CyberCraft: Concept Linking NCW Principles with the Cyber Domain in an Urban Operational Environment

Topic: Effects Based Operations

By Dr. Paul W. Phister, Jr., Dan Fayette, Emily Krzysiak

Point of Contact
Dr. Paul W. Phister, Jr.
AF Research Laboratory, Information Directorate
AFRL/IFB, Bldg 106, Room B-113
26 Electronic Parkway
Rome NY 13441-4514

Phone: (315)330-3315
FAX: (315)330-7043

paul.phister@rl.af.mil

CyberCraft: Concept Linking NCW Principles with the Cyber Domain in an Urban Operational Environment

Dr. Paul W. Phister, Jr., Dan Fayette, Emily Krzysiak

Abstract

With the entry into the Information Age comes a new theory of warfare—Network Centric Warfare (NCW). Currently, discussions regarding NCW have concentrated on the traditional forms of warfare, namely those that occur within the sub-surface, surface, air and space mediums. Additionally, limited discussions have centered on the asymmetric aspect of the new threat, i.e., joint urban operations. Great strides are being made linking NCW to asymmetric threats, but again these have centered on sub-surface, surface, air and space mediums. There is another medium that can be utilized that has the potential of becoming the most effective use of military force in the Information Age. Using the Cyber Domain to conduct military operations within an urban environment has significant potential. This paper presents an introduction of a new "cyber vehicle", called the "CyberCraft", which performs similar operations as conventional vehicles, such as as a "strike" platform (e.g., deny, destroy, degrade, disrupt or deceive) or as an "Intelligence Surveillance Reconnaissance (ISR)" platform (e.g., find, fix, track, monitor); however, the "CyberCraft" operates solely within the cyber domain to extend the arm of military application of force. Additionally, within the concept of this new vehicle, this paper discusses the: a) factors unique to conducting military operations within an urban environment; b) challenges of performing NCW and Effects Based Operations (EBO) within an urban environment; and, c) research areas and technology challenges to pursue regarding utilizing the "CyberCraft" in an urban environment.

Introduction

With the entry into the Information Age comes a new theory of warfare—Network Centric Warfare (NCW). Currently, discussions regarding NCW have concentrated on the traditional forms of warfare; namely, those that occur within the sub-surface, surface, air and space mediums. Additionally, limited discussions have been centered on the asymmetric aspect of the new threat, i.e., Joint Urban Operations (JUO). Great strides have been made linking NCW to asymmetric threats, but again these have centered on sub-surface, surface, air and space mediums. There is another medium that can be utilized that has the potential of becoming the most effective use of military force in the Information Age. Using the cyber domain to conduct military operations within an urban or global environment will allow us to globally project our influence with minimal or no collateral damage. The "Cyber Craft" is our concept to accomplish this objective.

Unique Factors of JUO Environment

Urban operations have historically been characterized by a slower operational-level tempo, with higher casualty rates among both combatants and noncombatants, and extensive collateral damage by the same types of forces conducting operations in non-urban terrain. Operations in the urban environment can no longer be considered an "elective" competency of the joint force. Our adversaries have already recognized the potential of using the urban battlespace to mitigate our overwhelming military advantages. [1] Our civilian and military leaders must understand how we deal with urban operations and how it will resonate with the adversary, populace, the US population, nongovernmental organizations, and the international community.[2] We see this playing out every day in places like Iraq.

The Joint Urban Operations Integrating Concept specifies eight principles to guide the planning, preparation, deployment, employment, and sustainment for urban operations. These principles illustrate differences and similarities with conventional military engagements. The eight principles are: 1) understanding the complex urban environment, 2) see first, see clearly, and see in depth, 3) control the urban environment, 4) identify and isolate the adversary, 5) take the initiative and control the tempo of operations, 6) engage the adversary comprehensively, 7) ensure every action contributes to achieving the desired end state, and 8) balance restraint and overmatching power.[3]

Probably the most significant factor regarding engagements within an urban environment is the complexity of that environment. First, the physical terrain is composed of highly developed urban landscape, with urban canyons (streets with buildings on both sides), vertical terrain (high rise structures), and subsurface maneuver space (underground sewers, subways, rivers). Second, the urban environment includes political, cultural, religious, economic, legal, information, and infrastructure networks by which a society functions. Third, the density and collective thoughts of the urban population vary greatly and are arguably the most important and difficult factors influencing urban operations.[4] We propose adding cyber operations with its variety of devices, telecommunications, internet café's, networked systems and systems, etc to the complexities described above and as a means to affect them as well.

