ACCELERATING THE KILL CHAIN VIA FUTURE UNMANNED AIRCRAFT

Julian C. Cheater, Major, USAF
April 2007

Blue Horizons Paper
Center for Strategy and Technology
Air War College

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. It is not copyrighted in accordance with Air Force Instruction 51-303, *Intellectual Property—Patents, Patent Related Matters, Trademarks and Copyrights*, but it is the property of the United States government.

About the Author

Major Julian "Ghost" Cheater is a 1994 graduate of the United States Air Force Academy with a Bachelor of Science in Political Science. He is a senior pilot with over 3,100 flying hours in C-21s, F-16s, and T-38s. After completing Air Command and Staff College, he will attend the School of Advanced Air and Space Studies at Maxwell Air Force Base, Alabama.

Acknowledgements

I would like to thank everyone that helped with and participated in the Unmanned Aircraft (UA) survey. Dr. Steve Hansen did an outstanding job with his survey support despite firewall constraints. Many experts provided valuable insights through detailed comments in the survey. Both your anonymous and self-identified answers gave me direction for my research paper. At the risk of leaving someone out, I would like to thank the following experts for their time and insights: Mr. Dyke Weatherington, Mr. Michael Pitts, Rear Adm Thomas J. Cassidy, Jr. USN (Ret), Col Michael Francis, (PhD), USAF (Ret), Col Tom Ehrhard, (PhD), USAF (Ret), Lt Col Ed "Mel" Tomme, (PhD), USAF (Ret), Dr. Arun Ayyagari, Mr. Steven Rasmussen, Mr. Bruce Carmichael, Mr. Jerry Madigan, Mr. Chris Miller, Mr. Gary Nault, Mr. Todd Bruner, Dr. Ali Minai, Dr. Jack Langelaan, Dr. Eric Frew, Mr. Cory Dixon, (PhD candidate), Dr. John Baker, Dr. Bruce Clough, and Lt Col Brent Marley, USAF (Ret). None of these individuals read any part of this research paper nor would they necessarily agree with the conclusions. However, each did provide a perspective that related to a technical aspect of future unmanned aircraft.

Others helped with their insights via interview or e-mail exchange including: Lt Col Wes "WW" Long, Lt Col Kelly Greene, (PhD), Lt Col John Harris, Mr. Brian Martinez, Mr. Joe Macker, Mr. Jon Park, Mr. Jerry Holdiness, Dr. Sacky Holdiness, Lt Col Stephen Rothstein, and Col Fred Stein, USA (Ret). Blue Horizons research seminar instructors stimulated thinking "outside of the container" by inviting high-level speakers and assigning nontraditional readings.

I would like to thank my family for their patience during my preoccupation with this research paper. You especially helped by convincing me to take study breaks and play T-ball, play hide-and-seek, or watch *Prison Break*. My goal in writing this paper was to increase US military capability in some small way and generate discussion across disciplines.

Abstract

Unmanned aircraft (UA) have evolved from simple reconnaissance assets into capable and persistent strike platforms in a short period of time. Looking ahead to the year 2025, what technologies will help the US military reduce the time it takes to find, track, and neutralize a target with UA? The United States can have the greatest impact in accelerating the kill chain by investing in research that advances autonomous UA operations and enables a Mobile Ad-hoc Network (MANET) using UA as communications nodes. This MANET should interface with the Internet to provide maximum warfighter access and it will relay information via a combination of radio frequency, laser communication, and satellite communication links.

As warfighters, we tend to focus more on the kinetic effects such as improving munitions instead of unglamorous but critical tasks such as gathering, analyzing, and distributing vital information to the right person for action. Autonomous UA operations will reduce manpower and bandwidth requirements while an improved airborne communications network will increase situational awareness for warfighters and decrease reliance on satellites.

The military often seeks to "revolutionize" warfighting via cutting-edge technologies, but it can often gain more by selectively improving existing technologies to promote autonomy and interoperability with less risk. Ironically, accelerating the kill chain with capable sensor-shooters may be delayed more by political, cultural, and service doctrine biases than technological barriers. UA airspace integration, deconfliction methods, and inter-service command and control still warrant attention. By overcoming both technical and cultural barriers, the United States can accelerate the kill chain and anticipate enemy actions instead of reacting to attacks.

Contents

Page

Background Information

Hypothetical Scenario

The year is 2025 and teams of US unmanned aircraft (UA) are autonomously coordinating attacks against radical insurgents following a major war in the Middle East. A UA analyzes the facial features of a man driving a Sports Utility Vehicle (SUV) through busy streets towards a crowded marketplace. Two suspicious-looking passengers are in the car with what appear to be backpacks loaded with wires. The UA matches the suspect's features with that of a known terrorist and requests consent from you, the Combined Air Operations Center (CAOC) Commander, to fire a next-generation Hellfire missile. With seconds to engage the SUV before it reaches the marketplace, do you grant permission to fire the missile into a busy, urban environment with the hopes of preventing even more casualties?

The US military does not know which non-state or state actors will threaten its interests in the year 2025. What is certain is that it must prepare now to fight an enemy who will not wear uniforms and will choose an urban battleground, perhaps on US territory. However, it cannot neglect the less likely but more catastrophic threat of a state actor that seeks grave harm to America. A country that wants to limit US influence will likely attack its computer and communications networks and engage in a proxy war by selling advanced arms to smaller countries willing to challenge the US giant. This paper briefly discusses how unmanned aircraft can contribute to the future fight due to their persistence, lethality, and lower risk to humans.

Question, Thesis, and Justification

While this scenario raises numerous political, ethical, and weapons employment questions, the intent is to focus on two technologies that have the greatest potential to increase future unmanned aircraft capabilities. Which technologies enabling UA will have the greatest effect in reducing the time it takes to identify and neutralize a target in 2025? Technologies

enabling autonomous operations and an effective communications architecture will have the greatest influence on compressing the time required for UA to find and prosecute a target. The requirement for autonomous operations will increase as the US military collects even more data, reduces manpower, and exceeds satellite bandwidth availability. Next, collected data must be transformed into usable information that can be effectively disseminated to shape the battlespace.

Methodology and Survey Results

The researcher used an anonymous, online survey to compare answers of leading government, industry, and academic professionals with experience related to UA. An "expert" was defined as someone who briefed at a national conference on UA operations, authored three or more articles on technology related to UA operations, or served as a Division Chief of a UA group (See Appendix C for survey).[1] Potential problems or biases with the survey responses include: 1) industry experts may have been biased towards technologies that they are developing, 2) the researcher did not survey space experts who might have disagreed with the utility of air-breathing ISR assets, and 3) multiple choice questions can be interpreted differently.[2] The 16-question survey was sent to 73 UA experts and 46 people responded.

The survey asked UA experts to identify the top three enabling technologies that will have the greatest impact on future UA in 2025. The top four selections were: 1) Artificial Intelligence (AI) with 29 votes, 2) propulsion advances with 19 votes, 3) information technology with 18 votes, and 4) computer processing with 17 votes. (See Appendix D) These responses partially justified the researcher's focus on AI (and autonomy) and information technology (or communications architecture). Detailed answers from a cross-section of experts provided great insight and candid responses. (See Appendix E for survey quotes) All answers were anonymous unless the respondent gave specific authorization to release their answers.

The researcher avoided accessing classified information to prevent inadvertent disclosure but risked proposing a concept or technology that was in use or had been abandoned. Surveys and telephone interviews provided different views from professors, researchers, industry partners, government leaders, and authors to provide a holistic look at future UA operations.

Terminology and Definitions

Numerous terms for unmanned aircraft create confusion, even within the military. The Office of the Secretary of Defense (OSD) published the *Unmanned Aircraft Systems Roadmap 2005* that included the terms Unmanned Aircraft System (UAS) and Unmanned Aircraft (UA). This comprehensive publication used the term Unmanned Aircraft Systems when referring to the entire system and the term Unmanned Aircraft when referring only to the airborne component.[3] In this paper, the terms UAS or UA will be used to comply with the most recent Department of Defense (DoD) guidance in the *UAS Roadmap 2005*. The common term Micro Air Vehicle (MAV) will be used when referring to UA whose wingspan is approximately one foot.

Other common terms still used include "killer drones," Unmanned Aerial Vehicles (UAV), and Unmanned Combat Aerial Vehicles (UCAV). Air Force Doctrine Document (AFDD) 2-1.3, *Counterland Operations* approved on 11 September 2006 uses the term UA but joint doctrine still uses the older term "UAV." However, joint doctrine does provide a good working definition of UA in the 2007 *DoD Dictionary of Military and Associated Terms*:

> 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 nonlethal payload. Ballistic or semiballistic vehicles, cruise missiles, and artillery projectiles are not considered unmanned aerial vehicles.[4]

Problem and Significance

> *To subdue the enemy without fighting is the acme of skill…thus what is of supreme importance in war is to attack the enemy's strategy.* [5]
>
> *— Sun Tzu*

As seen in Iraq, enemies of the United States will challenge it asymmetrically since few can match its conventional military strength. This asymmetric challenge will require greater international intelligence cooperation and more persistent Intelligence, Surveillance, and Reconnaissance (ISR). However, fleeting opportunities to neutralize high-value targets will continue to demand sensor and shooter integration to minimize the time it takes to find, fix, track, target, engage, and assess (F2T2EA) a target, more commonly known as the "kill chain."

Neutralizing individuals with UA on foreign soil raises many political, moral, and legal questions. Discussing these issues is beyond the scope of this paper but all of these issues will affect UA weapons employment and the time it takes to neutralize a target in 2025. How will a UA distinguish between a common criminal and enemy combatant from 25,000 feet? How will UA integrate into the National Airspace System (NAS) and what level of Federal Aviation Administration (FAA) approval and certification will be required? Manned aircraft face some of these obstacles but all of these questions affect UA to a greater degree.

The United States is not the only country to capitalize on the importance of UA as sensor-shooters. According to OSD, over 32 countries are developing more than 250 different versions of UA.[6] Military leaders in many countries will likely conclude that it's cheaper and more efficient to maintain large wings of UA than purchase advanced manned platforms and maintain a high pilot proficiency level. Even non-state actors such as Hezbollah have used offensive UA enabled by Google Earth imagery against a state actor. According to *Defense Update*, Hezbollah penetrated Israeli airspace with Iranian-made UA loaded with explosives on 13 August 2006 but

Israel downed both UA.[7] An enemy UA could be used on US soil to cause it harm instead of developing sophisticated aircraft to rival advanced US F-22s and F-35s. (See Appendix B)

Future UA will rely on network-centric operations but this can be seen as both a force multiplier and a vulnerability. The ability to minimize the time it takes to identify and neutralize a target depends less on munitions and other kinetic advances and more on communicating efficiently and securely. UA can serve as critical nodes of an airborne communications network to allow greater Service and interagency coordination so that critical information reaches the right person at the right time to take the appropriate action. China's demonstration of using a ballistic missile to down an aging weather satellite on 11 January 2007 revealed that US satellites may be at risk.[8] An airborne communications network will still allow theater commanders to control warfighters with some limitations. (See Appendix A for non-military applications)

The Kill Chain and the Decision Cycle

> *I think you will find that in all cases, no matter how quickly we can find, fix, track, and target, the decision to engage (assuming there is a human in the loop) will probably take longer than all the rest of the cycle combined.* [9]
>
> *— Lt Col Wes "WW" Long, Chief of Offensive Combat Ops, CENTCOM CAOC*

The kill chain and decision cycle apply to emerging targets rather than targets that were previously approved during the Air Tasking Order (ATO) process. During this process, targets are approved if destroying or degrading them supports objectives set by the Combined Forces Commander (CFC). Engaging emerging or time-sensitive targets (TST) requires real-time approval because they have not been evaluated. The kill chain includes a "mini-ATO process" that must be compressed in order to neutralize a target before it escapes or becomes a threat.

Sensor-shooter UA can accomplish all six phases of the kill chain process, but they cannot make the *decision* to engage. The six steps of the kill chain are abbreviated as F2T2EA and include: 1) Find, 2) Fix, 3) Track, 4) Target, 5) Engage (implying that a decision was made),

and 6) Assess.[10] UA excel at *finding* targets of opportunity due to their sophisticated sensors and persistence, and this capability will increase in the future with greater autonomy and "intelligent" operations. Improved sensors will help UA *fix* or determine exact target location in preparation for an attack. UA can *track* a target in order to find the best time to attack or to follow the target back to its base of operations. Future UA can speed up the *targeting* phase where the target is validated and restrictions are applied. After a decision is made, the UA can *engage* the hostile target with on-board weapons. Finally, during the *assess* phase, a UA conducts a battle damage assessment to determine if the desired effects were achieved or if the target must be re-attacked.

Today this streamlined process from finding a target to engaging it takes less than 45 minutes (with a goal of 10 minutes), reducing the window of opportunity for an enemy combatant to flee or blend into the crowd.[11] However, thanks in part to technical advances, the kill chain can be compressed to seconds by the year 2025. This involves presenting the weapons release authority with attack justification in the form of distilled intelligence and weaponeering.

Before a UA can engage a target, it must first gather and then forward critical information to decision makers in the CAOC. Advances in autonomy, intelligent control, and micro-processing will allow future UA to quickly gather accurate data and conduct a comprehensive on-board analysis. This analysis includes rapidly cross-checking collected data against stored memory to produce: valid target identification, mensurated coordinates, an attack axis, weapons selection, fusing (if applicable), estimated weapon time of flight, collateral damage estimates, location of friendly forces, application of Rules of Engagement (ROE) and Laws Of Armed Conflict (LOAC), cross-checks against the restricted target list (RTL) and no-strike list (NSL), estimated risk level, and proposed strategic effects. According to AFDD 2-1.9 *Targeting*, "The effort to mensurate coordinates, especially for a target set with a large number of DPIs [Desired

Points of Impact], can be extremely long."[12] By 2025, the process of obtaining exact coordinates and target elevation should be completed in seconds based on projected technical advances.

The kill chain will be accelerated if UA "push" only vital information to the right decision maker with weapons release authority (CAOC Commander in this scenario). Information should include all pertinent but no extraneous information that a commander would want before authorizing a strike. He or she may want to cross check the target with another type of sensor but time may not permit this luxury. The purpose of these autonomous operations, advanced sensors, and efficient filtering schemes is to ensure that the CAOC Commander has all relevant information in a short time to make the decision whether to engage or not.

Jon Park, senior functional analyst for the Air Force's C2ISR Center, shared that the USAF is working to reduce the decision cycle time now by using a common machine-to-machine language. He is part of a team that is developing the use of "XML" tags to leverage the Global Information Grid (GIG) via the NIPRNET or SIPRNET.[13] XML (short for eXtensible Markup Language) tags provide the capability to sort, filter, and fuse information from many diverse databases. These behind-the-scenes efforts will be transparent to the warfighter as TST cells conduct Internet searches for information related to targets. Members of the TST team will search based on knowledge about target time and location, but they can further refine their search if armed with additional facts such as target type, proximity to a point, or intelligence source. While these efforts are required now, future "intelligent" UA may make these processes obsolete if they can perform them on-board.

If the weapons release authority delays the engagement decision, the kill chain will not be accelerated. Roman, a contributor to the *Air Force 2025* study stated, "Unfortunately, decision-making technology, such as computer-assisted logic tools and artificial intelligence, has not

progressed as rapidly as information-gathering technology."[14] This decision now can take hours depending upon the situation in counter-insurgency operations. A request for weapons release may also trigger other decision branches such as CAOC coordination for inserting Special Operations Forces (SOF) to evaluate the situation. A delayed decision to attack could prevent excessive collateral damage but it may also result in a lost opportunity to prosecute a valid target. The delayed decision *could* mean that a terrorist will escape and live to plan another attack.

Centralized Control and Decentralized Execution

Target sensitivity will dictate the approval authority to engage an emerging target. This authority typically ranges from the Chief of Combat Operations in the CAOC to the Combined Forces Air Component Commander (CFACC) but it is situation-dependent. AFDD 2-1.9 states:

> The authority to engage should be delegated to the *C2 node that has the best information or situational awareness* to execute the mission and direct communications to the operators and crews of the weapon systems involved. If the CFACC is delegated TST engagement authority by the CFC, that commander may delegate his engagement authority to a lower level (e.g., CAOC director or chief of combat operations).[15]

Flexibility in USAF doctrine means that the CFC will typically delegate this responsibility to the CFACC who can then delegate it to lower levels. Driving this approval authority to the lowest levels means less coordination and a faster kill chain. Accelerating the kill chain is consistent with the 2003 *Air Force Transformation Flight Plan's* call for change to "achieve decision cycle dominance to strike adversaries before they can mount an effective defense."[16] By acting more rapidly than the enemy, the US military can drive the fight instead of reacting to the adversary.

Many UA missions today follow a model of centralized control and *centralized* rather than decentralized execution. The debate over the benefits of centralized versus decentralized execution will rage well into 2025, but generally centralized execution incorporates higher fidelity information to control strategic effects at the cost of slowing down the kill chain due to

additional coordination. Higher levels of authority generally have access to more information about the battlespace than a tactical UA operator who may have more detailed data about the target. Today, centralized execution for UA on TST missions makes sense since the CAOC Commander will have greater overall situational awareness (SA) than a UA controller located outside the CAOC.[17] However, for a UA mission performing (Close Air Support) CAS, the approval authority should be delegated to the lowest levels to promote quicker response times in support of ground forces. This does not mean that UA should be tethered to the ground commander because they can be re-roled to other missions such as ISR or strategic attack to maximize their effectiveness. With the addition of Small Diameter Bombs (SDB), long-duration UA will likely run out of targets before weapons.

In the future, if many operators have access to the same information as the CAOC Commander via the GIG, the real question will be who can process the information the quickest to build the most SA. This person should have weapons release authority as long as they are supporting the commander's intent. As technology improves, it is possible that this level will be delegated below the Chief of Combat Operations but strategic effects must be considered.

The reality is that decision makers and not technology will often be the limiting factor in reducing the time it takes to kill a target. The decision maker will rarely have *all* the necessary information but instead will likely have to make a very difficult call. In 2025, technological improvements in autonomous UA operations and communications will quickly provide most of the information required but strict ROE can prevent weapons release. Until the United States improves technically and changes culturally, its kinetic capabilities will exceed its abilities to quickly decide, slowing the kill chain, and providing its enemies with opportunities to escape.

Justification for Unmanned Aircraft

> *Now it is clear the military does not have enough unmanned vehicles. We're entering an era in which unmanned vehicles of all kinds will take on greater importance—in space, on land, in the air, and at sea.* [18]
>
> *— President Bush, 2001 remarks at the Citadel*

UA should be used in lieu of manned aircraft only where they can offer an advantage. Range, payload, persistence, complexity, and risk level are key factors for determining which platform to select for a specific mission. UA should be considered instead of manned aircraft for missions that are repetitive, require persistence, and pose great risk to humans. The Global Hawk and Predator can fly up to 40-hour missions[19] although standard missions today are about 20 hours (depending upon configuration and model).[20] Future sortie durations may only be limited by oil changes, required maintenance, or weapons reloading thanks to Automated Aerial Refueling (AAR). UA in the form of pilot-less Learjets have already performed AAR, potentially increasing UA sortie durations. (See Appendix L) Long sortie durations allow UA to provide continuous coverage of threat areas and increase the chances of locating a TST. Also, on high-risk missions, it will be more politically acceptable to lose UA instead of pilots.

