C. 2003., p. 27.

[3] NCW is fully described in the book by David Alberts, John Garstka, and Frederick Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority.* C4ISR Cooperative Research Program (CCRP), Washington, D.C. 1999. p. 86

[4] Alberts, *Network Centric Warfare*. pp. 88-93.

[5] This definition comes from Rumsfeld, Donald H. *Transformational Planning Guidance*, Department of Defense. April 2003.

[6] Stompka, Piotr. *Trust: A Sociological Theory*. United Kingdom: Cambridge University Press, 1999.

[7] These terms come from Robert Axelrod's *The Evolution of Cooperation*, a highly recommended book showing how trust and cooperation can form using an iterative version of the Prisoner's Dilemma game theory. Publishing Information: New York : Basic Books, 1984.

[8] This definition comes from Taylor, R. M. (1990). "Situation awareness rating technique (SART): the development of a tool for aircrew systems design." *Situational Awareness in Aerospace Operations* (Chapter 3). France: Neuillysur-Seine, NATO-AGARD-CP-478. http://www.raes-hfg.com/crm/reports/sa-defns.pdf 19 May 2004.