DAHLGREN DIVISION
NAVAL SURFACE WARFARE CENTER
Dahlgren, Virginia 22448-5100

NSWCDD/TR-05/36

A DEFINITIVE WORK ON FACTORS IMPACTING THE ARMING OF UNMANNED VEHICLES

MAY 2005

BY: John S. Canning
Engagement Systems Department

REPORT DOCUMENTATION PAGE	Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	May 2005	Final

4. TITLE AND SUBTITLE
A Definitive Work on Factors Impacting the Arming of Unmanned Vehicles

5. FUNDING NUMBERS
---

6. AUTHOR(s)
John S. Canning

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Commander
Naval Surface Warfare Center
Dahlgren Division (Code G80)
17320 Dahlgren Road
Dahlgren, VA 22448-5100

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
---

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE
---

13. ABSTRACT (Maximum 200 words)
We realize that the weaponizing of unmanned vehicles (UXVs) takes us into largely uncharted waters. This document is an attempt to examine as many of the issues surrounding this area as possible.

14. SUBJECT TERMS
UXV, unmanned vehicle

15. NUMBER OF PAGES
48

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	UNCLASSIFIED	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev 2-89)
Prescribed by ANSI std. Z39-18
298-102

FOREWORD

We realize that the weaponizing of UXVs begins to take us into largely uncharted waters. This document is an attempt to examine as many of the issues surrounding this area as possible, but it is realized that we may have missed some. Because of this, the author invites readers to return comments on the presented material, and on issues that may not have been covered. The purpose is to gather thoughts from as many sources as possible to ensure a robust treatment of this important area. Please return comments, or new issues, to one of the following:

Mailing address:

ATTN G80/Canning
Naval Surface Warfare Center, Dahlgren Division
17320 Dahlgren Road
Dahlgren VA 22448

E-mail address: John.S.Canning@navy.mil

Approved by:

CRAIG SMITH, Deputy Department Head
Engagement Systems Department

CONTENTS

TABLES

ACRONYMS

ABHA	Agent-Based High Availability
ACTD	Advanced Concept Technology Demonstration
AI	Artificial Intelligence
ATR	Automatic Target Recognition
BDA	Battle Damage Assessment
CONOPS	Concept of Operations
COTS	Commercial Off-the-Shelf
CVNX	Aircraft Carrier, Nuclear, Unnumbered
DARPA	Defense Advanced Research Projects Agency
DoD	Department of Defense
DOE	Department of Energy
DUF	Discriminate Use of Force
EA	Electronic Attack
FAA	Federal Aviation Administration
FOV/I	Field of View or Influence
GHz	gigahertz
HDTV	High Definition Television
IBM	International Business Machines
ID	Identification
IM	Insensitive Munitions
IR	infrared
JAG	Judge Advocate General
JPL	Jet Propulsion Laboratory
KIF	Knowledge Interchange Format
KQML	Knowledge Query and Manipulation Language
LADAR	laser radar
LOCAAS	Low Cost Autonomous Attack System

Mbps	megabits per second
MHz	megahertz
Mk	Mark
MLS	Multi-Level Security
NASA	National Aeronautics and Space Administration
NRAC	Naval Research Advisory Committee
OCR	Optical Character Recognition
OODA	Observe, Orient, Decide, and Act
PEO	Program Executive Office
RF	radio frequency
ROE	Rules of Engagement
SFCs	Squad Functional Capabilities
UAV	Uninhabited Air Vehicle
UCAS	Uninhabited Combat Air System
UCAV	Uninhabited Combat Air Vehicle
UGV	Uninhabited Ground Vehicle
U.S.	United States
USMC	United States Marine Corps
UXV	Unmanned Vehicle(s)
Wi-Fi	Wireless-Fidelity
WMD	Weapons of Mass Destruction

INTRODUCTION

The Naval Surface Warfare Center, Dahlgren Division's Coastal Systems Station initiated a special study in 2000 to examine the potential of unmanned systems to augment United States (U.S.) Naval Forces in the future. In June 2001, Summey, et al,[1] published a report on this study effort. The report found that "…there is a coherent overall framework for the development, deployment, and operation of unmanned systems on a broad basis across the major naval mission areas." The study found that, "Standardization and modularity across all unmanned systems will be the key to affordability." While touching on the issue of arming unmanned systems, the document did not go into the topic in detail.

A Panel for the Naval Research Advisory Committee (NRAC) conducted a study during June 2002 – March 2003, producing a draft report on roles for unmanned vehicles (UXVs).[2] The panel arrived at the following conclusions: (1) the combat potential for the use of UXVs is virtually unlimited; (2) quantitative analysis and metrics are lacking; (3) Naval programs are not coordinated or focused; (4) lessons learned are not institutionalized; and (5) cultural and policy obstacles exist. One of the recommendations in this report was to, "focus on technology obstacles for the next generation of unmanned vehicles." Again, while touching on the topic of arming UXVs, this second document did not go into detail, except in noting their unlimited potential for combat, and noting the fact that there are cultural and policy obstacles to their use.

Regarding the cultural issues, it was stated that the U.S. political and civilian culture expects a minimum number of U.S. casualties, arguing for the use of UXVs in combat by substituting them for people on the battlefield. Diametrically opposed to this is the policy issue regarding the fear of autonomous operations being too dangerous or "going out of control," causing unintended casualties or collateral damage. This has resulted in a general reluctance to arm UXVs. This reluctance has decreased to some degree with the recent successful use of the Predator unmanned aerial vehicle (UAV) armed with *Hellfire* missiles in both Afghanistan and Yemen.

The remainder of this document examines the issues of arming UXVs in some detail. The issues fall into two categories: (1) those associated with the arming of any vehicle, manned or unmanned, and (2) those that are peculiar to UXVs. In some instances the issues of the first category are concerns that are somewhat different between manned systems and UXVs. The use of UXVs has been stated to be desirable in missions that are "dirty (dealing with hazardous materials), dull (long dwell or duration), or dangerous (extreme exposure to hostile action)." These mission requirements translate to technology requirements for increased platform endurance, increased platform survivability, and/or lower platform cost. The dirty mission set implies low cost disposable (generally small) UXV systems, focusing on simple Commercial Off-the-Shelf (COTS)-based solutions.

ARMED VEHICLE HISTORY

The general public's view of armed UXVs is framed by the recent events in Afghanistan and Yemen, attacking members of Al-Qaida and the Taliban. In fact, regarding events in Afghanistan, the Washington Post[3] reported:

> "The star in the air campaign has been the lethal drone aircraft… More than any other innovation, the use of a Predator reconnaissance drone to launch *Hellfire* missiles is likely to be what the Afghan war is remembered for."

Despite this perception, we have had armed UXVs for a very long time, the first being the torpedo. As pointed out previously, "Robert Whitehead, the father of the torpedo, designed the first unmanned, self-propelled, underwater vehicle, packed with explosives in 1866."[1] Torpedo development has continued over the years. The U.S. now has the Mark (Mk) 48 torpedo – a very capable armed UXV. A submariner once told the author that you only had to answer two questions in order to use this weapon: (1) "Is the target in range?" and (2) "Do you want to kill it?" Obviously, the remark was a bit tongue-in-cheek, but it very effectively demonstrates that the technology has come a long way since 1866 in the development of armed UXVs. Besides torpedoes, mines also represent a version of armed vehicles. As an example, consider the Mk 60 CAPTOR mine. This mine launches a smart torpedo that then goes after a submarine target. The weapon lies dormant until a target is detected, at which time the torpedo swims out of its capsule to attack and destroy its target.

Likewise, the *Tomahawk*® Land Attack Missile, in its many variants, has become the armed vehicle of choice for opening attacks on enemy states. The newer Tactical *Tomahawk*® is poised to soon come available for use with more flexibility through in-flight retargeting. On the horizon is the Uninhabited Combat Air Vehicle – Navy (UCAV-N, recently renamed by Defense Advanced Research Projects Agency (DARPA) as the Uninhabited Combat Air System (UCAS)), a more traditional thought for an armed vehicle. Note, however, the Joint Publication 1-02 Department of Defense (DoD) Dictionary's definition of a UAV:

> "A powered, aerial vehicle that does not carry a human operator, uses aerodynamic forces to provide vehicle lift, can fly autonomously or be piloted remotely, can be expendable or recoverable, and can carry a lethal or non-lethal payload. Ballistic or semi ballistic vehicles, cruise missiles, and artillery projectiles are not considered unmanned aerial vehicles."

Many people would have a difficult time accepting an Aegis cruiser, or destroyer, as an unmanned, armed, vehicle, but once one of these ships has engaged the "Auto-Special" doctrine for weapon control, to a certain extent, that is precisely what we have. Conceived in the early 1970s, as a means to counter the massive air raids that the Soviets intended on mounting against our carrier battlegroups, this mode of operation was designed to take the human out of the loop in the target engagement process, thereby buying back reaction time, and ensuring that the battlegroups could survive.

These examples illustrate that we are not completely strangers in a strange land, when it comes to arming UXVs. There is an extensive history behind us, and many "lessons learned." The appearance of the armed Predator UAV on the battlefield is just a recent addition to the growing body of expertise in arming UXVs.

TRUST AND BLAME: TWO SIDES OF THE SAME COIN

Why is there reluctance to arming UXVs? People don't trust them, yet. (Note: There is a trust issue today with UAVs just being allowed to fly in the National Airspace System. Once the FAA is willing to regulate the flight of UAVs in this system, it will provide a legal precedent for wider acceptance around the world.) What is it that we don't trust? We don't trust that they will think and respond like humans when it comes time to pull the trigger. When we send a soldier out into the battleground, we have a set of expectations about his behavior that are framed by his orders, the established Rules of Engagement (ROE), his training, and his past experience in both the Service and society, and we trust that he will live up to those expectations. For example, we don't expect him to shoot women and children. Armed UXVs have yet to earn that trust.

Can we design-in trust? Not really, but we can design-in and test for reliability, and if, over time, these vehicles are found to be reliable by their human masters, then trust will follow. Designing-in reliability won't be easy, however. There are a host of issues that will have to be addressed in this process, but it will add up to the vehicles acting as reliably as humans do on the battlefield.

In ancient times, this would have meant standing shoulder-to-shoulder with your fellow warriors, slaying the enemy directly in front of you with your axe, sword, spear, arrow, or other weapon. Today, things have changed, and you may have difficulty telling who the enemy is amongst those around you. As an example, how do you tell the difference between a terrorist and an innocent civilian out on the street? Human warriors have trouble doing this today. It is not any easier for armed UXVs.

On the flip side of the coin: What happens when that soldier does not live up to our expectations of him on the battlefield? He may find himself facing a court-martial, or other disciplinary action. For example, consider the following case:

During the early 1970s, onboard a U.S. aircraft carrier, two F-4 fighter aircraft were catapulted off the ship for a mission. The first aircraft successfully completed the launch, but the second encountered a problem. During the launch, the catapult bridle slapped the centerline external fuel tank that the aircraft was carrying, causing it to rupture. The leaking fuel quickly flowed aft and was ignited by the aircraft's engine, which was operating in afterburner mode. The flight safety officer onboard the ship observed this event and immediately radioed, "You're on fire. Eject! Eject!" The pilot of this damaged aircraft lost no time and ejected immediately. Unfortunately, the pilot of the first aircraft off the ship was still on the same radio frequency, and thought the radio transmission was meant for him. He also ejected, and a perfectly good F-4 was sent to the bottom of the ocean. The ensuing accident investigation faulted the pilot of the

damaged aircraft for not checking his instruments to verify the fire, and not verifying that it wasn't controllable before he ejected. The flight safety officer was faulted for not identifying in his radio transmission which aircraft he was referring to, and the pilot of the first aircraft off the deck was faulted for not checking his instruments to verify the fire before he too ejected.

Was this an odd situation? Yes. Do other equally bizarre events happen? Yes. Accidents happen all the time, and blame is assigned. At issue is whether a particular incident is a career-ender, or not? Given that we are dealing with systems that can take human life, the probability that the incidents could be career-enders goes up considerably. No one wants to be in a position where something that occurs under his or her command could cause him or her to be forced out of the Service, or even court-martialed.

