# ENABLING BATTLESPACE PERSISTENT SURVEILLANCE: THE FORM, FUNCTION, AND FUTURE OF SMART DUST

SCOTT A. DICKSON, 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(s) and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

#### Abstract

In 2025, the military's need for persistent surveillance applications will extend beyond current airborne platforms such as Global Hawk and Predator. The future of 2025 contains potential enemies with a material and information focus capable of conducting regular and irregular warfare on foreign lands as well as the continental United States. The US military must invest their energy and money today into researching enabling technologies such as nanotechnology, wireless networks, and micro-electromechanical systems (MEMS) to develop persistent surveillance applications such as Smart Dust for the future.

The enabling aspects of these technologies, based in academia or business today, form the basis for the disruptive combat applications in the next 20 years. Nanotechnology, while fantastic in some aspects, reduces today's technology to the molecular level contributing to increased performance for the future. Facilitating globalization, wireless networks link people, computers, and sensors beyond the borders of nations without the need for costly hardwareintensive infrastructure. Finally, MEMS sense a wide array of information with the processing and communication capabilities to act as independent or networked sensors. Fused together into a network of nanosized particles distributed over the battlefield capable of measuring, collecting, and sending information, Smart Dust will transform persistent surveillance for the warfighter.

With technological, social, and ethical challenges preventing growth, the US military should lead research, development, and education on these enabling technologies to realize the full benefits of Smart Dust by 2025. Through policy decisions, the United States, as the world's superpower, must continue to lead the development of innovative technologies to preserve the balance of power for the future.

# **Table of Contents**

Disclaimer	i
Abstractii	i
NTRODUCTION 1	
SMART DUST	;
NANOTECHNOLOGY	;
WIRELESS SENSOR NETWORKS	)
MICRO-ELECTROMECHANICAL SYSTEMS 13	;
ETHICAL, ENVIRONMENTAL, AND BIOLOGICAL IMPLICATIONS	ý
FUTURE FORECASTING 19   Exploring State Scenarios 21   Exploring Non-State Scenarios 26	L
RECOMMENDATIONS AND CONCLUSION	)
APPENDIX A: Summary of BLUE HORIZON Scenarios	
Bibliography	ŀ

#### INTRODUCTION

Information superiority is fundamental to joint operations. -- Joint Planning 3-0

From the invasion of Normandy to the most recent Iraq War, the level of US success stemmed from either an abundance or a lack of intelligence. The United States typically rushes to build ways of gathering this intelligence with the persistence needed to provide relevant and current information. For example, US military leaders chose to deploy the Global Hawk ISR platform to Operation Enduring Freedom's area of operations prior to full operational certification to improve intelligence gathering.<sup>1</sup> However, this focus on the present sometimes prevents the US from foreseeing the possible benefits of future technologies to provide a persistent and more effective picture of the battlespace.

Throughout military operations, intelligence of the operational environment dictates the level of mission success or failure since it shapes the decision-making process of military leaders. "By 'intelligence', we mean every sort of information about the enemy and his country—the basis, in short, of our own plans and operations."<sup>2</sup> According to joint doctrine, "...the fusion of all-source intelligence along with the integration of sensors, platforms, command organizations, and logistic support centers allows a greater number of operational tasks to be accomplished faster, and enhances awareness of the operational environment — a key component of information superiority."<sup>3</sup> Without doubt, future warfare requires information superiority.

From this requirement, intelligence technologies grow. However, their growth depends on present and future contexts composed of enabling and detracting conditions. The present context sets the initial starting conditions and the continued growth of these technologies depends on future positive conditions. Specifically, global events and strategic policy drive the conditions of the future context in which the United States will exist and persevere. In addition, societal and ethical concerns represent negative conditions hindering the growth of technologies. For example, the current ethical debate over stem-cell research is one such case.

Therefore, to develop, benefit, and prepare for uses of future intelligence technologies, United States military leaders must understand the contexts of current enabling technologies including their possible capabilities and their limitations. "The future GNR (Genetics, Nanotechnology, Robotics) age will come about not from the exponential explosion of computation alone but rather from the interplay and myriad synergies that will result from multiple intertwined technological advances."<sup>4</sup> In this complex system-of-systems world, combinations of enabling technologies produce powerful and effective technological applications. One application, from the fusion of nanotechnology, wireless sensor networks, and microelectronic mechanical systems (MEMS), is Smart Dust, networked molecular particles capable of measuring, collecting, and sending information remotely.

In the future world of 2025, Smart Dust could fulfill United States' persistent surveillance needs despite current ethical and social concerns. After defining Smart Dust, this paper examines the possible military applications of this type of fusion in light of military doctrine. It surveys each of the enabling technologies behind the fusion including their current development, capabilities, and limitations. Additionally, a review of current ethical and social concerns highlights potential challenges in developing and using Smart Dust. Finally, and most importantly, it analyzes future state and non-state scenarios focusing on how these scenarios will affect the use, development, and limitations to senior military leaders regarding military actions and policies to shape the form, function, and future of Smart Dust.

2

#### **SMART DUST**

The combination of nanotechnology, wireless sensor networks, and MEMS forms a new meaning to network-centric warfare while creating a new application of persistent surveillance beyond current systems, such as Global Hawk and Predator. This combination, Smart Dust, creates a wireless network of nanoscaled sensors, called motes, across a battlespace, like dust on furniture, yielding real-time information about enemy or friendly movements, habits, and intentions.

Historically, the US deployed this concept in Vietnam using 1960-era technology under the auspices of Igloo White as part of the informal McNamara barrier.<sup>5</sup> In January 1968, the sensors contributed to the defense of the Marines at Khe Sanh; "the sensors were very effective

in tracking the enemy at Khe Sanh-even the Marines said so—but, when the siege lifted in April, work on the barrier did not resume."<sup>6</sup> Later, used to support interdiction of the Ho Chi Minh Trail, "the sensors—a network of some 20,000 of them-were planted mostly by Navy and Air Force Figure 1: US airman planting Igloo airplanes, although some of them were placed by special



White sensors in Vietnam Reprinted from Correll

operations ground forces."<sup>7</sup> While Igloo White's impact is debatable, the Air Force reported Igloo White had a contributory effect on interdiction operations.

Today's technology makes this concept even more effective. The Smart Dust project at the University of California-Berkeley created a mote measuring the size of a grain of rice.<sup>8</sup> Earthscope, a \$200 million project sponsored by the National Science Foundation, deposited 400 mobile devices designed to "move east in a wave from California across the nation over the course of a decade."<sup>9</sup> Additionally, as part of a Defense Advanced Research Projects Agency (DARPA) information sensor technology demonstration called SensIT, the University of Berkeley and the United States Marines deployed six motes from an unmanned aerial vehicle (UAV) which formed a wireless network, sensed a moving vehicle, and reported its data to the orbiting UAV.<sup>10</sup>

Militarily, leaders demand this capability. Michael W. Wynne, Secretary of the Air Force, calls its spherical situational awareness, "a new habit of thought and joint and coalition operational capabilities -- a comprehensive view, at once vertical and horizontal, real-time and predictive, penetrating and defended in the cyber-realm."<sup>11</sup> According to the United States Air Force Deputy Chief of Staff for Intelligence, Surveillance and Reconnaissance (ISR), General Deptula, "the biggest challenge facing Air Force intelligence today is similar to that of the rest of the intelligence community-understanding the intent, strategy and plans of a potential adversary."<sup>12</sup> From this guidance, the Air Force Research Laboratory declared unprecedented proactive reconnaissance and surveillance as an Air Force-focused long-term challenge.<sup>13</sup> In regards to the future, Chairman of the Joint Chiefs of Staff Gen Hugh Shelton said, "...future trends — such as the weaponization of information technologies or the increased probability of combat operations in urban terrain - foreshadow a dramatic growth in requirements for the finegrained, time sensitive intelligence collection and analysis."<sup>14</sup> Network-centric persistent surveillance applications, such as Smart Dust, aim to deliver contextual information on the adversary more completely, quickly, and reliably than other ISR methods.

Strategically, Smart Dust has strong application to the arenas of battlespace awareness, homeland security, and weapons of mass destruction (WMD) identification. The 2004 National Military Strategy outlines decision superiority through enhanced battlespace awareness and states, "Developing the intelligence products to support this level of awareness requires collection systems and assured access to air, land, sea, and space-based sensors."<sup>15</sup> Smart Dust is a tailorable collection system supporting battlefield awareness. Furthermore, the 2005 Strategy

for Homeland Defense and Civil Support describes an active layered defense relying "on early warning of an emerging threat in order to quickly deploy and execute a decisive response."<sup>16</sup> Smart Dust could provide this early warning. Additionally, the 2006 Quadrennial Defense Review highlighted the capability for "persistent surveillance over wide areas to located WMD capabilities or hostile forces."<sup>17</sup> Configured with the correct sensors, Smart Dust provides a localized WMD detection layer supplementing US global detection equipment.<sup>18</sup> While future scenarios will change the most appropriate use of Smart Dust, the applicability of Smart Dust to current and long-lasting challenges is undeniable.

Doctrinally, Smart Dust offers the advantages of ubiquity, flexibility, timeliness, and persistence of intelligence to military leaders, planners, and operators. The molecular size of motes minimizes their noticeable footprint providing access to locations normally unavailable to traditional persistent surveillance applications while still covering a large area at reasonable cost. Information delivered on demand at the speed of electronic communication to the strategic, operational, and tactical levels of warfare turns planning and execution unknowns into reliable facts.<sup>19</sup> Furthermore, equipping each mote with different types of sensors offers instantaneous information flexibility for analysis conducted by soldiers in the field or analysts via reachback.