In the future, UA may become the CAS and Hunter-Killer platforms of choice thanks to long loiter times, improved data-link, and limited numbers of in-theater manned assets. Even though the dynamic CAS role requires adaptation, technology can help UA overcome *some* inherent limitations. Friendly ground forces can validate the UA's target of interest or illuminate the enemy with a laser so that the UA can drop Laser-Guided Bombs (LGB). Today, the USAF and Army use the Remotely Operated Video Enhanced Receiver (ROVER), a rugged laptop computer with support equipment that allows ground forces to watch real-time UA images and video. [21] In the future, the USAF should integrate accurate individual blue force tracker information and data-link precise Global Positioning System (GPS) coordinates of the UA's

sensor point of interest to ground personnel to minimize the chance of fratricide. UA will only be required to perform minimal on-board processing and information relays, marginalizing advantages enjoyed by pilots.

Missions such as the Suppression or Destruction of Enemy Air Defenses (SEAD/DEAD) can pose grave danger to aircrews. With the exception of Conventional Air-Launched Cruise Missiles (CALCM), the ranges of sophisticated SAMs usually exceed the ranges of ordnance dropped from aircraft.[22] John Tirpack, a senior editor for *Air Force Magazine*, claimed that the SA-20 "Triumph" has a range of 248 statute miles and can engage up to six targets simultaneously.[23] This system and follow-on systems to the SA-20 will share targeting information between launchers, reducing the time required for radar transmissions, and complicating US ability to target them.[24] Incorporating GPS and Inertial Navigation System (INS) units with active radar seekers into High speed Anti-Radiation Missiles (HARM) will help negate this tactic, but the US military should anticipate GPS jamming in this high-threat environment.[25] Stealthy UA carrying future standoff missiles may be the answer for DEAD missions if they can exceed the range of future SAMs.

Limitations of Unmanned Aircraft

UA offer the warfighter tremendous capabilities but sometimes their limitations are overlooked. Currently, several personnel are required to operate UA but this will change with advances in autonomy. With less autonomy, controllers must frequently transmit commands to UA, increasing demand on bandwidth. Many view UA as cheap alternatives to manned aircraft but sophisticated sensors, expensive propulsion systems, and advanced communication suites make the cost of many UA comparable to manned platforms. Often airspace restrictions due to safety concerns affect UA operational utility and experimental testing. This was exacerbated by

the high initial accident rates of UA (many due to icing) and raised concerns about survivability in a high-threat environment. The ability for a variety of UA to communicate with each other will become even more important with the proliferation of different operating systems. Current UA provide valuable situational awareness, especially through real-time video, but this does not offer a panoramic view enjoyed by a pilot.[26]

Autonomous Operations

Artificial Intelligence Applications to Unmanned Aircraft

By increasing autonomy now and incorporating Artificial Intelligence (AI) as it matures, one person can effectively monitor several UA depending on mission phase and task loading. In Afghanistan, it was reported that four or five controllers were required to control a single UA.[27] With advances in autonomy, one supervisor or "team captain" will control several UA in order to reduce overall costs and manpower requirements.

How will an operator know if a system is malfunctioning? Even with increased autonomy, human supervisors need to know enough about the systems to realize when something is wrong. This also requires investment in man-to-machine interfaces to make it easy for a supervisor to understand the UA decision matrix to identify system problems.

Advances in AI will continue to increase the utility of UA but one cannot conveniently forget their limitations. Although the human brain is much slower than a computer, it uses simultaneous or parallel processing through thousands of nerve fibers to process complicated decisions more quickly than computers.[28] A pilot can integrate visual, auditory, and olfactory cues in a dynamic environment to make decisions that future AI systems cannot. Even with these limitations, UA will replace manned aircraft due to their persistence and should be upgraded with more intelligent systems as they become available. (See Appendix P)

While single UA have achieved high levels of autonomy, *multiple* UA operating together can achieve even greater mission effectiveness. A universal control architecture that allows communication between different UA but promotes individual optimization may have the greatest success. According to Lewis and Weiss, the collaborative efforts of many UA have a measurable, synergistic effect to achieve overall mission objectives.[29]

If future UA(s) are built with intelligent control, they can adapt to new situations and provide more valuable information to decision makers. In 2003 test scenarios, the National Aeronautics and Space Administration (NASA) used neural networks in a highly-modified F-15 to "learn" new flight characteristics and adjust the flight control system after a simulated structural failure.[30] Building on these tests, future UA should incorporate similar intelligent control systems to accelerate the kill chain. Within seconds, UA with AI should be able to analyze, filter, and send vital information to the CAOC Commander for an engagement decision.

In order to make accurate decisions about investing in AI technology, one must understand the differences between AI, autonomy, and capability (See Appendix G). Increased autonomy will reduce the number of UAS operators or decrease use of satellite bandwidth but "intelligence" and information sharing between different sensors and platforms will accelerate the kill chain. A combination of highly autonomous, "intelligent," and capable systems should be developed through a focused effort that spans many academic disciplines. (See Appendix H)

Deconfliction

> *"Artificial intelligence poses a certification challenge because you cannot verify the safety of an evolving operating system."*[31]
>
> *– Anonymous*

Deconfliction issues are *indirectly* linked to slowing the kill chain because they can potentially limit UA use. While much of this debate is beyond the scope of this paper,

deconfliction will likely remain a contentious issue due to the increasing number and variety of UA. The United States needs to resolve these issues to promote UA advancements, allow host nation operations, and prevent the tragedy of a mid-air collision. Most survey respondents felt strongly that airspace issues were more political than technical in nature and they limited UA development. (See Appendix E) The preferred deconfliction method will require UA to take early evasive action to avoid manned aircraft from having to do so. Small, timely adjustments made earlier result in minor overall deviations but will require sophisticated UA algorithms.[32]

Beyond smart route programming, designers of future UA must consider political constraints of regulatory departments of foreign countries and even the FAA. After Hurricane Katrina, the United States failed to make full use of UA due to safety concerns and a lack of coordination. General Keys provided insight by explaining how the USAF improvised by strapping UA sensors to helicopters because of FAA restrictions:

> We brought 10 Unmanned Aerial Vehicles to New Orleans to provide an awareness capability that we continued to work on. And our first intent was to fly these UAVs around the New Orleans area and help Gen. Russell Honoré with situational awareness. The FAA looked at that and said "not so fast." So we ended up – with the flexibility of key air power, cutting the wings off – they're made of Styrofoam – the wings off the UAVs and strapping them to helicopter struts, and now you've got cameras everywhere. Or put them on the tallest hotels out there – I think we put four of them on the Wyndham building downtown – with a 360 degree view of the city.[33]

Coordination and technical solutions highlight the importance of deconfliction and illustrate how this issue can save lives. Algorithms must be developed to allow UA to adjust from operations in civilian airspace to operations in a combat environment. With AI advances, UA integration into civilian airspace will become more of a technical than political issue.

With the growing number of small Army and Marine UA, the mid-air potential between a UA and manned fixed or rotary wing aircraft will increase exponentially unless the military solves these issues with a joint mindset. By considering these factors early in the design phase,

the US military can help streamline efforts and ensure that valuable ISR assets are effectively used when needed most. A mid-air resulting from inadequate deconfliction procedures will result in UA flight restrictions and will have the cascading effect of slowing the kill chain.

Autonomous Routing

Before a UA can find, track, or engage a target, it must be able to fly a desirable routing and deconflict from other aircraft and objects attached to the ground. While this is relatively easy for a pilot, this task for future UA should not necessarily dictate a simple preprogrammed route. Instead, it must be somewhat unpredictable in order to survive ground fire.

Mission types will dictate desired routing and influence the development of supporting algorithms. Should UA monitor roads used by coalition convoys to find combatants planting Improvised Explosive Devices (IED)? Should UA hunt enemy snipers by searching for muzzle flashes or triangulating the sounds of gunshots? Should UA penetrate formidable Integrated Air Defenses (IAD) to kill enemy C2 nodes for follow-on strike packages? In any case, the routing must be flexible enough to change priorities quickly even with highly autonomous UA. This will require scientists and engineers to design algorithms that allow mission priorities to be easily changed to support ever-changing mission requirements. While an armed UA can perform many missions, a stealthy and "intelligent" UA is best suited for SEAD/DEAD missions.

Some UA may have to operate intelligently in high-threat environments where they cannot use GPS navigation due to enemy jamming. Instead, they will have to rely on terrain contour matching (TERCOM) and other dead-reckoning methods to arrive at the target (See Appendix J). In this high-threat environment, communications jamming will prevent UA from querying the CAOC Commander for strike approval due to unexpected changes (target moved).

An autonomous UA tracking a moving target will face even more difficulties than a human "flying" a UA with a limited field-of-view. For a human controller, it has been compared to flying while "looking through a soda straw" to illustrate the lack of peripheral vision. In order to track a moving target, the UA must know its own position, continually update the target's position and velocity from two-dimensional images, make wind corrections, and finally keep the moving target within the UA's sensor field-of-view.[34] (See Appendix I) The complexity of flight path algorithms will increase as the USAF coordinates actions of *multiple* UA.

Swarming Versus Teaming

During the first phase of the kill chain, a single autonomous UA may find a target of interest but several UA working cooperatively will have even greater success. How they work together will depend on many factors, but the terms "swarming" and "teaming" have often been used to describe this relationship. These terms are not interchangeable, since teaming involves more complex interactions than swarming to achieve a goal. Clough defines swarming as "a collection of autonomous individuals relying on local sensing and reactive behaviors interacting such that a global behavior emerges from the interactions."[35] Clough also describes a swarm as reactive, homogeneous, simple, probabilistic, expendable, and somewhat inefficient. In contrast to swarming, one may define teaming as a group of individuals who each accomplish a critical task to efficiently achieve a complex objective.

UA can each collect a vital piece of information to aid the commander in making a life or death decision. The "intelligence" level and ability to share information within this team or swarm will impact the length of the kill chain. The decision may not always require a kinetic response but instead may trigger other branches such as additional intelligence gathering. Teams of UA will be capable of passing high fidelity information to the CAOC for decision-making, but

swarms of UA will likely only be capable of providing raw intelligence to analysts. However, swarms can still serve a useful purpose as long as they are inexpensive and have enough sophistication to prompt a team of UA to investigate a target of interest. (See Appendix K)

Automated Sensor Cueing

During phase one of the kill chain, a UA can efficiently *find* the target through automated sensor cueing. The most effective surveillance network consists of a layered approach where space assets provide strategic coverage, UA deliver responsive tracking and weapons delivery, and Micro Aerial Vehicles (MAV) offer close-in monitoring (See Appendix F). In this ultimate neighborhood watch, satellites can cue UA to investigate suspicious activity via data bursts but high altitude UA will also accomplish this. If the UA confirms the presence of enemy, this will trigger human intervention for higher level analysis and action.

Due to the long loiter times of UA, the USAF should minimize constant sensor monitoring by personnel in future operations. Instead, advances in automated sensor cueing can decrease operator workloads while still quickly finding and tracking the enemy. These advances must consist of sophisticated on-board algorithms and processing to find individual targets or enemy weapons systems. By leveraging facial recognition software used by casinos, UA can use sophisticated sensors to identify individuals with a high degree of certainty.[36]

High-resolution UA video feeds will help decision makers gather information but this has limitations. They must realize that watching video is like staring at the corner of a frame—you can get a perspective but you may not see the big picture. However, real-time information will still help them make quicker decisions, even if it is disapproving a strike. Automated sensor cueing will find targets of interest but *integration* with decision-makers is the key to success.

Sensor cueing can also enhance overall situational awareness (SA) through battlespace preparation. Knowing target locations before the fighting starts will result in fewer friendly casualties and operational success. For example, in the battle to regain control of Fallujah, Iraq on 7 November 2004, the USAF used ISR assets to map individual buildings before surgical strikes and CAS operations. Enabled by precision munitions and air supremacy (often erroneously assumed), US air and ground forces eliminated up to 2,000 insurgents in a challenging urban environment in eight days. This battle showed how real-time, persistent surveillance could help "cue" the firepower of aircraft and ground forces. *Air Force Magazine's* Rebecca Grant stated, "Round 2 in Fallujah…was to show the full impact of the new sensor and shooter technology when integrated with other forces in joint operations."[37] While the Fallujah model did *not* incorporate automated sensor cueing, it did demonstrate how ISR assets could reduce collateral damage, concentrate firepower, and anticipate attacks by finding targets.

Communications Architecture

Net-Centric Warfare

Net-centric advances have promoted integration and merged planning and execution but this does not necessarily mean that the actionable information reaches the right person. Many warning signs hinted to the 9-11 attacks but the United States missed the big picture by failing to connect the intelligence dots. Analyzing many intelligence clues and forwarding this actionable intelligence to the right people so that they may take the proper action at the right time also applies to military action. A network-centric communications architecture should provide this common operating picture based on a fusion of only relevant information. UA can serve as nodes to relay vital information to leaders in the CAOC who will make the engagement decision.

Military personnel know that there is no trophy for second place and that these high stakes demand complete mission dedication. This focus often leads warfighters to overemphasize kinetic effects such as developing better munitions at the expense of other improvements. Promoting secure and quick information passage between reconnaissance platforms, command and control centers, and joint warfighters will allow the US military to overwhelm the enemy by operating within their decision cycle. UA can play roles in this cycle by acting not only as both persistent sensors and shooters, but also as communications nodes to provide reliable theater alternatives to satellite communications.

Net-centric warfare may be seen as combat that relies on a communications network using computers to integrate, analyze, and disseminate multi-source information so that warfighters can make timely decisions. Future UA will provide valuable network contributions by collecting data and distributing information to enhance SA. If warfighters can see critical information via data link, they can make better and quicker decisions as long as they can select the data overlay to reduce the impact of information overload. Even allies who do not have the latest aircraft or equipment may have the ability to see threat information in their cockpits via data link, enhancing interoperability, and coalition warfighting effectiveness.

The challenge in the net-centric environment is to filter and manage excess information. Information management must involve a combination of smart algorithms that allows authorized warfighters to "pull" information from UA and other communications platforms while also prompting UA to "push" information that warrants immediate attention. A flight lead or UA operator may not need to know the location of all friendly forces unless he or she is preparing to attack a target. *Then* requesting blue force tracker information via data link would be useful to provide real-time information about friendly forces in the area. The ability to "push" and "pull"

large amounts of information will require strict data-link discipline to prevent an information overload. Upon request from an authorized user, a ground force tracker would transmit an encrypted, low power transmission "buried within Ultra-High Frequency (UHF) background noise thereby making it difficult to detect or intercept."[38] During Operation Iraqi Freedom (OIF), these blue force trackers allowed commanders to maintain awareness of advances by key command vehicles but it didn't show when friendly forces halted to engage in combat.[39]

Global Information Grid

While joint doctrine provides a lengthy definition for the Global Information Grid (GIG), the Government Accountability Office (GAO) provided a more succinct description. In a 2004 report, it stated that, "The GIG represents a collection of programs and initiatives aimed at building a secure network and set of information capabilities modeled after the Internet."[40] This concept of operations will enable net-centric warfare by providing a framework that uses Internet standards and protocols. Future UA can serve as key components on the GIG by acting as intermediate communications nodes and sensors within a mobile ad hoc network that also happen to provide real-time surveillance and combat firepower in their other jobs.

Lt Gen Michael Peterson, USAF Chief of Warfighting Integration, shared an experience that demonstrates how an airborne platform could serve as an Internet gateway on the GIG:

> I was talking on what we call voice-over internet protocol to the pilot of an F/A-18 at China Lake, which is just across the border from Nellis AFB. And I was looking at his targeting pod; I was looking at the synthetic aperture radar scope, and said "Hey, could you move the cursor up to the building on the left?" And with no delay at all, the cursor jumps up to the building on the left. You can't imagine how important that is, to sharing information in an environment where everything happens right now.[41]

Information once available only to pilots can now be shared with the world, indicating the US military's shift towards net-centric warfare. Managing this information hold the key to success.

Unmanned Aircraft in Mobile Ad Hoc Networks

> *Without LDHD [low density high demand] C2 [command and control] platforms in theater and confronted with line-of-sight radio limitations, commanders should consider dedicating some UA for C2 support to provide the vital link between the ASOC [Air Support Operations Center] and inbound combat aircraft tasked for CAS.*[42]
>
> *— AFDD 2-1.3, Counterland Operations*

A Mobile Ad hoc Network (MANET) may be defined as a structure-less and wireless network that consists of mobile nodes that temporarily link together to forward data to a destination. These network nodes can communicate with each other but they may not all have Internet access.[43] One can visualize this wireless network as a roadmap that lists average driving time between major cities. The quickest travel route may take you slightly out of the way but use faster roads (more efficient packet routing) than the shortest distance between the origin and destination which had road construction (loss of link between nodes).

The quote from AFDD 2-1.3, *Counterland Operations*, implies that UA should play vital roles as communications platforms. In 2025, it is likely that a MANET consisting of UA or an "Internet in the sky" will allow unrivaled interoperability. Airborne nodes, especially those that fly at high altitudes like Global Hawk, lend themselves to an efficient MANET due to their ability to transmit in all directions. However, extending this MANET to include any US aircraft, Army vehicle, Naval ship, and perhaps individual soldier may result in a more robust network. Increasing the number of UA will overcome limited transmission ranges of individual nodes and boost network reliability by providing alternative paths to failed nodes. Antenna technology advances will increase transmission ranges and improve power management. (See Appendix O)

The desired number of UA forming a constellation will be influenced by autonomy levels and transmission limitations. While highly autonomous UA will not transmit information frequently for routine activities, commanders must still retain tactical control via communication

links. By 2025, improved routing algorithms, antennas, and power sources will result in the creation of a very efficient routing scheme that incorporates many more nodes than just UA. Not only will these nodes increase overall SA for theater forces, they will feed critical information to CAOC decision-makers to adjust the war as it unfolds and determine the next course of action.

Communication Relays

We're already at war in cyberspace; have been for many years. [44]

— Gen Ronald E. Keys, Commander, Air Combat Command

The communications architecture describing UA in MANETs should consist of seamless links that include Radio Frequency (RF), laser communications (lasercom), and SATCOM (See Appendix N for lasercom discussion). Already scientists from the Air Force Research Laboratory (AFRL) have been working on a combination of lasercom and radio frequency links to connect ground, air, and space assets. Wireless networks are used today but they are usually slow (56 Kbps[45]) and do not follow Internet Protocol.[46] According to the AFRL, Internet-capable networks can reach transfer rates of 137 Mbps but they theorize that lasercom can boost this to 2,000 Mbps over 108 nautical miles.[47] To put this in context, a VHS image would require 1.5 Mbps and a DVD image would require 6 to 18 Mbps although transmission rate requirements vary widely based on image size, quality, and transmission time.[48] With high transmission rates, a constellation of UA communication nodes can provide routine beyond line-of-sight broadcasts, preserving SATCOM bandwidth for high volume or world-wide transmissions.[49]

With rapid communications developments in UA, tactics, techniques, and procedures may lag behind. In 2025, technology will support controlling UA via Internet gateways from "ground stations" that range from elaborate control rooms to forearm displays. While UA operators sitting in sophisticated control rooms will have high fidelity information from many sensors, a Joint Terminal Attack Controller (JTAC) may use a small laptop (such as ROVER).