The conduction of urban operations is not new to the military. Since World War II, the military has had to conduct operations within various urban environments, such as: Paris, Moscow and Berlin, not to mention the thousands of villages in France, Belgium, and Germany. What has significantly changed over the last 60-years is that attacks using firepower alone to destroy key infrastructure and degrade enemy operational capability to affect the enemy leadership's will and public support produce limited and often

---

[1] Joint Urban Operations Integrating Concept, DRAFT Version 1.0, 13 Oct 2004, page 9.
[2] Joint Urban Operations Integrating Concept, DRAFT Version 1.0, 13 Oct 2004, page 10.
[3] Joint Urban Operations Integrating Concept, DRAFT Version 1.0, 13 Oct 2004, page 10.
[4] Joint Urban Operations Integrating Concept, DRAFT Version 1.0, 13 Oct 2004, page 10.

counterproductive effects.[5] Thus, to achieve desired effects within an urban environment requires a totally different approach by our military forces. In addition to the conventional urban factors and military tactics against urban scenarios, the widespread use of wireless techniques and devices in the cyber realm offer us unique opportunities to approach urban warfare with unique methods that may produce the desired effect without the physical damage to the urban infrastructure.

Challenges of NCW within JUO Environment

With the entry into the Information Age comes a new theory of warfare—Network-Centric Warfare. The focus of NCW is networking battlespace entities (e.g., platforms with planners) so they can work in concert to achieve synergistic effects.[6] The postulates of NCW can be stated as follows: 1) a robustly networked force improves information sharing; 2) information sharing and collaboration enhances the quality of information and shared situational awareness; 3) shared situational awareness enables collaboration and self-synchronization which enhances sustainability and speed of command; and, 4) these in turn, dramatically increases mission effectiveness -- the bottom line). Alberts, etc. al., highlight the fact that NCW is based on adopting a new way of thinking, i.e., network centric thinking.[7] Figure 1 illustrates the value chain of Network Centric Warfare. Three attributes can be used to describe portions of NCW: "**Build** the net", "Protect the **net**", and "**Populate** the net" with the end goal of bringing "Power **to** the Edge". "Power to the Edge" is the ability of the total force to dynamically synchronize their actions in order to achieve Command and Control (C2) agility and increase the speed of command over a robust, networked grid that is not only well protected but allows any entity to join "the fight" in order to achieve a strategic/operational/tactical mission objective.

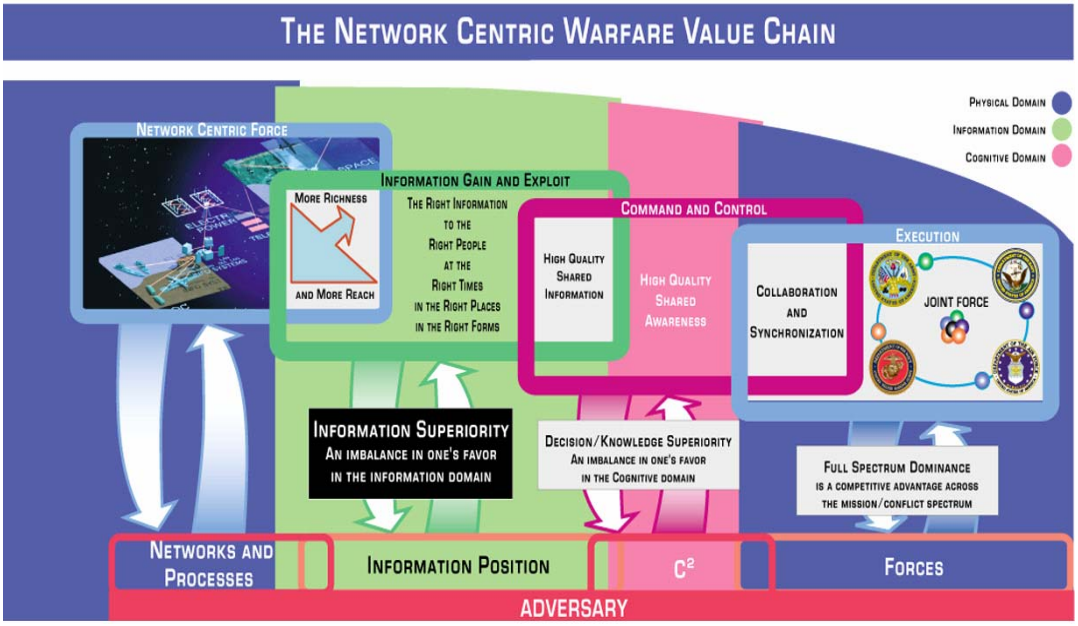


Figure 1: NCW Value Chain[8]

[5] Joint Urban Operations Integrating Concept, DRAFT Version 1.0, 13 Oct 2004, page 10.
[6] Alberts, D.S., Garstka, J.J., and Stein, F.P. "Network Centric Warfare: Developing and Leveraging Information Superiority," *CCRP Publication Series* (2002, 2nd Edition, page 2.
[7] Alberts, D.S., Hayes, R.E., "Power to the Edge: Command and Control in the Information Age," *CCRP Publication Series* (2003), page 18.
[8] Alberts, D.S., Garstka, J.J., Hayes, R.E., and Signori, D.A. "Understanding Information Age Warfare," *CCRP Publication Series* (2001), page 77.