Similar to the limitations of the enabling technologies, environment, sensor range, and frequency jamming constrain the usefulness of Smart Dust. High wind conditions overcome the static-electric effects of particle lifting dust, dirt, and nanoscaled sensors away from intelligence areas of interest. As nanoscaled motes settle into the crevices of the battlespace, environmental elements of all sizes from ant hills to foliage to mountains limit the line-of-sight range of wireless sensor networks. Furthermore, with a dependency on wireless communication, jammers or electro-magnetic pulses potentially disrupt the network's reliability and accuracy. While the next section examines the critical technical issues of each enabling technology, future situations

may frame and dictate other technical limitations.

#### NANOTECHNOLOGY

While the applications and uses for nanotechnology are endless, the broad nature and hype surrounding nanotechnology has weakened its credibility and direction. As David M. Berube stated, "the exaggeration and hyperbole infecting the discussion of nanoscience and nanotechnology have led to false expectations and apprehensions."<sup>20</sup> To separate useful possibilities from unproductive fiction, military leaders must thoroughly understand the truth surrounding nanotechnologies' capabilities and limitations.

"Nanotechnology (NT) is the manipulation and control of matter at the scale of the nanometer (one-billionth of a meter)—roughly the diameter of a small molecule."<sup>21</sup> This expands the field of microtechnology that deal with objects at the one-millionth of a meter. Any technology dealing with objects at the nano scale attribute themselves to the nanotechnology field. This definition derives two differing views on who manipulates the matter, the Drexler self-replicating view or an industrial view.

Eric J. Drexler, a renown proponent of nanotechnology, envisioned a world where nanoscaled robots, commonly called 'nanites', manipulated and controlled matter similar to living cells. "...Having gained control of the cell's molecular machinery, one could use it the same way that engineers did normal-size machines: making materials, structures, tools, and more machines."<sup>22</sup> From his 1987 book *Engines of Creation*, this concept of self-replicating nanites became the cornerstone of nanotechnology and grant money surged. While his vision drove the popularity of nanotechnology, some scientists believed his concept was too grandiose and without immediate practical application. Nonetheless, Drexler's vision caused a surge in investment money and high demand for achievable and useful nanotechnology applications that

drove the creation of a less grandiose version of nanotechnology, the industrial view.

The industrial view benefits from reducing the size of present technology. "After all, if nanotechnology means dealing with matter on the scale of nanometers, then a huge amount of existing science and engineering was, by definition, nanotechnology: chemistry, molecular biology, surface physics, thin films, ultrafine powders, and so forth."<sup>23</sup> Thus, risk-averse investment brokers can capitalize on the popularity of nanotechnology without the risk of Drexler's grand visions.

Today, these two competing views of nanotechnology continue to dominate the field and challenge scientists to overcome the limitations preventing them from becoming a reality. These limitations serve as a checklist for senior military leaders to track nanotechnology's progress. For Smart Dust, most of nanotechnology's limitations revolve around the scaling of objects to the nano level since this type of surveillance technology already exists at the micro level. Specifically, these limitations include reducing power supplies, assembly apparatus, and sensors.

To address energy concerns, scientists have reduced the size of power supplies while increasing available power density. "For example, researchers at Cornell University have created a cubic-millimeter-sized battery that can supply power for decades by drawing energy from radioactive isotopes, such as nickel-63."<sup>24</sup> The Defense Advanced Research Project Agency (DARPA) Micro Power Sources program explores new battery architectures, the use of new materials and their corresponding chemistries, and the incorporation of energy harvesting to maintain energy densities in substantially smaller volumes.<sup>25</sup> While reducing batteries to the nano level is achievable, the amount of available energy limits the utility of some nanotechnology applications, such as persistent surveillance.

To overcome the power output limitation, engineers currently offer three possibilities: miniaturized motors, protein engines, or imperceptible vibrations. Since scaling laws prohibit the use of magnetic forces, some scientists are tapping electrostatic forces to power these miniature motors.<sup>26</sup> In 2003, physicists at the University of California at Berkeley successfully created the first electrostatic nanomotor utilizing carbon nanotubes and a gold rotor. The motor was about 200 nanometers across or, compared to something tangible, 300 times smaller than the diameter of a human hair.<sup>27</sup> This achievement demonstrated the feasibility of using nanotubes as bearings, a necessary step in the creation of electrostatic engines. Groups of scientists, led by Carlo Montenagno of Cornell University and Viola Vogel of the University of Washington, reported the ability to harness the power from protein motors in living cells to twirl microscopic plastic beads.<sup>28</sup> Finally, "Paul Wright of UC Berkeley and his doctoral student Shad Roundy have developed tiny devices that can generate up to 200 microwatts from low-level vibrations that are commonplace in buildings, pumps, air-conditioning ducts, and even microwave ovens."<sup>29</sup> To develop Smart Dust, military leaders should support and fund research in nanoscaled power supplies.

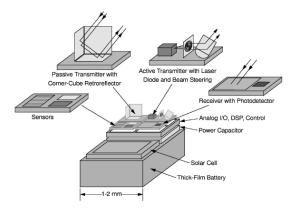
While no one has announced the creation of an electrostatic or biological nanoengine, the success of the nanomotor highlighted another nanotechnology limitation--assembly. To produce higher order devices, manufacturers need measuring and assembly equipment capable of manipulating nanoscaled objects. In the Berkeley motor demonstration, the physicists quantified the frequency of the motor at 30 times per second because the scanning electronic microscope was unable to capture pictures any faster. The full capability of the motor was probably faster, but without appropriate measuring equipment, verification is not possible. In addition, the assembly techniques and equipment used by Berkeley physicists do not support mass production of nanomotors. Although mass production techniques exist to produce large quantities of carbon nanotubes, scientists need to develop assembly capabilities and equipment to produce large quantities of nanoscaled objects cheaply and efficiently. Military support and funding should

include research into nanotechnology measurement and manufacturing.

Another challenge involves reducing sensors to the nano scale while not adversely influencing their frequency, sensitivity, or resolution. In the Berkeley example, the SEM was unable to capture images at a faster frequency. However, Charles M. Lieber of the Air Force Research Laboratory created an Integrated Nanoscale Nanowire Correlated Electronic Technology (INNOCENT) system with the sensitivity of detecting chemical or biological threats at concentrations of only 100 parts per billion. It seems only a matter of time before scientists reduce workable micro-sensors to the nano level. To further development, the military should continue funding research and manufacture of nanoscaled sensors.

#### WIRELESS SENSOR NETWORKS

Enabled by nanotechnology, wireless sensor networks form the ubiquitous backbone to each Smart Dust mote. Simply defined, wireless sensor networks are "groups of devices that send data from sensors to a central application using wireless protocols."<sup>30</sup> These protocols



allow two-way communication to collect and disseminate information via data packets between motes. The motes of a wireless sensor network (Fig 1) include a transmitter/receiver, a central processor, coordination software, sensors, and a power supply. Depending on the application, the

Figure 2: Anatomy of a Mote Reprinted from Kahn

transmitter/receiver can send and receive data via radio frequencies, modulated light, MEMS movement, physical orientation, or color shifts. At the heart, coordination software utilizes the hardware of the central processor to process the data, route communications, or reconfigure the

network. The MEMS sensors, discussed further later, are capable of capturing temperature, pressure, vibration, acceleration, light, magnetic, or acoustical data. Finally, the power supply energizes all of these components.

In addition to the physical devices of a wireless network, the topology of the network (Fig 2) affects the network's effectiveness. The most common topologies are the hub-and-spoke and the mesh. In a hub-and-spoke model, one of the motes acts as a clearinghouse for all of the

data of the network. In a mesh arrangement, each mote acts as an independent agent: gathering its own data, passing or storing data of its neighbors, or reporting all of its stored data when polled.

Depending on the application, engineers tailor the topology and different sections of the mote to overcome any technological limitations.

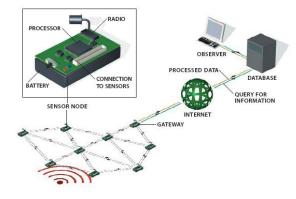


Figure 3: Topology of a Wireless Sensor Network Reprinted from Huang

For example, power availability, as mentioned earlier, limits the effectiveness of the wireless sensor network in a Smart Dust application. To this end, scientists have developed coordination software protocols to minimize energy consumption. One protocol, called sleep-awake, utilizes some motes in the network as sentries and activates the rest of the network if the sentries detect a sudden change in the data.<sup>31</sup> The sentry wakes up once a second, spending about .05 of a millisecond collecting data from its sensors and another 10 milliseconds exchanging data with neighboring motes.<sup>32</sup> In the remainder of each second, the mote consumes no power. During one experiment with 5% of deployed motes serving as sentries and the non-sentries operating at a 4% duty cycle, the algorithm extended the lifetime of a sensor network up to 900%.<sup>33</sup> In another possible protocol, motes, using their location from a GPS, relay data to the mote closest to the final destination. This relay minimizes the transmission distance of each mote conserving

a mote's limited power supply for the benefit of the entire network.

Despite these advances in energy conservation, technological challenges remain for wireless networks. Fortunately, within the context of Smart Dust, scientists must solve only a subset of these limitations. Specifically, the requirements for coordination of a large quantity of motes over varied terrain highlight the limitations of transmission reliability, race conditions, and false alarm handling.