This mobile interface is used today to provide a final check of where the UA's laser designator is pointing to prevent excess collateral damage but its capabilities will continue to expand.

The kill chain will be accelerated if the decision to engage is delegated to the lowest levels but the risk level of an unwanted attack also increases. Communication relays and data links will allow *authorized* ground personnel to observe what the UA sensors are seeing, and, in specific cases, manipulate target designators. Transferring UA sensor control introduces the possibility of error, but this capability may be warranted when neutralizing an enemy combatant in an urban environment to minimize collateral damage. While technology in 2025 will allow transfer of UA control, this creates numerous command and control issues that blur the line between centralized control and decentralized control.

Bandwidth Constraints

> *The system [of laser links] at times seems to have been portrayed as the Holy Grail in military communications capability, but the military has proved adept at rapidly expanding its bandwidth use to immediately soak up any additional capacity.* [50]
>
> *— Jeremy Singer, Air Force Magazine*

The US military's appetite for bandwidth has increased with each major conflict and that trend will likely continue. If bandwidth issues are not resolved, it is possible that restrictions on transmissions could delay access to critical information by decision-makers, slowing the kill chain. Reducing and compressing transmissions through automation and on-board processing may slow the demand for bandwidth but it will not reverse the trend. Kurt Klausner, previous communications and computer squadron commander, relayed several statements that highlight US bandwidth dependency:

> Lt Gen Harry Raduege Jr., director of the Defense Information Systems Agency (DISA) observed, 'Today, in Operation Enduring Freedom, we're supporting one-tenth the number of forces deployed during Desert Storm with eight times the commercial SATCOM bandwidth.' Additionally, 'Global Hawk consumed five times the total

bandwidth used by the entire US military in the Gulf; and operations in Kosovo used 2.5 times what was used in the Gulf War.'[51]

The transmission of hyperspectral images will consume even larger amounts of bandwidth. This type of imaging collects data from hundreds of narrow spectral bandwidths to help identify and discriminate parts of a cube image. While *multi*spectral imaging uses fewer bands to generate a composite picture, *hyper*spectral imaging (HSI) uses continuous bands to create higher resolution images than can be used to detect chemical or biological weapons, assess damage to underground bunkers, or penetrate foliage to detect hidden targets.[52] To reduce the amount of bandwidth required, only parts or chunks of these images may be transmitted.

Near competitors view US reliance on commercial communications satellites as a vulnerability. During OIF, DISA reported that commercial satellites supplied up to 84% of the SATCOM, revealing the risk associated with relying on leased commercial satellites.[53] While bandwidth restrictions will ease if future satellites launch as scheduled, funding and technical success are not guaranteed. (See Appendix M) With limited bandwidth, an autonomous UA may not be able to transmit critical information to CAOC decision-makers via SATCOM. However, the combination of using MANETs and autonomous operations reduces bandwidth requirements and provides a workaround to the SATCOM bottleneck.

Interoperability

Greater interoperability will allow all Services, agencies, and countries to contribute information that will impact the CAOC Commander's decision to engage a target. Interoperability starts with a joint vision, determination of joint requirements, joint acquisitions, joint testing, and joint training. This emphasis on jointness should be extended to interagency and coalition operations for major players in a wartime scenario. Through early coordination, Services can understand how future systems will communicate and integrate with sister service

weapons systems. This affects the development of algorithms and autonomous operations, but it shapes communications architectures to a greater degree.

Even with separate systems, the United States can promote interoperability by developing communications nodes that convert different types of communication into a format consistent with Internet Protocol. Joe Macker, senior communications engineer for the Naval Research Laboratory, has written extensively on MANETS and stated:

> Reflecting upon past Internet technology development, it is clear that support for a heterogeneous mix of technologies and devices is one of the great successes of IP. In the near future, computing and network routing devices may typically have multiple wireless media interfaces (e.g., Ultra-wideband, Bluetooth, Zigbee, 802.11 variants, cellular).[54]

The ability to convert different types of communication gives the warfighter greater flexibility and could mean that before 2025 any *authorized* user with a cell phone, laptop, or radio can contact an orbiting UA for permission to conduct a time-sensitive strike. The ability to include information from a variety of sources may help the weapons release authority in the CAOC make a better-informed (but not necessarily quicker) decision. This may also provide an effective way of integrating human intelligence to help build a common operating picture.

Looking ahead to 2025, if US coalition partners lack the same capabilities, the US military should data link selected information to allow them to prosecute targets. Coalition partners in the CAOC who influence the decision-making cycle for an airstrike need to have access to much of the same information as the CAOC Commander. A common language consistent with Internet Protocols allows the greatest chance for interoperability and maximum warfighting effectiveness. Current developments such as using XML format are a step in the right direction towards seamless interoperability in military communications.

Wireless Network Security Concerns

The *National Strategy to Secure Cyberspace* (NSSC) states that "wireless communications can be intercepted and that wireless networks can also experience denial-of-service attacks."[55] As the NSSC alludes to, wireless networks by their dynamic nature are more prone to communications interception or sabotage. This may be accomplished by compromising a communications node (such as a UA) or overloading the system with useless information. If the MANET consisting of UA and other airborne assets cannot protect against intrusion with high confidence levels, the benefits of the network do not outweigh the risks.

Potential adversaries have already identified US communication systems as critical vulnerabilities. According to Stokes, "Chinese writings have specifically noted the threat of UAVs and have strongly advocated striking out at nodes within the UAV C3I system."[56] (See Appendix R for foreign intelligence concerns) To prevent compromising future MANETs, the US military must invest in advanced cryptographic techniques and routing schemes that allow classified information to securely transit wireless networks and unclassified lines. Future MANETs must be able to isolate and bypass nodes that are potentially compromised.

By advocating and implementing the latest Internet Protocols and providing military advisors to civilian organizations such as the Internet Engineering Task Force (IETF), the United States can help secure military and civilian networks. Internet Protocol version 6 (IPv6) uses a 128-bit encryption standard for Internet addresses instead of the current 32-bit encryption for IPv4.[57] This provides greater security, better routing schemes, and dramatically increases the number of IP addresses so that "almost any electronic device can have its own address."[58] By having more IP addresses, the US military should be able to use UA and other mobile nodes as Internet-capable interfaces on the GIG. (See Appendix Q for expanded explanation on security)

Conclusions

In 2025, future unmanned aircraft (UA) *can* reduce the kill chain to a matter of seconds, largely due to advances in autonomous operations and streamlined communications. Consolidating capabilities into a single platform reduces coordination requirements for UA acting as sensors, shooters, and communicators and allows them to complete all phases of the kill chain. Limiting factors in accelerating the kill chain will be the fidelity of information provided to the engagement authority and the willingness for that person to trust an automated system.

UA are especially well-suited to *find* and *engage* high-value targets thanks to inherent advantages such as long loiter times, improved offensive capabilities, and sophisticated sensors. However, sometimes their current utility is overstated and their limitations are not fully realized. Even in 2025, pilots will still make higher level decisions, adapt more quickly to changing situations, and will probably enjoy weapons release authority that UA will not have.

Technological advances in UA autonomy will aid in the engagement decision through on-board analysis of critical information while reducing bandwidth and manpower requirements. The CAOC Commander will receive this distilled information and weapons release request via a machine-to-machine interface using Internet Protocols. It is this decision to engage or not that will have the greatest influence in lengthening or shortening the kill chain.

In 2025, UA and other airborne platforms will also serve as communication nodes in a Mobile Ad-hoc Network (MANET) to provide beyond-line-of-sight transmissions. This MANET will use a seamless combination of lasercom, radio frequency, and SATCOM links to boost the situational awareness of all warfighters on the network. The MANET must have robust security measures since adversaries will target what they already perceive as a critical vulnerability. In the event US communications satellites are attacked or degraded, a

constellation of UA can provide a limited theater backup and act as the eyes, ears, mouth, and even fists for the forward-deployed Combined Forces Commander.

The United States will likely overcome technological barriers to maximize UA effectiveness and compress the kill chain, but political, cultural, and doctrinal challenges may be harder to surmount. Unless political will is used to quickly solve the issues of UA airspace integration and certification, the operational utility and research testing of UA will be limited. Culturally, it will be difficult to trust automated systems to provide all the information for a life or death decision. For example, it is unlikely that there be a rush of volunteers to fly on the first unmanned airliner, even if the algorithms have been "debugged." As the US military buys more UA, the extent to which each Service controls and integrates them will pose command and control as well as deconfliction challenges that will influence joint doctrine.

So as the CAOC Commander in the hypothetical scenario, did you authorize weapons release to neutralize the SUV before it reached the marketplace? Future autonomous UA and streamlined communications should give you valuable bits of information to make the decision. Even though the SUV driver did nothing illegal, the system should have built a profile based on probabilities that allowed you to *anticipate* that person's actions rather than simply *react* to a possible attack. However, even armed with this timely information, it will still be a tough call.

Recommendations

The US military should invest in the following areas as a subset of recapitalization:

1) Use a combination of military research laboratory studies, university research grants, corporate development contracts, design competitions, and international consortia (where appropriate) to generate **sophisticated algorithms used for UA autonomous operations**

and apply intelligent control as it advances. The military must provide incentives so that pure research translates into practical military applications.

2) Use DARPA and other agencies to sponsor conferences and information sharing on UA **development that spans a variety of disciplines.** This cross-flow of information between disciplines has the potential to promote military advancements in many areas.
3) **Ensure joint requirements shape the research and development** phase to preclude interoperability issues and unwanted duplication. This joint mindset will require sub-optimizing some processes to achieve the greatest overall effect.
4) Continue to **invest in lasercom** for both atmospheric and space applications. Lasercom will enable the transfer of large amounts of data at high speeds with little chance of interception.
5) **Develop Mobile Ad-hoc Networks** (MANETs) as a theater backup to communications satellites and use a variety of airborne platforms **including UA as nodes**. MANETs will accelerate the kill chain by *distributing* actionable intelligence to in-theater warfighters.
6) Develop a communications architecture using a **combination of lasercom, RF, and SATCOM links** to enable MANETs. These links should securely pass classified and unclassified information **via Internet Protocols** to maximize interagency interoperability.
7) Develop **robust security measures for MANETs** during the research and development phase with a clear understanding of the impact of a compromised network.
8) **Comply with current Internet Protocols** (IPv6 in 2008) and **provide military advisors to shape future standards** decided by organizations such as the Internet Engineering Task Force. This partnership with civilian working groups benefits the Air Force because it enhances security of civilian infrastructure that augments military communications.

9) Allow **commercial influences to drive advances in computer processors**. Faster processing speeds will accelerate the analysis and information flow to decision-makers.

Other significant non-technical factors will play a significant, but indirect role in helping/hindering UA development and accelerating/slowing the decision cycle:

1) **Resolve UA airspace integration and certification issues** to allow operational and experimental access to airspace. New flight control algorithms should not require detailed FAA coordination for each upgrade as long as reasonable safety measures are enforced.
2) **Determine UA command and control relationships between the Services.** The goal should be to maximize the use of these limited resources in support of Combined Force Commander objectives. Delegating operational control of UA to ground commanders usually prevents using this high-demand asset from being used in the most efficient way.
3) **Establish better UA deconfliction procedures.** In the future, many more UA with varying sophistication levels will occupy the same space, complicating the deconfliction problem.
4) Ensure that **appropriate background checks** are conducted on personnel conducting sensitive research since they will be likely targets of espionage from foreign competitors.
5) **Develop comprehensive joint tactics, techniques, and procedures for UA.** This ongoing process must evolve quickly since technology will advance rapidly in UA.
6) **Centralize execution due to technological advances only where it offers a clear advantage**. For example, use decentralized execution on CAS missions and centralized execution on time-sensitive strike missions. Relying solely on centralized execution can form bad habit patterns resulting in decision paralysis or mass confusion if the enemy attacks the CAOC or during major combat operations.

Appendix A

Non-Military Applications of Unmanned Aircraft

> *"Domestically, there is an overlap of missions, roles, and responsibilities between DoD and DHS in their respective homeland defense and homeland security functions—one being military operations and one being law enforcement. UAVs will support both homeland defense and security."*[59]
>
> *– Michael J. Pitts (Director, UAS Program Office DHS, Customs and Border Protection, Air and Marine)*

Technological advances in UA have many non-military applications that can also bolster US security and improve the US standard of living. Persistent surveillance by UA will help the United States achieve one of its top four priorities—defending the homeland in depth.[60] They can help detect suspicious activities at border crossings, ports of entry, and major sporting events. Other possible uses include: 1) pinpointing forest fires, 2) providing wide-area, real-time traffic reporting, 3) monitoring oil pipelines, and 4) providing communication links and surveillance after natural disasters such as Hurricane Katrina.

Law enforcement could benefit from a 9-1-1 call that cues an aerostat or UA to focus high-resolution cameras on the caller's location. These eyes in the sky can help emergency responders find the residence and police find fleeing suspects. Military applications of future UA technologies can greatly benefit non-military organizations through spin-off technologies.

Appendix B

Brief History of Unmanned Aircraft

> *Sometimes you guys write that fighter pilots don't like UAVs, I love UAVs! I like them for any number of reasons. I like them because of the persistence; I like them because you can stay over a target for hours.*[61]
>
> *— Gen T. Michael Moseley, Gulf War II JFACC*

Unmanned platforms have been used for over 144 years but recent advances have resulted in their widespread use. Although it fails to meet the current definition of a UA, a balloon was used as an unmanned aerial bomber in February of 1863 during the Civil War. Perhaps one of the earliest UA to meet the definition of joint doctrine was a radio-controlled Navy Curtiss N-9 trainer that flew in 1917.[62] While these platforms had limited utility for combat operations, today the reliance on UA has caused many commanders to view it as a necessity for enhancing situational awareness.

In a short period of time, UA have evolved from simple reconnaissance vehicles to effective weapons delivery platforms. Central Intelligence Agency (CIA) agents first employed Hellfire missiles from the Predator in a coordinated attack with F-18s in November of 2001 when they killed Mohammed Atef, Al Qaeda's number three leader in Afghanistan (linked to anti-US operations in Somalia and embassy bombings in Kenya and Tanzania).[63] This successful strike against Al Qaeda's leadership was repeated one year later, when another Predator killed Ali Qaed Sinan al-Harithi and five other terrorists in Yemen linked to the U.S.S. Cole bombing.[64] Soon afterwards the Air Force introduced the Predator B, a lethal machine also known as the "Reaper" that made terrorists painfully aware of the offensive capabilities of UA.

UA are increasing in lethality and will be tasked for more dangerous missions. The Predator A used a laser designator to enable other fighters to drop Laser-Guided Bombs (LGBs)

during Operation Allied Force in Kosovo, but now the Predator B can carry a 3,000 pound payload that will include Small Diameter Bombs (SDB) and Joint Direct Attack Munitions (JDAM), making it perfect for the "Hunter-Killer" mission (combination of ISR and strike duties).[65] While the SDB is not operational yet for UA, Boeing lists this 250-pound weapon's range as "more than 60 nautical miles," providing a significant standoff capability.[66]

In the future, it is likely that UA will take over the DEAD role, especially against a peer competitor that has advanced Surface-to-Air Missiles (SAM). A hypersonic, stealthy UA combined with a volley of cruise missiles may be the best way to neutralize advanced SAM threats so that F-22s and F-35s can conduct follow-on operations. The United States has already invested in stealth technology that can be used for future UA thanks to production of the B-2, F-22, and stealthy UA prototypes like the X-45 and X-47.[67]

Appendix C

Online Survey on Projections about Future Unmanned Aircraft Technologies

ACSC Research Project #06-1188 (ACSC Survey Control Number 07-001)

- Thank you for taking a few minutes to answer the following 16 questions. As a recognized leader in the field, your responses are important to this research.
- This research will help us address the question: "Which technologies supporting Unmanned Aircraft Systems (UAS) will have the greatest positive impact in 2025?"
- Your answers will be treated as anonymous unless you desire otherwise. If you authorize your answers to be attributed to you, please electronically sign the block after the last question.
- For further questions or if you would like a final copy of this research report, please contact Major Julian Cheater (Cell phone (xxx) xxx-xxxx or email Julian.Cheater@maxwell.af.mil).

1. Please indicate the top three enabling technologies that you believe will have the greatest impact on future Unmanned Aircraft in the year 2025
    a. Artificial Intelligence
    b. Computer processing
    c. Fuel cells
    d. Information Technology
    e. Laser communications
    f. Materials science
    g. Nanotechnology
    h. Propulsion advances
    i. Solar cells
    j. Stealth technology

   Optional Comments:

2. Which phrase best describes the level of autonomy unmanned aircraft are projected to have by 2025
    a. Completely autonomous
    b. Autonomous except for weapons release
    c. Autonomous but constantly monitored by personnel
    d. Autonomous except for takeoffs and landings
    e. Limited autonomy

   Optional Comments:

3. What type of communications architecture do you believe unmanned aircraft will use in 2025?
    a. A common operating system shared between different aerial platforms
    b. A system enabled primarily by satellite relay
    c. A constellation of unmanned aircraft systems serving as a wireless network
    d. A system reliant on laser communications

e. Other (Please specify)

Optional Comments:

4. Please comment on any communications architecture bandwidth limitations you think might affect unmanned aircraft systems:

5. How do you think unmanned aircraft systems will communicate between ground stations, airborne assets, and ground commanders?