As an example, consider the development and deployment of technology to support Multi-Level Security (MLS) in military command & control and information systems. The technology to support MLS is available today. The reason why it isn't more widely deployed has more to do with sociological issues of fielding it than with the technology itself. Everyone is concerned about what happens if it fails. Who gets court-martialed if some classified information gets released automatically to the wrong people? The certification process for MLS is incredibly long and arduous.

Who do we court-martial if an UXV doesn't live up to our (human) expectations on the battlefield? The remote operator? Depending on the level of autonomy, he may not be in direct control of the vehicle at the time of an incident. The battlefield commander? He would give the order that led to the use of the vehicle in an, ultimately, accidental manner. The vehicle designer? While not likely, current attempts by some individuals to sue firearm manufacturers for deaths caused by one of their products gives one pause to think about this aspect of the problem. As will be seen later, blame could be assigned to the independent organization that tests the vehicle, and certifies it ready for combat duty, if the testing is not extensive enough to uncover hidden problems.

Testing can be problematic, however, as can be seen from Live Fire Test & Evaluation (LFT&E) programs. Truly realistic testing may not be possible. As an example, consider the firing of a cruise missile directly at a ship to see if the ship's onboard defenses can shoot it down. You cannot take the risk of what might happen if the defenses fail to knock the missile down. Consideration must be given to extensive testing through wrap-around modeling and simulation.

Regardless of how robust the design of an UXV, we should understand the reliability built into it, and the limitations of our understanding of that reliability. We should trust it to do the job it was designed to do, but accept the fact that accidents will occur, and look at each occurrence to assign blame on a case-by-case basis, establish "lessons learned" as recommended by the NRAC Panel, and incorporate them into new versions of the vehicle (or its software).

Metrics are important for establishing norms and tracking trends. It has been suggested that some appropriate metrics for UXVs might be Mishap Rate, Mean Time Between Failure, Availability, and Reliability. These could be extended to cover armed UXVs.

DEGREE OF AUTONOMY

The reliability we need to build into these vehicles will be, to a large extent, a function of the degree of autonomy we give them. There is hardware reliability and there is software reliability. We are referring primarily to the reliability of the software because it will be the software that will be the primary determinant of "human-like" behavior.

Generally, there are three levels of autonomy that need to be examined: Tele-operated, Semi-autonomous, and Fully-autonomous. These correspond to always having a man-in-the-loop, sometimes having a man-in-the-loop, and not needing a man-in-the-loop, respectively. We avoid stating that there is never a man-in-the-loop, simply because a vehicle must respond to some human input, even if only at the beginning of its mission. Additionally, the designs must be human-centric to fully support whatever human presence is left. At the lower levels of autonomy, the degree of reliability built into the software is not as critical as that built into the software of higher levels of autonomy, simply because there can be a human operator in the loop to watch over operations, to step in when needed to take control. Which level of autonomy a vehicle is in may depend on where in its mission profile it is, or what its current circumstances are? Tele-operation capabilities are important to the warfighter because they enable standoff operations and thereby reduce or remove operator risks in highly stressful and dangerous environments, such as minefields and in areas of potential explosive hazards. However, these capabilities alone do little to reduce operator task loading or to reduce the ratio of operators to platforms. Moreover, it is generally recognized that future second generation high payoff capabilities can only be realized when platforms exhibit semi-autonomous (or higher) mobility capabilities, navigation, and mission accomplishment.

Scalable levels of autonomy will probably be necessary to accommodate varying ROE for contingencies from peacekeeping to force-on-force. Specifically, the Air Force Research Laboratory has defined ten levels of autonomous control for UAVs (Table 1).

Table 1. Level Of Autonomous Control

LEVEL OF AUTONOMOUS CONTROL	*DEFINITION*
1	Remotely Guided
2	Real Time Health/Diagnosis
3	Adapt to Failures and Flight Conditions
4	Onboard Route Replan
5	Group Coordination
6	Group Tactical Replan
7	Group Tactical Goals
8	Distributed Control
9	Group Strategic Goals
10	Fully Autonomous Swarms

The Army has defined ten levels of semi-autonomous uninhabited ground vehicle (UGV) behavior for the Future Combat Systems (Table 2).

Table 2. Level Of Autonomous Behavior

LEVEL OF AUTONOMOUS BEHAVIOR	*DEFINITION*
1	Remote Control/Tele-operation
2	Mission and Task Planning
3	Improved Route Following on Paved Roads
4	Unimproved Route Following Dirt Roads
5	Off-Route Mobility No Roads
6	Obstacle Detection and Alert Operator (>0.2 meter Obstacles)
7	Obstacle Detection and Auto Negotiation (>0.2 meter Obstacles)
8	Tactical Payload Mission Behaviors
9	Cooperative Behaviors with Manned and Unmanned Systems
10	Reactive Intelligent Tactical Behaviors

For higher levels of autonomy, we need to begin to look to the concept of "autonomic computing."[4] Autonomic computing is so-named because it is a systemic view of computing modeled after a self-regulating biological system, and it must act like a being's autonomic nervous system. Like the human autonomic nervous system, an autonomic computing system automatically reacts to changing external conditions without outside intervention. Autonomic computing is a phrase that describes self-managing computers, or computers that can monitor themselves and automatically adjust to optimize performance and circumnavigate hardware and software failures. An autonomic system must provide an unprecedented level of self-regulation while hiding system complexity from the user. This leaves the human user free to concentrate on higher level, more important tasks, such as weapons release-related functions. This will be extremely important as the number of humans involved in the control of multiple vehicles declines, and especially important since we are dealing with lethal force systems. We will have to view the combination of multiple vehicles, human controllers, and the control systems, as a single large information system. The shortage of "operators/supervisors," combined with the complexity of information technology infrastructure, prevents us from taking advantage of the larger system's full potential, unless we embrace autonomic computing precepts. This is a radical shift away from the way we develop computing systems today. Among the goals for autonomic computing systems are:

- Manage complexity
- "Know" themselves
- Continuously tune themselves
- Adapt to unpredictable conditions
- Prevent and recover from failures
- Provide a safe environment

Autonomic computing is run by control loops. A sensor collects operational data from a working system. Preset behavioral models analyze the data, and unusual behavior is passed onto

decision-making software, which can then adjust the system to compensate for unusual activity. Behavioral models that better predict how applications, networks and systems behave still must be created before autonomic computing can become a full-fledged reality.

Besides the efforts of International Business Machines (IBM), DARPA has sponsored some work in autonomic computing, under the Dynamic Assembly of Systems for Adaptability, Dependability, and Assurance program at the Pacific Command by the Programming Systems Laboratory, Columbia University ("Kinesthetics eXtreme"). The command tried autonomic computing tools created by a consortium funded by DARPA to build a reference architecture for self-healing computing. DARPA's Self-Regenerative Systems program seeks to develop systems that can respond automatically to cyberattacks. Some of the desired capabilities of this effort include self-optimization, self-diagnosis, and self-healing. Hewlett-Packard is investigating the autonomic concept with its Adaptive Enterprise Initiative. Sun Microsystems, Inc. has another autonomic effort ongoing with its N1Grid program. The object of this program is to try to manage a group of computers as if it were just one. This is interesting, since it could easily be extended to the concept of multiple UXVs operating as an information grid under a single operator. Specialty firms Stottler Henke Associates, Inc., and Cassatt Corp. also have related efforts. Stottler Henke has been working on efforts for the Department of Energy (DOE), under a Small Business Innovative Research contract, to develop its Agent-Based High Availability (ABHA) system smart job recovery software. The software is to be put to use at DOE's Lawrence Berkley National Laboratory in an application that analyzes data from a nuclear physics experiment. The object is to help cluster long-running batch jobs, and when a job fails, the software diagnoses the problem, restarting the job, if possible. While ABHA is to be initially deployed on a Linux/Intel cluster involving several hundred nodes, the belief is that it will become more valuable as researchers submit jobs to run across multiple clusters. Cassatt is pursuing efforts in a grid-computing environment to make it self-healing and self-optimizing. The Office of Naval Research also sponsors the Autonomous Operations Future Naval Capability efforts.

As the degree of autonomy increases, the trust of designing a vehicle that uses lethal weapons decreases. Conversely, the situation is more-or-less reversed for non-lethal weapons. The reason for this is that people get nervous when considering a driverless vehicle that could kill someone accidentally. However, if the same vehicle were to just temporarily incapacitate the victim, people are more accepting. Regardless of using lethal or non-lethal weapons, positive means must be provided for control of weapon employment.

Another aspect of fully autonomous operations will be the degree of "reactivity" that a UXV must employ. As an example, a UXV could be preprogrammed to travel from point A to point B, deliver a weapon at point B, and then return to point A. As long as nothing interferes with executing the stored program, then the reactivity of the vehicle in executing the mission is low. If, however, the conditions encountered along the way don't match those that were programmed into the UXV at the beginning, then the UXV will need to react to the differences, and adjust its behavior in order to complete the mission. This is an example of replanning.

We can also easily fall victim to what is known as the "automation irony." In the past, when the operations of systems have indicated that certain processes commonly fall victim to operator error, the immediate reaction is to automate the process to remove the human from that

portion of the loop. The need for human input can usually be reduced, but not totally eliminated, causing designers to focus on automating the easier-portions of the process, leaving the humans with the tougher jobs to do. This means that *all* the jobs left to the human operators tend to be the more difficult ones, thereby *increasing* the likelihood of operator error. As the level of automation goes up, the chance of encountering this problem increases. We must take care to ensure that the remaining man/machine interface is human-centered and human-friendly.

A final item that we must pay attention to with respect to the degree of autonomy designed-into a vehicle is the real-time environment constraints. This is where we must respond to real-world events, sometimes on a timescale of milliseconds, as in Anti-Air Warfare engagements, in order to maintain precious reaction time. As the degree of autonomy goes up, the total amount of computer code that must be executed increases, but the time in which it needs to run does not. If the code does not execute quickly enough, the vehicle's "intelligence" will not keep up with real-world events and operations will quickly fall apart. This problem has been illustrated in attempts to build robots that walk. In early attempts, the processors onboard the robots could not process sensory data fast enough to compensate for uneven ground or objects quickly put in their way. The result was that they would begin to fall over, not be able to process the new sensory data fast enough that indicated they were falling, and then crash to the ground.

This will be of increasing importance as time progresses, and we move from engaging men to engaging other UXVs. Today, it is important that we operate inside a human adversary's Observe, Orient, Decide, and Act (OODA) loop. The OODA loop is a concept coined by Colonel John R. Boyd, United States Air Force (deceased), in the 1950s to help describe the need to be able to sense what's on the battlefield, figure out where everything is on the battlefield in relation to yourself, decide what to do, and then act upon that decision before your adversary can act. Armed UXVs will need to be faster than people are today at doing this, but as adversaries begin to field their own UXVs, our armed UXVs will need to be able to stay inside the OODA loops of their UXVs.

Today's processors are much faster than in the past, and are getting increasingly faster. Still, silicon chips have their fundamental limits. Eventually we will have to look at computing technologies such as optical, biochemical, molecular, or quantum processing. One other avenue to explore is parallel processing to make gains in throughput from more traditional computing hardware.

ACHIEVING "RELIABILITY"

Recall that we said that we would like to trust an UXV to behave like a person on the battlefield, exhibiting expected types of behavior that a person would exhibit. As the level of autonomy increases, the need to have this reliability built-in increases. Oddly enough, a machine may be better suited to achieving battlefield reliability than the human. Consider the comparison between man and machine (Table 3).

Table 3. Comparison Between Man And Machine

HUMAN EXPERTISE	***MACHINE EXPERTISE***
The Good News:	*The Bad News:*
Creative	Uninspired
Adaptive	Needs to be Told
Sensory Experience	Symbolic Input
Broad Focus	Narrow Focus
Commonsense Knowledge	Technical Knowledge
The Bad News:	*The Good News:*
Perishable	Permanent
Difficult to Transfer	Easy to Transfer
Difficult to Document	Easy to Document
Unpredictable	Consistent
Expensive	Affordable

It is readily apparent from this comparison that human and machine expertise are complementary. However, many times we've heard references to really good combat troops behaving like robots on the battlefield. What we'd really like to do is to have unmanned combat systems that combine the good characteristics from both human and machine expertise. People behave in unpredictable ways at times, whereas a machine will always be predictable. This is not the same as acting in an *unexpected* manner, however. Software-based performance, unlike its human counterpart, is guaranteed to be repeatable when circumstances are repeated. If we have *fully* tested an UXV in its expected battle environment, then we can reasonably predict what it will do in a given situation. However, if the testing was incomplete, the vehicle may behave in an unexpected manner when it finally gets to the battlefield and meets a situation it was not tested for.