The usefulness of a network depends on the reliability of the delivered information, commonly called transmission reliability, despite interference from the operational environment. Current studies show up to a 20% loss in delivery of transmission packets due to all types of interference. Just as aircraft reliability improved from the days of the Wright Brothers to today, the reliability of wireless network equipment will improve with popularity, development, and time. However, to ensure reliable operation independent of the operating environment, scientists are experimenting with the coordination software of the motes. "There is no such thing as a reliable network, unless you do very aggressive network management."<sup>34</sup> One solution relies on motes repeatedly broadcasting their reception or equipment status. In this manner, other motes can isolate the unreliable mote until its reliability improves. To develop Smart Dust, the military should research alternative methods of increasing transmission reliability of wireless networks.

While status updates potentially improve transmission reliability, this increased message traffic exacerbates the race condition limitation. A race condition occurs when a mote misses a transmission due to the receipt of another transmission. Compounding the problem, each new mote exponentially multiplies transmissions on the network. Attempts to solve this problem involve tuning the coordination software and topology. Deborah Estrin, a UCLA laboratory scientist, uses a divide-and-conquer approach similar to people-to-people communications at a large party.<sup>35</sup> Initially, the network temporarily divides into hub-and-spoke clusters for

communication, like small groups at a party. However, each mote, like people, independently adjusts its involvement based on energy or reliability concerns. Within the group, one mote determines the priority and sequence of polling the other motes in the group preventing possible race conditions. This topology repeats itself depending on the number of motes in the network. While simplifying communications, this solution depends heavily on the mote's coordination software. Currently, an open-source operating system called TinyOS, initially built by students at The University of California-Berkeley, powers some small mote networks.<sup>36</sup> Its open-source availability expands the pool of scientists and students available to solve these coordination challenges. To realize Smart Dust, the military should encourage and fund research into other creative solutions to the race conditions of networks.

Further complicating wireless sensor networks, motes deliver false alarms based on their sensitivity or condition after deployment. Burst distortions of readings due to power state transitions or incorrect readings from faulty sensors normally cause false alarms.<sup>37</sup> Additionally, motes could report without a corresponding stimulus, called a false positive, or not report despite the presence of a stimulus, called a false negative. Experimental results show a decrease in false positives and an increase in false negatives when the number of motes increases.<sup>38</sup> However, as the number of motes increased, the time from sensing an event to receiving a report, called network latency, increased because of the number of motes involved in passing the report. This increase in latency decreased the overall effectiveness of the network.

While increases in computing speed and sensor sensitivity will decrease false alarms, current solutions optimize the trade-off between false alarm rate and network latency depending on the specific application. This tradeoff leverages the triangular relationship between capability to detect, probability of detection, and probability of false alarm.<sup>39</sup> Since some applications demand precise sensing, a low false alarm rate is necessary and longer network communications

are acceptable. Conversely, applications needing quick communications can sacrifice a little reliability for the lower latency. In the long term, increases in computing speed will improve network speed and reduce communication time. Additionally, sensors with enhanced sensitivity will more accurately distinguish between actual events, false positives, or false negatives. The military should support further research into the tradeoffs between false alarms and network latency to achieve effective Smart Dust applications.

#### MICRO-ELECTROMECHANICAL SYSTEMS

As components of wireless networks, micro-electromechanical systems (MEMS) mix electrical and mechanical systems that "sense, control, actuate, and function individually or in arrays."<sup>40</sup> "The simplest example of a MEMS device resembles a diving board with a mass mounted on the end. Gravitational forces or acceleration cause the mass to spring up and down, forces that can easily be converted into a digital signal."<sup>41</sup> MEMS exist today in equipment such as inkjet printers, display projectors, automobiles, and data communication routers. Reduced with nanotechnology, MEMS become nano-electromechanical systems (NEMS).



In the future, NEMS will evolve to contain sensing, processing, and communication capabilities despite current limitations. In March 2003, the University of California-Berkeley developed Spec, a special-purpose MEMS designed for low-cost production and low-power operation.<sup>42</sup> About five square millimeters, Spec (Fig 3)

Reprinted from Brain contains a transmitter capable of transmitting over short distances.<sup>43</sup> Depending on the size of the attached battery, its power consumption of 18-27 milliwatts with a duty cycle of .1-.5 percent support operations on the order of years.<sup>44</sup> As mentioned earlier, future developments in nanotechnology will decrease battery size while increasing operational duration. However, MEMS limitations, including antennas, environment effects, and cost, prevent MEMS from becoming effective Smart Dust motes.

Specifically, the size and efficiency of an antenna limit its communication distance and bounds frequency agility by establishing the possible range of transmitting frequencies. This limitation rests on the fundamental relationship between size, efficiency, and bandwidth of a single antenna. The effective area of the antenna with its associated gain (increase in signal strength) and efficiency dictates the frequencies the antenna can transmit.<sup>45</sup> As nanotechnology shrinks MEMS components, the effective area of antennas will correspondingly decrease. While atmospheric attenuation complicates the issue, the military should develop new antennas capable of larger gains to offset the reduction in size and maintain the same range of transmitting frequencies.

One possible solution, antenna arrays, coordinates the antennas of nearby MEMS to transmit the message. This pooling of resources increases the effective antenna size and allows for greater frequency bandwidth but demands more processing overhead by the coordination software and hardware. As part of an ad-hoc antenna array, individual MEMS must derive time and their relative location from GPS, thus instilling an exploitable dependence into Smart Dust. To realize Smart Dust, the military should conduct further research on antenna arrays and other possible solutions of antenna efficiency to offset future miniaturization by nanotechnology.

Beyond antenna effectiveness, combat environments, from cities to jungles, potentially impede line-of-sight (LOS) MEMS communications. Like cell phones, obstacles such as skyscrapers or trees hinder communications while power lines or other high-power emitting equipment potentially distort signals. Cell phone users simply outlast the distortion or reestablish LOS with the central hub. However, in contrast to cell phone communications, connectivity with a central hub is not mandatory for MEMS. Similar to computers on the Internet, one MEMS device may relay communications to other MEMS with the needed LOS contact. Again, this solution requires coordination processing and communication overhead affecting overall network efficiency. To achieve Smart Dust, military leaders should develop and research alternative solutions to minimize the effects of environmental obstacles.

Currently, the complexity of nanoscaled electromechanical integration prohibitively raises individual MEMS cost. Since Smart Dust demands millions of individual sensor nodes, the cost of a MEMS network skyrockets. However, research conducted in these technologies over the next 25 years will reduce costs. "Depending on the application, the total cost per sensor net node now ranges from \$50 to \$100. In a couple of years, look for prices to drop to about \$25."<sup>46</sup> In 2003, Kristof Pister, a past professor of electrical engineering at UC-Berkeley and scientist at Dust Inc., predicted costs of \$1 within 5 years.<sup>47</sup> Military investment in continued research and development in nanotechnology and MEMS over the next twenty years will reduce the cost to pennies on the dollar.

#### ETHICAL, ENVIRONMENTAL, AND BIOLOGICAL IMPLICATIONS

With any technology, the rigor of science demands an examination of the ethical, environmental, and biological impacts to society. Unfortunately, profit or ignorance occasionally hinders this review and betrays American's high degree of confidence in science.<sup>48</sup> In the case of enabling technologies looking to revolutionize the way Americans live, curtailing this examination could prove fatal to the development of the technology, our environment, or our society.

As one of the largest ethical roadblocks, the use of large-scale aggregate surveillance data to infringe on an individual's privacy threatens the development of persistent surveillance

15

applications. The intense fervor generated from the introduction of the US Patriot Act and Privacy Act demonstrates the high level of governmental and public interest regarding privacy. As Mr. Chaudhari of IBM Watson Center said best, "In the United States, for example, the right to privacy is protected by the law (the law of torts), enshrined in the constitution (first, fourth and fifth amendments), and underpinned by a philosophy (Adam Smith) generally embraced by the people."<sup>49</sup> Although the issue of privacy is complex, the US military should ensure the use of persistent surveillance data is for the public good, i.e. preventing another 9/11, rather than its detriment.

Current societal research in the US and the UK validates this concern. When presented with five potential nanotechnology risks, 32 percent of respondents chose "losing personal privacy to tiny new surveillance devices" as the most important risk in a 2004 US survey.<sup>50</sup> In a 2004 UK study, negative reactions to nanotechnology also included concerns for privacy, especially "nanotechnology enabled surveillance equipment to be made that was invisible to the naked eye."<sup>51</sup>

While past governmental invasions of privacy adversely affect perceptions, future positive actions and education prevent the buildup of negative perceptions. A decade ago, Britain installed sixty remote controlled video cameras in high crime areas within the city of King's Lynn reducing crime to 1.4 percent of previous levels. "Today, over 250,000 cameras are in place throughout the United Kingdom, transmitting round-the-clock images to a hundred constabularies, all of them reporting decreases in public misconduct."<sup>52</sup> While these cameras observed public places, mobile nanoscaled cameras or sensors risk invading private places. Fifty-five percent of Americans surveyed in a 2005 nanotechnology survey felt government regulation beyond voluntary safety regulations would be necessary to control the risks associated with nanotechnology.<sup>53</sup> While some privacy legislation exists, the military should advocate

refining privacy legislation on the monitoring of individuals, especially within private places. Additionally, the Department of Defense must examine laws of armed conflict and other regulations regarding the monitoring of individuals to determine Smart Dust's potential impact on them, especially in the wake of human rights concerns at Abu Grahib. Furthermore, since the acceptance of privacy-reducing technology depends on the public's perception of its benefit, the US government should measure public reaction to these technologies, especially nanotechnology, through sponsored surveys every five years to redirect research and public educational efforts.