Given the variety of elements involved in the Information Age of warfare and its effects-based orientation, command intent must be congruent across several elements (joint forces), coalition elements (combined), interagency partners, international organizations, and non-governmental organizations[9].
Currently, discussions regarding NCW have concentrated on the traditional forms of warfare, namely those that occur within the sub-surface, surface, air and space mediums. Additionally, limited discussions have been centered on the asymmetric aspect of the new threat, i.e., joint urban operations. Great strides have been made linking NCW to asymmetric threats, but again these have centered on sub-surface, surface, air and space mediums. What is missing is the conduction of operations within the cyber domain. NCW is about human and organizational behavior as well as the traditional systems interactions to achieve effect. As previously stated, this discussion has focused mainly on "traditional" forces and not cyber. One reason could be that employing cyber forces, with trust, is a very daunting task.

Additionally, the current thrust of NCW centers around a network-centric infrastructure that is controlled by the US and her Allies. One of the largest challenges of NCW is applying the theory in a Joint Urban Operations environment where the warfighter wants to interject into an adversary's network which may or may not be of similar composition to our own. Figure 2 illustrates challenge to be able to influence into an adversary's network in real-time. Consequently, the theory of NCW needs to be expanded to include not only the networking of friendly battlespace entities, but having the ability to conduct warfare against or within an adversary's network, wireless device, telecommunications system, etc.

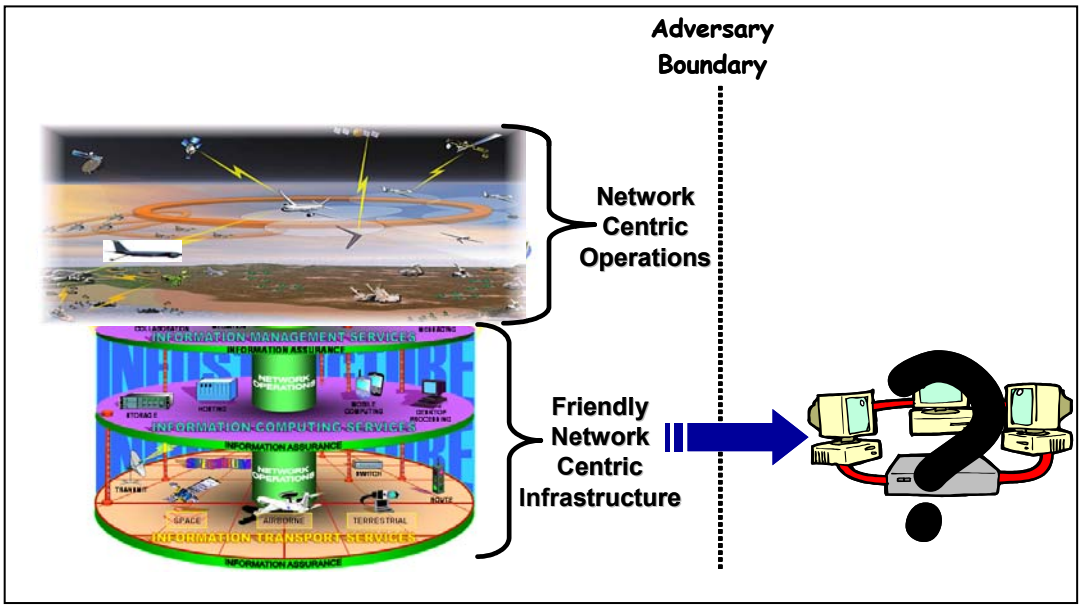


Figure 2: Network Centric Infrastructure, Friendly vs. Adversary

What is a Cyber-Craft?

As mentioned earlier, there is another medium that can be utilized that has the potential of becoming the most effective use of military force within the Information Age. Using the cyber domain to conduct military operations within a military environment (urban operations, anti-terrorism, and near-peer traditional operations) has significant potential to create the desired effects with either little or minimal collateral damage. This leads us to the new concept called the "CyberCraft". There are a lot of similarities between the "CyberCraft" which operates in the cyber domain with that of aircraft that operate in the air domain. Table 1 below shows some of these similarities. This new capability, "Cyber-Craft", can perform similar operations as conventional vehicles (e.g., UAV's), such as a "strike" platform (e.g., deny, destroy, degrade, disrupt or deceive) or as an "ISR" platform (e.g., find, fix, track, monitor); however, the "Cyber-Craft" operates solely within the cyber domain to extend the arm of military application of force application and force protection. The characteristics of a "Cyber-Craft" include the ability to be launched from a network platform, the ability to embed control instructions within the craft, the ability to positively

control the "Cyber-Craft" from a remote network location, the capability for the craft to self-destruct upon being recognized, the capability for the craft to operate with minimal or no signature/footprint, and the ability for the "Cyber-Craft" to rendezvous and cooperate with other friendly "Cyber-Craft".[9]

There are some important challenges of NCW and EBO, which is enabled by NCW, and its relationship to JUO. Key attributes like self-synchronization and collaboration play a vital role within a joint urban operations environment. However linking ourselves to synchronizing force structure employed today and not taking full advantage of the cyber domain is restricting possibilities which could be the "tool" of choice.