In the past, we have developed expert systems technology. There are rule-based systems that mimic human experts in particular domains of interest. Knowledge engineers work with the human experts to develop strategies, rules-of-thumb, and domain rules. The knowledge engineers then code these items into a set of rules that can be used to automatically solve complex problems that occur within a given domain. As long as the problems encountered fall within the domain of problems explored and coded by the knowledge engineers, rule-based expert systems work very well. However, their solutions tend to fall apart if they are applied to problems that have not been previously addressed within the domain by the knowledge engineers and their human experts. (As, for example, when something that was not originally tested for is encountered.) This gets to the difference in focus and adaptivity between human and machine expertise, noted above. The machines lack knowledge of the world *context* that they are in, something that people learn from birth.

There is an issue dealing with emerging missions not currently being performed. Today's forces are fairly flexible, and can handle changes. Some changes are handled more easily than others. Machines are designed with specific purposes in-mind. They are not as flexible as people. There may be some difficulty in adapting UXVs to new missions that had not previously been considered.

How do we overcome this situation and further extend the reliability of our UXVs? One solution is to extend the rule-set for the problem domain addressed by the expert system. (This is providing additional world context.) However, one will only be able to do this after it has become apparent that there is a hole in the current domain space that needs to be covered.

There are also other methods of addressing expert systems. One such method is to employ semantic nets. This approach uses a network structure of nodes and arcs. The arcs describe relations between nodes, and nodes represent objects, concepts, or events. It uses the arc relations to infer conclusions about node “things.”

Another method is a frame-based approach. It is organized like semantic nets, but in an inheritance hierarchy. The topmost nodes represent general concepts, and lower nodes are more specific instances. Concepts at each node are defined by attributes in “slots.” It uses the inheritance of the slots to infer conclusions.

Traditional expert systems work well within their defined domains, but not outside of them. Fortunately, there are other forms of artificial intelligence (AI) that have been developed to address the *uncertainty* that besets tackling things that occur outside the known problem domain.

There are some newer, natural-based approaches. One deals with neural networks. There is no one definition of neural nets, with every author seemingly coming up with his own. Where do we want to use neural nets? We want to use them where we can’t easily formulate an algorithmic solution. We also want to use them where we can get lots of examples of the behavior we require, and where we need to pick out a structure from existing data. Normal computers, and traditional artificial intelligence, are based on an abstraction of human information processing. Neural networks, on the other hand, are based on the parallel architecture of animal brains. They are a form of a multi-processor computer system. They can be used in supervised, or unsupervised nets. In a supervised network, a “teacher” is needed to tell the network what the “desired” output should be. In an unsupervised net, the network adapts purely in response to its inputs. It then learns to pick out structure from the input. They are particularly useful in dealing with sensory data.

Another deals with genetic algorithms. Genetic algorithms are a part of evolutionary computing, which is a rapidly growing area of artificial intelligence. Genetic algorithms are inspired by Darwin's theory about evolution. Simply said, the solution to a problem solved by genetic algorithms is evolved. If we are solving some problem, we are usually looking for some solution, which will be the best among others. The space of all feasible solutions is called the search space (also state space). Each point in the search space represents one feasible solution. Each feasible solution can be "marked" by its value or fitness for the problem. We look for a solution, which is one point (or a collection of points) among feasible solutions. The looking for a solution is then equal to looking for some extreme (minimum or maximum) in the search space. The search space can be wholly known by the time we are through solving a problem, but usually we know only a few points from it and we are generating other points as the process of finding “the” solution proceeds. The problem is that the search can be very complicated. One does not know where to look for the solution and where to start. There are many methods of how to find some suitable solution. The algorithm is started with a set of solutions (represented by chromosomes) called the population. Solutions from one population are taken and used to form a

new population. This is motivated by a hope that the new population will be better than the old one.

Solutions that are selected to form new solutions (offspring) are selected according to their fitness - the more suitable they are the more chances they have to reproduce. This is repeated until some condition (for example, the number of populations or improvement of the best solution) is satisfied.

Still a third method is fuzzy logic. A fuzzy expert system is an expert system that uses a collection of fuzzy membership functions and rules, instead of Boolean logic, to reason about data.

Fuzzy logic allows for numbers between 0 and 1, shades of gray, and “maybe” as valid answers. When the approximate reasoning of fuzzy logic is used with an expert system, logical inferences can be drawn from imprecise relationships. It is used, for example, to optimize automatically the wash cycle of a washing machine by sensing the load size, fabric mix, and quantity of detergent. Fuzzy logic is used to control passenger elevators, household appliances, cameras, automobile subsystems, and oddly enough, smart weapons. What's crucial to realize is that fuzzy logic is logic *of* fuzziness, not a logic that is *itself* fuzzy. But that's fine: just as the laws of probability are not random, so the laws of fuzziness are not vague.

Another AI area that needs to be investigated is that dealing with abstract board game technologies. The pre-eminent example in this field that comes to mind is IBM’s “Deep Blue” chess playing program, which has made worldwide headlines in its matches with the Russian grandmaster chess champion Gary Kasparov. These programs look into the future to see the results of possible strategies and moves, and then select courses of action that best optimize the chances of achieving success from the current position.

One such technology is “Linguistic Geometry,” a product of Russian émigrés to this country, and associated with Stilman Advanced Technologies, Denver, Colorado. This particular technology has been in development for about 30 years, and has shown a remarkable flexibility in the uses that it can be adapted to.

Still, even with these technologies that deal with handling uncertainty, there may be an issue of how an UXV will respond if it encounters a situation it wasn’t tested for. Contacting the human controller is one approach, and is an example of dialing-down the level of autonomy, but that may not always be possible. (Communications might be jammed, for example.) One approach may be to have it automatically withdraw from an area in order to re-establish communications with its human controller, download the situation to him, and wait for new instructions. Presumably, the human operator can figure out what to do, give the UXV further instructions, and add the situation to the “lessons learned” database for future reference. As time goes by, and other odd situations are added to the database for use in future planning, eventually the number of new incidents would drop off. Thus, the level of reliability would go up.

As was said previously, we are primarily concerned with the reliability of the software in developing trust, but that does not mean that we are focused on this aspect to the exclusion of all else. There is also a hardware component to reliability. In manned combat systems, we have

found it best to design systems that don't have single points of failure. Besides providing fault-tolerant architectures, we have found it necessary to design systems with parallel, redundant, paths for operations. This will also be necessary for armed UXVs. The ALTAIR,[5] a variant of the militarized Predator B, is to be the first UAV to meet requirements for flights in the National Airspace System. It is doing this with a dual fault-tolerant architecture flight-control system, and triple-redundant avionics to increase reliability. The ALTAIR, while unmanned, is not armed. We can do no less for armed UXVs.

THE IMPACT OF CONCEPT OF OPERATIONS (CONOPS)

The basic CONOPS for an UXV can be broken-down into offensive or defensive operations. Which of these operations an UXV is addressing can have a huge impact on arming it. These equate to either acting (offensive operations), or reacting (defensive operations). The problem space, in general, is much bigger for defensive operations than offensive operations. This is because one cannot anticipate every eventuality of what a potential adversary might throw at you. This is less the case when you are the one doing the throwing, as in offensive operations. In the world of intelligence, this is summed-up by the phrase, "You don't know what you don't know." In defensive operations, you may not know the size of the problem space – let alone the details.

Another issue is that there is a CONOPS for the UXV, and another one for the weapons that it carries. These two CONOPS must be compatible, and the vehicle and weapon combination must be up to the combined task.

Part of the considerations for CONOPS must involve the tactics to be used. Will a UXV be operating by itself, or as part of a larger group? The tactics used will likely be different for single units than for multiple units, acting in close coordination. In either case, the arming of these UXVs must consider the tactics to be used, and match the sensors and weapons to the tactics. Tactics involving cooperating, multiple units will likely be more difficult to develop, since there will likely be complex interactions between these units. However, the logic built into the UXV's computer programs, and interface with human operators, must allow for the development and use of these tactics.

COST CONSIDERATIONS

UXVs are touted for use in applications that are "dirty, dull, or dangerous." While it may be attractive to use UXVs in these contexts, the contexts themselves will likely not be the driver that determines if UXVs get used or not. The determining driver will likely be the cost of providing a particular warfighting capability.

As an example, consider the case of the Navy's next-generation aircraft carrier, CVNX (a.k.a. CVN-21/78). The original Mission Need Statement for this platform did not ask for more,

or improved, performance over the existing *Nimitz*-class carriers. Instead, the number one requirement for this new ship class was for it to be more affordable than the *Nimitz*-class from keel laying to scrap yard (i.e., Total Ownership Cost).

In the studies that were conducted by Program Executive Office (PEO) (Carriers) on the elements that made up Total Ownership Cost, it was discovered that the long pole in the cost tent for the *Nimitz*-class was the cost of manning a ship over its lifecycle. The result of this was a push to reduce the manning of CVNX, and so investigations were held into technologies related to automation, robotics, and artificial intelligence. Concepts considered for this included such things as aircraft deck handling robots, floor scrubbing and waxing robots, maintenance robots, automated aircraft fueling and arming stations, more automation of reactors, automated damage control, and other ideas for reducing manning levels. (Interestingly enough, in the beginning, even though the concept of the uninhabited combat air vehicle (UCAV) was well established, and there was a joint Air Force and Navy program for developing UCAV technology, and it was readily apparent that UCAVs and the CVNX would coexist over the majority of their lifespans, PEO (Carriers) would not concede to UCAVs operating from the deck of the CVNX. This attitude has since changed.)

The point to this discussion is that moving to UXVs likely won't occur because it is "the right thing to do," considering the "dull, dirty, and dangerous" paradigm, but because we can provide a warfighting capability at a lower cost than with manned systems. That cost could include a cost in lives. (Note, however, that even a life can be given a monetary value for the military. As an example, consider the cost of replacing a pilot that has been shot down in battle. Besides the dollar cost of his salary and benefits to the point of his death, there is a dollar cost associated with training him to be a pilot, and to keep him proficient in his skills, right up to the point of his demise. All that then becomes a sunk cost that is not recoverable.)

As time goes on, it is expected that there will be a desire to raise the level of autonomy for UXVs. We must look at the cost of "unmanning" a vehicle, and its weapons, to achieve a particular degree of autonomy. First, how badly do you need an armed UXV? Is it the only way of accomplishing the mission, or are there other alternatives? As has been seen in many systems in the past, we can achieve 80 percent of the desired capabilities with the expense of 20 percent of the funding, but achieving the remaining 20 percent of the desired capabilities uses the remaining 80 percent of the funding. This is particularly true in dealing with the unmanning of systems, since the really difficult parts are likely going to be very costly to develop. (see the section *Degree of Autonomy*) At what point is it no longer cost effective to continue to try to unman a system? Can these functions remain off the vehicle, done remotely by a person, instead of being fully automated, and have the overall design still work correctly?

Reducing the number of operators, and having one operator able to control more than one UXV at the same time through the concept of "supervisory control" will help to lower the cost of manning a system of UXVs by developing the vehicles as a one-time "sunk cost" as opposed to the continuing cost of having to train new operators for each and every one of the vehicles. This concept allows the remaining operator to make high-level decisions about operations and vehicle conditions when needed, but the detailed running and monitoring of the vehicle on a minute-by-minute basis is done automatically.

It is expected that the cost of deploying UXVs will decrease through the standardization and modularity of components. Standardization allows the same component to be purchased from multiple sources, and competition between these sources will act to keep the cost of that component low. Modularity of components allows us to swap functionality in and out of vehicles, configuring them for specific missions just prior to their use. We must also consider standardization and modularity between different vehicles. As an example, we might have a UGV and UAV. While the exteriors may be different for their different environments, the computers they use could be the same, and some weapons might be interchangeable modules between the two vehicles. (Consider, for example, a gun that could engage enemy soldiers when mounted on the UGV, might also engage similar targets when mounted on a UAV.) We can purchase standardized vehicle frames at lowered costs, and then adapt them with standardized modular components for each mission. These can be powerful allies in the efforts to produce cost-efficient systems, but it is important to not lose sight of some mitigating factors, both pro and con.