In addition to ethical concerns, the environmental effects of nanotechnology could limit the development of persistent surveillance applications. The dispersal of non-biodegradable nanoscaled particles throughout an environment potentially alters the soil content, water sources, plants, and animal food pyramids. Additionally, depending on the coalescing characteristics of the particles, negative impacts to water treatment plants and other infrastructure will require repair during stability operations. If determined to alter nature's food chain, the long-term effects on the environment are disastrous.

The lack of current knowledge on the environmental consequences drives this fear.

"There remains virtually no data on the potential negative impacts of nanomaterials on the environment. Research into the ecotoxicology is urgently required."<sup>54</sup> Of the ten billion dollars spent on nanotechnology research in 2005, the United States and European Union spent only 39 million dollars on issues effecting the environment and health.<sup>55</sup> According to the United Nations Environment Programme, "...it is impossible to say with any certainty whether nanomaterials, which can be constructed from virtually any chemical structure, are similar to natural nanoparticles (which are mostly neutral or mildly toxic) or vastly different and therefore cause for concern."<sup>56</sup>

17

In addition, the military needs to research and identify the true environmental concerns for nanotechnology. In examining environmental concerns, researchers tend to assign the same causes and effects from micro-scaled particles to nanoscaled particles; however, this assumption may not be true. Since public companies fund about 50 percent of nanotechnology research, new policies may force companies into pursuing further research. "For example, late in 2006 the US Environmental Protection Agency announced that it would require manufacturers using nanosilver to produce scientific evidence that such usage will not harm waterways or public health."

With humans at the top of the food chain, the risk of ingesting nanosized particles, through consumption, inhalation, or skin absorbtion, concerns health professionals. When the US chooses to deploy weapons, it accepts the legal and economic responsibility for the unintended side effects of those weapons on both enemy and friendly forces. For example, the repercussions caused by the release of Agent Orange in Vietnam are a case in point. While the scientific consensus today dispels veteran's claims, comprehensive initial research by military or private companies may have prevented or mitigated the liability.<sup>57</sup>

Current research regarding the toxicity of nanoparticles suggests caution despite inconclusive results. Increased since 2004, toxicity research exposes microbes, fish, and rats to fullerenes and other nanoparticles. All of the current research shows some effect, such as damaged brain cells or adverse reactions within the lungs.<sup>58</sup> "Research indicated a plethora of problems associated with inhalation of ultra-fine and nanosized particles, including fibrosis or scarring, the abnormal thickening of brachioles, the presence of neutrofils (inflammatory cells), dead macrophages, and some chemical hitchhiking (metals and hydrocarbons)."<sup>59</sup> However, conclusions on the effects to humans were inconclusive because of exposure method, instillation rather than inhalation, or using uncommon nanoparticles.<sup>60</sup> In some cases, chemical means of

altering the surface of nanoparticles reduced toxicity levels.<sup>61</sup>

For these reasons, the military should fund or conduct more ingestion experiments to confirm, deny, or alleviate the toxic effects of nanotechnology. Unfortunately, the results of some research are not available to the public, "either for competitive reasons or because of the costs of preparing the data for publication in scientific journals."<sup>62</sup> Despite the possible consequences, corporations and government agencies need to release their independent research. According to the president of Japan's National Institute of Advanced Industrial Science and Technology (AIST), "...we can no longer limit the execution and evaluation of our research to a closed community of researchers but must open it up to society as a whole."<sup>63</sup> This type of opensource environment could foster collaborative research into potential solutions to ingestion problems. Furthermore, US agencies need to adopt regulations concerning the handling of nanoscaled particles, especially in manufacturing, until proven completely safe. While the National Science Foundation's FY 2008 budget request included 62.92 million to research environmental and social dimensions of nanotechnology, this amount only represents a 6% increase from FY 2007.<sup>64</sup> To realize Smart Dust, military leaders should support continued research into the societal consequences of these enabling technologies.

#### **FUTURE FORECASTING**

Along with the current state of nanotechnology, wireless sensor networks, and MEMS, military leaders must also understand the future and its influence on fusing these technologies into Smart Dust. According to a RAND futures study, "Various technologies—including biotechnology, nanotechnology (broadly defined), materials technology, and information technology—have the potential for significant and dominant global impacts by 2020."<sup>65</sup> To realize these impacts and the possibility of Smart Dust in 2025, each technology must mature and

overcome its limitations.

The exploratory forecasting process, similar to the military's Joint Operational Planning Process, steps futurists through the definition and analysis of the future to determine the potential positive or negative growth or impact on an item of interest. According to Jerome Glenn, "Exploratory forecasting explores what is possible regardless of what is desirable."<sup>66</sup> Exploration of these potential futures supports present planning and, ultimately, leads to better decisions by our military leaders. As Hall says, "the question of when devolves into the questions of how much effort is put into which pathways."<sup>67</sup> Through inference, analysis of the possible futures yields predictions regarding the long-term growth of these technologies and, more importantly, actions necessary to expedite their potential growth. Within the context of a specific application, exploratory forecasting pinpoints specific recommendations for leaders to follow to achieve Smart Dust by 2025.

One method of exploratory forecasting is scenario building, which provides the futurist a potential range of future scenarios to explore. "The purpose of scenarios is to systematically explore, create, and test both possible and desirable future conditions. Exploratory or descriptive scenarios describe events and trends as they could evolve based on alternative assumptions on how these events and trends may influence the future."<sup>68</sup> The key to successful scenario building is identification of the driving factors encompassing the uncertainty of the future in 2025.

In earlier Blue Horizons research, Myers and Luker presented eight possible future scenarios for 2025 involving state and non-state actors. Analysis of the future concerning state actors highlighted *type of warfare* and *technology focus* as key driving factors. Combinations of these factors yielded four state actor scenarios: David & Goliath, The Phantom Menace, Wishful Thinking, and Information Immobilization (Fig 5).<sup>69</sup> In the non-state actor scenarios, combinations of *location* and *technology focus*, as driving factors, produced Guerrillas in the

Mist, Blind Battlefield, Cyber 9/11, and American Insurgency (Fig 6).<sup>70</sup> Appendix A contains a brief description of each scenario. The next section explores these scenarios to determine positive and negative impacts, potential use, and recommendations to achieve Smart Dust.

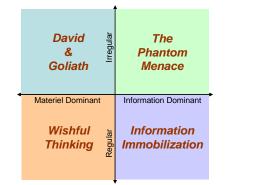




Figure 5: State Actor Scenarios Reprinted from Luker

#### **Exploring State Scenarios**



According to Myers' analysis, a state actor's preference for conflict location and technological nature shapes the future threat environment with the United States. Examining these scenarios highlights the use, development, and limitations on the employment of Smart Dust against state actors.

In an Information Immobilization future, the information dominance of the opponent mandates US' development and use of persistent surveillance technology like Smart Dust to negate their potential asymmetric advantage. Smart Dust allows US strategists to leverage a near-instantaneous regional common operating picture (COP) to direct attacks or counter actions faster or at the same speed of the enemy. Additionally, a localized COP supports regular warfare with a complete intelligence picture of friendly, enemy, and civilian personnel and ground equipment. Smart Dust, coupled with the future precision of US combined arms, minimizes collateral damage to both personnel and buildings.

Prior to the occurrence of this scenario in 2025, adversaries will fuel the development of

the discussed technologies, especially wireless networks and nanotechnology. While building their information dominance, enemy state actors will strive to create an asymmetrical advantage by increasing the speed and processing power of their computers and networks. As Moore's law supports, increases in information system performance directly relates to the decrease in size of semiconductors, transistors, and other electronic components. In our globalized world, other states' investment to improve performance through miniaturization techniques will indirectly enhance US development of these technologies.

However, information-dominant states without strong US ties will research counter technologies or hide their own persistent surveillance developments, especially as an adversarial relationship builds. While broad electromagnetic pulses on foreign soil renders enemy assets equally ineffective, judicious use of regional jamming could reduce US access to Smart Dust at critical times. If jamming results in significantly opportunistic events, enemy forces will exercise this asymmetric advantage decisively. To minimize this vulnerability, Smart Dust should exercise alternate methods of communicating rather than radio frequency as future warfare becomes even more dependant on accurate and reliable intelligence.

In the Phantom Menace scenario, the timely and effective use of ISR information will dictate the tempo and outcome of irregular warfare against an information-dominant opponent. Smart Dust applied regionally over an operations area or locally on known offensive or defensive targets will yield timely information if accomplished prior to a conflict. This surveillance and reconnaissance data will aid analysts in the United States and soldiers abroad with tracking, monitoring, and, most importantly, predicting enemy attacks. If irregular attacks do occur, current sensor information fed directly to ground forces, such as enemy numbers or location, will support effective offensive operations. Defensively, Smart Dust enables quick notification of a CBRNE event to protect US forces against irregular attacks.

Like other future scenarios framed by information dominance, an enemy state's investment in information dominant applications accelerates the growth of enabling technologies; however, enemies in Phantom Menace will tailor their research into non-traditional domains like space and cyber. Despite their domain direction, their research will lead towards miniaturization efforts to gain computer speed and performance. Additionally, research into specific space applications will also spur additional sensor and antenna research potentially extending the range and speed of smart dust communications.

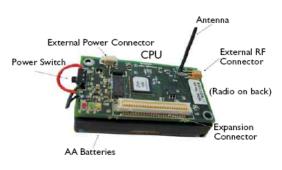
Based on this direction of growth, an information-dominant enemy conducting irregular warfare will attempt to nullify US persistent surveillance advantages through non-traditional means such as space anti-satellite or cyber attacks. Smart dust's communication and collection hub vulnerabilities are likely targets for irregular attacks. Information-dominant adversaries could inject incorrect information into the network, causing military leaders to misdirect forces, order inappropriate actions, etc. Additionally, electromagnetic jamming and direct attacks against network radio frequency communications remain effective in this scenario unless Smart Dust contains appropriate counters.