6. By 2025, unmanned aircraft should be able to monitor or neutralize the following threats (click all that apply):
   a. Enemy integrated air defenses
   b. Enemy aircraft
   c. Fixed targets (like buildings)
   d. Mobile targets (like vehicles)
   e. Individual combatants/terrorists
   f. Illegal border crossings
   g. Illegal maritime shipping

Optional Comments:

7. In your opinion, what is the best reason for investing in unmanned aircraft instead of piloted aircraft?
   a. Longer loiter times
   b. Reduced the risk to human operators
   c. They perform routine operations more effectively
   d. They are less expensive
   e. None of the above; piloted aircraft should be used instead

Optional Comments:

8. Do you believe unmanned aircraft will be used to find, track, and target individuals anywhere in the world by 2025?
   a. Yes, using mostly on-board sensors
   b. Yes, using a combination of on-board sensors, space assets, and human intelligence
   c. Yes, but we will primarily use space assets
   d. Yes, but we will primarily use manned assets
   e. No, technical limitations will prevent this
   f. No, political limitations will prevent this

Optional Comments:

9. By 2025, which role do you think will be best suited for unmanned aircraft?
   a. Homeland Defense
   b. Wartime operations
   c. Civilian / Corporate use
   d. Scientific research
   e. Other (please specify)

Optional Comments:

10. Which unmanned aircraft mission do you believe government users will demand most in 2025?
    a. Intelligence, Surveillance, and Reconnaissance (ISR)
    b. Communications
    c. Weapons delivery
    d. Weather reporting
    e. Other (please specify)

Optional Comments:

11. Which unmanned aircraft mission will civilian users demand the most in 2025?
    a. Intelligence, Surveillance, and Reconnaissance (ISR)
    b. Communications
    c. Weapons delivery
    d. Weather reporting
    e. Other (please specify)

Optional Comments:

12. What is the best way for the US government to develop future technologies?
    a. University research grants
    b. Corporate development contracts
    c. Design competitions
    d. Acquisition law reform
    e. International consortia

Optional Comments:

13. Please comment on the role you envision between artificial intelligence and unmanned aircraft systems around 2025:

14. In 2025, what type of aerial platform do you think will be the most useful in detecting and tracking enemy threats?

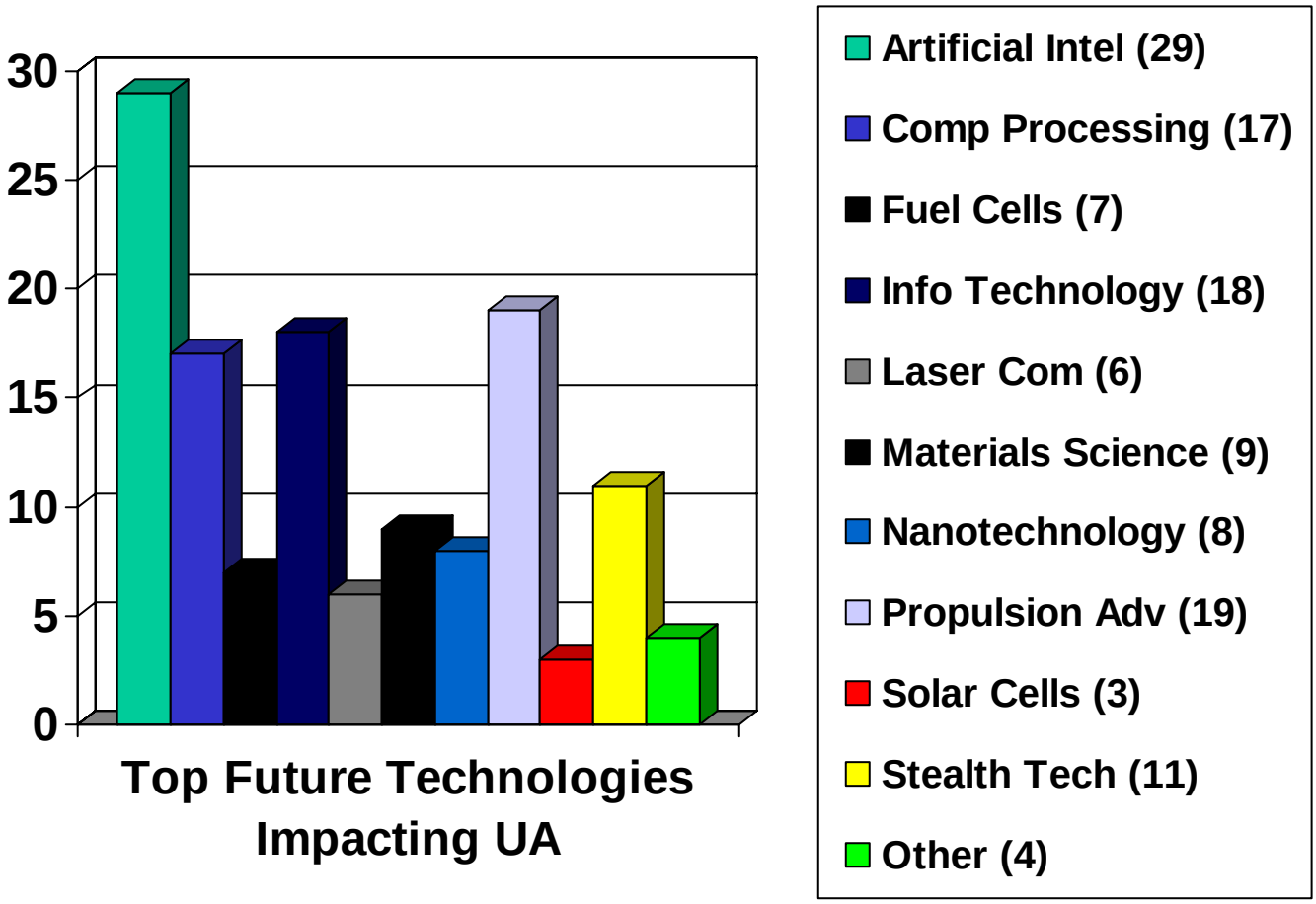
15. Please comment on the government policies you think will be needed to maximize the role of unmanned aircraft at home and abroad by 2025:

16. What do you think about the need in 2025 for airborne systems to augment missions typically performed by space assets today?

1. Please select the level of anonymity you would like your participation treated:
    a. Anonymous: I do not want my name associated with my responses
    b. By name: I authorize ACSC researchers to associate my name with my answers in the final report, as appropriate
2. Please enter your name as you would like it to appear for attribution (without this block filled in, we cannot match your responses to you):
3. If you would like an electronic copy of the final report, please enter your email address here:

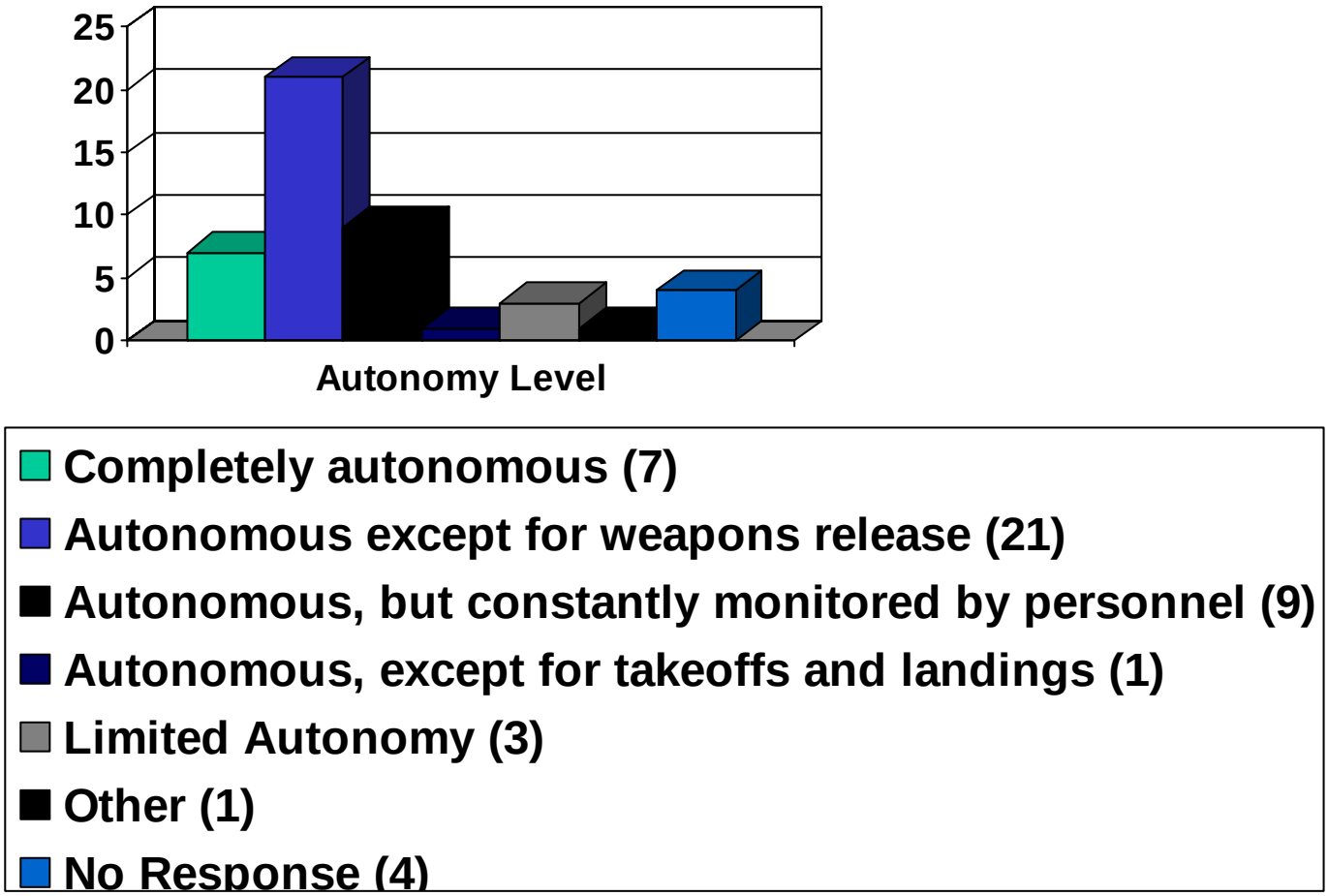
Appendix D

Selected Survey Results: Top Three Enabling Technologies Impacting Future UA in 2025



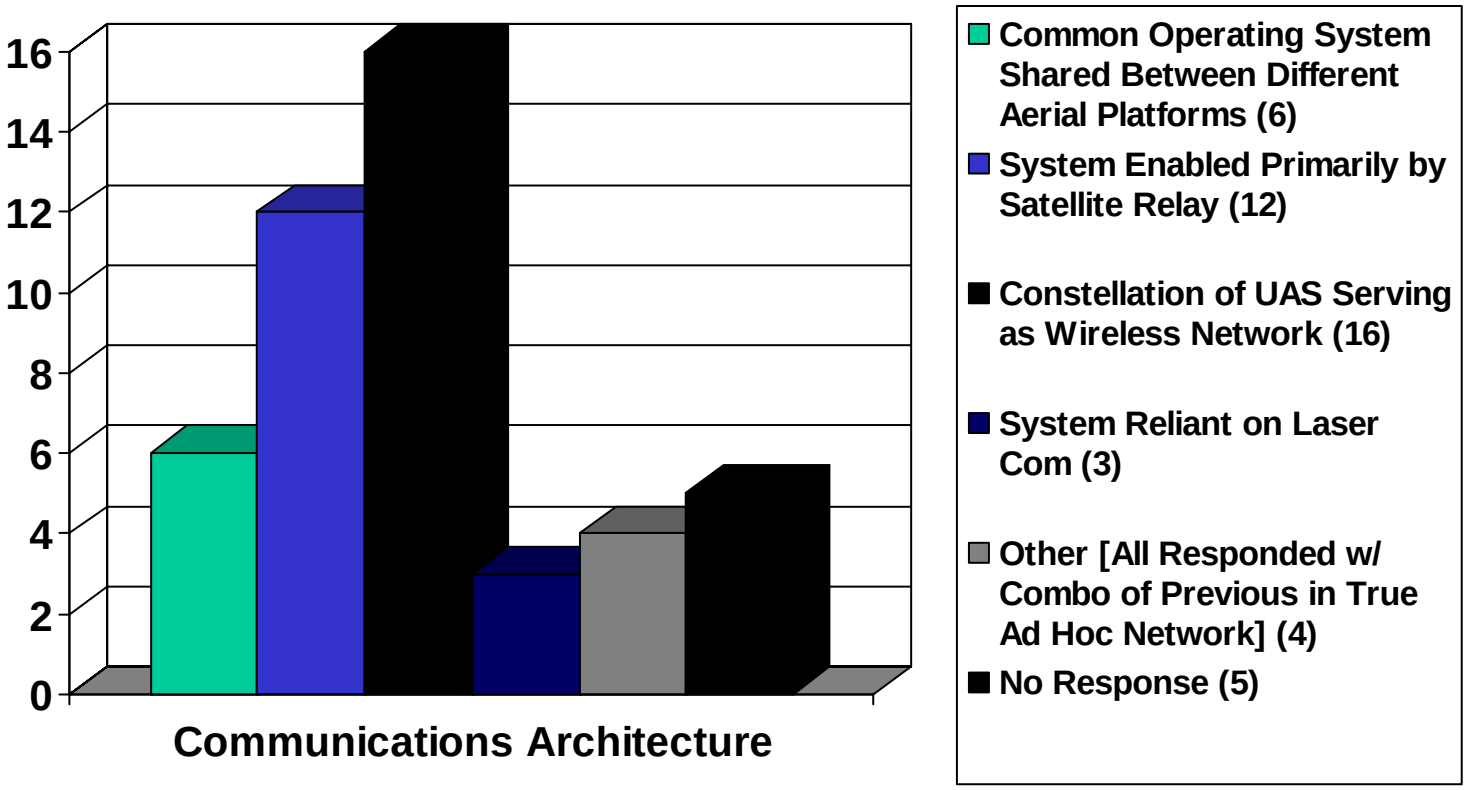
Appendix D (Cont.)

Which phrase "best" describes the level of autonomy of UA in 2025?



Appendix D (Cont.)

Type of Communications Architecture UA will use in 2025



Appendix E

Releasable Survey Quotes[68]

Due to space limitations, only a sample of survey quotations is provided. Almost every survey response noted the need to resolve airspace integration and certification issues. Otherwise, viewpoints on the future of UA varied which should generate discussion. The following quotes are roughly organized by affiliation with government, industry, and academia without preference for any category. A sample of anonymous responses follows and provides some candid insights. The researcher is indebted to the all survey respondents for taking time out of their busy schedules to answer a survey from someone they knew very little about.

Mr. Dyke D. Weatherington (Deputy, UAS Planning Task Force, Office of the Under Secretary of Defense):

How do you think unmanned aircraft systems will communicate between ground stations, airborne assets and ground commanders?

"Much as cell phone networks today provide a range of communication options, future UAS will interface with other systems to maintain necessary SA"

Do you believe unmanned aircraft will be used to find, track, and target individuals anywhere in the world by 2025?

"Anywhere is a very large place, but for many of the most likely operating environments, UAS in combination with other collection systems (Space, fixed ground sensors, Unmanned Ground systems) will provide the majority of the F2T2EA cycle"

Mr. Michael J. Pitts (Director, UAS Program Office DHS, Customs and Border Protection, Air and Marine):

"Regarding the employment of UAVs domestically, unmanned aircraft must operate safely in the national airspace system. UASs must incorporate a sense and avoid system either internal or external to the aircraft where the FAA can ensure separation and segregation between crewed and remotely piloted aircraft. Hence, situational awareness and aircraft deconfliction is paramount where unmanned aircraft operate in the NAS with military, government, commercial, and private aircraft."

"Along with the federal government, state and local governments will employ UAVs for law enforcement, emergency medical services, search and rescue, and fire fighting."

"Domestically, there is an overlap of missions, roles, and responsibilities between DoD and DHS in their respective homeland defense and homeland security functions—one being military operations and one being law enforcement. UAVs will support both homeland defense and security."

Rear Adm Thomas J. Cassidy Jr. USN (Ret) (President, Aircraft Systems Group, General

Atomics Aeronautical Systems, Inc):

Please comment on the government policies you think will be needed to maximize the role of unmanned aircraft at home and abroad by 2025:

"Executive direction to the FAA to treat UAVs that are controlled like and act like manned aircraft in the same manner as they treat manned aircraft."

What type of communications architecture do you believe unmanned aircraft will use in 2025?

"A system enabled primarily by satellite relay"

Col Michael S. Francis, PhD, USAF, (Ret) (Chief Operating Officer, Photonics Division, General Atomics; Previous J-UCAS Director):

Please comment on the government policies you think will be needed to maximize the role of unmanned aircraft at home and abroad by 2025:

"Not a policy issue, per se—need to reduce cultural and institutional obstacles that have arisen over the years. The technologies will remove many of the technical and operational limitations. Tightened defense budgets will also force the services to more affordable solutions, including UAS."

"Ready access to the airspace is major inhibitor to commercial applications ... largely an institutional and cultural problem"

Do you believe unmanned aircraft will be used to find, track, and target individuals anywhere in the world by 2025?

"Answers depend on countermeasures developed and the airborne threat environment. ISEAD is most difficult mission ... Cancellation of J-UCAS limits time to mature this most technologically complex capability."

Col Tom Ehrhard, PhD, USAF (Ret) (Senior Fellow at the Center for Strategic and Budgetary Assessments):

Please comment on the role you envision between artificial intelligence and unmanned aircraft systems around 2025:

"We will not see artificial intelligence, per se, but we will see such dramatic increases in capability that machines will appear intelligent and will be able to perform at a much higher level then pilots…"

What do you think about the need in 2025 for airborne systems to augment missions typically performed by space assets today?

"There will be a great need for it due to the vulnerability of space assets to solar phenomena and adversary interdiction"

Lt Col Ed "Mel" Tomme, PhD, USAF (Ret) (Sci-Ops Consulting):

Please comment on the government policies you think will be needed to maximize the role of unmanned aircraft at home and abroad by 2025:

"First and foremost is a rational way to integrate them into the national airspace structure. Current limitations on UAV flights in the US are seriously stifling development of hardware and conops."

"Without laser communications, network centricity is about to hit a hard stop. We're already squeezing about as much information into the RF spectrum as we can."

"The tactical layer, air breathing UAVs, need to have speed and resolution (and weapons in some cases) to respond to cues received from space and near-space. This layered approach

makes the air-breathers much more effective since they don't spend time searching through a soda straw, only responding to potential threats already tagged by the wider area searches performed by space and near-space assets."

Mr. Arun Ayyagari (Technical Fellow, The Boeing Company):
"Government needs to take more active role in dynamic spectrum management and in developing and providing dynamic spectrum management tools."
"AI would be used in the area of decision support and in establishing inferences from the large amounts of information gathered."
"Due to the need for multi-disciplinary technologies and research experience coupled with high level of systems engineering competence it would be ideal for corporations to perform the role of large scale integrator (LSI) whereby they can leverage efforts from other entities such as Universities in specific sub-areas."

Mr. Steven Rasmussen (Senior Aerospace Engineer, General Dynamics Advanced Information Systems):
"*There is a need to simplify the procedures for obtaining FAA approval for flight testing these technologies. Rules must be established to protect the public while giving researchers/developers enough latitude to try out designs without having to spend time and money traveling to areas with restricted air space."*
"For missions that do not require lethal force, the UAVs could be completely autonomous."

Mr. Bruce Carmichael (Vice President, Programs—West, L-3 Communications):
"Move out on the operation of UAVs in the national airspace system. This issue has been around for a long-time and not enough progress has been made."
"Network-centric operations that make members of networks 'pass-through' facilitators of data destined for other users. We will, less and less, think in terms of point-to-point stove-piped comms and relate comms capacity more in terms of total network throughput rather than individual platform needs."

Mr. Jeremiah Madigan (VP, High-Altitude, Long-Endurance Systems, Northrop Grumman):
"There will always be bandwidth limitations, the real challenge is deciding what is important to communicate versus ship everything and figure out later."