It is important to consider the relative cost ratio between the projected target set and the weapon being considered. We don't want to be in a position where we are engaging a target that costs an adversary $5,000 to produce with a one-shot weapon that cost us $500,000 to produce. Ideally, the weapon should be much cheaper than the target it is engaging. Complicating this to some degree is the need to consider the value of the asset we might be defending with our weapon. If, for example, we are defending a very expensive asset, we may consider spending more on a weapon used to defend that asset than the cost of the weapon that an enemy might use against that asset.

Likewise, one must examine the issue of reusability, both for the weapon and for the vehicle, in our cost equation. (Note: every UXV can likely be used as a weapon just once by deliberately crashing it into a target.) We can stand to spend more for the item, if there is a reasonable expectation that it will be used to engage more than one target, and the collective costs of all the targets engaged is greater than the costs of the vehicle and weapons used. (Closely coupled with this is the issue of survivability: Does it need to be survivable, or is it expendable? Survivability is a balance of tactics, technology [for both active and passive measures], and cost for a given threat environment. For manned vehicles, survivability equates to crew survivability, on which a high premium is placed. For UXVs, this equation shifts, and the merits of making them highly survivable, vice somewhat survivable, for the same mission come into question.) Large complex UXVs will likely need to be reusable, simply because of the cost to procure them.

Unfortunately, operators are not the only personnel required to field and deploy UXVs. There are also personnel associated with servicing, launching, and retrieving (if not expendable) the vehicles. The primary objection to unmanned systems in today's Fleet deals with the additional manpower required to deal with these support needs. Armed vehicles may also require the services of properly trained weapons handlers. Care must be taken to ensure that there is an overall reduction in shipboard manning, not just a shift in billets, and that the remaining personnel are not overburdened. Ultimately, the measure of effectiveness will be the Total Ownership Cost, as previously discussed.

Another cost related issue is reliability. When National Aeronautics and Space Administration (NASA) launches lunar and Mars landers, they travel for long distances and periods of time without direct, hands-on human attention, and are expected to work upon arrival at their destination. This is expected to be done with great attention during the design and manufacturing phases to the reliability of components and software of the landers. Achieving this reliability is costly. Similarly, one will want to deploy reliable weapons on reliable UXVs in order to achieve expected results. The reliability of UXVs will be tied to their affordability because we have come to expect UXVs to be less expensive than their manned counterparts.

On 11 December 1998, NASA launched the Mars Climate Orbiter on a Delta II rocket. The payload contained two packages: (1) The Mars Climate Orbiter Color Imager, which was meant to acquire daily atmospheric weather images and high-resolution surface images and (2) the Pressure Modulated Infrared Radiometer which was to allow measurement of the atmospheric temperature, water vapor abundance, and dust concentration. The orbiter was also to serve as a data relay satellite for the follow-on Mars Polar Lander and other future NASA and international lander missions to Mars. The Orbiter was to remain in orbit for two years after reaching Mars. In this way NASA would get two smaller, cheaper missions, instead of one larger, more expensive mission. This “two-for-one” approach was hailed for economy and efficiency, and was the direct product of NASA having adopted the philosophy of “Faster, Better, Cheaper,” which was to allow them to fly more missions at lower cost.

On 23 September 1999, the Mars Climate Orbiter was supposed to enter orbit around Mars and commence operations. Instead, it crashed. The investigation that followed showed that this was caused by a grade school-level calculation error when the builder, Lockheed Martin, designed the Orbiter based on the English system of measurements, but that the NASA Jet Propulsion Laboratory (JPL) navigation team assumed use of the metric system of measurements. They entered the wrong values into the navigational computer. The changes made to the spacecraft’s trajectory were 4.4 times greater than what the JPL navigation team believed them to be. This loss cost the U.S. taxpayers $125 million.

Even though this mission had failed, NASA had already committed to the next Mars mission: the $165 million Mars Polar Lander, which was launched on 3 January 1999. The payload on this mission was meant to land near the Martian South Pole, looking for traces of water. NASA expected to see a signal from the surface of Mars on 3 December 1999, but no signal was ever received. It crashed, too, but for a different reason: a software error caused the Lander to deploy its legs too early, and to shut off its landing engines too soon. NASA had very visibly lost two missions in as many months at a total cost to the U.S. taxpayer of about $290 million.

Failure analyses of these two programs lead to a direct indictment of NASA’s much-touted “Faster, Better, Cheaper” philosophy. It was found that it works well if the appetite doesn’t exceed the resources, but that in these two missions there was a need for far more resources than were available.

There is a lesson to be learned from this: DoD is being urged to adopt the same “Faster, Better, Cheaper” philosophy that NASA did in efforts to modernize and transform the military. We must not make the same mistakes that NASA made. There is an old “rule of thumb” in

systems engineering design: “Good, Fast, Cheap – Pick any two.” This still holds true, and we must balance it with the demands of “Faster, Better, Cheaper.”

Severe operational environments can be cost-drivers, and the need to operate in a wide range of environments can be exceptionally expensive. Whatever environments the host vehicle is to operate in, its weapons need to operate reliably in the same environment.

In addition to the associated dollar-cost in deploying unmanned and armed systems, there is a comfort cost: People become nervous when thinking about a robot that could potentially kill someone without asking, or gaining, human permission to do so first. It is a question of having a “man-in-the-loop” for weapons release authority, or not, and how much is he involved in that loop? People are less nervous about the employment of non-lethal weapons, since a potential victim might actually be able to walk away from an engagement with minor injuries, if any at all.

VEHICLE SCALE

It isn’t possible to haul a 2,000 pound weapon on an unmanned platform weighing 2 pounds, so the scale of the vehicle must be considered in arming it. Small vehicles equate to small weapons, and large vehicles can equate to large weapons, but not always. Given the advent of precision-guided munitions, it is possible to take out a specific target with a smaller weapon than was typically used in the past. By going to smaller munitions, more aim points can be attacked by a single vehicle on a single mission. In this case, it can be better to stick with smaller weapons. However, if the intended target is hardened, a large weapon may be the only choice that will work. (Note that for hardened targets, it may be possible to trade weapon speed for size.) Common sense must be used.

On smaller vehicles, particularly those meant to be man-packable, weight becomes critical. A tradeoff needs to be done to see if it is worth the effort of putting a weapon on a small vehicle, vice just sensors, and, instead, relying on the weapons carried by the accompanying troops to provide use of force.

Vehicle scale can also be a driver for range and endurance, thus impacting the target set that can be addressed within an Area of Operations. This can impact the variety of missions that a vehicle may be called-on to address, and the quick-change flexibility that needs to be designed into the vehicle. There is also the consideration that a UXV capable of carrying a given weight of reconnaissance sensors and data links on a round trip could be modified to carry an equal weight of explosives twice that distance on a one-way mission.

Available power is affected by vehicle scale as well. A Directed-Energy Weapon will require a substantial power supply. This, in turn, will likely equate to a larger vehicle. Power requirements are also likely to drive range capability, which can then impact the threatened target set.

SAFETY

Safety must be considered in shipping and handling, loading, launching, arming, and "Return-To-Base, Weapons Loaded" scenarios. It could be said that, because a vehicle is unmanned, less thorough safety testing is required. While this may be true in regards to not having to certify the vehicle as "man-safe," the exact opposite is true in regards to ensuring safety of weapons use. In short, it is no longer a question of the safety of a human operator, since there isn't one, but a question of the safety of a potential victim (as opposed to the reliability of hitting an intended target) – inadvertent or otherwise.

Planning and testing for safety is a primary concern during the development of an UXV. An armed UXV, or at least the munitions used by one, are subject to Insensitive Munitions (IM) testing, in order to ensure safety over the entire life cycle. Naval Safety Instruction 8010.5 requires that all U.S. Navy and Marine Corps conventional munitions used or stored aboard Navy ships, without regard to the source of design or manufacture, must be subjected to IM testing. Military-Standard-2105C provides the latest testing requirements and passing criteria for IM tests including humidity and temperature, vibration, drop, cook-off, bullet impact, fragment impact, sympathetic detonation, shaped charge jet impact, and spall impact tests. Passing these tests is critical for developmental success and for the safety of people and property over the course of an armed UXV's lifetime.

Consideration must be given to the development of a master arm/de-arm capability for armed UXVs. This would be something the human operator would engage just prior to sending a vehicle out for a mission, and disengage upon the vehicle returning from the mission. While in the "de-armed" position, the vehicle should be incapable of releasing a weapon. While in the "armed" position, the vehicle would be able to release a weapon, if all target engagement criteria are met.

Another safety issue deals with armed expendable UXVs, or ones that break down on the battlefield, and are not retrievable. Provisions must be made for the weapons to sterilize themselves, so that they don't become a hazard.

What is the appropriate scope of safety concerns where autonomous armed UXVs are concerned? It is interesting and instructive to compare them in this regard to the safety concerns involved in the development of nuclear weapons. Nuclear weapons, as Weapons of Mass Destruction (WMD), have very stringent requirements laid on their development in a Nuclear Safety Certification Program. The goal of such a program is to prevent nuclear weapon accidents and incidents, which could result in great tragedies if they occur, but these programs are not easy, or cheap, to go through. They represent the upper-end of the scale for safety programs. Nevertheless, it is believed that no one would ever argue that they are not worth the expense.

How does this relate to autonomous armed UXVs? No one is likely to consider an armed UXV to be in the same class as WMD, unless the UXV is actually carrying WMD. However, consider the following: While the inadvertent damage, or deaths, caused by one or two armed UXVs with some sort of latent design flaw in the employment of their weaponry would likely be minimal, the inadvertent damage or deaths caused by this same latent design flaw by hundreds,

possibly thousands, of the same sort of autonomous armed UXVs could be potentially devastating in the aggregate. Where do we draw the line between the numbers of casualties and/or damage that differentiate WMD system from a non-WMD system?

Mitigating the situation a bit is the fact that as reports of misdeeds by these autonomous armed UXVs begin to roll in, that their human overseers will likely step into the control loop to kill this bad behavior. The question will be how soon does this override occur?

It is not the point here to argue for a full-blown WMD Safety Certification Program for autonomous armed UXVs, but to indicate that it may be very desirable to set up a Safety Certification Program for these vehicles with some features similar to those in a WMD Safety Certification Program in order to reduce the risk of accidents and incidents to acceptable levels. As an example, consider the Nuclear Safety Certification Program requirement for the splitting of software with nuclear safety implications into three categories with different levels of safety evaluation attached (Table 4).

Table 4. Nuclear Safety Certification Program Requirement

CATEGORY	***PURPOSE***
I	Controls critical function(s) and/or has been designated as a critical component.
II	Controls critical function(s), but is not designated as a critical component. Independent Verification and Validation is required.
III	Does not control critical function(s), but interfaces with hardware/software, which does control critical function(s).

Furthermore critical functions defined for nuclear weapons have surprisingly similar equivalent functions in considering autonomous armed UXVs (Table 5).

Table 5. Nuclear Weapons Equivalent Functions

FOR THE CRITICAL FUNCTION OF	***PROBABILITY OF OBTAINING NUCLEAR YIELD IS LESS THAN***	***IN THE EVENT OF***
Authorization	None	(Safety evaluations of combat delivery vehicle systems must consider that the authorization device is part of the command and control function and assume the authorization device has been activated.)
Prearming	10^{-6} per delivery vehicle over the system's lifetime	Inadvertent transmission of prearm.
Arming	10^{-4} per prearmed weapon	Arming and fuzing system failure resulting in arming after the system has been prearmed but before launch or release.
Launching	10^{-7} per missile over the system's lifetime 10^{-12} per missile over the system's lifetime	Accidental propulsion system ignition Inadvertent programmed launch of ground-launched missile during fully assembled weapon system operation.