In the Wishful Thinking scenario, Smart Dust coupled with US effects-based networkcentric warfare acts as a force multiplier, increasing US asset effectiveness against a materialdominant opponent conducting regular warfare. This ideal scenario showcases the benefits of coupling Smart Dust with regular warfare theoretical models to gain insight on the enemy. As Spencer Abbot wrote regarding Warden's parallel warfare five-ring model, "...the understanding and use of a conceptual model is not a satisfactory substitute for specific knowledge of the state or organization that the United States seeks to influence and is only useful if a thorough knowledge of the targeted system is applied to the theoretical model."<sup>71</sup> Similar to the benefits received from GPS or space-based technology, the ubiquitous and persistent nature of Smart Dust provides real-time intelligence preparation of the battlespace (IPB). Instantly updated upon request, this "sight picture" of both enemy and friendly forces supports all levels of warfare throughout the range of military operations.

The materially minded enemy's desires for stronger, lighter materials and faster, cheaper electronics will hasten mote durability and network communication speed while decreasing cost. The increased durability improves Smart Dust's survivability in rugged and wet environments and supports flexible antennas increasing transmission range. Minimizing some of Smart Dust's weaknesses, faster electronics boost transmissions through quicker computer processors and coordination software enabling improved communication reliability and speeds. Overall, material research will improve production methods lowering a mote's individual cost stretching US defense dollars.

Despite enemy attempts in this scenario to reduce US combat effectiveness by negating Smart Dust, the inexpensive cost of motes and durability of wireless networks could protect a US information advantage. In this scenario, material-dominant adversaries could target the persistent surveillance network as a US center of gravity. Deployed over their land, the network is highly susceptible to attack. However, if the enemy destroys an area of motes, the low purchase cost allows for easy replacement. Furthermore, like the Internet, the design of wireless networks allows for continued operation despite the losses of some nodes.

In the David and Goliath scenario, US Smart Dust employment will center on monitoring an adversary's assets to determine the direction and type of irregular warfare, such as cyber, space, insurgent, or terrorist attacks. Depending on the type of embedded sensors, dispersal of Smart Dust over known enemy locations will aid in collecting visual, measurement, or signal intelligence to determine enemy intentions. In 2003, Dr Akos Ledeczi of Vanderbilt University, with funding from DARPA, successfully used over 200 MICA2 motes (Fig 6) in an urban



environment to locate the position of a gun shot within two seconds with an average accuracy of one meter.<sup>72</sup> As opposed to observing nuclear, biological, or chemical testing from space, Smart Dust supports a lower level of granularity of information regarding readiness levels of adversaries. This improved data

Figure 7: Anatomy of MICA2 Reprinted from Hall

will enhance US military officials' decision-making process and offers an earlier decision opportunity to conduct prevention or preemption efforts against irregular warfare attacks.

As in other material-dominant scenarios, demand for better materials and faster electronics contributes to the development of nanotechnology and MEMS, enhancing US capability to sense and counter irregular attacks. In terms of growth enhancement, this scenario parallels the Wishful Thinking scenario.

To hinder Smart Dust employment, enemies could leverage their material-dominance to overwhelm or distract US forces using irregular warfare. For example, an enemy could send multiple decoys through a Smart Dust-seeded area causing multiple race conditions to overwhelm the coordination software and reduce the reliability of the sensor network. If successful, this tactic potentially hides the true intention of the movement. Additionally, other distraction tactics, similar to operations at Calais prior to the US invasion of Normandy during WWII, could divert US attention to data from wireless networks in insignificant regions of the operational area. While the enemy could hinder Smart Dust with other methods, the reliability and performance of Smart Dust must resist these types of tactics.

In all state scenarios, enemy states contribute to the growth of nano-, wireless network, and MEMS technology in achieving their respective material or information dominance. While surmountable, this dominance provides avenues of attack to weaken Smart Dust's effectiveness. The US must develop strategies and invest in technological counters to protect this asymmetric advantage, especially against a material-dominant adversary. In those scenarios against an information-dominant opponent, the US must continue to wield their material-dominant assets in advantageous ways to succeed. With the insights from this future forecast, the continued development of Smart Dust should prevent state adversaries from achieving information dominance relative to the US.

#### **Exploring Non-State Scenarios**

In the 2006 Quadrennial Defense Review, Donald Rumsfeld characterized the era of transformation as a shift in emphasis. "In this era, characterized by uncertainty and surprise, examples of this shift in emphasis include: from nation-state threats – to decentralized network threats from non-state enemies, from conducting war against nations – to conducting war in countries we are not at war with (safe havens), from an emphasis on ships, guns, tanks and planes – to focus on information, knowledge and timely, actionable intelligence."<sup>73</sup> Myers translated Rumsfeld's vision into warfare scenarios against non-state actors framed by geographic location and technological focus: Cyber 911, Blind Battlefield, American Insurgency, and Guerillas in the Mist. An examination of the use and growth of persistent surveillance applications such as Smart Dust within these scenarios highlights recommendations for senior leaders.

In a Cyber 911 future, the United States will need ISR data on the non-state actor executing information-dominant warfare, such as cyber attacks, on our soil. Possible US applications of Smart Dust include tracking cyber insurgents, monitoring key infrastructure, and consequence management operations. Depending on the type of sensor employed, dispersal of a wireless sensor network on the actual bodies, vehicles, or computer equipment of cyber

26

insurgents could provide vital tactical information, such as location and numbers, to support counterinsurgency operations. These networks could protect key hardened information infrastructure by notifying homeland defense personnel of unauthorized entrance or access. While wireless sensor networks provide little protection regarding virtual aspects of a cyber attack, modification of the software aspects of the wireless network, specifically the coordination software, could coordinate and present virtual situational awareness about nodes in the US information network.

Fortunately, a non-state adversary focused on information dominance fosters the growth of Smart Dust for the United States by funding other information-technology research. Without significant manufacturing infrastructure, non-state actors must purchase information technologies or equipment from companies or sponsoring nations. In the spirit of capitalism, companies will need to invest money into research to produce competitive products. With globalization increasing in the future, companies with only a monetary allegiance to the non-state actor could share or sell this technology or equipment to other states. While nations could institute non-proliferation of certain technologies like the US barred F-22 foreign sales, an information-focused enemy could indirectly contribute to the future development of Smart Dust.

On the other hand, enemy attacks on US soil spotlights limitations of Smart Dust, specifically its reliance on network connectivity and the public's willingness to surrender parts of their privacy. Cyber attacks on our information infrastructure threaten the reliability of wireless networks supporting Smart Dust. Unless motes contain electromagnetic protection, electromagnetic pulses could destroy vast areas of the Smart Dust network. Additionally, once the United States utilizes Smart Dust, the cyber terrorist could undermine its use with an information operations campaign exploiting the public's privacy concerns. To maintain Smart Dust's asymmetric advantage, the United States needs to mount an effective information

operations campaign now and in the future to educate the public on the benefits of Smart Dust to their way of life.

In Blind Battlefield, the United States sacrifices not only information dominance but also familiarity with the local environment by combating a non-state actor on foreign soil. With Smart Dust, US military forces wield a mobile intelligence-gathering force capable of producing localized information superiority to conduct offensive operations. Additionally, "in combating an enemy that seeks to hide in the shadows and strike without warning, information becomes one of America's most important defenses."<sup>74</sup> Without a unique US persistent surveillance application like Smart Dust, an information-dominant opponent maintains a critical asymmetric advantage over the US within this type of scenario.

Similar to other information dominant scenarios, adversary actions will support the growth of the enabling technologies within Blind Battlefield through investment in their own technological research. This research will center on the enabling technologies that contribute to information-focused warfare such as nanotechnology and wireless sensor networks.

However, jamming and indiscriminate ISR operations on foreign soil potentially hinders the use of Smart Dust within Blind Battlefield. Since non-state actors typically operate outside of national and international law, an information-dominant adversary ignoring privacy or environmental regulations could incite outcries from the host public. Collaterally, these actions could prevent the US from utilizing Smart Dust on foreign soil for fear of sacrificing credibility and legitimacy. If employed, an information-dominant opponent could utilize blanket jamming over Smart Dust's range of frequencies to hide their operations within surveillance shadows. Again, military leaders must develop frequency-agile Smart Dust to defeat enemy jamming efforts.

In American Insurgency, Smart Dust's use in the US readily delivers persistent localized

information superiority from an already established communication infrastructure of telephone and wireless networks. According to the Army's Counterinsurgency Manual 3-24, "the function of intelligence in COIN is to facilitate understanding of the operational environment, with emphasis on the populace, host nation, and insurgents."<sup>75</sup> Smart Dust offers a low observable ISR asset providing detailed information on the insurgents and the US populace.

Despite contributing the least to the growth of Smart Dust, American Insurgency stimulates Smart Dust development when a material-dominated non-state actor purchases equipment through private companies or organizations. According to sound economic principles, this funding to acquire current kinetic and non-kinetic weapons and equipment eventually funds research into the next generation of kinetic and non-kinetic weapons. Since reduction in size improves performance by minimizing many engineering trade-offs, nanotechnology and MEMS are profitable avenues for future research and development. This research, if shared in an open environment, accelerates US creation of Smart Dust.