Mr. Christopher A. Miller (Smart Information Flow Technologies):
Please comment on the role you envision between artificial intelligence and unmanned aircraft systems around 2025:
"AI (and especially through its links to control, human interaction, sensor processing, planning, etc.) is the way to achieve higher levels of autonomy. Since I see increasing level of autonomy as the largest challenge for UAVs, AI (and human factors) development issues are the primary drivers to achieve this."
By 2025, unmanned aircraft should be able to monitor or neutralize the following threats (click all that apply): Enemy IADs, Enemy aircraft, Fixed targets (like buildings), Mobile targets (like vehicles), Individual combatants/terrorists, Illegal border crossings, Illegal maritime shipping
"UAVs (e.g., Predator, Global Hawk) are already able to monitor most of these and neutralize some, in some circumstances. The issue is level of autonomy. Of the threats listed, I'd say those

that can shoot back and/or dynamically evade are harder (especially to deal with more autonomy)—terrorists/combatants, mobile targets, enemy AC."
Do you believe unmanned aircraft will be used to find, track and target individuals anywhere in the world by 2025?
"Again, this is already being done with (at least) Predator-- though not 'anywhere in the world', much less 'any time, anybody'. Again, the biggest challenge to extending this ability is level of autonomy and, perhaps, ability to fly in general airspace."

Mr. Gary D. Nault (VP, Advanced Programs and Business Development, Communications and Electronics Unit, Cubic Defense Applications):
What do you think about the need in 2025 for airborne systems to augment missions typically performed by space assets today?
"UAVs are cheaper than Space Based Systems"
How do you think unmanned aircraft systems will communicate between ground stations, airborne assets and ground commanders?
"Broad Band Ad hoc mesh"

Mr. Todd Bruner (VP, Advanced Information Systems Recon & Surveillance Solutions, General Dynamics):
Please comment on any communications architecture bandwidth limitations you think might affect unmanned aircraft systems:
"If one increases the intelligence in the vehicle, then the communications between the vehicles can be minimized. Increased intelligence means high entropy messages can be sent which means a lower data rate. However if one wants to have a "man-in-the-loop" with an RF or laser tether, then one will need gobs of data…"
Do you believe unmanned aircraft will be used to find, track and target individuals anywhere in the world by 2025?
"This depends on where one thinks the onboard processing capability will be. If a vehicle can have a data-link then of course updated info via any asset including a person is possible. Some of these choices are not mutually exclusive…"

Dr. Ali Minai (Associate Professor, Department of Electrical and Computer Engineering and Computer Science, University of Cincinnati):
Please comment on the role you envision between artificial intelligence and unmanned aircraft systems around 2025:
"I think that by 2025 unmanned aircraft will often comprise modular vehicles capable of assembly 'on the fly.' These will need intelligence for deployment, self-assembly and optimal autonomous reconfiguration."
Please comment on any communications architecture bandwidth limitations you think might affect unmanned aircraft systems:
"With greater autonomy and intelligence, communication will actually become a lesser problem, and will be needed mainly for coordination within teams of vehicles. That communication will likely use a distributed architecture to resolve bandwidth issues."

Dr. Jack W. Langelaan (Assistant Professor, Aerospace Engineering Department at The Pennsylvania State University):

"No single platform will be ideal. A mix of vehicles at high, medium and low altitude will be required."
"Bandwidth limitations are one of the drivers of autonomy requirements: a vehicle must have enough autonomy to cope with 'gaps' in communication caused by bandwidth limits or communications delays."

Dr. Eric W. Frew (Assistant Professor Aerospace Engineering Sciences Department, University of Colorado at Boulder):
"The US government must facilitate civil and commercial USE of unmanned systems. The main impediment to unmanned operations in the National Airspace System is regulations. The FAA must standardize its regulations across the entire spectrum of unmanned systems."
"I think unmanned aircraft should communicate using a meshed network of ground and airborne systems, however I expect them to still primarily use satellite relays in 2025."

Mr. Cory Dixon (PhD candidate/Research Assistant, Aerospace Engineering Department, University of Colorado at Boulder):
"While the FAA is developing methods and regulations for UA, there is little talk on how to properly regulate the development and testing of the smaller university sized vehicles while still allowing them to fly under a COA."
How do you think unmanned aircraft systems will communicate between ground stations, airborne assets, and ground commanders?
"Through mobile ad hoc networks (MANETs) with multiple RF interfaces such as TCDL, CDMA, 802.xx, and satellite"

Dr. John Baker (Assistant Professor, Mechanical Engineering, University of Alabama):
"I believe near space systems will be the most useful in detecting and tracking enemy threats because such systems would typically be out of the range of enemy fire. They will be more responsive and have superior imaging capabilities relative to satellites. Future near space systems will also have superior loitering capabilities compared to UAVs."
"I believe artificial intelligence will be critical for the long term development of unmanned aircraft systems. I see AI systems serving for guidance, navigation, and control. I also see AI being important for target recognition."

Mr. Brent Marley (Air War College Professor):
"Unmanned high altitude airships could have long loiter times (months) for general surveillance. They could then cue lower altitude assets for a closer look or attack."
"In 2025 hyperspectral imagery will be a bandwidth hog and will require higher capacity communications links such as laser links."

Anonymous survey quotes:
By 2025, unmanned aircraft should be able to monitor or neutralize the following threats (click all that apply): Enemy IADs, Enemy aircraft, Fixed targets (like buildings), Mobile targets (like vehicles), Individual combatants/terrorists, Illegal border crossings, Illegal maritime shipping
"UAVs will only be limited by the weak constituencies they have in military bureaucracies—there will be no serious engineering limitations that will prevent them from doing all these missions."

What do you think about the need in 2025 for airborne systems to augment missions typically performed by space assets today?

"UAVs will offer a highly responsive and flexible capability that will augment space assets."

"It is possible that space assets will be effectively useless since most could be considered sitting ducks."

"Unless they would act as relay stations at very high altitudes I don't see a need."

In 2025, what type of aerial platform do you think will be the most useful in detecting and tracking enemy threats?

"I think that most of this will be done from space except for urban areas where low altitude or hopping UAVs may work best or where weather limits E/O observation and radar observation is needed."

Airspace issues:

"Allow the certification standard for UAVs to be comparable in risk experienced in manned systems. Holding UAVs to higher standards (near flawless) than human performance will limit the introduction of UAV missions."

"The FAA needs to develop consistent and reasonable guidelines for UASs in the national airspace. Air traffic control needs to be decentralized and automated. There needs to be different rules for different sizes of vehicles."

"Artificial intelligence poses a certification challenge because you cannot verify the safety of an evolving operating system."

Please comment on the role you envision between artificial intelligence and unmanned aircraft systems around 2025:

"I do not believe that artificial intelligence will be readily available in 2025. However, if this is to mean a series of preprogrammed choices based on external or internal information - time, location, detection, etc. - than this will a normal element of the control of UAVs."

Research sources:

"Universities are much more effective at developing new technology. However, there needs to be a heavy emphasis on transitioning technology out the University."

How do you think unmanned aircraft systems will communicate between ground stations, airborne assets and ground commanders?

"For micro air vehicles, there is a need for short range digital communication links. Satellite relays are not practical for this size of vehicle."

"A common operating system shared between different aerial platforms"

"I believe that UAS operation will be collaborative between many unmanned air, surface, and sub-surface platforms, with the primary human input being high order commands."

Bandwidth limitations:

"Bandwidth (and frequency deconfliction) will be a major issue for high numbers of UASs. Laser comms will help, but it is not the answer for all-weather ops, especially at low and intermediate altitudes."

"Spectrum management will need to be given careful consideration, but there are technologies under development which will help."

Appendix F

Space versus Air-breathing Assets

UA should augment rather than replace space assets. Weaknesses of platforms in either space or the earth's atmosphere can be minimized by using assets in the other operating environment. Perhaps a layered approach forms the best framework for describing how "air-breathers" and space assets can complement each other. The "high ground" of space offers strategic coverage of many areas and it enables numerous communications links. The realm of near space offers sanctuary from many ground threats while allowing the US military to persistently monitor enemy activity. UA in lower altitudes allow responsive tracking of individual targets and the ability to quickly employ weapons. In 2025, Micro Air Vehicles (MAV) will provide indoor or high-resolution surveillance as well as detection of nuclear, biological, and chemical weapons particles near ground level.

Satellites offer many advantages over UA including sophisticated sensors, large bandwidth capability, wide coverage, and freedom of over flight. Since satellites cover a much larger area, fewer are needed for surveillance, and consequently, their sensors are generally more robust than UA. In the space environment, the atmosphere does not interfere with laser communications (lasercom) and this increases bandwidth available. Freedom of over-flight offers many political and military advantages as long as a sophisticated country does not attempt to dazzle US satellites with lasers or shoot them down.

Despite these advantages, satellites also have several disadvantages that UA can minimize. Satellites are limited in number but the demand on them is great, making availability an issue. Next, many countries know when US satellites will pass overhead and this predictability can allow foreign militaries or insurgents time to conceal or temporarily cease

suspicious activities. Solar weather can temporarily prohibit or limit satellite operations while cloud layers can also impact the ability to see in the electro-optical spectrum. Low Earth Orbit (LEO) satellites are vulnerable to laser interference, jamming, and even potential interdiction as demonstrated by a successful Chinese ballistic missile launch against an aging weather satellite 530 miles above the earth on 11 January 2007.[69] The fragments from this event and others like it could threaten US satellites unless it continues to closely track all space debris. Finally, satellites currently cannot be launched on short-notice, are costly, and cannot be easily upgraded in space.

UA offer many advantages over satellites such as higher resolution images, lower cost, offensive capabilities, highly maneuverable systems, and responsiveness to theater needs. However, these platforms tend to fly slowly, monitor smaller areas, lack survivability (depending theater threats), and lack communications and autonomy advances. Here satellites can augment these air-breathers by cueing UA to specific areas of suspicious activity. High-altitude UA can also accomplish this function by cueing medium-altitude UA to track individuals or vehicles. As sensor advances are made, UA can be quickly upgraded to provide greater resolution or hyperspectral analysis whereas satellites cannot be easily upgraded. Despite expanding capabilities, UA will continue to suffer from bandwidth limitations due to increasing demand at least until TSAT is launched in 2016.

In a period of shrinking budgets, many may view the relationship between space and air-breathing assets as competitive. While competition is healthy to a degree, the United States must realize that satellites and UA complement each other and help minimize the weaknesses of platforms in each operating environment. One must take a holistic look at proposed future programs to see the best combination of UAS and satellites that avoids duplication where it is desirable.

Appendix G

Common Terms and Concepts Related to Autonomy

What is the relationship between artificial intelligence (AI), autonomy, and capability? Confusion over these terms often leads one to think of them interchangeably but they have important differences. John McCarthy, professor emeritus of computer science at Stanford University, was credited with coining the phrase "artificial intelligence" in a paper he authored in 1955.[70] Marvin Minsky, another leading cognitive scientist and colleague of McCarthy's, defined AI as "the science of making machines do things that would require intelligence if done by men."[71] Of course the term "intelligence" is debatable as well, but the researcher modified a definition of intelligence offered by Gunderson as *the ability to determine the best course of action to achieve a goal in a dynamic and uncertain environment*.[72] This implies that machines with AI must learn or reason like humans. Second, capability *is the ability to successfully pursue a course of action in a dynamic or uncertain environment*. However, capability does not guarantee the selected course of action will be the best choice or that machine (UA) will achieve the desired goal. Finally, an autonomous system may be defined as, "one that makes and executes a decision to achieve a goal without full, direct human control."[73] While this definition implies that autonomous machines process multiple inputs to make a decision, it does not necessarily mean that the machine makes a good decision since it is independent of intelligence.

The definitions of these terms are important because engineers and programmers must decide how intelligence, capability, and autonomy will interact when designing future UA. Increasingly autonomous UA will not necessarily reduce the time it takes to find and neutralize a target unless they have sufficient intelligence and capability levels to do so. Autonomous operations will reduce the workload of pilots and sensor operators located at ground stations or

with laptop computers halfway around the world. However, the "brain" of the UA must be advanced enough to allow it to efficiently find and track potential targets. The high demand on ISR assets means that the US military should build UA that can determine the best courses of action to achieve the initial goal of finding an enemy combatant. Next, complicated decisions must be made about which platform and weapon should be used if a strike is warranted. Software programs and algorithms aboard UA must consider many factors such as distance to the target, collateral damage considerations, weather affecting weapons employment, low fuel state, higher priority taskings, and the availability of nearby friendly forces to apprehend the enemy.

If the US military's goal by 2025 is to reduce the number of UA system operators or decrease use of satellite bandwidth, then it should continue to develop UAS autonomy. If the priority is to reduce the kill chain to seconds from first seeing a suspect to positively identifying that person as a lawful enemy combatant, the US military must invest in developing the "intelligence" and the capability to share information between different sensors and platforms. Ideally, a combination of highly autonomous, intelligent, and capable systems will be developed through focused efforts that span many disciplines including computer science, engineering, psychology, and applied mathematics.

Appendix H

Intelligent Control

"AI would be used in the area of decision support and in establishing inferences from the large amounts of information gathered."[74]

— Mr. Arun Ayyagari, Technical Fellow, The Boeing Company

Engineers, programmers, and scientists have used many different methods of intelligent control for making UA act in a desired manner. While in-depth explanations of these control methods exceed the scope of this paper, common computing approaches have included neural networks, Bayesian control, fuzzy logic control, neuro-fuzzy control, expert systems, genetic control, and intelligent agents.[75] Although there are different types of neural networks, they all solve complex problems in parallel, are error tolerant, and can "learn" by adapting.

A neural network could use sensor inputs to prompt an UA to change speed or direction to avoid hitting another UA. Bayesian control includes many schools of thought that use a mathematical equation or model for reasoning about uncertainty through probabilities. For example, a Bayesian filter might compare real-time activities of a suspect to characteristics from reference terrorist behavior in order to classify him or her as a terrorist. Fuzzy logic has subsets but it involves reasoning with values that are imprecise such as "slightly" or "very." This type of control might be used in facial recognition software where values for the image cannot be easily defined as a "1" or "0." Neuro-fuzzy control uses a hybrid of artificial neural networks and fuzzy logic to use human-style reasoning to prioritize interpretability or accuracy. An expert system is a computer program that consists of rules that analyze information and could provide a course of action. For example, your "wizard" interactive program on your computer may help you accomplish tasks without simply asking only "yes" or "no" questions. There are multiple types of intelligent agents but they are essentially software packages that can reason or modify

the way in which they achieve their objectives. For example, an intelligent autonomous agent on a UA can decide which targets to track and then prompt a human controller for permission to release weapons.[76]

While sophisticated algorithms will increase the capabilities of future UA, sometimes simpler yet more robust algorithms may help find the enemy sooner. Minai et al. related, "The implication is that a simple assignment process that pays little attention to expertise can, at a little extra cost, achieve better results than a highly optimized process that tries to match tasks and agents at great computational cost."[77] In other words, it may be better for UA to make repeated attempts to find a target than declaring an early success with more sophisticated search patterns. As UA increase in autonomy and intelligence, they will evolve from being data-driven to eventually achieving knowledge-driven status.

Appendix I

Expanded Explanation of Autonomous Routing

Combinations of algorithms need to be developed to determine optimum UA flight paths. These algorithms will change the flight path of the UA depending upon target speed and anticipated threat level. Husby's analysis of several automated UA flight paths can be visualized as no-wind ground tracks that included a square, circular, and standoff model. Each flight path or ground track had advantages and disadvantages.[78] While a "square" pattern (ground track resembled the profile of teeth with spaces in between) allowed a UA to track a fast moving target, it prevented the UA from monitoring a stationary track. The "circular" pattern needed fewer updates but had trouble tracking fast moving targets and, surprisingly, required a complicated algorithm to implement. The "standoff" pattern (ground track resembled a bowtie or figure eight) had a much more complicated algorithm that also had trouble keeping up with fast moving targets. However, this pattern had several tactical advantages: 1) it allowed the UA to loiter on one side of the target and use the sun to prevent the enemy from visually acquiring it and 2) it minimized any unwanted effects of sun angle on image processing. The complexity of flight path algorithms will continue to increase as the USAF coordinates actions of multiple UA. However, these additional UA will also provide greater capabilities.

Appendix J

Autonomous Navigation

In an electronic jamming or low-altitude urban environment, UA may not be able to rely on GPS navigation. Therefore, more sophisticated UA should have navigation systems that integrate GPS signals from satellites and an on-board mapping system that compares UA position to known terrain features. The second type of navigation, known as terrain contour matching (TERCOM), has been successfully used in cruise missile technology.[79] While GPS navigation is more accurate, TERCOM may be required in high-threat scenarios.

Recent advances using data sharing and lasers show promise for future navigation systems that do not rely on GPS. In a 2004 experiment, researchers from the University of Sydney demonstrated how two UA could fly in different regions and build a common map through decentralized data fusion communication.[80] This preliminary work on sharing terrain information between UA can serve as a stepping stone for future capabilities. In a separate experiment, Ohio University researchers demonstrated how a UA with two lasers could dead-reckon over unknown territory by keeping track of its position over time. Instead of matching observed terrain features with on-board databases, this method used precision timing, a forward-looking laser to map features, and a rear-pointing laser to navigate.[81] Although the position drift error of approximately 60 meters per hour was unacceptable, future improvements could allow a scout UA to map and navigate over unfamiliar terrain and pass this information to other UA.

High-resolution maps collected from satellites may not always be available if US satellites are disabled and, therefore, the USAF may have to use terrain navigation. Incorporating a combination of navigation systems will be appropriate for UA tasked for high threat missions such as SEAD or DEAD where GPS will likely be unavailable.

Appendix K

Expanded Explanation Teaming Versus Swarming

> *"With greater autonomy and intelligence, communication will actually become a lesser problem, and will be needed mainly for coordination within teams of vehicles."*[82]
>
> *– Dr. Ali Minai, Associate Professor, Department of Electrical and Computer Engineering and Computer Science, University of Cincinnati*

Mission type and expendability will likely determine whether UA will swarm or team. Swarms of miniature UA may be suitable in an area where the US military must conduct surveillance in an urban or indoor environment. Here swarms of Micro Air Vehicles (MAV) may fly short duration missions to identify combatants or the presence of chemical weapons with little concern for losing several platforms. *Swarms* of UA should not be armed since collateral damage or civilian deaths will have unwanted, strategic consequences. Instead, by the year 2025, the USAF should use *teams* of UA to accomplish strike missions or complex ISR missions at altitudes that protect them from MANPADs and AAA. Teams of UA will be more expensive due to their sophistication, but their utility over swarming UA for complex missions will justify the cost in the majority of cases.

Swarming also indicates that UA will operate in close proximity to one another, requiring precise deconfliction methods. While GPS/INS-aided tools may be the easiest method to maintain desired separation between UA, integrated light detection and ranging (LiDAR) could be of use in a jamming environment. This method can be thought of as "radar based on light energy instead of RF [radio frequency] energy" where laser beams determine the range to each pixel in its field-of-view.[83] While this method is accurate, the range is currently limited to the tens of meters.