Table 5. Nuclear Weapons Equivalent Functions (Continued)

FOR THE CRITICAL FUNCTION OF	*PROBABILITY OF OBTAINING NUCLEAR YIELD IS LESS THAN*	*IN THE EVENT OF*
Releasing	10^{-6} per weapon station over the system's lifetime	Inadvertent release or jettison of a bomb or a missile when release system is locked.
	10^{-3} per unlocking event	Inadvertent release or jettison of a bomb or missile when release system is unlocked
Targeting	10^{-3} per missile	Erroneous issuance of good guidance signal (for ground-launched missiles).
	10^{-4} per delivery vehicle over the system's lifetime	Inadvertent application of power or signals (other than the prearm command) to warhead or bomb interface.

While the probabilities listed above are for use with nuclear weapons, the gold standard for safety, they provide a yardstick that we can use in determining what might be appropriate for use with autonomous armed UXVs.

Finally, there is an issue regarding the testing of armed UXVs during development. Test ranges will have to be utilized that are certified for weapons tests, and appropriate controls implemented to ensure safe disabling of the weapons and UXVs, if necessary.

LEGAL

There are two primary legal aspects that must be considered in the design of armed UXVs: (1) the legality of an armed UXV itself, and (2) the legal use of that armed UXV on the battlefield to engage targets. Not surprisingly, these two aspects are linked together.

Regarding the legality of UXVs: The Judge Advocate General (JAG) of the Navy is required to conduct a legal review of all weapons and weapon systems intended to meet a military requirement of the Department of the Navy in order to determine if they comply with U.S obligations under international law, specifically the law of armed conflict and any treaties that may effect their use. The Army and Air Force have a similar review requirement. Any armed UXV *may be* required to undergo such a review. As will be shown, this review is *independent* of the actual battlefield use of a vehicle, but it is *not* independent of design features built into the vehicle that are used on the battlefield.

The determination of the need for a *specific* armed UXV to undergo a legal review may be somewhat arbitrary. As an example, consider the case of the armed Predator UAVs, the MQ-1 and MQ-9. The Air Force legal review of these aircraft stated that the governing DoD and Air Force Instructions "…require a legal review of all weapons to ensure compliance with applicable domestic and international law, including customary international law and the law of war." This legal review then went on to state that because the governing Air Force Instruction, "…excludes

aircraft from the definition of 'weapon,' a weapons legal review of the weaponized Predator is not required." The Air Force did a legal review anyway, stating as the reason, "Because deployment of weapons from unmanned aerial vehicles is a new initiative for the U.S. Air Force, this memorandum addresses international law considerations, to include the law of war, associated with employment of the subject aircraft."

E-mailed remarks from Major G. William (Bill) Riggs, United States Marine Corps (USMC), of the Navy's JAG Office (International and Operational Law Division) on this topic state, "Under the accepted Navy JAG definition of what constitutes a weapon or weapon system, 'platforms' such as aircraft and ships are not themselves 'weapons or weapon systems.'" These platforms would not then qualify for the need of a legal weapons review. However, he continued, regarding even more autonomous UAVs that have an AI capability, stating, "I think they will be 'weapon systems' under our definition as the AI, weapon and platform they are delivered on will be so integrated as a whole. …We'll have to look at each UAV as the technology is: a) still emerging; b) will/may differ from system to system." Thus, it is clear that this JAG office is of the opinion that the need for a legal review will be tied to the level of integration between the installed AI, the weapon (system), and the vehicle.

In the case of the armed Predator, it is a tele-operated vehicle with weapons on it, not an integrated-weapon system, so no review was really required, even though one was done. For fully-autonomous armed vehicles, it seems fairly clear that they will likely require a legal weapons review. There is a large gray-area, however, concerning the need for a legal review of armed, semi-autonomous vehicles, and where the line gets drawn may be somewhat arbitrary.

Assuming that a legal review is required, this review requires an analysis of three factors: (1) whether there is a specific treaty provision, domestic law, or international law, specifically the law of armed conflict, prohibiting the weapon's acquisition or use; (2) whether the weapon is capable of being controlled so as to be directed against a lawful target, (i.e., it is not used in an *indiscriminate* manner); and (3) whether the weapon causes suffering that is needless, superfluous, or disproportionate to the military advantage reasonably expected from the use of the weapon. These three factors are analyzed in relation to the weapon's primary intended employment. Note that the second criteria concerns the capability of the weapon to be directed at a target – not what target it is directed at. This is an important distinction relating to the second primary legal aspect noted above (i.e. the use of an armed UXV on the battlefield to engage targets), and provides the link between the two aspects.

Regarding the first factor for being a legal weapon, the U.S. is a party to a number of international agreements that relate to the law of war. As an example, the U.S. adheres to the Missile Technology Control Regime, an informal and voluntary political agreement among 33 countries to control the proliferation of unmanned rocket and aerodynamic systems capable of delivering weapons of mass destruction. UAVs fall under this agreement. An absolute treaty ban on something is a show stopper; e.g., a biological or chemical weapon on a UAV. The other factors become irrelevant if there is a ban. If there is no absolute treaty prohibition, then the other two factors are weighed.

Regarding the second factor, a fundamental principle of the law of armed conflict is that combatants must be distinguished from noncombatants and innocent civilians. Only combatants

and military objectives can be legitimately targeted. Indiscriminate, or "blind," weapons are prohibited. Indiscriminate weapons are those that are as likely to hit civilians and non-combatants as well as military targets. A legal weapon does not have to have perfect accuracy. There is no requirement that a system hit the intended target 100 percent of the time, or that it its effects affect only the intended target. Weapons that are incapable of being controlled (directed at a military target) are forbidden as being indiscriminate in their effect. A weapon is not indiscriminate simply because it may cause incidental damage or collateral civilian casualties, provided such damage or casualties are not foreseeably excessive in light of the expected military advantage. The basic purpose of this principle is to protect civilians, non-combatants and non-military property as well as preserve the distinction between combatants, civilians and noncombatants. Thus, the link between the two primary legal aspects for armed UXVs can be seen. The design features that are provided in the vehicles to allow them to discriminate between legitimate targets and non-legitimate targets on the battlefield are used in the pre-battlefield use determination of the legality of the armed UXV. The battlefield commander then uses these features to direct the armed UXVs to attack legal targets.

Regarding the third factor: Article 22 of the Annexed Regulations of Hague Convention IV states the “right of belligerents to adopt means of injuring the enemy is not unlimited.” Article 23(e) of this same document prohibits the employment of “arms, projectiles, or material calculated to cause unnecessary suffering.” Whether a weapon or munition causes unnecessary suffering is ascertained by determining whether the injury to combatants is manifestly disproportionate to its stated purpose, that is, its intended use, and the military advantage to be gained from its use. The balancing test cannot be conducted in isolation. A weapon system’s intended effect must be weighed in light of comparable, lawful weapons or munitions in use on the modern battlefield. The prohibition of unnecessary suffering constitutes acknowledgement that necessary suffering to combatants is lawful, and may include severe injury or loss of life. A weapon cannot be declared unlawful merely because it may cause severe suffering or injury. The correct criteria is whether the weapon is calculated to cause injury or suffering greater than that required for its military purpose and, in this regard, a weapon which is found inevitably to cause injury or suffering manifestly disproportionate to its military effectiveness could contravene the prohibition.

A State is not required to foresee or anticipate all possible uses or misuses of a weapon, for almost any weapon can be misused in ways that might be prohibited. As an example, consider the use an overly large weapon to take out a small target. If there is nothing else left in the magazine, then the use of that lawful weapon is authorized. There may be an issue of "asset management," applying the least expensive capability, but that is not a legal issue.

Finally, we must consider the second legal aspect: the use of an armed UXV on the battlefield to engage targets. We must consider this aspect when we are designing armed UXVs that can employ higher levels of autonomy, including full autonomy, to ensure that, when these vehicles are operating in an autonomous mode, they don’t violate lawful targeting concerns. It revolves around the need to use the “Discriminate Use of Force” (DUF).

Within the cover memorandum of a DUF document published by the Defense Science Board to the Chairman, Defense Science Board, the authors make the following statement:[6]

"Our concept of DUF strongly aligns with much of the current thinking about Effects-Based Operations. The coming of age of these concepts is influenced both by *opportunity* and *need*.

- DUF brings new concepts for collaboration and massing of effects, which are joint in character and integrated among joint force echelons and components. It is enabled by new weapons; improved intelligence, surveillance, and reconnaissance; shared situation understanding; improved individual and collaborative training; greater agility; smaller footprints; and other emerging capabilities of the U.S. military that allow more timely and precise use of force than heretofore possible.
- *The* need is driven by the nature of current military campaigns. A striking feature of these campaigns is the tension among multiple strategic and operational objectives: cause regime change, destroy a terrorist organization, decapitate leadership, but preserve infrastructure, don't wage war on a people, do hold an international coalition together, etc."

Thus, we can see that while DUF relies on improvements in technology to better be able to discriminate, it also is fed by the need to meet increasingly refined requirements.

Law of war issues related to lawful targeting must be addressed at the time of employment, to be determined by the on-scene commander under the circumstances ruling at the time. The responsibility of legal use ultimately resides with the commander. The commander authorizing a weapon's use must consider its characteristics where civilians are present in order to ensure consistency with mission rules of engagement and law of war proscriptions on the directing of attacks at civilians not taking an active part in hostilities, or who otherwise do not pose a threat to U.S. and friendly forces. The commander must have a means by which he can impose restrictions, and permissions, on the operations of the armed UXV such that it will conform to his understanding of what constitutes both valid and invalid targets. This imposes a tremendous responsibility on the vehicle designer to ensure that the armed UXV will have the necessary means to provide positive target identification (ID). It is these design features that are fed back into the legal review to determine the lawfulness of the armed UXV.

In any targeting analysis the need for positive target ID is critical. This is no less true for a UXV. (The use of a "voting" scheme between cooperating UXVs on the battlefield to make a positive ID on a target should be considered.) Trust in the ability of the UXV to attain the specified level of target ID will dictate the required accuracy level used. The degree of effective identification could impact the ROE. (ROE are mission specific, and can be more restrictive or permissive depending on many different factors such as the political situation or military objectives.) A valid target *may* be located such that engaging it could cause "collateral damage." This does not make the target any less legitimate, however the military commander will have to weigh the military advantage to be gained against the collateral damage that will be caused (proportionality analysis). For example, if there are civilians located near a valid target it is no less a valid target, but the civilians will have to be considered when the commander decides whether to strike the target or not.

Chapter 8, "The Law of Targeting," in Naval Warfare Publication 1-14M[7], "The Commander's Handbook on the Law of Naval Operations," plus other supporting material from

this Handbook, provide a good basis for understanding more of the legal factors that need to be considered in the use of armed UXVs.

Some interesting items to consider:

- In certain situations, armed UXVs might be considered to be equivalent to mines, and need to be fenced, marked and monitored. An example of this might be the use of armed UXVs to patrol the borders of a prisoner of war camp.
- Self-destruct devices may need to be included in the design of all future armed UXVs to “sterilize” them should they become disabled, in order to prevent them from inadvertently harming civilians at a later date. Anti-tamper devices may or may not be lawful and will have to be considered in the context of the characteristics of the entire weapon system.
- The right of “self-defense” for armed UXVs is an open question, due to the fact that this is an area where the development of technology has out-paced the development of law. International law defines a warship as a ship belonging to the armed forces of a nation bearing the external markings distinguishing the character and nationality of such ships, under the command of an officer duly commissioned by the government of that nation and whose name appears in the appropriate service list of officers, and manned by a crew which is under regular armed forces discipline. There is no question that a warship has the right to self-defense. While armed UXVs may belong to the armed forces, and we may be able to put flags on them (external markings), and they may be "commanded" by members of the armed forces (albeit remotely), they will still be unmanned by definition. Is it enough to flag them? We will likely not have any difficulty arguing that we returned fire on forces that fired on one of our UXVs as part of the right of self-defense.
- Certain platforms, such as aircraft, are not able to “accept surrender.” Considering the Law of Armed Conflict: If an enemy does surrender, will an autonomous armed UXV recognize the surrender and not kill him? This issue was illustrated during the first Gulf War when a number of Iraqis tried to surrender to an orbiting UAV. How are we to address the surrender of forces when beaten by the UXVs that we employ, since it is likely that these will be the first combat units that an enemy sees in an engagement?