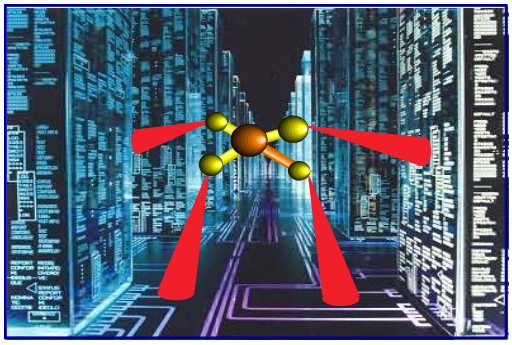
	
Air and Space Vehicles: UCAVs	Cyberspace Vehicles: Info-Crafts
Flight Medium: Air & Space	Flight Medium: Cyberspace
Weapons: Missiles & Bombs	Weapons: Virus, Worm, Control, Information…
Desired "Effect": Destroy Target	Desired "Effect": Destroy, Degrade, Co-opt, Control, Access, Confuse
Control: Air/Space/Ground movement	Control: Network Links that support enemy Air/Space/Ground movement
Low Probability of Intercept: Stealth (Physical)	Low Probability of Intercept : Stealth (Software, RF)
Low Probability of Detection: Terrain Masking	Low Probability of Detection : Network Masking
Home Base: Predetermined Airfield	Home Base: Any Cyberspace Portal
Logistics: Heavy, Continual	Logistics: Light, Infrequent (software, RF)

Table 1: Characteristics of Kinetic vs. Cyber "Vehicles"

[9] Information taken from a 2005 AFRL/IF MURI Proposal.

Cyber-Craft Operations within JUO Environment

It is envisioned that the "Cyber-Craft" could operate at three levels, namely strategic, operational and tactical. The mission and objectives would be different at each level, for example:

1. At the strategic level the "cyber-craft" could be sent out to perform long-standing intelligence requirements. Some examples being to monitor a military barracks, accumulate financial information on a potentially hostile nation, or provide status on the political climate of a South American country. This "cyber-craft" would essentially operate for months or years gathering this long-term information.
2. At the operational level, the "cyber-craft" could be sent out to perform near-term operational requirements. Some examples would be how many tanks or trucks are currently at a specified military installation, is a deeply buried bunker occupied and conducting operations, where the political and military leaders are, what is the status of their C2 infrastructure, or how many aircraft are usable at a specified airfield. Due to the volatility of operational information, the "cyber-craft would just have to operate for days and weeks.
3. The lowest level, tactical, the "cyber-craft could be sent out for minutes to hours collecting real-time information. This information would be used to answer more immediate questions, like who is in this building across the street, where are the tanks located in a particular town or village that is going to be entered by friendly forces, or what's the latest intelligence regarding adversarial forces in a particular town or village.

No matter what level the "cyber-craft" operates, to be effective, as either a strike asset or an ISR asset, it must function in an effects based operation context as depicted in Figure 3. Effects based planning is defined in the Air Combat Command (ACC) white paper[11] as actions taken against enemy systems designed to achieve specific effects that contribute directly to desired military and political outcomes. Furthermore it goes on to state that decision-makers must have a clear idea of what it is they are trying to accomplish, what actions might be taken and how the proposed actions will contribute to the desired end-state. They must also have some reasonable explanation of why they expect the operations to work. Once armed with this information we need to turn our attention to effects based assessment. Effects based assessment can be loosely defined as Battle Damage Assessment (BDA) focused on the first order effect combined with combat and campaign assessment which is focused on complex and cascading 2nd and nth order effects as they ripple through the enemy as a system. Key to this is clearly defined well understood Measures of Effective (MOE) and Measures of Performance (MOP) of the kinetic or non-kinetic weapon used. Accomplishing effects based planning and assessment for kinetic weapons which are relatively well understood is still difficult today as confirmed from Iraqi Freedom Lessons Learned and at the C4ISR Summit held last summer (Aug 04). Including non-kinetic information operation weapons in to the mix and defining causal linkage of actions to effect is a truly daunting task. The following are areas needing to be addressed by our CyberCraft to truly be an effective resource for the warfighter of the future.