Yet, regardless of good intentions, the use of Smart Dust on American soil will exacerbate the growing privacy issue and provide insurgents a propaganda tool to wield in US media outlets. Unless the US government provides assurances against unethical use through a transparent system of checks and balances, insurgents will have a weakness to exploit. However, the low profile of Smart Dust over other persistent surveillance applications such as Predator or Global Hawk, especially in the dense airspace of the United States, offers some operational benefits to both the military and the public.

For Guerillas in the Mist, the use of Smart Dust minimizes the home field advantage of the material-oriented non-state actor by providing accurate and reliable information on the foreign population, such as movement, and battlespace, such as building layouts. As in Blind Battlefield, Smart Dust provides a granularity and fidelity unavailable in current airborne ISR platforms to pinpoint movements of a material-minded non-state actor. Additionally, the information from Smart Dust complements these other platforms allowing airpower planners to more accurately conduct effects-based operations.

In similar fashion to American Insurgency, this scenario offers a low benefit of growth to Smart Dust but receives the greatest benefit from its existence. As evidenced from our lack of good human intelligence (HUMINT) in Iraq and Afghanistan, developing human relationships with non-state actors on foreign soil is difficult. Smart Dust, configured with relevant sensors, enhances the intelligence provided by HUMINT.

However, unless improved power supplies and antennas increase Smart Dust's effective radiating power, material-dominant enemies could negate its effectiveness through area jamming. While not guaranteed, non-state actors might hesitate to utilize area jamming for fear of reducing their own wireless communications network or the network of their host nation. As mentioned earlier, Smart Dust must demonstrate jam-resistant communications.

#### **RECOMMENDATIONS AND CONCLUSION**

The broad nature of these scenarios reflects the range of possible futures in which the United States must operate in 2025. To maintain our information dominance, the US, and specifically the military, must continue to pursue revolutionary persistent ISR applications such as Smart Dust through increased funding, focus, and, most important, policies. "Over the next several decades, choices in policy and strategy will have far more to say about the future of U.S. air power than will exciting technological possibilities, a military tradition of success, or skilled and dedicated people."<sup>76</sup> While Gray downplays the influence of technology and people, his assertion about the influence of policy stands clear.

To support the creation of future-shaping policy, Appendix B lists the specific

recommendations mentioned throughout this paper in priority order. These recommendations represent the initial strategic steps for the United States to grow and develop Smart Dust. While private development of these technologies or undiscovered governmental policy decisions could fulfill some of these recommendations in the near future, military leaders should aggressively pursue the remaining ones to realize Smart Dust.

Since this paper does not cover all issues regarding Smart Dust's development, use, and employment in the future, further research is necessary, specifically in the areas of intelligence analysis and dependence. For example, the processing of the enormous volume of information available from Smart Dust could possibly overwhelm and paralyze the military rather than inform and aid. A method of filtering, analyzing, and presenting the information must be researched and developed to integrate Smart Dust into the complete intelligence picture. Furthermore, as alluded in this paper, the dependence of military leaders on accurate and actionable intelligence will only increase with the creation of Smart Dust. Future research should explore the possibility of overdependence on intelligence by military leaders and, if exploited by an enemy, the ramifications to our conduct of warfare.

In conclusion, Smart Dust is achievable by 2025 based on the current state of the enabling technologies and the potential future scenarios for the United States. As a future persistent surveillance solution for battlespace awareness, homeland defense, and WMD identification, Smart Dust offers the intelligence advantages of ubiquity, flexibility, timeliness, and persistence to military leaders, planners, and operators. For the future, Smart Dust represents a revolutionary leap in persistent surveillance and produces an informational asymmetric advantage for whomever, friend or foe, possesses it.

31

# **APPENDIX A: Summary of BLUE HORIZON Scenarios**

SCENARIO DESCRIPTIONS	
STATE ACTORS	
Information Immobilization	A state actor attacks the United States leveraging sensor fusion and networks to enhance their regular warfare capability.
The Phantom Menace	A state actor attacks the United States using irregular warfare with information-oriented weapons through the electronic or electromagnetic spectrum.
Wishful Thinking	A state actor attacks the United States in a large force-on- force conflict using regular warfare with traditional material- oriented weapons, such as airplanes, tanks, and ships.
David & Goliath	A state actor attacks the United States using irregular warfare with material-oriented weapons to conduct large-scale information operations campaigns.
NON-STATE ACTORS	
<i>Cyber 9/11</i>	A non-state actor attacks the United States from our soil using information-oriented weapons to destroy US information infrastructure.
Blind Battlefield	A non-state actor attacks the United States from foreign soil using information-oriented weapons to minimize US intelligence, command, and control capabilities.
American Insurgency	A non-state actor attacks the United States from our soil using material-oriented weapons such as chemical, biological, radiological, nuclear, or explosive bombs to reduce US public will.
Guerillas in the Mist	A non-state actor attacks the United States from foreign soil using material-oriented weapons to reduce world opinion

### **APPENDIX B: Prioritized Recommendations**

## PRIORITIZED RECOMMENDATIONS

1) Support and fund research into nanotechnology measurement and manufacturing

2) Continue funding research and manufacture of nanoscaled sensors

3) Develop new antennas capable of larger gains to offset the reduction in size

4) Support and fund research to nanoscaled power supplies

5) Encourage and fund research into alternative methods to increase the transmission reliability of wireless networks

6) Encourage and fund research into creative solutions to the race conditions of networks

7) Support further research into the tradeoffs between false alarms and network latency

8) Develop and research alternative solutions to minimize the effects of environmental obstacles

9) Ensure the use of persistent surveillance data is for the public good rather than its detriment

10) Measure public reaction to these technologies, especially nanotechnology, through sponsored surveys every five years to redirect research and public educational efforts

11) Research and identify the true environmental concerns for nanotechnology

12) Educate the public on the benefits of Smart Dust to their way of life

13) Develop frequency-agile Smart Dust to defeat enemy jamming efforts

14) Fund or conduct more ingestion experiments to confirm, deny, or alleviate the toxic effects of nanotechnology

#### **Bibliography**

- Abbot, Spencer, ed. *Air Power Strategy and the Problem of Coercion*. Edited by Stephen Wrange, Immaculate Warfare. Westport: Praeger Publishers, 2003.
- Ackerman, Robert. "New Flight Plan for Air Force Intelligence." *Signal Magazine*, 2 Mar 2007 2007, 2.
- Alda, Javier, José M. Rico-GarcÃ-a, José M. LÃ<sup>3</sup>pez-Alonso, and Glenn Boreman. "Microand Nano-Antennas for Light Detection." *Egyptian Journal of Solids* 28, no. 1 (2005): 1-13.
- Allan, Roger. "Wireless Sensors Land Anywhere and Everywhere." *Electronic Design* 53, no. 16 (2005): 65-70.
- Ananthaswamy, Anil. "March of the Motes." New Scientist 179, no. 2409 (2003): 26-31.
- Arora, A., P. Dutta, S. Bapat, V. Kulathumani, H. Zhang, V. Naik, V. Mittal, H. Cao, M. Demirbas, M. Gouda, Y. Choi, T. Herman, S. Kulkarni, U. Arumugam, M. Nesterenko, A. Vora, and M. Miyashita. "A Line in the Sand: A Wireless Sensor Network for Target Detection, Classification, and Tracking." *Computer Networks* 46, no. 5 (2004): 605-34.
- ATC/DOT, HQ. "Afp 51-45, Electronic Combat Principles." edited by Department of Defense, 1987.
- "Background Check with Photoelectric Sensors." Packaging Digest 42, no. 5 (2005): 10-11.
- Bailey, Dennis. The Open Society Paradox: Why the Twenty-First Century Calls for More Openness--Not Less. 1st ed. Vol. 1. Dulles: Brassey's, 2004.
- Beach, Tarre. "Building Blocks
- Building Blocks." Wireless Review 16, no. 23 (1999): 22.
- Beermann-Curtin, Sharon. "Micro Power Sources." DARPA, http://www.darpa.mil/dso/thrust/matdev/mps.htm.
- Berube, David M. *Nano-Hype: The Truth Behind the Nanotechnology Buzz.* 1st ed. Amherst: Prometheus Books, 2006.
- Board, National Science. "Science and Engineering Indicators 2006." 521. Arlington: National Science Board, 2006.
- Brain, Marshall. "How Motes Work." http://computer.howstuffworks.com/mote.htm.
- Brin, Dr David. The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom? Reading: Addison-Wesley, 1998.
- Broad, William J. "A Web of Sensors, Taking Earth's Pulse." New York Times 154, no. 53210 (2005): F1-F4.
- California-Berkeley, University of. "29 Palms Fixed/Mobile Experiment." <u>http://www-bsac.eecs.berkeley.edu/~pister/29Palms0103/</u>.
- Chatzigiannakis, Joannis, Tassos Dimitriou, Marios Mavronicolas, Sotiris Nukoletseas, and Paul Spirakis. "A Comparative Study of Protocols for Efficient Data Propagation in Smart Dust Networks." *Parallel Processing Letters* 13, no. 4 (2003): 615-27.
- Chaudhari, P. "Future Implications of Nanoscale Science and Technology: Wired Humans, Quantum Legos, and an Ocean of Information." In *Societal Implications of Nanoscience and Nanotechnology*, edited by Engineering Nanoscale Science, and Technology Subcommittee, 4. Arlington: National Science and Technology Council, 2001.
- Chemical, DOW. "Background on Agent Orange." <u>http://www.dow.com/commitments/debates/agentorange/background.htm</u>.