The legal review process for a UXV looks for information regarding relative accuracy of proposed weapon systems vis-à-vis comparable lawful weapons. A human-identified and directed system (in theory) would raise fewer positive ID questions than fully autonomous UXVs. So if we were providing an armed UXV for legal review, we would need to provide information regarding (a) types of targets the system would be intended to engage, (b) accuracy data, and (c) positive ID features. The challenge to the designer is to deliver to the warfighter a weapon or system that when aimed or unleashed at a legitimate military objective, does not go awry and hit an unlawful target.

VEHICLE SIGNATURE

Vehicle signature addresses the ability of the vehicle to be detected and located against the backdrop of its surrounding environment. In other words, how easily can enemy sensors find it? In some uses of armed UXVs, like sentry duty, it may be desirable to be very visible, so its design should look at enhancing its inherent signatures. This is similar to use as a decoy where it may be desirable to enhance the vehicle's signatures in order to draw fire, thereby unmasking potential targets for attack. In other uses, such as a stealthy strike platform, it would be desirable to minimize its signatures. (Note, however, that the cost to minimize the signature must be weighed against expected improvements in survivability and strike performance. It may not be worth the expense.) Still in other cases it may be desirable to be able to rapidly alter a vehicle's signature to mimic another vehicle for deception purposes.

The object is to influence the detection of the vehicle by an adversary to be either inside, or outside, of the UXV's weapons release range. In the case of an armed sentry, it may be desirable to deter an adversary before ever having to resort to the use of a weapon. (A notable exception to this is in the use of UAVs in a Force Protection role. The Combatant Commander's Integrated Priority Lists for these missions have indicated the need for a reduced acoustic signature.) In the case of the stealthy strike platform, we'd like to get as close to the intended target as possible, without being detected, before releasing the weapons.

An example of a signature issue can be found in the dissipation of heat from a vehicle, or its infrared (IR) signature. Smaller systems usually have more heat to dissipate (relative to their size) than larger systems. Their relative power needs may increase as size and weight decrease, which may cause the size of their IR signature to stand out, compared to its other signatures.

The issue that must be addressed is signature balance. To achieve signature balance in a vehicle is to ensure that no one signature is detectable from a longer range than any other signature. In the case of the sentry, it may be desirable to paint the vehicle a bright color in order to draw attention to it, thus providing it with an unbalanced signature. While with the stealthy strike platform, no single signature should give away the location of the vehicle prematurely. In this latter case, the signatures need to be very balanced.

MISSION PLANNING

Mission planning is time-critical. For an armed UXV, the mission planning involves many factors. Mission planning must consider such things as attack coordination (cooperative hunting) with multiple sensors, vehicles and weapons; environmental impacts on vehicles, sensors, and weapons; available battlefield intelligence; existing ROE; the possibility of fratricide; other "Blue-on-Blue" engagements; "Blue-on-White" engagements; collateral damage (discriminate use of force concerns); and Battle Damage Assessment (BDA). The goal is to incorporate consideration of these factors as rapidly as possible in order to produce a plan that is still relevant when a mission is launched.

Today, much mission planning for UXVs is done for operations in a *segregated* mission space. The goal for *armed* UXVs in the future will be for operations in an *integrated* mission space.

Automation in the planning process to achieve a time-relevant plan will be essential, but will the automation of the individual components of the planning process lead to "glossing over of the details" that misses some important interactions that a human might better consider? Will the human understand why the machine made the choices it did? There will be a need for an expert system-like "explanation function" that will allow an operator to query the system as to why choices were made, and an opportunity given to tweak these choices, if something is deemed to be incorrect.

The level of mission planning will be an important factor to consider as well: Are we planning for a single vehicle, several vehicles, an entire battlefield, or a theater full of UXVs? Plans must flow seamlessly from one level to the next in order to keep the number of personnel in the loop to a minimum. (The involvement of people usually takes too much time.) This is similar to what is done today with an automated Air Tasking Order, but will be a machine-to-machine flow and coordination of data.

What happens if the battle plan isn't working? Offensive operations can turn into defensive operations very quickly if something wasn't accounted for in the original plan. Operations planning must take this into account.

As the level of autonomy increases, some of the mission planning functions may be pushed out to the vehicles to do, and coordinate this planning, autonomously, with other vehicles. One consideration in this will be the need to communicate the intent of the plan to the UXVs, in order to provide appropriate context for the vehicles to do their planning. This is being addressed today with knowledge-sharing efforts, such as Knowledge Query and Manipulation Language (KQML) and Knowledge Interchange Format (KIF). KQML can be used as a language for an application program to interact with an intelligent system or for two or more intelligent systems to share knowledge in support of cooperative problem solving. KIF is used for the interchange of knowledge among disparate programs.

A critical factor in this will be the ability of a UXV to be able to do BDA in order to desist from re-attacking once the target is dead, or to re-engage if the target is still viable, and adjust the mission plan appropriately. Another critical factor will be the ability to perform weapons allocation between vehicles such that a target doesn't suffer from either over- or under-kill.

SUPPORT

There are additional support issues, such as maintenance and logistics, of an armed UXV that one would either not have to consider for an unarmed UXV, or at least not to as great a degree.

For example, consider how to handle the maintenance of a vehicle that has been designed with active anti-tamper mechanisms (which could be considered a weapon) built into it. While we build no such mechanism today, there may be a need for one in the future.

Some other support functions to consider:

- Weapon/Sensor Interface
- Weapon/Sensor Power Management
- Munition Storage
- Weapon/Sensor Communication and Control
- Automated Maintenance Aids and Parts Management

Some issues dealing with support to consider:

- Weapon System Reliability
- Weapon System Sustainment Cost
- Parts Repair and Replacement

COMMAND & CONTROL

The use of armed UXVs must consider the level of control and/or interest in their use. Consider the situation that must have been faced in the recent war on Iraq in the discussions surrounding the removal of the upper-levels of the Iraqi command structure. The debates revolved around the decision to target Saddam Hussein, or not, and the existence of policy not to assassinate leaders of other countries. It was widely reported in the open press that President Bush, himself, made the decision to target Mr. Hussein. This is command and control at the very highest levels. The same issues can revolve around the use of armed UXVs.

In a world driven by time-critical strike concerns, this highlights the problem of who has weapons release authority, and the related problem of the timeline to gain that release authority by the individual who is in actual control of the vehicle. (This leads to a Speed of Command issue, and Chain of Command, Accountability, and Responsibility issues.)

Another command and control issue deals with “situational awareness” of the whereabouts of UXVs in the battlespace. Care must be taken to ensure that the location, and status, of these vehicles is included in the appropriate “Blue Force” tactical pictures, as battlefield commanders do not like to have “unknowns” roaming their Area of Responsibility. The fact that the vehicles might be armed is of particular interest to them. The level that these pictures will be seen at will depend on the level of interest in their missions.

Similar to the problem in mission planning, there is an issue with the scope of command and control for these vehicles: Are we controlling one? Several? How many is too many? What is the appropriate operational mode and “Span of Control”? (Note: DoD is currently working

with the Federal Aviation Administration to allow a single pilot to control up to four UAVs simultaneously.)

What we would like to achieve is “operational transparency,” (sometimes referred to in computer science circles as the “Turing Test,” so named after Alan Turing, the great British mathematician, long considered to be the founding father of computers) where the operator cannot tell the difference between dealing with the machine and dealing with humans. Related to this is the issue of vehicle safety. We would like for the vehicle to be responsible for its own safety as much as possible, only contacting the operator for instructions when there is a real need.

Interoperability is another command and control issue for weapon control. As an example, there have been five levels of interoperability defined for UAV control in Standardization Agreement 4586 that run from indirect receipt of secondary imagery to full tactical control, including launch and recovery. For weapon control there will have to be interoperability standards chosen to handle such things as “forward pass” of weapons handoff from one platform to another, such as might occur with weapon launch occurring from one platform, but coded target illumination occurring from a second platform.

COMMUNICATIONS

Communication with UXVs is always important. We need to be able to tell them what we want them to do, and we need reports back from them on the battlespace environment, and the results of their actions.

Communication with armed UXVs is of even more importance, due to the sorts of things that might go wrong during a mission. Bad behavior, such as misidentifying and engaging friendlies, could lead to someone being dead that shouldn’t be.

Communication factors that need to be considered in the arming of UXVs include range (Line-Of-Sight, or Beyond-Line-Of-Sight), robustness (link margin, jam resistance and cryptography), signature (Low Probability of Detection and Low Probability of Intercept), and bandwidth (how much data can you either transmit to, or extract from, the vehicle in a given length of time). The amount of bandwidth needed at any given point in time may be linked to the level of autonomy granted to the vehicle at that time. It can also be linked to the types of sensors onboard a vehicle. As an example, there is a goal within the UAV Roadmap to provide UAVs with high definition television (HDTV) capability for precision targeting. A conventional National Television System Committee image requires 3.35 megahertz (MHz) of bandwidth, but an HDTV image requires 18 MHz of bandwidth. There is great pressure from the commercial sector for the federal government to sell-off large chunks of bandwidth so that it can be used for commercial purposes. A proactive stance must be taken to prevent this resource from being lost, undermining efforts to produce effective UXVs. Efforts must also be made to better manage the use of the bandwidth that is available. Current efforts to move from circuit-switched bandwidth to bandwidth on demand via Internet protocol should help to alleviate this problem. Another

related item of importance is the degree of automation involved in getting data on and off a vehicle, or telematics.

Data link rates and processor speeds are in a race with respect to enabling future UXV capabilities. Today, and for the near term, the paradigm is to relay virtually all data to the control station and process it there for interpretation and decisions. Eventually, however, onboard processing power will outstrip data link capabilities and allow UXVs to relay *information*, based on their data, vice the data itself, to the control station for decision making. At that point, the requirement for data link rates in certain applications, particularly imagery, should drop significantly. Meanwhile, data compression will remain relevant into the future as long as band-limited communications exist, but it is unlikely compression algorithms alone will solve the near term throughput requirements of advanced sensors. A technology that intentionally discards information is not the preferred technique. For now, compression is a concession to inadequate bandwidth.

The type of data link used dictates how much data can be transmitted. An acoustic link, as might be used with a unmanned underwater vehicle, is the most restricted. With radio frequency (RF) links limited spectrum and the requirement to minimize System Size, Weight, and Power have been strong contributors for limiting data rates. At gigahertz (GHz) frequencies however, RF use becomes increasingly constrained by frequency congestion, effectively limiting its upper frequency to about 10 GHz. Optical data links, or lasercom (i.e., future satellite communications), will potentially offer data rates two to five orders of magnitude greater than those of the best future RF systems, but are constrained by line-of-sight connectivity requirements that include pointing, acquisition, and tracking issues. These will not work well in tight spaces with limited sight lines, without relay capabilities. This is important to armed UXVs because, typically, to obtain a valid fire control solution, the data rates for target location are much higher than to just support command and control issues.

Swarms of UXVs carry additional communications needs. Effective distributed operations require a battlefield network of sensor-to-sensor, sensor-to-shooter, and UXV-to-UXV communications to allocate targets and priorities and to position vehicles where needed. While the constellation of sensors and vehicles needs to be visible to operators, human oversight of a large number of UXVs operating in combat must be reduced to the minimum necessary to prosecute the war. Automated target search and recognition will transfer initiative to the vehicles, and a robust, anti-jam communications network that protects against hostile reception of data is a crucial enabler of UXV swarming.

These short-range communication needs might be answered by such technologies as “wireless USB.” This technology is based on an ultra-wideband link in the 3.1-10.6 GHz range. Throughput is range-dependent with current speeds of 480 megabits per second (Mbps) at a range of 2 meters and 110 Mbps at 10 meters. Reports of 1 gigabits per second speeds by the year 2007 have been seen. Compare this with speeds of 12 Mbps for Bluetooth and 54 Mbps for wireless-fidelity (Wi-Fi) technologies. (Note that effective Wi-Fi range is only about 300 feet)

A longer-range RF technology to consider might be World-wide Interoperability for Microwave Access. With a range capability of up to about 31 miles, this technology is being considered as a “last mile” alternative to today’s cable modem and digital subscriber lines

services, bringing broadband technology to office parks and neighborhoods where these other services might not be available. With speeds of 5-10 Mbps it is an efficient, cost-effective alternative. A drawback is that it is currently designed for use from fixed locations. A competing technology is "Mobile-Fi," which was designed from the beginning for mobile communications from fast-moving vehicles.