On future hunter-killer missions, many UA from different classes will cooperate to determine real-time taskings. Professors from the University of Cincinnati proposed a hybrid algorithm that prioritized quick response for known target locations and an efficient search pattern for targets of opportunity.[84] Their algorithm assigned a nearby UA a specific target while alerting other UA in the area to be available for target tracking if required. Distant UA would continue their search patterns for potential targets but still share data about changing priorities. This algorithm also prevented a UA from searching an area already evaluated by another UA unless there was a valid reason to do so. Although still in the infant stages of autonomy, this example of team-cooperation serves as a building block for more complex algorithms that will allow UA to share information and assign tasks based on many dynamic factors.

Several swarming algorithms were inspired by observing how bees, birds, and other insects interacted in nature to determine appropriate formations. These algorithms may be less complicated than teaming algorithms, but they must allow the group to achieve the assigned task even with the loss of several UA. Leung et al. noted that the ability for a swarm of UA to communicate was more important than detailed algorithms and resulted in self-organizing behavior.[85] Slear noted that due to the fact that these UA were expendable, they would likely be non-stealthy and would have to rely on low-altitude flight for threat protection.[86]

Swarming algorithms will likely be incorporated in future MAVs, especially since their tiny propulsion systems and power supplies will limit their range and communications transmissions. While the development of micro UA is still in its infancy, McCarthy related that he has developed a formation algorithm that can guide UA "relative to each other using a waypoint guided autopilot."[87]

Appendix L

Autonomous Aerial Refueling

On 15 August 2006 a UA in the form of pilot-less Learjet autonomously refueled from a KC-135R for 23 minutes after being manually flown to the pre-contact position (not publicly released until September).[88] Tests will continue in August of 2007 when the pilot-less Learjet will autonomously fly from the observation position beside the KC-135 to the pre-contact position behind and slightly below the tanker. The ability to autonomously refuel will increase the loiter time and utility of UA. Once this Automated Aerial Refueling (AAR) capability has been thoroughly tested, the limiting factor for UA will probably be an oil change or required maintenance instead of fuel exhaustion. This capability will increase flexibility for commanders and allow future unmanned bombers to conduct deep strikes with a small logistics footprint.

AAR capability could even be adopted on manned aircraft to reduce fatigue. On ocean crossings, it is not uncommon for fighter aircraft to refuel 11 times and it is highly likely that they will experience poor weather during such a long flight. Incorporating this AAR control computer and the associated station keeping control laws into a selectable mode for other aircraft would significantly reduce fatigue on these types of missions. Several weeks after the pilot-less Learjet autonomously refueled, an F-18B autonomously refueled using a "blended relative GPS/INS solution and an optical tracker" to judge closure with a pilot on-board as a safety observer.[89] Based on current advancements, it is possible that both the tanker and receiver will be UA by the year 2025.

Appendix M

Brief Communications Satellite Overview

One of the most useful innovations will be greater use of UAVs to provide backup to satellites, ensuring greater resilience of the communications network against the effects of antisatellite weapons and other disruptions. [90]

— Michael O' Hanlon, author of Technological Change and the Future of Warfare

Satellites have enabled secure communications for years but increasing demand on bandwidth and aging systems means the United States must periodically replace its fleet. While a constellation of future UA will be able to serve as a backup to satellite communications, this airborne constellation in the form of a MANET will not be able to provide as many capabilities. In order to understand MANET limitations, it is useful to examine several major communications satellites in use and preview those that are still on the drawing board.

The Defense Satellite Communications System (DSCS) and the Military Strategic and Tactical Relay (MILSTAR) system provide US satellite communications today even though half of these satellites have exceeded their design life. Consisting of nine satellites, DSCS is considered the "workhorse of military satellite communications."[91] MILSTAR consists of five satellites that provide secure, jam-resistant communications.[92] This aging and bandwidth-strained system was first launched in 1994 and it will be replaced by a three-satellite constellation of Advanced Extremely High Frequency (AEHF) satellites.[93] With a planned April 2008 launch, AEHF will also provide secure communications, but it will supply thousands of connections simultaneously at 10 times the total capacity and six times the channel data rate of MILSTAR II.[94]

To provide more immediate communications capabilities, a less-protected constellation of satellites known as the Wideband Global System (WGS) [previously known as the Wideband

Gapfiller System] will launch in June of 2007. Consisting of a projected total of five satellites using commercial technology, WGS offers significant bandwidth expansion and flexibility by allowing X-band and Ka-band links (Ka-band used by Predator) to communicate with each other.[95]

While these systems will improve communications, the Transformational Satellite Communications System (TSAT) has the potential to significantly improve US warfighting abilities. With a projected 2016 launch, TSAT will use Internet Protocols to provide secure communications to troops on the move with roughly 10 times the bandwidth capacity of AEHF satellites.[96] Considered a key GIG component, TSAT will use packet-routed communications instead of the circuit-switched services in use today. According to the AFRL, "Whereas conventional, circuit-switched systems manage communications links according to static precedence schemes, packet-routed communications use the Internet Protocol environment to manage information transfer according to dynamic, session-by-session priority and the time criticality of transferred information."[97] This system of satellites will interface with small, mobile antennas such as those used by UA and will depend upon advancements in mobile communications, dynamic bandwidth allocation, antenna technology, lasercom, and future processors and routers.[98]

Appendix N

Laser Communications

In the future, it is likely that laser communications will be used extensively in communication networks. Lasers, or optical links, enable large data transmissions at high rates with robust security. Optical communications use photons to carry information whereas RF communications use electrons. Laser communications (lasercom) are a subset of optical communications and use the atmosphere as the medium instead of a fiber optic cable. In the context of a MANET, it is possible that intelligent UA nodes will sense other nodes dropping off the network and alternate between RF links and lasercom to maintain network connectivity.

Technical challenges still limit the use of lasers transmitting data through the atmosphere over long distances. Moisture and dirt particles in the air scatter these beams of light making communication difficult. Lockheed Martin reported that it tested baseline lasercom at the Massachusetts Institute for Technology's (MIT) Lincoln Laboratory at rates of 10 to 40 gigabits per second (Gbps).[99] Such high transmission rates make it promising that future communications networks will incorporate miniaturized versions of this technology in both space and the atmosphere.

Lasercom should perform better in the near space environment than the atmosphere because fewer particles can scatter the beam. Despite this, some researchers have reported initial success with lasercom within the atmosphere using a variety of techniques. In a technical white paper, Tom Chaffee of Attochron LLC reported that they used lasercom to transmit up to 15 nautical miles away by firing two ultra fast lasers in sequence to ionize the air. The first laser "affects an ionized aerial waveguide unaffected by the diffraction of the atmosphere" while the second laser "maintains the stability of the ionized pathway and provides, with its beam, the

medium for either communications or power delivery."[100] A different company, Ball Aerospace, claimed to have produced an airborne terminal that supported a 2.5 Gbps link between an aircraft and a Geosynchronous Earth Orbit (GEO) satellite that "could withstand harsh airborne environments."[101] This achievement had to solve many technical challenges such as mechanical vibration, pointing and tracking from a mobile platform, and adverse atmospheric effects (attenuation or decrease in signal intensity due to absorption and scattering, scintillation or intensity fluctuations, etc.).

In 2003, Ortiz et al. demonstrated that UA could use lasercom to link an Altair UA (Predator variant) to a *ground station* at the California Institute for Technology.[102] In their tests, they were able to achieve a 2.5 Gbps transmission rate and a maximum range of slightly over 17 nautical miles. At this high transmission rate, a temporary fade in the optical link caused by the atmosphere could translate into a large data loss rate measured in the Mbps range. However, inertial sensors kept the laser pointing at the receiver for up to three seconds, which was longer than the fade duration and therefore minimized the possibility of data loss.[103] While the maximum ranges and data rates will likely be different for solely airborne communications, Ortiz reported that "the [optical communications] design architecture, with minor modifications, can support UAV-to-UAV, aircraft, GEO and LEO satellite links."[104] These test results show promise for a future communications architecture based on a seamless combination of RF and lasercom. Lasercom will work well in the higher altitudes where particles will not affect its transmission as much and can be used to relay bandwidth-intensive information like video or hyperspectral imaging. In this case, high altitude UA like Global Hawks may be the best candidates to serves as communications nodes which use lasercom as the primary transmission method.

Appendix O

Film and Conformal Antennas

> *The Information Age has created an environment where collaborative decision making can be employed to increase combat power, partly because of the emergence of coalition operations, partly because of the distribution of awareness and knowledge in the battlespace, and partly because of the compression of decision timelines.*[105]
>
> *– Fred Stein et al. in Network Centric Warfare: Developing and Leveraging Information Superiority*

Advances in antenna technology will greatly enhance a Mobile Ad Hoc Network (MANET) of UA by increasing transmission ranges and improving power management. Ayyagari et al. claimed that, "High-gain electronically steered antenna technology is a key element for mobile wireless communication."[106] If a UA can intelligently track general locations of its "neighbor" nodes, it can steer its antenna for optimum communication transmissions. This also allows it to either decrease the power required in order to transmit or increase the distance between nodes.[107] Future antenna improvements may include miniaturization to save weight or constructing an antenna from the UA shell or spray-on film. The conformal antenna could use the UA shell to arrange up to thousands of individual antenna elements on a curved surface.[108] Given the limited size of UA, antennas must be miniaturized and efficient in order to improve connections that ultimately enable information flow to accelerate the kill chain.

Appendix P

Microprocessors

Gordon Moore, co-founder of Intel, devised the popular Moore's Law which states that the number of transistors on a computer chip doubles approximately every 18 months (originally it was two years).[109] This exponentially increasing trend also drives down costs as more people buy advanced microprocessors. The USAF should allow the computer industry to drive this trend and invest scarce resources in autonomous operations and robust MANET research.

Complex processors also provide the capability to conduct more on-board processing, which increases autonomy and reduces the need to transmit information (bandwidth demand). Numerous advances in microchip technology challenge the traditional production of silicon-based chips. MIT researchers reportedly integrated photonic circuitry on a silicon chip to speed computing power.[110] Several researchers are applying nanotechnology to processors by building "Gold Nano Particles" that convert light into electric signals, with the potential of creating routers three to six times faster than the ones in use today.[111] Intel announced it had experimented with a silvery metal called hafnium which is just 45 nanometers thick (about five atoms) but this has also resulted in electricity leaks that need to be addressed.[112] On 6 March 2007 scientists at the University of Manchester claimed to have constructed a transistor made from graphene that had the thickness of an atom.[113] Recently IBM stated that it used a three-dimensional approach to stack processor and memory chips vertically, allowing significantly faster data transfer rates since these transmissions traveled only microns instead of inches.[114] Since researchers funded by computer corporations around the world have a vested interest in improving processor speeds, the USAF can adapt these technologies for military use.

Appendix Q

Expanded Explanation of Wireless Network Security Concerns

Providing security for MANETs is very challenging for many reasons. Loo from the University of Tokyo cited five: 1) *channel* vulnerability where adversaries could "eavesdrop," 2) *node* vulnerability where UA can be attacked, 3) no infrastructure making *certification and authentification* difficulty, 4) changing *topology* (nodal arrangement) that places routing protocols at risk, and 5) *power and computational limitations* which may restrict the use of sophisticated encryption algorithms.[115] If a MANET consisting of airborne assets cannot defend against intrusion with high confidence, the benefits of promoting autonomous operations, extending communication ranges, and reducing reliance on SATCOM do not outweigh the risks.

Adversaries can use a variety of methods to attack US MANETs. Yang et al. explained that the majority of attacks can be categorized as either routing or packet-forwarding attacks.[116] When conducting routing attacks, hackers cause packets to be forwarded on slow or fictitious routes, either preventing the information from reaching its destination or degrading network performance. During packet forwarding attacks, hackers may attempt to deny service, drop, change, or duplicate packets by overloading the system with "junk" packets.[117]

Hong et al. stated that one of the greatest difficulties is when "the attackers try to be *protocol compliant*, so they are harder to be detected before potential devastating physical attacks are launched."[118] Depending upon the type of mobile network, an intruder can determine the physical location of each node with GPS and localization algorithms. This applies mostly to *proactive* wireless networks where every node maintains route information about all other nodes more than *reactive* wireless networks (also known as on-demand routing) where routing

information expires when not actively used by a node.[119] In addition, *Defense Update* claims that worms spreading malicious code posed one of the greatest threats to MANETs.[120]

To prevent compromising future MANETs, the US military must invest in advanced cryptographic techniques and routing schemes that allow both classified and unclassified information to securely transit common lines and wireless networks. These future MANETs must allow information packets to bypass isolated nodes that are potentially compromised. Hong et al. proposed an anonymous routing scheme to make it harder for potential intruders to hack into the network.[121] They also discussed an "onion routing" approach where each successive node would decode a layer of an information packet and the intended recipient node would decipher the final message.[122] Hubaux et al. from the Swiss Federal Institute of Technology proposed a self-organized security architecture where each node issued, stored, and distributed a "public key certificate."[123] On the other hand, Yang et al. claimed that security measures should span the application, transport, network, link, and physical layers.[124] *Defense Update* advocated dynamically reconfiguring the entire network to isolate essential nodes from attack but all of these security procedures will likely reduce network efficiency.[125] In fact, Kong and Gerla stated, "The cipher algorithms cannot achieve flexible trade off between the overly protected data privacy and the throughput on demand."[126] They proposed using encryption procedures that were "throughput-adaptive" or adjusted the data flow rate based on requirements.[127]

The state or non-state actor that develops the best cyber-teams to protect and infiltrate wireless networks will have a battlespace advantage in the future. The technologically-dependent United States must continually invest in advanced IP, algorithms, and cryptography to protect its networks. While these security measures reduce efficiency, the consequences of a compromised military network justify reduced system performance to an extent.

Appendix R

Foreign Intelligence Security Concerns

By approaching a problem from a potential adversary's perspective, one may predict where and how they will try to exploit the United States. Warning signs are out there that many countries have stepped up espionage efforts against communications and UA technologies. Paul Richfield, writer for C4ISR Journal, related this concern:

> The noticeable surge in espionage by East Asian and Pacific Rim nations will continue in the short term, DSS [Defense Security Service] said, as gaps in technological capability become apparent in their weapons development processes. Lasers, optics and aeronautics — **especially UAV control systems — appear to be priority targets** for this region.[128]

Various US agencies must be vigilant about foreign intelligence services trying to collect sensitive information on UA control systems from US allies, defense industry partners, and sub-contractors. The researcher discovered that many foreign professors contribute to US science and engineering knowledge base and advances in future weapons systems. These experts who receive Air Force or DARPA funding often stay in the United States and contribute to US national security. However, some of these professors, engineers, and scientists may return to their native countries and share their sensitive research findings with governments hostile towards the United States. In these cases, this disclosure could aid foreign militaries and may result in the production of effective countermeasures to the US military's newest weapons systems. A doctorate student at the University of Idaho studying cyber security was arrested for suspected terrorist connections, highlighting the need to be attentive for foreign intelligence gathering.[129]

While this scenario is alarming, the *worst* course of action is to over-react and discourage foreign experts from participating in vital research. However, the US military must weigh the

danger of disclosing sensitive research against the risk of discouraging the world's greatest minds from helping. Experts who receive federal funding for sensitive research and who maintain strong ties with hostile foreign governments should undergo a comprehensive background check. If they return to hostile countries, appropriate agencies should assess the security risks. Currently Service research laboratories conduct background checks but this does not always apply to academia. By attracting and providing incentives to top-notch scientists and engineers working in Service research laboratories, the US military can promote security and effectively apply pure research to military needs.

Glossary

AAA	Anti-Aircraft Artillery
AAR	Automated Aerial Refueling
AEHF	Advanced Extremely High Frequency
AFDD	Air Force Doctrine Document
AFRL	Air Force Research Laboratory
AGM	Air-to-Ground Missile
AI	Artificial Intelligence
ALCM	Air Launched Cruise Missile
ASOC	Air Support Operations Center
ATO	Air Tasking Order
C2	Command and Control
CALCM	Conventional Air-Launched Cruise Missile
CAOC	Combined Air Operations Center
CAP	Combat Air Patrol
CAS	Close Air Support
CFACC	Combined Forces Air Component Commander
CFC	Combined Forces Commander
CIA	Central Intelligence Agency
DARPA	Defense Advanced Research Projects Agency
DCA	Defensive Counter-Air
DEAD	Destruction of Enemy Air Defenses
DISA	Defense Information Systems Agency
DoD	Department of Defense
DMPI	Desired Mean Point of Impact
DPI	Desired Points of Impact
DSCS	Defense Satellite Communications System
DSS	Defense Security Service
EHF	Extremely High Frequency
EO	Electrical Optical
FAA	Federal Aviation Administration
F2T2EA	Find, Fix, Track, Target, Engage and Assess
GAO	Government Accounting Office
Gbps	Gigabits per second
GIG	Global Information Grid
GPS	Global Positioning System
HARM	High Speed Anti-Radiation Missile
HSI	HyperSpectral Imaging
IAD	Integrated Air Defense

IED	Improvised Explosive Device
IETF	Internet Engineering Task Force
IMINT	IMagery INTelligence
INS	Inertial Navigation System
IP	Internet Protocol
IPv6	Internet Protocol Version 6
ISR	Intelligence, Surveillance, Reconnaissance
JACC	Joint Automated Control Capability
JDAM	Joint Direct Attack Munition
JFACC	Joint Forces Air Component Commander
JFC	Joint Force Commander
JMEM	Joint Munitions Effectiveness Manual
JTAC	Joint Terminal Attack Controller
JTRS	Joint Tactical Radio System
Lasercom	Laser communications
LDHD	Low Density High Demand
LEO	Low Earth Orbit
LGB	Laser Guided Bomb
LiDAR	Light Detection And Ranging
LOAC	Laws Of Armed Conflict
MANET	Mobile Ad-hoc NETwork
MANPAD	Man Portable Air Defense Systems
MASINT	Measurement And Signatures INTelligence
MAV	Micro Air Vehicle
Mbps	megabits per second
MILSTAR	Military Strategic and Tactical Relay
MIT	Massachusetts Institute for Technology
NAS	National Airspace System
NASA	National Aeronautics and Space Administration
NIPRNET	Unclassified but Sensitive Internet Protocol Router Network (previously Non-secure IP Protocol Router NETwork)
NSL	No-Strike List
NSSC	National Strategy to Secure Cyberspace
OIF	Operation Iraqi Freedom
OSD	Office of the Secretary of Defense
OSINT	Open Source INTelligence
RF	Radio Frequency
ROE	Rules of Engagement
ROVER	Remotely Operated Video Enhanced Receiver
RTL	Restricted Target List
SA	Situational Awareness
SAM	Surface-to-Air Missile
SAR	Synthetic Aperture Radar
SATCOM	SATellite COMmunications
SDB	Small Diameter Bomb
SEAD	Suppression of Enemy Air Defenses

SIGINT	SIGnals INTelligence
SIPRNET	Secret IP Router NETwork for timely information flow
SOF	Special Operations Forces
SUV	Sports Utility Vehicle
TCA	Transformational Communications Architecture
TSAT	Transformational Satellite Communications System
TERCOM	TERrain COntour Matching
TSAT	Transformational Communications Satellite system
TST	Time-Sensitive Target
UA	Unmanned Aircraft
UAS	Unmanned Aircraft System
UAV	Unmanned Aerial Vehicle
UCAV	Unmanned Combat Aerial Vehicle
UHF	Ultra-High Frequency
US	United States
USAF	United States Air Force
XML	eXtensible Markup Language
WGS	Wideband Global System
WMD	Weapons of Mass Destruction

Bibliography

Aerospace, Ball. "Laser Communications--Airborne Laser Terminal." Ball Aerospace and Technologies Corporation, http://ballaerospace.com/lasercomm_airborne_terminal.html (accessed on 17 March 2007).