- Clausewitz, Carl von, ed. On War. Edited by Michael Howard. Princeton: Princeton University Press, 1989.
- Coll, Steve. "The Unthinkable; a Reporter at Large." *The New Yorker*, Mar 12, 2007.

Correll, John T. "Igloo White." Air Force Magazine, November 2004.

- "Darpa Sensit Demo." University of California-Berkeley, http://basics.eecs.berkeley.edu/sensorwebs/29palms/.
- Defense, Department of. "Quadrennial Defense Review Report." 92. Washington DC: Department of Defense, 2006.
  - ——. "Strategy for Homeland Defense and Civil Support." edited by Department of Defense, 46, 2005.
- Development, Organisation for Economic Co-Operation and. "Space 2030: Exploring the Future of Space Applications." edited by OECD Publications Service, 239. Paris: Organisation for Economic Co-Operation and Development, 2004.

—. "Space 2030: Tackling Society's Challenges." edited by OECD Publications Service, 332. Paris: Organisation for Economic Co-Operation and Development, 2005.

- Eisenberg, Anne. "Dust That May Have Eyes and Ears." *New York Times* 149, no. 51654 (1999): G12.
- Feder, Barnaby J. "Study Raises Concerns About Carbon Particles." *New York Times* 153, no. 52803 (2004): C5-C5.

Forbes. "Nanotech Report." edited by Josh Wolfe, 8. New York, 2003.

- Foundation, National Science. "Fy 2008 Budget Request to Congress." National Science Foundation, <u>http://www.nsf.gov/about/budget/fy2008/toc.jsp</u>.
- Frenzel, Louis E. "Smarter Antennas Breed Success in Wireless Arena
- Smarter Antennas Breed Success in Wireless Arena." Electronic Design 53, no. 7 (2005): 48-52.
- Glenn, Jerome C. "Future Research Methodology." Place Published: AC/UNU Millennium Project, 1996.

Gorman, J. "Miniature Motor." Science News Vol 164, no. Issue 4 (2003): 2.

- Gray, Colin S. "The Advantages and Limitations of Air Power." *Explorations in Strategy* (1996): 55-82.
- Group, Interagency Working. "Nanotechnology: Shaping the World Atom by Atom." edited by Interagency Working Group, 12. washington DC: National Science and Technology Council, 1999.

—. "National Nanotechnology Initiative: Leading to the Next Industrial Revolution." edited by Committee on Technology, 100. Washington D.C.: National Science and Technology Council, 2000.

Hall, J. Storrs. *Nanofuture: What's Next for Nanotechnology*. Edited by Prometheus Books. 1st ed. Amherst, 2005.

- He, Tian. "Energy-Efficient Surveillance System Using Wireless Sensor Networks." University of Virginia, 2004.
- Hill, Jason, Mike Horton, Ralph Kling, and Lakshman Krishnamurthy. "The Platforms Enabling Wireless Sensor Networks." *Communications of the ACM* 47, no. 6 (2004): 41-46.

Hoffman, Thomas. "Smart Dust." Computerworld 37, no. 12 (2003): 32.

Huang, Gregory T. "Casting the Wireless Sensor Net." Technology Review 106, no. 6 (2003): 50.

- Initiative, Committee for the Review of the National Nanotechnology. "Small Wonders, Endless Frontiers." edited by National Academy Press, 57. Washington D.C.: National Research Council, 2002.
- Intel. "Instrumenting the World: An Introduction to Wireless Sensor Networks." 6: Intel, 2004.

- Johnson, R. Colin. "Smart Dust Made to 'Escort' Molecules to Sensors." *Electronic Engineering Times*, no. 1348 (2004): 39-39.
- "Joint Intelligence." In Joint Publication (JP) 2-0, edited by Department of Defense, 2006.
- Keller, John. "The Nanotechnology Winter." *Military & Aerospace Electronics* 15, no. 12 (2004): 1-6.
- Kloeppel, Kirk M. "Pesky Critters." In *Netted Bugs and Bombs: Implications for 2010*, edited by Marsha J Kwolek, 33. Maxwell AFB: Center for Strategy and Technology, 2005.
- Kurzweil, Ray. The Singularity Is Near. New York: Penguin Group, 2005.
- Laboratory, Air Force Research. Focused Long Term Challenges: Integrated Capability Planning Process Status Update, 2006.
- Ledeczi, Akos. "Shooter Localization in Urban Terrain." Institute for Software Integrated Systems,

http://www.isis.vanderbilt.edu/projects/nest/documentation/Vanderbilt\_NEST\_ShooterLoc.ppt.

- Levanon, Nadev. Radar Principles. New York: John-Wiley & Sons, 1988.
- Luker, Joel J. "State Actor Threats in 2025." Air University, 2007.
- Macoubrie, Jane. "Informed Public Perceptions of Nanotechnology and Trust in Government." Woodrow Wilson Internatonal Center for Scholars, 2005.
- Masami, Matsuda, ed. *Nanotechnologies and Society in Japan*. Edited by Geoffrey Hunt and Michael Mehta, Nanotechnology: Risk, Ethics, and Law. Sterling: Earthscan, 2006.
- Mills, Kirsty, ed. *Nanotechnologies and Society in the USA*. Edited by Geoffrey Hunt and Michael Mehta, Nanotechnology: Risk, Ethics, and Law. Sterling: Earthscan, 2006.
- Myers, James W. "Nonstate Actor Threats in 2025: Blue Horizon Scenarios." Air University, 2007.
- "Nanotechnology Delivers Military Power." *Military & Aerospace Electronics* 16, no. 5 (2005): 34-37.
- Northrup-Grumann. "Global Hawk Overview." Northrup-Grumann, <u>http://www.northropgrumman.com/unmanned/globalhawk/overview.html#History</u>.
- Opperman, Ian, Lucian Stoica, Alberto Rabbachin, Zack Shelby, and Jussi Haapoloa. "Uwb Wireless Sensor Networks: Uwen -- a Practical Example." *IEEE Communications Magazine* 42, no. 12 (2004): s27-s32.
- Petraeus, David H. "Fm 3-24: Counterinsurgency." edited by Department of the Army, 282: Department of the Army, 2006.
- Research, BMRB Social. "Nanotechnology: Views of the General Public." edited by The Royal Society and Royal Academy of Engineering Nanotechnology Working Group, 68: The Royal Society and Royal Academy of Engineering Nanotechnology Working Group, 2004.
- Rhea, John. "Defying the Gods of Physics." *Military & Aerospace Electronics* 11, no. 7 (2000): 7.
  - ——. "Mems Guidance Devices Derived from Auto Industry Planned for Missiles." *Military* & *Aerospace Electronics* 11, no. 12 (2000): 7.
- ————. "Mems: Following in the Footsteps of the Internet?" *Military & Aerospace Electronics* 11, no. 9 (2000): 8.

Ross, Philip E. "Tiny Toxins?" Technology Review, May/Jun 2006 2006, 66-69.

Russell, Richard. "The National Nanotechnology Initiative: Supplement to the President's 2007 Budget." edited by Engineering Subcommittee on Nanoscale Science, and Technology, 61. Washington DC: National Science and Technology Council, 2006. Service, Robert F. "Borrowing from Biology to Power the Petite." *Science* 283, no. 5398 (1999): 27.

- Silberglitt, Richard. "The Global Technology Revolution 2020, in-Depth Analyses: Bio/Nano/Materials/Information Trends, Drivers, Barriers, and Societal Implications." edited by RAND Corporation, 281. Pittsburgh: RAND, 2006.
- Society, The Royal. "Potential Health, Environmental, and Societal Impacts of Nanotechnologies." 15. London: Science Council of Japan, 2005.
- Spangler, Todd. "Wireless Sensor Networks." Baseline, no. 49 (2005): 74-74.
- Staff, Joint. "JP 2-01, Joint and National Intelligence Support to Military Operations." edited by Department of Defense, 297, 2004.
- Staff, Joint Chiefs of. "National Military Strategy of the United States of America." edited by Joint Staff, 24. Washington DC: Joint Chiefs of Staff, 2004.
- UNEP. "Emerging Challenges: Nanotechnology and the Environment." In *Global Environment Outlook Yearbook*, 88, 2007.
- Vandermolen, LCDR Thomas D. "Molecular Nanotechnology and National Security." *Air and Space Power Journal* Fall 2006, no. Fall 2006 (2006): 2.
- Warneke, Brett, and Matt Last. "Smart Dust: Communicating with a Cubic-Millimeter Computer. (Cover Story)." *Computer* 34, no. 1 (2001): 44.
- Watts, Daniel. "Particle Surface Characteristics May Play an Important Role in Phytotoxicity of Alumina Nanoparticles." *Toxicology Letters* 158, no. 2 (2005): 122-32.
- Weaver, Bill. "A Sensor in Every Pot." Scientific Computing and Instrumentation, no. April (2002): 16, 61.
- Webb, Warren. "Smart-Dust Designers Deliver Dirt-Cheap Chips." EDN 48, no. 26 (2003): 1.
- Wood, Stephen. "The Social and Economic Challenges of Nanotechnology." 54. Swindon: The Economic and Social Research Council, 2003.
- Wynne, Michael W. "'Spherical Situation Awareness' Will Be Key to Global Security." *Aviation Week & Space Technology* 166, no. 3 (2007): 444.

#### **Endnotes**

<sup>9</sup> William J. Broad, "A Web of Sensors, Taking Earth's Pulse," New York Times 154, no. 53210 (2005).

<sup>10</sup> University of California-Berkeley, "29 Palms Fixed/Mobile Experiment," http://www-

bsac.eecs.berkeley.edu/~pister/29Palms0103/.