It is proposed that this "cyber-craft" take on fused multi-mission roles of combined information warfare, information assurance, intelligence gathering, information dissemination, deception, and electronic warfare. The "cyber-craft" needs to take on the mission of affecting not only strategic assets but tactical systems as well. To be effective in urban environments the Cyber mission will need to be cooperative with the space, land, air, and sea missions of the region and be coordinated with Joint operations.

Today's modern wireless communications have expanded greatly from the single concept of the Internet of LANS and WANS to include wireless networks, wireless devices such as PDA's and telecommunication devices. Cell phones are rapidly morphing into combinations of audio, text, Internet access, PDA's, and location devices.

The sophisticated infrastructure of wired and wireless systems in Urban Environments will pose unique challenges to the development of the Cyber Craft. C2 systems while based on high-speed communications and computers are including wireless devices into their infrastructures. Urban environments pose additional challenges because their infrastructures are heavily impacted by urban canyons, increased use of local area

loops, micro cells, very dense peak time usage, very mobile targets with the ability to change from computer network structures to RF network structures in real time while maintaining their information access and dissemination requirements. These environmental factors require the Cyber Craft to consider RF penetration methods in combination with traditional network approaches to cyber weapon delivery. The Cyber Craft payloads will be required to traverse densely populated heterogeneous networks rapidly changing from the wired world to the wireless world as information changes mediums depending on the user's access requirements and information demands. A traditionally overlooked, but critical capability is the ability of the Cyber weapon to sift through and process massive amounts of data in real-time with little or no apriori knowledge to determine the intelligence value of the target and thereby be able to invoke the proper attack to achieve the desired effect.

The "Cyber-Craft" will need to seamlessly traverse from the wired to the wireless and back as information travels the maze of access devices to its end user. Cyber agents will need to embody the ability to covertly travel across these mediums, constantly assessing the network layout, morphing itself as networks change, and remaining covert while maintaining the integrity of its mission. Increased use of data hiding techniques and data hiding detection techniques add additional complexity to the Cyber craft weapon arsenal. An agent will constantly have to reassess itself to insure it is not being tracked or has not become a carrier for an adversaries cyber weapons. Cyber weapons will need to perform real-time continuous self-assessment of the adversary's detection capability and be able to make instant decisions to morph or self-destruct. Both these functions will be required in covertness and with the decision information sent back to its Cyber Craft home.

Significant technological and doctrine challenges remain to be solved before the Cyber Craft can become an effective military weapon. Agent development, agent size and complexity, detection technology, real-time agent learning and self morphing technology, RF and network penetration technology are a few of the technological challenges requiring additional investment. Doctrine issues for fusing missions, weapon effect profiles, service/agency roles and missions are a few of the doctrine challenges to be solved.

Cyber warfare is an emerging art and many countries recognize its importance in the future of war fighting. The US needs to assess the investment being made in conventional warfare weapons and make a commensurate investment in the Cyber Craft and adding it to its weapon arsenal.

Direct action leads to a desired effect, it is critical that we determine that the action or actions taken are creating the effect we want both spatially and temporarily. Note every effect has a spatial and temporal component (includes when to apply an action and how long is the effect going to last). This leads to the need to clearly define measures of performance which drives information collection requirements to "measure of effectiveness" has been achieved. Put a different way did all the actions applied achieve the objective effect. Prior to and after the fact, we perform actions we want to make sure that our battlespace understanding is still relevant (Did our adversary change the situation). This change may negate the effect we want to achieve from the actions planned.

To this point we have focused mainly on the tactical level of war. Now we need to deal with campaign level. Are our combat operations achieving commander's intent? To determine this we need to be collecting "holistic" information on the enemy as a system to assure ourselves that the positive effects we are trying to achieve are indeed happening and hopefully no negative effects we didn't think of. We need to be able to monitor before, through, and after a cyber attack to determine the effect. In addition Cyber warfare uniquely presents challenges in our ability to monitor, track and direct attacks. It also presents unique challenges in requiring warfare tactics to be covert and non-traceable. Additionally the density of systems and usage in urban environments presents unique challenges to conducting cyber warfare. We need all source fusion of information to achieve timely situation awareness and knowledge. When we talk situation awareness we mean blue, red and gray. Where are we, where are they and where are the non-combatants. What are our perceptions on what they are doing? Again, positive effects, versus negative effects.

We need the ability to understand the dynamics of the campaign and if a situation presents itself be able to understand whether we should take action or not. We need indications and warning to alert the commander

when something is not going as planned as well as I&W we specifically tasked our sensors to look for adverse effects because we don't want a situation to happen (Like deploy WMD). Finally, agility will be the key to success. We need to dynamically and in time synchronize our actions to achieve desired effect. This applies to force application (weapon) and sensing.