Of special importance is the behavior of the vehicle and its weapons during times when communications have either not been scheduled (i.e., for covert operations) or have been disrupted for some reason. There needs to be a solid degree of assurance that a weapon will not be inadvertently released during these times at an incorrect target.

Cryptographically-covered transmissions both to and from the vehicles will be critical to ensure that they can't be hijacked and turned against us. It is little wonder cryptographic technologies have been considered "weapons grade" technologies in the past. It will be important to ensure that the cryptographic keys and algorithms don't fall into the wrong hands. Given that these need to be resident within the UXVs in order to enable transmissions, how do we do this and ensure that we keep this material out of enemy hands in the event that one of these machines is captured? A self-destruct mechanism could be contemplated, but one then runs the risk of these UXVs being considered to be in the same category as landmines. A better approach might be to have the cryptographic algorithms and keys contained in software, and the software run resident on random access memory that ceases to function when power is removed, thus automatically wiping any program and data running within it. (Note that, if this approach is taken, we need to guard against inadvertent power loss during normal operations that could render the UXV effectively disconnected from the rest of the world.)

SENSORS

Sensors used for targeting the weapons onboard UXVs must be shown to be immune to deception, or there must exist alternative methods of targeting to overcome any potential use of deception.

There must be some sort of facility for self-calibration of sensors so that we can be reasonably certain that what is being reported by the sensors is, in fact, correct. This argues for the inclusion of Built-In-Test and Built-In-Test Equipment capabilities onboard these vehicles.

The sensors onboard an UXV must provide the remote "eyes and ears" for its human masters, and be matched to the threats that the vehicle is intended to counter. Sensors chosen must work well in the anticipated operational environments, and should serve to extend and enhance the abilities of an unaided human. As an example, today it is difficult for a human to detect the presence of explosives, or other weapons, being carried by a terrorist/suicide bomber without coming into close proximity with the person to perform a physical check of the person's clothing and body. Sensors chosen for such work should include capabilities to check for the presence of these items remotely, if possible, so that physical contact is not necessary.

Sensors should be matched to the weapons being carried by the armed UXVs, so that the weapons carried can be employed directly by the vehicle, if possible. They should also be networked with the sensors onboard other vehicles in order to contribute to, and draw from, the Relevant Tactical Operational Picture/Common Operational Picture, thus supporting engagements of weapons on other platforms, too.

WEAPON TYPE

Weapons can be classified as “lethal” or “non-lethal.” However, deaths have occurred in the past with non-lethal technologies, such as rubber bullets. Sometimes the lethality of a weapon is range-dependent. A normally non-lethal weapon used at close range could be lethal. Therefore, it should be noted that any use of force must be undertaken with care. What non-lethal technologies bring is the legal right to first use of force in defensive postures, if it appears that friendly forces are in danger. They can be used to determine, or deter, hostile intent.

One category of weapons is peculiar: those used for Electronic Attack (EA), for example, in stand-in jamming. These can encompass both lethal and non-lethal weapons. Care must be taken in employing EA techniques that the data links to/from the UXVs aren’t blocked for extended periods of time. Additionally, reactive EA requires very short reaction times in order to be effective against pop-up targets.

The application of force must be matched to the target. One doesn’t use a sledgehammer to kill a mosquito. In doing this, the damage mechanism that the weapon employs, along with the degree of damage, must be examined in concert with the target characteristics.

WEAPON CHARACTERISTICS

When arming an UXV, one must know and understand the characteristics of a weapon. One primary concern is whether the weapon is to be fully integrated into the vehicle or carried as a payload. This can be illustrated by the difference between a bomb and a bullet. Typically, a bomb would be carried as a payload, mounted on a hardpoint, whereas a bullet would be used in a gun that has been fully integrated into the vehicle. (Note that guns can be carried on hardpoints, and bombs built into vehicles, such as missiles with explosive warheads.)

The range of the weapon must be matched to the sensors used to target it. This also impacts the location of the platform employing the weapon relative to the location of the intended target.

An employment consideration is the weapon being guided or unguided. As an example, one form of guidance uses a laser illuminator to illuminate the intended target. Typically, this illumination comes from a vehicle or location other than the one that fires the weapon. It is critical that the considerations for proper illumination of the target be taken.

The relative “intelligence” of the weapon itself must be considered as well: Is it “dumb,” “smart,” or “brilliant?” Smarter weapons may be easier to use, but there is an increased risk that they might also attack the wrong target. There is a limit to the brilliance.

The accuracy of the weapon is critical. It does no good to precisely target a victim, if the weapon can’t reasonably be expected to hit it. Poor accuracy also increases the risk of collateral damage. Tied in with accuracy is the Field of View or Influence (FOV/I) on a weapon’s seeker, if it has one. The larger the FOV/I the more likely it is to acquire a target. The issue, of course, is “Is it the right one?” Poor accuracy can be partially overcome if the weapon’s damage radius is large enough. However, large damage radii also invite collateral damage.

One must consider any residual effects that a weapon might produce. For example, a weapon that dispenses landmines indiscriminately can render an area unusable for a very long period of time. In general, lethal technologies will leave people either dead or permanently injured. However, some non-lethal technologies may have effects that disappear in a matter of minutes to hours.

TARGET CHARACTERISTICS

The characteristics of the intended target set must also be accounted for in matching both the weapon and the vehicle that will be carrying it. As an example, consider the speed of an intended target, relative to the speed of the vehicle that will be carrying a weapon. If the target is faster than the vehicle carrying the weapon, then the weapon will have to make up for the shortfall, otherwise the target may be able to outmaneuver the vehicle, making engagement very difficult, or impossible. Making the weapon longer ranged, and/or much faster might do this. Unfortunately, this also will likely make the weapon more expensive. As previously pointed out, the cost of the weapon must be balanced against the cost of the intended target. It may be more advantageous to have the weapon mounted on a faster vehicle.

TECHNOLOGY

The rate of technology obsolescence as compared to the normal shelf life designed into today’s weapon systems needs to be addressed. Technology today rapidly becomes outdated, and we face the situation with many systems that we can no longer get spare parts for them. This has led to situations in which there have been serious discussions about cross-decking systems from ships that are about to be scrapped, to ships being considered for new construction. (What many fail to comprehend is that, while they may move the system to a new ship, they will have no way of maintaining the system after it has been moved, due to lack of spares, because the spares are no longer manufactured, and the manufacturers have no intention of re-starting their production lines for almost any amount of money.) The tendency for this to occur is increasing as the rate of technology development explodes. We are currently exploring a concept referred to as “Open Architecture” that holds the promise of being able to overcome this problem.

Addressing the Navy's Open Architecture program: In broad and general terms, architecture is defined as "the structural design of an entity." Adding "openness" to the list of architectural characteristics implies that the "structure" of the architecture explicitly promotes interoperability, both internally and externally, as well as ease of modification and extension.

It is an engineering truism that what is achievable in system design (architecture) is a function of not only the task to be accomplished but also the technologies that are available.

However, the evolution of high performance COTS, combined with continued growth of weapon system and combat system requirements, provides an opportunity to design an architecture more capable of exploiting new technologies than the federated legacy architecture that has served the Navy for well over two decades. The need for evolution toward an open architecture is motivated by both performance and supportability considerations. Commensurate with this dual set of motivating factors, the goals of the Navy's Open Architecture Program are as follows:

- Combat system, weapon system, command support system and Hull, Mechanical & Electrical capabilities that continue to pace the threat
- System design that fosters affordable development and life-cycle maintenance
- System design that reduces upgrade cycle time and time-to-deployment for new features
- Architecture that is technology refreshable despite rapid COTS obsolescence
- Improvements in Naval Weapon Systems Human Systems Integration

A second technology-related item has to do with the issue of proliferation. Some of the things we have been doing aren't difficult, technically, but can have some significant social costs associated with their adoption, if it offends someone's sense of morals. What happens when another country sees what we've been doing, realizes it's not that hard, and begins to pursue it too but doesn't have the same moral structure we do? You will see a number of countries around the world begin to develop this technology on their own, but possibly without the same level of safeguards that we might build-in. We soon could be facing our own distorted image on the battlefield.

Closely coupled with the concern of proliferation is the trend in today's software industry to outsource software research and development – many times to firms located overseas. The David Watkins article[8] does a very good job of examining the economic issues associated with this accelerating trend, including the tradeoff between security and confidentiality for the perception of lower labor cost. The temptation for contractors to do this is great; however, national security concerns must dictate that we insist that they not use the services of companies outside the U.S.

TARGETING

One fundamental issue of targeting is if the target is going to be engaged with direct or indirect fire. This is a question of the shooter being in a position of sensing the target or needing to have targeting data relayed from someone else who can sense the target. The situation is obviously more complex for indirect fire than for direct fire.

Besides someone just seeing a contact to shoot, we must establish what the contact is and the intentions of the contact. This is the process of establishing a target's ID.

Typically, there are four general classifications of ID: Friendly, Hostile, Neutral, and Unknown. A good deal of effort is expended attempting to convert Unknowns to Friendly, Neutral, or Hostile status. The case of identifying Neutrals is not straightforward. As an example, is that woman in front of us really pregnant, or does she have a load of explosives strapped to her stomach? This is a difficult problem for a human to solve today, and it is not any easier for a machine. There is a need for a lot of effort to be expended in just bringing the level of performance of machines up to that of humans in this regard.

Another item to consider in targeting deals with target tracking which can be split into separate considerations of data latency, location accuracy, and the agility of a target, compared to the ability of the UXV/weapon combination to follow the target's motions, and unmask it from obstacles.

The data latency issue deals with real-time operational environment considerations. We need to be able to process tracking data quickly enough to maintain reasonable assurance that we are pointing the weapon in the appropriate direction.

The location accuracy issue translates into the question of "How well do you know he is where you think he is?" This relates to the center of damage, or kill radius, of a weapon compared to where you think he is, as opposed to where he really is. If the location accuracy is too low, you may not be able to guarantee killing him with a single shot and may well miss the target altogether. (Stabilized firing platform issue.)

Lastly, there is a question of dealing with a rapidly maneuvering target that may be able to hide. This latter item takes into consideration the other two, but also includes the ability of the vehicle/weapon combination to maneuver quickly to improve its chances of achieving a kill. As an example, consider a gunfight where an enemy soldier might duck behind a rock, or some other solid object, after just having shot at you. You know where he was, and are reasonably sure of where he is now, but it does no good to shoot back right now, because the solid object would block your shot. Instead of doing this, you opt to circle around the rock, and shoot at him from the side. The Navy has dealt with the issue of battery unmasking for years. This is a combination of battery and target unmasking. Coupled with this is the issue of relative navigation, as opposed to absolute navigation, which is how many UXVs navigate today. The vehicle will need to be able to solve the relative navigation problem between itself and the target on the fly.

Addressing the issue of target ID from a different standpoint: What if, instead of attempting to design a system that tries to tell the difference between an enemy soldier and an enemy civilian, we design a system that will recognize a weapon, and go after it to either render it harmless, or to otherwise ensure that enemy combatants cannot use it against us again, thereby disarming the entire enemy force? This leads into the area of Automatic Target Recognition (ATR), and there has been, and continues to be, a great deal of research done in this area.

The legal community tells us that the reason why we have ROE is to ensure that we inflict as few casualties on a civilian population as we can, and the reason for this is that it greatly eases the process of ending a conflict. Killing people tends to lengthen a conflict, due to the ill will towards us generated in the families of the survivors who had to bury their dead.

A system that targets weapons, instead of people, should go a long way toward alleviating the kinds of problems we know could occur following a conflict. If we let it be known to the public that our armed UXVs target weapons, instead of people, then when the enemy is confronted with our armed UXVs on the battlefield, they will know that they can save themselves by abandoning their weapons, or risk being killed by our armed UXVs when these vehicles go after the weapons that the enemy holds.