AFDC/DR, HQ. "Air Force Doctrine Document 2-1.9 Targeting." (2006): 129.

Aftergood, Steven. "Hyperspectral Imaging." (2007), http://www.fas.org/irp/imit/hyper.htm (Accessed on 20 February 2007).

"Air Force Doctrine Document 2-1.3, Counterland Operations." edited by HQ AFDC/DR, 113, 2006.

"Air Force Doctrine Document 2-1.9, Targeting." edited by HQ AFDC/DR, 129, 2006.

"Air Force Doctrine Document 2, Operations and Organization." edited by HQ AFDC/DR, 173, 2006.

Alberts, David S., John J. Garstka, and Frederick P. Stein. "Network Centric Warfare: Developing and Leveraging Information Superiority." Place Published: C4ISR Cooperative Research Program, 2000.

"All About Bandwidth." *Internet Videomag* (2004), http://www.internetvideomag.com/articles1/ImportanceofBandwidth.htm.

Ayyagari, Arun, Jeff P. Harrang, and Sankar Ray. "Airborne Information and Reconnaissance Network." In *Military Communications Conference, 1996. MILCOM '96, Conference Proceedings, IEEE*, 230-34 McLean, VA: IEEE, 1996.

Bolkcom, Christopher and Kenneth Katzman. "Military Aviation: Issues and Options for Combating Terrorism and Counterinsurgency." In *CRS Report for Congress*, edited by Congressional Research Service, 41. Washington D.C., 2005.

Braasch, Michael S. "Unmanned Aerial Vehicle (UAV) Swarming and Formation Flight Navigation Via Lidar/INS." 5. Athens, OH: Ohio University, 2006.

Bush, President George W. "National Strategy to Secure Cyberspace." 60. Washington D.C.: The White House, 2003.

———. "President Speaks on War Effort to Citadel Cadets " http://www.whitehouse.gov/news/releases/2001/12/20011211-6.html (accessed 11 December 2006).

Cambone, Stephen, Kenneth Krieg, Peter Pace, and Linton Wells II. "Unmanned Aircraft Systems Roadmap 2005-2030." edited by Office of the Secretary of Defense, 213, 2005.

Cheater, Julian C., and James P. Lake. "Survey on Projections About Future Unmanned Aircraft Technologies. ACSC Research Project #06-1188 (ACSC Survey Control Number 07-001)." 17 January 2007.

Clough, Bruce T. "UAV Swarming? So What Are Those Swarms, What Are the Implications, and How Do We Handle Them?" In *AUVSI Unmanned System Conference*, 15. Orlando, FL, 2002.

Connelly, J., W.S. Hong, R.B. Mahoney, and D.A. Sparrow. "Challenges in Autonomous System Development." In *Performance Metrics for Intelligent Systems Workshop*. Gaithersburg, Maryland: National Institute of Standards and Technology, 2006.

Covault, Craig. "Chinese Test Anti Satellite Weapon." http://www.spaceref.com/news/viewnews.html?id=1188 (accessed 18 January 2007)

Curry, Marty "Intelligent Flight Control System." http://www.nasa.gov/centers/dryden/news/FactSheets/FS-076-DFRC.html (accessed on 10 April 2007).

Curtis, David. "Conformal Array Antenna Technology." *Air Force Research Laboratory Horizons* (2004), http://www.afrlhorizons.com/Briefs/Feb04/SN0310.html.

"Enabling Machines to Reason." Stanford University, http://soe.stanford.edu/AR04-05/profiles_mccarthy.html.

Eshel, David. "Israel Intercept Two Attack UAV Launched by Hezbollah." *Defense Update* (2006), http://www.defense-update.com/2006/08/israel-intercept-two-attack-uav-html (accessed 31 March 2007).

Fry, Vice Admiral S.A. . "Department of Defense Dictionary of Military and Associated Terms." edited by Department of Defense, 584, 2007.

Garcia, Gilbert and David Joseforsky. "Transformational Communications Architecture for the Unit Operations Center; Common Aviation Command and Control System; and Command and Control on-the-Move Network, Digital over-the-Horizon Relay." Naval Postgraduate School, 2004.

Ghashghai, Elham. "Communications Networks to Support Integrated Intelligence, Surveillance, Reconnaissance, and Strike Operations." 35. Santa Monica, CA: RAND, 2004.

"The Global Information Grid and Challenges Facing Its Implementation." 37. Washington, D.C.: Government Accountability Office 2004.

Gordon, Michael R., and Bernard E. Trainor. *Cobra II: The inside Story of the Invasion and Occupation of Iraq*. New York: Pantheon Press, 2006.

Grant, Rebecca. "Eyes Wide Open." no. 11 (2003), http://www.afa.org/magazine/Nov2003/1103eyes.asp (accessed on 4 March 2007) p. 42.

———. "The Fallujah Model." *Air Force Magazine*, no. 2 (2005), http://www.afa.org/magazine/feb2005/0205fallujah.asp (accessed on 15 February 2007) pp. 51-53.

Greene, Kate. "New Graphene Transistors Show Promise " *Technology Review* (2007), http://www.technologyreview.com/Infotech/18264/page2/ (accessed on 6 March 2007).

Gunderson, J.P., and L.F Gunderson. "Intelligence ≠ Autonomy ≠ Capability." In *Performance Metrics for Intelligent Systems Workshop*

Gaithersburg, Maryland: National Institute of Standards and Technology, 2004, p. 2.

Harris, Lt Col John. (Deputy Commander, Joint Air-Ground Operations Group; 15th Reconnaissance [Predator] Squadron Commander from June 2004 to May 2006) Telephone Interview 13 April.

Hines, John. "Transformational Communications Air Layer." (2005), http://www.afrlhorizons.com/Briefs/Jun05/IFH0508.html (accessed 6 March 2007).

Hong, Xiaoyan, Jiejun Kongy, and Mario Gerlay. "Mobility Changes Anonymity: New Passive Threats in Mobile Ad Hoc Networks." *Wireless Communications & Mobile Computing, Special Issue of Wireless Network Security*, no. 3 (2006), http://cs.ua.edu/~hxy/Publications.htm (accessed on 3 February 2007) p. 2.

Hubaux, Jean-Pierre, Levente Buttyan and Srdan Capkun. "The Quest for Security in Mobile Ad Hoc Networks." In *Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing*. Long Beach, CA: ACM Press, 2001.

Husby, Craig R. "Path Generation Tactics for a UAV Following a Moving Target." University of Washington, 2005.

"IBM Announces New Chip-Stacking Technology " *International Herald Tribune*, no. 12 April 2007 (2007), http://www.iht.com/articles/2007/04/12/business/chips.php (accessed on 13 April 2007).

Intelligence, U.S. Marine Corp. "Blue Force Tracker." no. 1 (2002), http://www.mccaonline.org/Oct%20Intel%2002.pdf (accessed on 3 March 2007).

"Internet Protocol Version 6." 41. Washington D.C.: Government Accountability Office, 2005.

Irvine, James H. *A Revolution in Military Affairs Brief: Where Are Science and Technology Taking War*, 2007. PowerPoint Presentation (Slides 56-57).

Jin, Yan, Yan Liao, Marios Polycarpou, and Ali Minai. "Balancing Search and Target Response in Cooperative UAV Teams." In *43rd IEEE Conference on Decision and Control*, 2923-28. Atlantis, Paradise Island, Bahamas, 2004.

Kelly, Wallace E., III. "Deconfliction of Multiple, Autonomous Vehicles." (2000), http://www.bluerocketresearch.com/paper/us2000_kelly.pdf (accessed 13 December 2006).

Keys, General Ronald E. "Striking the Balance: Today's War, Tomorrow's Threat." Paper presented at the Air Force Association Air Warfare Symposium, Orlando, FL, 8 February 2007.

Kim, Jonghyuk, Lee Lin Ong, E. Nettleton, and S. Sukkarieh. "Decentralized Approach to Unmanned Aerial Vehicle Navigation: Without the Use of the Global Positioning System and Preloaded Maps." *Proceedings of the Institution for Mechanical Engineers* 218 Part G, no. Special Issue Paper (2004): 339-416.

Kinneard, Doug. "Boeing, U.S. Air Force Demonstrate UAV Automated Aerial Refueling Capability." Boeing, http://www.boeing.com/phantom/news/2006/q4/061127b_nr.html (accessed on 4 March 2007).

Klausner, Kurt A. "Command and Control of Air and Space Forces Requires Significant Attention to Bandwidth." *Air & Space Power Journal*, no. Winter (2002), http://www.airpower.maxwell.af.mil/airchronicles/apj/apj02/win02/klausner.html (accessed on 3 January 2007).

Kong, Jiejun and Mario Gerla. "Providing Real-Time Security Support for Multi-Level Ad-Hoc Networks." In *MILCOM 2002 Proceedings*. Anaheim, California, 2002.

Krock, Lexi. "Time Line of UAVs." In *Spies that Fly*, edited by Public Broadcasting System, 2002.

Kwiatkowski, Leornard. "Achieving Network-Centric Connectivity." *Insights Online*, no. 3 (2006), http://www.lockheedmartin.com/data/assets/13625.pdf (accessed on 3 January 2007).

LaPedus, Mark. "Intel Details New 45-Nm Processor Fabrication Technique." *EE Times Online*, no. 27 January (2007), http://www.informationweek.com/showArticle.jhtml;jsessionid=LMR3UTZXOXWQIQSNDLPCKHSCJUNN2JVN?articleID=197001070&queryText=Intel+and+IBM+ (accessed on 28 January 2007).

Leggett, Michael. "USAF Self-Propelled Munitions." 2004.

Leung, Henri, Ravi Kothari, and Ali A. Minai. "Phase Transition in a Swarm Algorithm for Self-Organized Construction." *Physical Review* 68, no. 4 (2003): 046111-1 to 11-9.

Lewis, A. Scott, and Weiss, Lora G. "Intelligent Autonomy and Performance Metrics for Multiple, Coordinated UAVs." *Integrated Computer-Aided Engineering* 12, no. 3 (2005): 251-62.

Long, Wes (Chief, Offensive Combat Operations) E-mail, 26 February 2007.
Loo, Foo Yee. "Ad Hoc Network: Prospects and Challenges." edited by Science and Technology Graduate School of Information: University of Tokyo, 2004.
Macker, Joe (Senior Communications Engineer for the Naval Research Laboratory). Telephone interview / e-mail correspondence, 28 March 2007.
Macker, Joe, and M. Scott Corson. "Mobile Ad Hoc Networks (MANET): Routing Technology for Dynamic, Wireless Networking." In *Mobile Ad Hoc Networking* edited by Stephano Basagni, Marco Conti, Silvia Giordano, Ivan Stojmenovic, 480: Wiley-IEEE Press 2004.
McCarthy, Patrick A. "Characterization of UAV Performance and Development of a Formation Flight Controller for Multiple Small UAVs." 2006.
Miller, Christopher A., Harry B. Funk, Michael Dorneich, and Stephen D. Whitlow. "A Playbook Interface for Mixed Initiative Control of Multiple Unmanned Vehicle Teams." In *Digital Avionics Systems Conference*. Irvine, CA: IEEE, 2002.
Minai, Ali A., Yan Jin, Yan Liao, and Marios M. Polycarpou. "Impact of System Design Parameters on Performance of Cooperative Agent Teams." (2005), http://www.ececs.uc.edu/~aminai/papers/jin_isic05.pdf (accessed on 3 January 2007).
Moore, Gordon E. "Moore's Law." http://www.intel.com/technology/mooreslaw/index.htm (accessed on 28 March 2007).
Moseley, T. Michael. "The Air Force Handbook 2007." edited by United States Air Force, 305, 2007.
O' Hanlon, Michael E. *Technological Change and the Future of Warfare*. Washington, D.C.: The Brookings Institution, 2000.
Ortiz, Gerardo G., Shinhak Lee, Steve Monacos, Malcolm Wright and Abhijit Biswas. "Design and Development of a Robust ATP Subsystem for the Altair UAV-to-Ground Lasercomm 2.5 Gbps Demonstration." *Free-Space Laser Communication Technologies* XV, no. 4975 of The International Society for Optical Engineering (2003): 12.
Ozburn, Marguerite. "Small Diameter Bomb Increment I Backgrounder." *Boeing Precision Engagement & Mobility Systems Global Strike Systems* (2007), http://www.boeing.com/defense-space/missiles/sdb/docs/SDB_overview.pdf.
Park, Jon (Senior Functional Analyst for the Air Force's C2ISR Center) Telephone Interview / e-mail correspondence, 29 March 2007.
Peterson, Lt. Gen. Michael W. "Providing Real-Time Information to the Warfighter." Paper presented at the Air Force Association Air Warfare Symposium, Orlando, FL, 8 February 2007.
"Predator B." (2006), http://www.ga-asi.com/products/predator_b.php (accessed 24 October 2006).
"Protecting the Military Cyberspace; DARPA Gears to Counter Network Worms " *Defense Update* no. 3 (2005), http://defense-update.com/features/du-3-05/feature-worms.htm (accessed on 26 November 2006).
Richfield, Paul. "Espionage against U.S. Industry on the Rise." http://www.isrjournal.com/story.php?F=2488537 (accessed on 5 March 2007).
Robertson, Lawrence, and Troy Meink. "Transformational Communications." (2005), http://www.afrlhorizons.com/Briefs/Jun05/VS0410.html (accessed on 17 March 2007).
Roman, Gregory. "The Command or Control Dilemma: When Technology and Organizational Orientation Collide." In *Air Force 2025*, edited by Victor Budura Jr. Montgomery, AL: Air University, 1996.

"Rover III / OSRVT Remote Video Terminal for One System GCS." *Defense Update* (2007), http://www.defense-update.com/products/r/rover.htm (accessed 30 March 2007).
Rumsfeld, Donald H. "Quadrennial Defense Review Report." 92: Department of Defense, 2006.
Singer, Jeremy. "Bandwidth Breakthrough." *Air Force Magazine*, March 2007, 76-79
Slear, James N. "AFIT UAV Swarm Mission Planning and Simulation System." Air University, 2006.
"SNC System Performs First Ever Autonomous Airborne Refueling Engagement." Sierra Nevada Corporation, http://www.sncorp.com/PDFs/SNC_news/SNC%20AARD%20Press%20Release%2013Sep06.pdf (accessed on 4 March 2007).
Staugaard , Andrew C., Jr. *Robotics and AI: An Introduction to Applied Machine Intelligence*. Englewood Cliffs, NJ: Prentice Hall, Inc., 1987.
Stokes, Mark A. "China's Strategic Modernization: Implications for the United States ". Carlisle, PA: Strategic Studies Institute, 1999.
Thompson, Elizabeth. "MIT 'Optics on a Chip' May Revolutionize Telecom, Computing." *EurekAlert* (2007), http://www.eurekalert.org/pub_releases/2007-02/miot-mo020507.php# (accessed on 6 February 2007).
Tiffany, Kent (Director of Operations for AFRL's Central Sciences Division), telephone interview. 13 April 2007.
Tirpak, John A. "The Double Digit SAMs." *Air Force Magazine* 84, no. 6 (2001): 48-49.
Tseng, Yuh-Min. "A Heterogeneous-Network Aided Public-Key Management Scheme for Mobile Ad Hoc Networks." *International Journal of Network Management* 17, no. 1 (2007): 3-15.
"The U.S. Air Force Transformation Flight Plan." edited by HQ USAF/XPXC, 176: USAF, 2003.
"U.S. Kills Cole Suspect: CIA Drone Launched Missile." *CNN Dot Com/World* (2002), http://archives.cnn.com/2002/WORLD/meast/11/04/yemen.blast/index.html.
Uijt de Haag, Maarten. "Use of Dual Airborne Laser Scanner in Conjunction with a Tactical Grade Inertial Measurement Unit for Unmanned Aerial Vehicle Navigation and Mapping in Unknown, Non-Global Positioning System Environments." 19, 2006.
"Unmanned Aircraft Systems Roadmap 2005." 213. Washington D.C., 2005.
"Unmanned X-45A Is Armed." *Signal* 58, no. 9 (2004): 6.
USAF. "AGM-86 Missile Fact Sheet " (2006), http://www.af.mil/factsheets/factsheet.asp?fsID=74 (accessed on 17 February 2007).
Wikipedia. "Intelligent Control." (2007), http://en.wikipedia.org/wiki/Intelligent_control (accessed on 3 February 2007).
Wilson, Clay. "Network Centric Warfare: Background and Oversight Issues for Congress." In *CRS Report for Congress*, 42. Washington D.C.: Congressional Research Service, 2005.
Yang, H., H. Y. Luo, F. Ye, S. W. Lu, and L. Zhang. "Security in Mobile Ad Hoc Networks: Challenges and Solutions." *IEEE Wireless Communications*, no. February (2004): 38-47.

Notes

[1] Julian C. Cheater, and James P. Lake, "Survey on Projections About Future Unmanned Aircraft Technologies. ACSC Research Project #06-1188 (ACSC Survey Control Number 07-001)," 17 January 2007.

[2] For example, nanotechnology can be considered a materials science but this was listed as a separate option.

[3] "Unmanned Aircraft Systems Roadmap 2005," (Washington D.C.: 2005), p. 1.

[4] Vice Admiral S.A. Fry, "Department of Defense Dictionary of Military and Associated Terms," ed. Department of Defense (2007), p. 576.

[5] "Air Force Doctrine Document 2, Operations and Organization," ed. HQ AFDC/DR (2006), p. 20.

[6] Stephen Cambone, Kenneth Krieg, Peter Pace, and Linton Wells II, "Unmanned Aircraft Systems Roadmap 2005-2030," ed. Office of the Secretary of Defense (2005), p. 38.

[7] David Eshel, "Israel Intercept Two Attack UAV Launched by Hezbollah," *Defense Update* (2006), http://www.defense-update.com/2006/08/israel-intercept-two-attack-uav-html (accessed 31 March 2007).

[8] Craig Covault, "Chinese Test Anti Satellite Weapon," http://www.spaceref.com/news/viewnews.html?id=1188 (accessed 18 January 2007)

[9] Wes Long, (Chief, Offensive Combat Operations) E-mail, 26 February 2007.

[10] HQ AFDC/DR, "Air Force Doctrine Document 2-1.9 Targeting," (2006): p. 49.

[11] Jon Park, (Senior Functional Analyst for the Air Force's C2ISR Center) Telephone Interview / e-mail correspondence, 29 March 2007.

[12] "Air Force Doctrine Document 2-1.9, Targeting," ed. HQ AFDC/DR (2006), p. 73.

[13] Park.