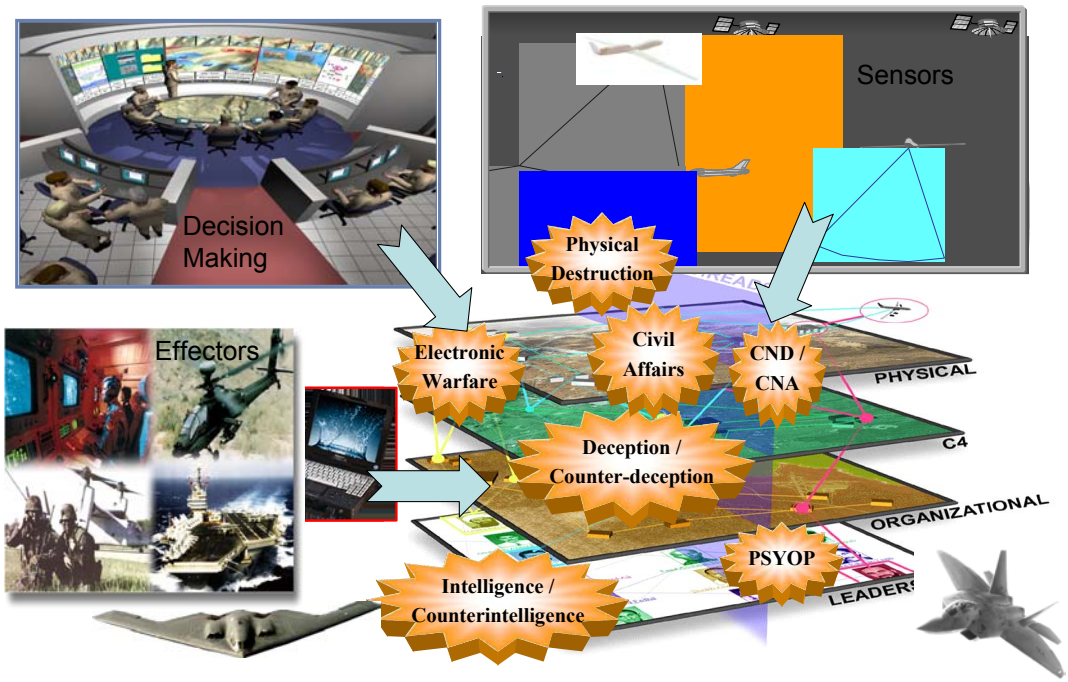
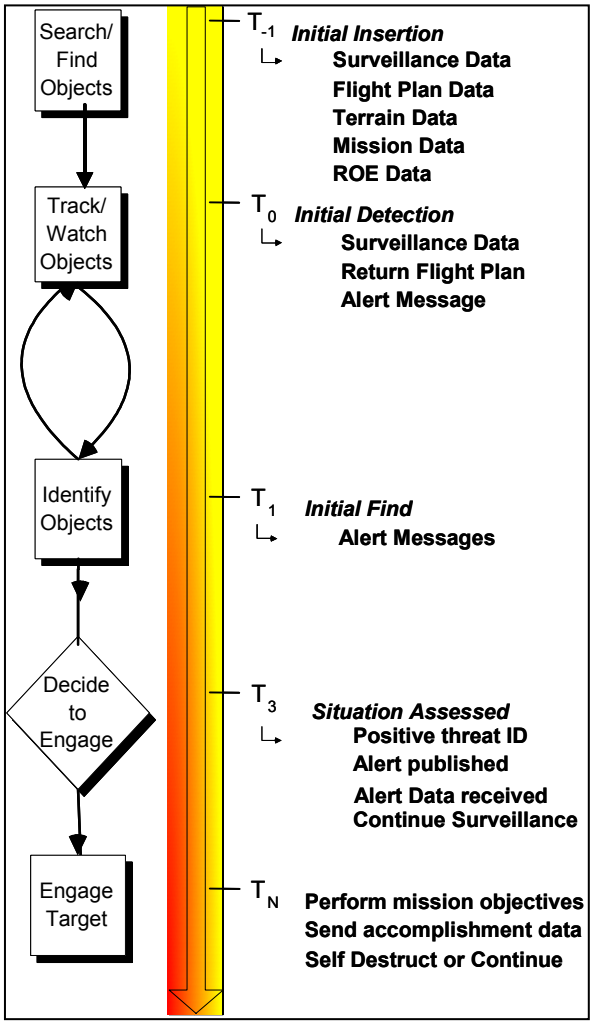


Figure 3: Effects Based Operations

"Cyber-Craft" Example



As an example of a "cyber-craft" application (refer to Figure 4), consider a squad of marines entering a residential area. Current intelligence is about 20-mins old and the squad leader requires updated information. The squad leader finds an electrical outlet and plugs in. This outlet allows access to the power grid of the town and subsequently access to the adversary's computer network. The squad leader injects a "cyber-craft" into the system (T_{-1} in Figure 4), whose mission is to locate a) any insurgents or b) locate any hidden military facilities. At time T_0 the "cyber-craft" has detected some activity at a military installation within 1000-ft of the Marines location. The "cyber-craft" performs a "recce mission" to gather intelligence on the insurgents (exact location, number, arms, etc.) and sends back data/information to the marines. However, in the meantime the marines have moved and have located a different means of connecting to the network. The "cyber-craft" has "sensed" this shift so readdresses the feedback information to the marine's new location and port. The "cyber-craft" acquires a positive ID (T_3), and sends an alert message back to the marines that the insurgents are about to leave and may be heading their way. At time T_N, the "cyber-craft" executes its orders (turns power off, locks the doors), sends back an acknowledgement and self destructs.