Identification of what constitutes a weapon will be an issue, but one that can be addressed: Since our UXVs will be communicating between themselves, an attack on one can be observed by the attacked vehicle, and the others monitoring communications from the attacked vehicle. Incoming fire can be correlated to a source, and the source recognized and attacked. (If the attacked vehicle doesn't survive, the remaining vehicles will correlate to the source, recognize it, and attack it.) The "weapon," whatever it is, can then be added to a shared database of weapons for future reference by other armed UXVs. Obviously, an extensive effort should be made in advance of combat operations to populate this database to the maximum extent possible with the characteristics of weapons likely to be encountered.

How will our UXVs recognize weapons when they see them on the batttlefield? Consider Optical Character Recognition (OCR) technology: In digital format, a computer has no problem interpreting a letter "A" as a letter "A," since it is represented by a standard string of ones and zeroes that have the universal meaning of the letter "A" to computers everywhere, and the knowledge that an "A" exists somewhere can rapidly be communicated to somewhere else, using this string. The problem that is encountered at the front end of this is in a computer attempting to recognize an "A" as an "A" when it is only on a sheet of paper, and not already in the standard string of ones and zeroes that represent an "A." The problem is further complicated by the existence of both "a" and "A," as a computer must be able to differentiate between lower and upper case instantiations of the same letter. The problem is also further complicated by the existence of different fonts that display an "A" differently. The essential problem is determining what constitutes the basic "A-ness" of the letter. Add to this the problems of trying to recognize text from graphics on what may be a Xerox of a bad fax sheet, and it is a wonder that OCR technology works at all! Nevertheless, it does, not always with perfect accuracy, but it works pretty well most of the time.

There are equivalents to each of these problems in consideration of recognizing weapons:

- To the problem of determining the basic “A-ness” of a letter, there is the weapons problem of recognizing the basic “gun-ness” of a weapon, or the basic “knife-ness” of a weapon, or whatever.
- To the problem of interpreting an “A” from an “a,” there is the weapons problem of trying to recognize a rifle from a pistol.
- To the problem of different fonts, there is the weapons problem of trying to recognize a Remington from a Kalashnikov.
- To the problem of recognizing text from graphics, there is the weapons problem of recognizing a weapon from everything else in the environment.
- Finally, to the problem of the “noise” introduced from Xerox and fax machines, there is the weapons problem of someone deliberately trying to conceal weapons under camouflage nets or clothing.

These all present significant challenges, but then so did all the above problems for OCR technology, and that technology works. There are probably lessons to be learned and applied here for recognizing weapons.

As an example of current efforts in this area, consider the Low Cost Autonomous Attack System (LOCAAS): The LOCAAS is envisioned as a miniature, autonomous-powered munition capable of broad area search, ID, and destruction of a range of mobile ground targets. LOCAAS is a low-cost laser radar (LADAR) sensor coupled with a multimode warhead and a maneuvering airframe to produce a high performance submunition. The warhead can be detonated as a long rod penetrator, an aerostable slug, or as fragments based on the hardness of the target. The LADAR allows target aimpoint and warhead selection to be determined automatically, using demonstrated ATR algorithms. (Note: Although proposed as a fiscal year 1998 ACTD program, LOCAAS was pulled from consideration during the final ACTD Breakfast Club meeting in May 1997. The perceived levels of the LADAR and ATR maturity were cited as the reason for the dropping of ACTD support. Development has continued however, resulting in a successful test at Eglin Air Force Base on 21 March 2003 where a LOCAAS unit, equipped with a multimode warhead, and with no outside control, located, attacked, and fired a warhead at a target for the first time. In this test, LOCAAS was released from a test aircraft over the Eglin range. After flying under its own power, LOCAAS used its on-board Global Positioning System and Inertial Navigation System to navigate to two waypoints before searching for the target — a relocatable surface-to-air missile launcher. In the target area, LOCAAS rejected a non-target military vehicle that was intended to confuse the system, as could occur in an actual battlefield scenario. The LOCAAS acquired and correctly identified the target, tracked it, and detonated the warhead above the target at the appropriate time and location.)

As previously mentioned, the field of ATR is very active. Typically, efforts in ATR deal with Image Understanding for images from various kinds of sensors to include different types of radars, thermal imagers, and other types of video images.

DEFENSES

While not a topic totally divorced from consideration by unarmed platforms, this topic takes on special meaning for armed platforms. Since they are designed to deliver fire, it is likely that they will also receive fire, much more so than unarmed platforms. The design of armed UXVs needs to take into consideration their own survival for purposes of accomplishing the assigned missions.

While not having human operators to protect, these vehicles must provide protection to their "vital" components. This protection can of course include traditional armor (both passive and reactive), but should also include consideration of redundant (and dispersed) components for graceful operations degradation, reconfiguration, and active defenses in order to take out the source of incoming fire, and possibly the incoming fire itself. (An example of this latter capability is found in the Army's Shortstop Electronic Protection System [e.g., AN/VLQ-9] that causes RF proximity fuzed munitions, such as artillery and mortar rounds, to detonate prematurely.) Another technology area that should be taken into consideration here would be self-repairing materials. Recent Air Force Research Laboratory-sponsored research shows promise in composites that may be capable of sealing small holes. In addition to this, we must remember that we will be driven to using COTS products to a large degree, so consideration must be given to how they will survive a shock environment, caused by the impact of incoming fire. Overall, consideration must be given to the "ruggedization" of COTS gear, to include consideration of vibration and extreme temperatures.

OTHER FUNCTIONS

In our efforts to reduce the manpower required for the CVNX by looking at automation possibilities, one thing became very clear. It was not enough to automate a single function performed by a crewmember, as that crewmember normally had multiple functions to perform while onboard. Automating this single function did not get that person off the ship. We had to look at the totality of the functions needed to be performed by that person, and lay plans for automating all of them, or organizing them differently, in order to guarantee reducing overall ship manning.

A similar situation exists in weaponizing UXVs. This is not so much the case with specialized UXVs, designed with a specific purpose in-mind for which there is no satisfactory human counterpart, but applies to the longer-term, more generalized battlefield UXV, meant to replace the infantry soldier, as an example. Besides bearing arms and shooting at enemy targets, the basic infantry soldier has other functions that he must perform, sometimes simultaneously with engaging enemy targets. As an example, he is charged with securing weapons found on the battlefield so that enemy combatants can no longer use them. He is also charged with gathering battlefield intelligence so that the Tactical Operational Picture can be kept current. This intelligence can be something as mundane as observing the condition of the boots found on dead enemy combatants, or the type and quality of the food they have been eating. New boots may

indicate fresh troops who are well equipped, while old, worn boots may indicate troops who have been in battle for some time. The presence of standard-issue food containers may indicate that an enemy's supply lines are intact, while the presence of fresh, locally grown, foods may indicate that the enemy is having trouble with his supply lines, and the troops are having to forage for food. This intelligence then feeds back into the weapons employment cycle when planning for future operations, indicating the state of readiness of opposing forces.

The Science Applications International Corporation,[9] documenting work done in support of the Integrated Infantry Combat System effort for the USMC. The primary purpose of this effort was "…to integrate all systems resident in the Marine Rifle Squad – weapons, target acquisition, computer and communications, navigation, and protective – in order to provide a quantum increase in mobility, lethality, command and control, survivability, and sustainability capabilities for the squad." One of the products of this effort was a detailed listing of Squad Functional Capabilities (SFCs), which were defined as the lowest common tactical behaviors that are performed by a Marine Rifle Squad. The SFCs form an integral part of an Objective Hierarchy that is made up of six top-level Functional Categories: mobility, lethality, command and control, survivability, sustainability, and training. Basically, this is a listing of all the functions that the members of a Marine Rifle Squad have to perform on the battlefield *as a group*. This is rather fortuitous, since we are expecting to field multiple weaponized UXVs to support a single operator. We can use this Objective Hierarchy as a jumping-off point for determining the functions that our weaponized UXVs will need to perform *in total* to support their single operator. While this was done to support developments for the infantry, there are parallels in other areas.

If we approach the weaponizing of UXVs without addressing the performance of these other functions, we will not eliminate people from the battlefield, since, somehow, the functions must still be performed, and we may end up *raising* the overall total cost of ownership, instead of lowering it, by requiring both UXVs *and* personnel to be on the battlefield.

REFERENCES

1. Summey, D. C.; Rodriguez, R. R.; DeMartino, D. P.; Portman Jr., H. P.; and Moritz, E., *Naval Readiness Augmentation: A Concept for Unmanned Systems in the Navy*, CSS TR-01/04, June 2001, Coastal Systems Station, Panama City, FL.

2. Bachkosky, J. M.; Begley, G. A.; Rumpf, R. L.; Eash, J. J.; Fratarangelo, P. A.; Hubbard, J. E.; Katz, D. J.; Mooney, J. B.; Morrish, A. A.; Sinnett, J. M.; Smith, J. A.; Toscano, M.; Zimet, E.; *Roles of Unmanned Vehicles*, NRAC 03-1 (Draft), March 2003, NRAC, Assistant Secretary of the Navy (RDA), Washington, D. C.

3. Loeb, Vernon, and Ricks, Thomas E., "1's and 0's Replacing Bullets in U.S. Arsenal. Success in Afghanistan Propels Shift to Equipping Forces with Digital Arms," *Washington Post*, 2 February 2002, Sec. A, pg. 1.

4. "Autonomic Computing," http://www.research.ibm.com/autonomic.

5. McHale, John, "Unmanned Aircraft Armed and Dangerous," *Military and Aerospace Electronics*, Vol. 14, No. 11, November 2003, pp. 18-25.

6. Gold, Ted, and Lederburg, Joshua, *Report of the Defense Science Board Task Force on Discriminate Use of Force*, July 2003, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics, Washington, D. C.

7. NWP 1-14M, MCWP 5-2.1, COMDTPUB P5800.7, Change 1 of 3 July 1996, Subj: *The Commander's Handbook on the Law of Naval Operations*, Department of the Navy, Office of the Chief of Naval Operations and Headquarters, U.S. Marine Corps, and Department of Transportation U.S. Coast Guard.

8. Watkins, David, "What's Wrong with Offshoring R&D," http://www.techupdate.com/techupdate/stories/main/wrong_with_offshoring_RD.html, accessed on 20 January 2004.

9. *Front End Analysis for the Integrated Infantry Combat System Concept Exploration Plan, Final Report*, Marine Corps Systems Command, Science Applications International Corporation, McLean, VA, 19 January 2001.

DISTRIBUTION

COPIES/CD

DOD ACTIVITIES (CONUS)

ATTN CODE A76
(TECHNICAL LIBRARY) 0/1
COMMANDING OFFICER
CSSDD NSWC
6703 W HIGHWAY 98
PANAMA CITY FL 32407–7001

DEFENSE TECHNICAL INFO CENTER 0/2
8725 JOHN J KINGMAN RD
SUITE 0944
FT BELVOIR VA 22060–6218

ATTN BARBARA J MACHAK 1/0
ACTING ASSOCIATE TECHNICAL DIRECTOR
SYSTEMS CONCEPTS AND TECHNOLOGY
ARDEC
PICATINNY ARSENAL NJ 07806-5000

ATTN CHARLES KIMZEY 1/0
DEPUTY UNDER SECRETARY OF DEFENSE
AS&C
3700 DEFENSE PENTAGON
WASHINGTON DC 20301-3700

ATTN ALEXANDER KOTT 1/0
DEFENSE ADVANCED RESEARCH
PROJECTS AGENCY
3701 NORTH FAIRFAX DRIVE
ARLINGTON VA 22203-1714

ATTN CHARLES SHOEMAKER 1/0
ARMY RESEARCH LABORATORY
AMSRL-WM-BR
ABERDEEN PROVING GROUND MD 21005

ATTN BOB WILCOX 0/1
JOINT ROBOTICS PROGRAM
59 FREESIA COURT
ROMEOVILLE IL 60446

COPIES/CD

NON-DOD ACTIVITIES (CONUS)

ATTN DOCUMENT CENTER 0/1
THE CNA CORPORATION
4825 MARK CENTER DRIVE
ALEXANDRIA VA 22311-1850

ATTN GIFT AND EXCHANGE DIVISION 1/1
LIBRARY OF CONGRESS
WASHINGTON DC 20540

INTERNAL

B60 (TECHNICAL LIBRARY) 0/3
G 1/0
G80 (CANNING) 1/1

This page is intentionally blank.

DAHLGREN