[14] Gregory Roman, "The Command or Control Dilemma: When Technology and Organizational Orientation Collide," in *Air Force 2025*, ed. Victor Budura Jr. (Montgomery, AL: Air University, 1996), p. 26.

[15] AFDC/DR, "Air Force Doctrine Document 2-1.9 Targeting," p. 53.

[16] "The U.S. Air Force Transformation Flight Plan," ed. HQ USAF/XPXC (USAF, 2003), p. 85.

[17] Lt Col John Harris, (Deputy Commander, Joint Air-Ground Operations Group; 15th Reconnaissance [Predator] Squadron Commander from June 2004 to May 2006) Telephone Interview 13 April.

[18] President George W. Bush, "President Speaks on War Effort to Citadel Cadets " http://www.whitehouse.gov/news/releases/2001/12/20011211-6.html (accessed 11 December 2006).

[19] "Predator B," (2006), http://www.ga-asi.com/products/predator_b.php (accessed 24 October 2006).

[20] According to a telephone interview with Col Tim Greene (99 MSG/CC) on 12 April 2007, MQ-1s typically fly 22-hour missions. A MQ-9 with combat load-out can fly for nine to 15 hours but in a clean configuration this is extended to 20-22 hours.

[21] "Rover III / OSRVT Remote Video Terminal for One System GCS," *Defense Update* (2007), http://www.defense-update.com/products/r/rover.htm (accessed 30 March 2007).

[22] USAF, "AGM-86 Missile Fact Sheet " (2006), http://www.af.mil/factsheets/factsheet.asp?fsID=74 (accessed on 17 February 2007).

Notes

[23] John A. Tirpak, "The Double Digit SAMs," *Air Force Magazine* 84, no. 6 (2001): p. 49.

[24] The SA-20 is included in the non-NATO designation of the S-300 missile series.

[25] Michael Leggett, "USAF Self-Propelled Munitions," (2004), slide 10.

[26] While UA are well-suited to homeland defense, the Posse Comitatus Act prevents active duty military personnel from performing any law enforcement duties unless specifically authorized.

[27] Christopher A. Miller, Harry B. Funk, Michael Dorneich, and Stephen D. Whitlow, "A Playbook Interface for Mixed Initiative Control of Multiple Unmanned Vehicle Teams," in *Digital Avionics Systems Conference* (Irvine, CA: IEEE, 2002), p. 7.E.4-1.

[28] Andrew C. Staugaard , Jr., *Robotics and AI: An Introduction to Applied Machine Intelligence* (Englewood Cliffs, NJ: Prentice Hall, Inc., 1987), p. 22.

[29] A. Scott Lewis, and Weiss, Lora G., "Intelligent Autonomy and Performance Metrics for Multiple, Coordinated UAVs," *Integrated Computer-Aided Engineering* 12, no. 3 (2005): p. 261.

[30] Marty Curry, "Intelligent Flight Control System," http://www.nasa.gov/centers/dryden/news/FactSheets/FS-076-DFRC.html (accessed on 10 April 2007).

[31] Cheater, "Survey on Projections About Future Unmanned Aircraft Technologies. ACSC Research Project #06-1188 (ACSC Survey Control Number 07-001)."

[32] Wallace E. Kelly, III, "Deconfliction of Multiple, Autonomous Vehicles," (2000), http://www.bluerocketresearch.com/paper/us2000_kelly.pdf (accessed 13 December 2006).

[33] General Ronald E Keys, "Striking the Balance: Today's War, Tomorrow's Threat" (paper presented at the Air Force Association Air Warfare Symposium, Orlando, FL, 8 February 2007).

[34] Craig R. Husby, "Path Generation Tactics for a UAV Following a Moving Target" (University of Washington, 2005), p. 1.

[35] Bruce T. Clough, "UAV Swarming? So What Are Those Swarms, What Are the Implications, and How Do We Handle Them?," in *AUVSI Unmanned System Conference* (Orlando, FL: 2002), p. 3.

[36] Kent Tiffany, (Director of Operations for AFRL's Central Sciences Division), telephone interview. 13 April 2007.

[37] Rebecca Grant, "The Fallujah Model," *Air Force Magazine* 88, no. 2 (2005), http://www.afa.org/magazine/feb2005/0205fallujah.asp (accessed on 15 February 2007) pp. 51-53.

[38] U.S. Marine Corp Intelligence, "Blue Force Tracker," 1, no. 1 (2002), http://www.mccaonline.org/Oct%20Intel%2002.pdf (accessed on 3 March 2007).

[39] Michael R. Gordon and Bernard E. Trainor, *Cobra II: The inside Story of the Invasion and Occupation of Iraq* (New York: Pantheon Press, 2006).

[40] "The Global Information Grid and Challenges Facing Its Implementation," (Washington, D.C.: Government Accountability Office 2004), p. 1.

[41] Lt. Gen. Michael W Peterson, "Providing Real-Time Information to the Warfighter" (paper presented at the Air Force Association Air Warfare Symposium, Orlando, FL, 8 February 2007).

[42] "Air Force Doctrine Document 2-1.3, Counterland Operations," ed. HQ AFDC/DR (2006), p. 61.

Notes

[43] Yuh-Min Tseng, "A Heterogeneous-Network Aided Public-Key Management Scheme for Mobile Ad Hoc Networks," *International Journal of Network Management* 17, no. 1 (2007): p. 8.

[44] Keys, "Striking the Balance: Today's War, Tomorrow's Threat".

[45] 1 gigabyte (GBps) per second = 8 gigabits (Gbps) per second; gigabytes are usually used to describe storage capacity and gigabits are usually used to describe transmission rates.

[46] John Hines, "Transformational Communications Air Layer," (2005), http://www.afrlhorizons.com/Briefs/Jun05/IFH0508.html (accessed 6 March 2007).

[47] Ibid.

[48] Elham Ghashghai, "Communications Networks to Support Integrated Intelligence, Surveillance, Reconnaissance, and Strike Operations," (Santa Monica, CA: RAND, 2004), p. 9.

[49] "All About Bandwidth," *Internet Videomag* (2004), http://www.internetvideomag.com/articles1/ImportanceofBandwidth.htm.

[50] Jeremy Singer, "Bandwidth Breakthrough," *Air Force Magazine*, March 2007, p. 79.

[51] Kurt A. Klausner, "Command and Control of Air and Space Forces Requires Significant Attention to Bandwidth," *Air & Space Power Journal*, no. Winter (2002), http://www.airpower.maxwell.af.mil/airchronicles/apj/apj02/win02/klausner.html (accessed on 3 January 2007).

[52] Steven Aftergood, "Hyperspectral Imaging," (2007), http://www.fas.org/irp/imit/hyper.htm (Accessed on 20 February 2007).

[53] Clay Wilson, "Network Centric Warfare: Background and Oversight Issues for Congress," in *CRS Report for Congress* (Washington D.C.: Congressional Research Service, 2005), p. CRS-4.

[54] Joe Macker, and M. Scott Corson, "Mobile Ad Hoc Networks (MANET): Routing Technology for Dynamic, Wireless Networking," in *Mobile Ad Hoc Networking* ed. Stephano Basagni, Marco Conti, Silvia Giordano, Ivan Stojmenovic (Wiley-IEEE Press 2004), p. 10 of chapter 10.

[55] President George W. Bush, "National Strategy to Secure Cyberspace," (Washington D.C.: The White House, 2003), p. 46.

[56] Mark A. Stokes, "China's Strategic Modernization: Implications for the United States " (Carlisle, PA: Strategic Studies Institute, 1999), p. 114.

[57] IPv6 is scheduled for implementation in 2008.

[58] "Internet Protocol Version 6," (Washington D.C.: Government Accountability Office, 2005), p. 11.

[59] Cheater, "Survey on Projections About Future Unmanned Aircraft Technologies. ACSC Research Project #06-1188 (ACSC Survey Control Number 07-001)."

[60] Donald H. Rumsfeld, "Quadrennial Defense Review Report," (Department of Defense, 2006), p. 19.

[61] Rebecca Grant, "Eyes Wide Open," 86, no. 11 (2003), http://www.afa.org/magazine/Nov2003/1103eyes.asp (accessed on 4 March 2007) p. 42.

[62] Lexi Krock, "Time Line of UAVs," in *Spies that Fly*, ed. Public Broadcasting System (2002).

Notes

[63] Christopher and Kenneth Katzman Bolkcom, "Military Aviation: Issues and Options for Combating Terrorism and Counterinsurgency," in *CRS Report for Congress*, ed. Congressional Research Service (Washington D.C.: 2005), p. 14.

[64] "U.S. Kills Cole Suspect: CIA Drone Launched Missile," *CNN Dot Com/World* (2002), http://archives.cnn.com/2002/WORLD/meast/11/04/yemen.blast/index.html.

[65] "Predator B."

[66] Marguerite Ozburn, "Small Diameter Bomb Increment I Backgrounder," *Boeing Precision Engagement & Mobility Systems Global Strike Systems* (2007), http://www.boeing.com/defense-space/missiles/sdb/docs/SDB_overview.pdf.

[67] "Unmanned X-45A Is Armed," *Signal* 58, no. 9 (2004).

[68] Cheater, "Survey on Projections About Future Unmanned Aircraft Technologies. ACSC Research Project #06-1188 (ACSC Survey Control Number 07-001)."

[69] Covault, "Chinese Test Anti Satellite Weapon."

[70] "Enabling Machines to Reason," Stanford University, http://soe.stanford.edu/AR04-05/profiles_mccarthy.html.

[71] Staugaard *Robotics and AI: An Introduction to Applied Machine Intelligence*, p. 23.

[72] J.P. Gunderson, and L.F Gunderson, "Intelligence ≠ Autonomy ≠ Capability," in *Performance Metrics for Intelligent Systems Workshop* (Gaithersburg, Maryland: National Institute of Standards and Technology, 2004, p. 2).

[73] J. Connelly, W.S. Hong, R.B. Mahoney, and D.A. Sparrow, "Challenges in Autonomous System Development," in *Performance Metrics for Intelligent Systems Workshop* (Gaithersburg, Maryland: National Institute of Standards and Technology, 2006), p. 221.

[74] Cheater, "Survey on Projections About Future Unmanned Aircraft Technologies. ACSC Research Project #06-1188 (ACSC Survey Control Number 07-001)."

[75] Wikipedia, "Intelligent Control," (2007), http://en.wikipedia.org/wiki/Intelligent_control (accessed on 3 February 2007).

[76] Ibid.

[77] Ali A. Minai, Yan Jin, Yan Liao, and Marios M. Polycarpou, "Impact of System Design Parameters on Performance of Cooperative Agent Teams," (2005), http://www.ececs.uc.edu/~aminai/papers/jin_isic05.pdf (accessed on 3 January 2007).

[78] Husby, "Path Generation Tactics for a UAV Following a Moving Target", pp. 17, 27, 38-40.

[79] Jonghyuk Kim, Lee Lin Ong, E. Nettleton, and S. Sukkarieh, "Decentralized Approach to Unmanned Aerial Vehicle Navigation: Without the Use of the Global Positioning System and Preloaded Maps," *Proceedings of the Institution for Mechanical Engineers* 218 Part G, no. Special Issue Paper (2004): p. 400.

[80] Ibid.: p. 410.

[81] Maarten Uijt de Haag, "Use of Dual Airborne Laser Scanner in Conjunction with a Tactical Grade Inertial Measurement Unit for Unmanned Aerial Vehicle Navigation and Mapping in Unknown, Non-Global Positioning System Environments," (2006).

[82] Cheater, "Survey on Projections About Future Unmanned Aircraft Technologies. ACSC Research Project #06-1188 (ACSC Survey Control Number 07-001)."

[83] Michael S. Braasch, "Unmanned Aerial Vehicle (UAV) Swarming and Formation Flight Navigation Via Lidar/INS," (Athens, OH: Ohio University, 2006), p. 1.

Notes

[84] Yan Jin, Yan Liao, Marios Polycarpou, and Ali Minai, "Balancing Search and Target Response in Cooperative UAV Teams," in *43rd IEEE Conference on Decision and Control* (Atlantis, Paradise Island, Bahamas: 2004), p. 2923.

[85] Henri Leung, Ravi Kothari, and Ali A. Minai, "Phase Transition in a Swarm Algorithm for Self-Organized Construction," *Physical Review* 68, no. 4 (2003): p. 046111-8.

[86] James N. Slear, "AFIT UAV Swarm Mission Planning and Simulation System" (Air University, 2006), P. 1-5.

[87] Patrick A. McCarthy, "Characterization of UAV Performance and Development of a Formation Flight Controller for Multiple Small UAVs" (2006), p. iv.

[88] Doug Kinneard, "Boeing, U.S. Air Force Demonstrate UAV Automated Aerial Refueling Capability," Boeing, http://www.boeing.com/phantom/news/2006/q4/061127b_nr.html (accessed on 4 March 2007).

[89] "SNC System Performs First Ever Autonomous Airborne Refueling Engagement," Sierra Nevada Corporation, http://www.sncorp.com/PDFs/SNC_news/SNC%20AARD%20Press%20Release%2013Sep06.pdf (accessed on 4 March 2007).

[90] Michael E. O' Hanlon, *Technological Change and the Future of Warfare* (Washington, D.C.: The Brookings Institution, 2000), p. 116.

[91] T. Michael Moseley, "The Air Force Handbook 2007," ed. United States Air Force (2007), p. 116.

[92] Ibid., p. 193.

[93] Singer, "Bandwidth Breakthrough," p. 78.

[94] Leornard Kwiatkowski, "Achieving Network-Centric Connectivity," *Insights Online* 3, no. 3 (2006), http://www.lockheedmartin.com/data/assets/13625.pdf (accessed on 3 January 2007).

[95] Singer, "Bandwidth Breakthrough," p. 78.

[96] Ibid., p. 79.

[97] Lawrence Robertson, and Troy Meink, "Transformational Communications," (2005), http://www.afrlhorizons.com/Briefs/Jun05/VS0410.html (accessed on 17 March 2007).

[98] Ibid.

[99] Kwiatkowski, "Achieving Network-Centric Connectivity."

[100] Gilbert and David Joseforsky Garcia, "Transformational Communications Architecture for the Unit Operations Center; Common Aviation Command and Control System; and Command and Control on-the-Move Network, Digital over-the-Horizon Relay" (Naval Postgraduate School, 2004), p. 207.

[101] Ball Aerospace, "Laser Communications--Airborne Laser Terminal," Ball Aerospace and Technologies Corporation, http://ballaerospace.com/lasercomm_airborne_terminal.html (accessed on 17 March 2007).

[102] Gerardo G. Ortiz, Shinhak Lee, Steve Monacos, Malcolm Wright and Abhijit Biswas, "Design and Development of a Robust ATP Subsystem for the Altair UAV-to-Ground Lasercomm 2.5 Gbps Demonstration," *Free-Space Laser Communication Technologies* XV, no. 4975 of The International Society for Optical Engineering (2003).

[103] Ibid.: p. 9.

[104] Ibid.: p. 4.

Notes

[105] David S. Alberts, John J. Garstka, and Frederick P. Stein. "Network Centric Warfare: Developing and Leveraging Information Superiority." (Place Published: C4ISR Cooperative Research Program, 2000), http://www.dodccrp.org/files/Alberts_NCW.pdf (accessed 13 December 2006).

[106] Arun Ayyagari, Jeff P. Harrang, and Sankar Ray, "Airborne Information and Reconnaissance Network," in *Military Communications Conference, 1996. MILCOM '96, Conference Proceedings, IEEE* (McLean, VA: IEEE, 1996), p. 233.

[107] Joe (Senior Communications Engineer for the Naval Research Laboratory) Macker, Telephone interview / e-mail correspondence, 28 March 2007.

[108] David Curtis, "Conformal Array Antenna Technology," *Air Force Research Laboratory Horizons* (2004), http://www.afrlhorizons.com/Briefs/Feb04/SN0310.html.

[109] Gordon E. Moore, "Moore's Law," http://www.intel.com/technology/mooreslaw/index.htm (accessed on 28 March 2007).

[110] Elizabeth Thompson, "MIT 'Optics on a Chip' May Revolutionize Telecom, Computing," *EurekAlert* (2007), http://www.eurekalert.org/pub_releases/2007-02/miot-mo020507.php# (accessed on 6 February 2007).

[111] James H. Irvine, *A Revolution in Military Affairs Brief: Where Are Science and Technology Taking War* (2007), PowerPoint Presentation (Slides 56-57).

[112] Mark LaPedus, "Intel Details New 45-Nm Processor Fabrication Technique," *EE Times Online*, no. 27 January (2007), http://www.informationweek.com/showArticle.jhtml;jsessionid=LMR3UTZXOXWQIQSNDLPCKHSCJUNN2JVN?articleID=197001070&queryText=Intel+and+IBM+ (accessed on 28 January 2007).

[113] Kate Greene, "New Graphene Transistors Show Promise " *Technology Review* (2007), http://www.technologyreview.com/Infotech/18264/page2/ (accessed on 6 March 2007).

[114] "IBM Announces New Chip-Stacking Technology " *International Herald Tribune*, no. 12 April 2007 (2007), http://www.iht.com/articles/2007/04/12/business/chips.php (accessed on 13 April 2007).

[115] Foo Yee Loo, "Ad Hoc Network: Prospects and Challenges," ed. Science and Technology Graduate School of Information (University of Tokyo, 2004), Slide 36.

[116] H. Yang, H. Y. Luo, F. Ye, S. W. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," *IEEE Wireless Communications*, no. February (2004): p. 39.

[117] Ibid.: p. 40.

[118] Xiaoyan Hong, Jiejun Kongy, and Mario Gerlay, "Mobility Changes Anonymity: New Passive Threats in Mobile Ad Hoc Networks," *Wireless Communications & Mobile Computing, Special Issue of Wireless Network Security* 6, no. 3 (2006), http://cs.ua.edu/~hxy/Publications.htm (accessed on 3 February 2007) p. 2.

[119] Ibid.

[120] "Protecting the Military Cyberspace; DARPA Gears to Counter Network Worms " *Defense Update* no. 3 (2005), http://defense-update.com/features/du-3-05/feature-worms.htm (accessed on 26 November 2006).

[121] Hong, "Mobility Changes Anonymity: New Passive Threats in Mobile Ad Hoc Networks."

Notes

[122] Ibid.

[123] Jean-Pierre Hubaux, Levente Buttyan and Srdan Capkun, "The Quest for Security in Mobile Ad Hoc Networks," in *Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking and Computing* (Long Beach, CA: ACM Press, 2001), p. 5.

[124] Yang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," p. 41.

[125] "Protecting the Military Cyberspace; DARPA Gears to Counter Network Worms ".

[126] Jiejun and Mario Gerla Kong, "Providing Real-Time Security Support for Multi-Level Ad-Hoc Networks," in *MILCOM 2002 Proceedings* (Anaheim, California: 2002), p. 5.

[127] Ibid.

[128] Paul Richfield, "Espionage against U.S. Industry on the Rise," http://www.isrjournal.com/story.php?F=2488537 (accessed on 5 March 2007).

[129] Wilson, "Network Centric Warfare: Background and Oversight Issues for Congress," p. CRS-13.