Figure 4: Possible "Cyber-Craft" Scenario

Technology Challenges of a Cyber-Craft within Joint Urban Operations

From the Joint Advanced Warfighting Program (JAWP), the following were determined to be challenging areas for improving military operations in urban environments:[10]

1. Intelligence, Surveillance, and Reconnaissance. The urban environment is composed of man-made structures, non-combatants, and a functional infrastructure. The challenges for ISR include: short line-of-sight, interiors and subterranean structures, clutter, target movement, positioning and vulnerability of sensors and platforms, identification friend, foe or neutral, maintaining covertness of sensors, communications and platforms, and increase requirements for precision targeting, timing, and weapon effects due to rules of engagements.
2. Command and Control. The urban challenges are in the areas of obstructions, shadowing and multi-path effects on communications and position location, cluttered information environment, reliable and secure C3, and position location of friend, foe or neutral.

[10] "Department of Defense Roadmap for Improving Capabilities for Joint Urban Operations," Volume 1 and Volum2 2; 2003; William J. Hurley, Task Leader; IDA Paper P-3643.

3. Weapons. Within an urban environment the weapons must: be employed in precise attacks where structures may interfere with trajectories or approaches, minimize collateral damage, attack targets that are indoors, underground, moving, intermittent, or near non-combatants.
4. Modeling and Simulations. M&S, if properly tied to architectures, concept development, experimentation, acquisition, testing and training will play an essential role in interoperability assessments to augment live testing and exercises.
5. Training and Training Facilities. There is a lack of interoperability and joint urban training requirements, and no recruiting, selection or training standards for urban warfare.

It seems apparent that the utilization of a "cyber-craft" could assist in solving items 1, 2 and 3 above. However, much work needs to be accomplished before the "cyber-craft" can be an operational entity. For example, research needs to be accomplished in the following areas:[11]

1) Simulations of multiple, interdependent infrastructures. Includes research into interdependencies and emergent behaviors of complex adaptive systems;
2) Basic research that connects decision-making behaviors (desired political-military outcomes at the operational and strategic levels) to specific physical effects (operations and military actions);
3) intelligent agent based systems to collaborate, coordinate and solve problems, automatically without human intervention. These agent based systems will have the ability to sense there environment and based on goals and constraints, provided by the user, achieve the objectives assigned;
4) Real-time updating of simulations. Includes real-time data ingestion and updating, dating mining, data validation, and methods of handling extremely large, dynamic datasets;
5) Self-organized modeling with the basic ability to have the models automatically organize themselves based on present conditions and predict the future battlespace environment;
6) Cyber defense and offense techniques including new ways of detecting attacks and executing attacks, countering adversary attacks, responding, performing forensics and anti-forensics and gaining real-time cyber situational awareness/understanding; and,
7) C2 theories such as control theory, uncertainty management and decision making theory.

Reflections

The path to developing a "cyber-craft" is not totally clear at this point in time. Not only are there technological challenges, but there are employment issues that need to be resolved as well. Some of the more challenging thoughts are as follows:

- **How do we develop a "Cyber-Craft?** It is envisioned that the "cyber-craft" would be tailored after the Joint Battlespace Infosphere's (JBI) concept of a "Fuselet". A "Fuselet" is a user directed software encapsulation that can provide some form of "sensemaking" within an information network. The user (in this case the warfighter) would simply be able to "publish or post" the "cyber-craft" onto the network in what ever manner that is available. Since the user must be mobile, the JBI's concept of "force template" must be taken into account. This is the ability to be able to rapidly "plug" back into the network, no matter where the entry port is located. It is the "infosphere" that keeps track of the various entities and ensures that the entity receives the desired information.

- **How can we "trust" the "cyber-craft" to "do the right thing"?** This is probably one of the more significant stumbling blocks in using a "cyber-craft" in an operational environment. How can the warfighter tell whether or not the information received is correct or not? Is the adversary interjecting "falseness" into the information? This needs to be investigated and technologies need to be developed in order to ensure high accuracy of the data/information so the warfighter will, in time, begin to trust the information provided. In regards to deploying a cyber weapon, it is the same thing. The warfighter will need to trust that the weapon will do what it is suppose to do in both time and place.

[11] Information taken from an AFRL/IF MURI proposal.

- **How do you control the "Cyber-Craft"?** The goal is to develop a system that follows the "fire-and-forget" methodology. However, with this philosophy comes the danger of a "cyber-craft" morphing into something that performs unintended actions that would be harmful to friendly forces or provide an adversary with information about the sender's intentions, position, etc. One way of controlling a "cyber-craft" is have it "dissolve" after completing its' mission. However, depending on the level of the "cyber-craft (strategic, operational, and tactical) the mission length can go from minutes to years... Thus, the damage that can be inflicted by a rogue "cyber-craft" could be significant.

- **How can a "cyber-craft" determine the "landscape" or "terrain" of an adversary's network?** The "cyber-craft" needs to "carry" along with it a set of "packets" that assist in analyzing the adversary's network (termed landscape or terrain) in real-time as it traverses the network in search of data/information. This can become extremely difficult the more the adversary's network structure diverges from the expected.

- **How do you provide stealthy feedback mechanisms?** Not only must the "cyber-craft" have stealth capabilities (refer to Table 1), but any return messages the "cyber-craft" sends back must not be able to be detected, intercepted, or modified. If the adversary was able to tell that data/information was accessed or somehow have the ability to "capture" any of the return messages from the "cyber-craft" then this will not only alert the adversary but may allow them to "insert" bogus messages into their network to provide conflicting information to the warfighter. Additionally, if the adversary could somehow "follow" the "cyber-craft" back to the source, then the warfighter could be placed in unknown danger.

- **What would be possible missions of the "cyber-craft"?** It seems reasonable to assume that once you can get access to an adversary's network, a "cyber-craft" could do a host of missions. Some of the more important ones being: a) intelligence gathering (non-traditional ISR asset), weapon delivery (in this case one could disable terminals, nodes or the entire network as well as send commands to "fry" their hard drives), intrusion detection (has our "cyber-craft" been detected or is it being followed) , effects monitoring.

- **What effect measures would the "cyber-craft" have to gather?** One of the challenges within effects based operations (monitoring, planning, assessment, execution) is determining what metrics to capture to tell whether or not desired effects are being accomplished (or not). Within the cyber domain, this is of equal challenge. It is the capturing of measurable metrics that is the challenge in order to be able to quantify the attainment (or not) of desired effects (as well as 2nd and 3rd order effects).

Summary

This thought provoking paper introduced the concept of a "cyber-craft" to complement the other domains operating under the Network-Centric Warfare construct in the Information Age. Utilizing the "cyber-craft" poses many challenges, especially with its use in the Global War on Terrorism (GWOT) and in a Joint Urban Operations (JUO) environment.

This "cyber-craft" will need to seamlessly traverse from the wired to the wireless and back as information travels the maze of access devices to its end user. Cyber agents will need to embody the ability to covertly travel across these mediums, constantly assessing the network layout, morphing itself as networks change, and remaining covert while maintaining the integrity of its mission. Increased use of data hiding techniques and data hiding detection techniques add additional complexity to the "cyber-craft's" arsenal. The "cyber-craft" will require the ability to constantly "ping" its surroundings to insure it is not being tracked or has not become a carrier for an adversary's cyber weapon. Additionally, these 21st Century cyber weapons need to perform real-time continuous self-assessment of the adversary's detection capability and be able to make instant decisions to morph or self-destruct or avoid "capture".

Significant technological and doctrine challenges remain to be solved before these "cyber-crafts" can become an effective military weapon. Agent development, agent size and complexity, detection technology, real-time agent learning and self morphing technology, RF and network penetration technology

are a few of the technological challenges requiring additional investment. Doctrine issues for fusing missions, weapon effect profiles, service/agency roles and missions are a few of the doctrine challenges to be solved.

These are only of thoughts of what could be and what is needed. Many technical and operational hurdles will need to be overcome if this vision is ever to become reality. We welcome any other opinions people may have on this subject.

Bibliography

Paul W. Phister, Jr., Ph.D., P.E.

Dr. Phister is the Air & Space Strategic Planner at the Air Force Research Laboratory's *Information Directorate* headquartered in Rome, New York. Dr. Phister holds two masters degrees and received his Ph.D. in Engineering from California Coast University. Dr. Phister is a licensed Professional Software Engineer from the State of Texas.

Daniel F. Fayette

Mr. Fayette is the Technical Advisor for the Command and Control Engineering Branch at the Air Force Research Laboratory's *Information Directorate* headquartered in Rome, New York. Mr. Fayette holds a Masters Degree in Electrical Engineering from Syracuse University and an undergraduate degree in electrical engineering from the University of Detroit.

Emily A. Krzysiak

Ms Krzysiak is the lead for the Communications Intelligence Group at the Air Force Research Laboratory's *Information Directorate* headquartered in Rome, New York. Ms Krzysiak has a BS in Mathematics and completed her course work for a masters in Computer and Information Science from the State University of New York.