<sup>11</sup> Michael W Wynne, "'Spherical Situation Awareness' Will Be Key to Global Security," Aviation Week & Space Technology 166, no. 3 (2007).

<sup>12</sup> Robert Ackerman, "New Flight Plan for Air Force Intelligence," Signal Magazine, 2 Mar 2007 2007.

<sup>13</sup> Air Force Research Laboratory, Focused Long Term Challenges: Integrated Capability Planning Process Status *Update* (2006). <sup>14</sup> Joint Staff, "JP 2-01, Joint and National Intelligence Support to Military Operations," ed. Department of Defense

(2004).

<sup>15</sup> Joint Chiefs of Staff, "National Military Strategy of the United States of America," ed. Joint Staff (Washington DC: Joint Chiefs of Staff, 2004).

<sup>16</sup> Department of Defense, "Strategy for Homeland Defense and Civil Support," ed. Department of Defense (2005). 17 -, "Quadrennial Defense Review Report," (Washington DC: Department of Defense, 2006).

<sup>18</sup> Steve Coll, "The Unthinkable; a Reporter at Large," *The New Yorker*, Mar 12, 2007.

<sup>19</sup> Staff, "JP 2-01, Joint and National Intelligence Support to Military Operations."

<sup>20</sup> David M. Berube, Nano-Hype: The Truth Behind the Nanotechnology Buzz, 1st ed. (Amherst: Prometheus Books, 2006).

<sup>21</sup> LCDR Thomas D. Vandermolen, "Molecular Nanotechnology and National Security," Air and Space Power Journal Fall 2006, no. Fall 2006 (2006).

<sup>22</sup> J. Storrs Hall, *Nanofuture: What's Next for Nanotechnology*, ed. Prometheus Books, 1st ed. (Amherst: 2005). <sup>23</sup> Ibid.

<sup>24</sup> Warren Webb, "Smart-Dust Designers Deliver Dirt-Cheap Chips," *EDN* 48, no. 26 (2003).

<sup>25</sup> Sharon Beermann-Curtin, "Micro Power Sources," DARPA, http://www.darpa.mil/dso/thrust/matdev/mps.htm.

<sup>26</sup> Hall, Nanofuture: What's Next for Nanotechnology.

<sup>27</sup> J Gorman, "Miniature Motor," Science News Vol 164, no. Issue 4 (2003).

<sup>28</sup> Robert F. Service, "Borrowing from Biology to Power the Petite," *Science* 283, no. 5398 (1999).

<sup>29</sup> Ananthaswamy, "March of the Motes."

<sup>30</sup> Todd Spangler, "Wireless Sensor Networks," *Baseline*, no. 49 (2005).

<sup>31</sup> Joannis Chatzigiannakis et al., "A Comparative Study of Protocols for Efficient Data Propagation in Smart Dust Networks," Parallel Processing Letters 13, no. 4 (2003).

<sup>32</sup> Ananthaswamy, "March of the Motes."

<sup>33</sup> Tian He, "Energy-Efficient Surveillance System Using Wireless Sensor Networks" (University of Virginia, 2004).

<sup>34</sup> Gregory T. Huang, "Casting the Wireless Sensor Net," *Technology Review* 106, no. 6 (2003).

<sup>35</sup> Ibid.

<sup>36</sup> Ananthaswamy, "March of the Motes."

<sup>37</sup> He, "Energy-Efficient Surveillance System Using Wireless Sensor Networks".

<sup>38</sup> Ibid.

<sup>39</sup> Nadev Levanon, *Radar Principles* (New York: John-Wiley & Sons, 1988).

<sup>40</sup> John Rhea, "Mems: Following in the Footsteps of the Internet?," *Military & Aerospace Electronics* 11, no. 9 (2000). <sup>41</sup> Intel, "Instrumenting the World: An Introduction to Wireless Sensor Networks," (Intel, 2004).

<sup>42</sup> Jason Hill et al., "The Platforms Enabling Wireless Sensor Networks," Communications of the ACM 47, no. 6 (2004).

<sup>3</sup> Marshall Brain, "How Motes Work," http://computer.howstuffworks.com/mote.htm.

<sup>&</sup>lt;sup>1</sup> Northrup-Grumann, "Global Hawk - Overview," Northrup-Grumann,

http://www.northropgrumman.com/unmanned/globalhawk/overview.html#History.

<sup>&</sup>lt;sup>2</sup> Carl von Clausewitz, ed., On War (Princeton: Princeton University Press, 1989).

<sup>&</sup>lt;sup>3</sup> "Joint Intelligence," in *Joint Publication (JP) 2-0*, ed. Department of Defense (2006).

<sup>&</sup>lt;sup>4</sup> Ray Kurzweil, *The Singularity Is Near* (New York: Penguin Group, 2005).

<sup>&</sup>lt;sup>5</sup> John T. Correll, "Igloo White," Air Force Magazine, November 2004.

<sup>&</sup>lt;sup>6</sup> Ibid.

<sup>&</sup>lt;sup>7</sup> Ibid.

<sup>&</sup>lt;sup>8</sup> Anil Ananthaswamy, "March of the Motes," New Scientist 179, no. 2409 (2003).

<sup>44</sup> Hill et al., "The Platforms Enabling Wireless Sensor Networks."

<sup>45</sup> HQ ATC/DOT, "Afp 51-45, Electronic Combat Principles," ed. Department of Defense (1987).

<sup>46</sup> Roger Allan, "Wireless Sensors Land Anywhere and Everywhere," *Electronic Design* 53, no. 16 (2005).

<sup>48</sup> Kirsty Mills, ed., *Nanotechnologies and Society in the USA*, Nanotechnology: Risk, Ethics, and Law (Sterling: Earthscan, 2006).

<sup>49</sup> P. Chaudhari, "Future Implications of Nanoscale Science and Technology: Wired Humans, Quantum Legos, and an Ocean of Information," in Societal Implications of Nanoscience and Nanotechnology, ed. Engineering Nanoscale Science, and Technology Subcommittee (Arlington: National Science and Technology Council, 2001).

<sup>50</sup> National Science Board, "Science and Engineering Indicators 2006," (Arlington: National Science Board, 2006). <sup>51</sup> BMRB Social Research, "Nanotechnology: Views of the General Public," ed. The Royal Society and Royal

Academy of Engineering Nanotechnology Working Group (The Royal Society and Royal Academy of Engineering Nanotechnology Working Group, 2004).

<sup>52</sup> Dr David Brin, The Transparent Society: Will Technology Force Us to Choose between Privacy and Freedom? (Reading: Addison-Wesley, 1998).

<sup>3</sup> Jane Macoubrie, "Informed Public Perceptions of Nanotechnology and Trust in Government," (Woodrow Wilson Internatonal Center for Scholars, 2005).

<sup>54</sup> The Royal Society, "Potential Health, Environmental, and Societal Impacts of Nanotechnologies," (London: Science Council of Japan, 2005).

<sup>55</sup> UNEP, "Emerging Challenges: Nanotechnology and the Environment," in *Global Environment Outlook Yearbook* (2007). <sup>56</sup> Ibid.

<sup>57</sup> DOW Chemical, "Background on Agent Orange,"

http://www.dow.com/commitments/debates/agentorange/background.htm.

<sup>58</sup> Philip E. Ross, "Tiny Toxins?," *Technology Review*, May/Jun 2006 2006.

<sup>59</sup> Berube, Nano-Hype: The Truth Behind the Nanotechnology Buzz.

60 Ross, "Tiny Toxins?."

<sup>61</sup> Daniel Watts, "Particle Surface Characteristics May Play an Important Role in Phytotoxicity of Alumina Nanoparticles," Toxicology Letters 158, no. 2 (2005).

<sup>62</sup> Barnaby J. Feder, "Study Raises Concerns About Carbon Particles," New York Times 153, no. 52803 (2004).

<sup>63</sup> Matsuda Masami, ed., *Nanotechnologies and Society in Japan*, Nanotechnology: Risk, Ethics, and Law (Sterling: Earthscan. 2006).

<sup>64</sup> National Science Foundation, "Fy 2008 Budget Request to Congress," National Science Foundation, http://www.nsf.gov/about/budget/fy2008/toc.jsp.

<sup>65</sup> Richard Silberglitt, "The Global Technology Revolution 2020, in-Depth Analyses:

Bio/Nano/Materials/Information Trends, Drivers, Barriers, and Societal Implications," ed. RAND Corporation (Pittsburgh: RAND, 2006).

<sup>66</sup> Jerome C. Glenn. "Future Research Methodology." (Place Published: AC/UNU Millennium Project, 1996.

<sup>67</sup> Hall, Nanofuture: What's Next for Nanotechnology.

<sup>68</sup> Glenn. "Future Research Methodology." (Place Published.

<sup>69</sup> Joel J. Luker. "State Actor Threats in 2025" (Air University, 2007).

<sup>70</sup> James W. Myers, "Nonstate Actor Threats in 2025: Blue Horizon Scenarios" (Air University, 2007).

<sup>71</sup> Spencer Abbot, ed., Air Power Strategy and the Problem of Coercion, Immaculate Warfare (Westport: Praeger Publishers, 2003).

<sup>72</sup> Akos Ledeczi, "Shooter Localization in Urban Terrain," Institute for Software Integrated Systems,

http://www.isis.vanderbilt.edu/projects/nest/documentation/Vanderbilt\_NEST\_ShooterLoc.ppt.

<sup>73</sup> Defense, "Quadrennial Defense Review Report."

<sup>74</sup> Dennis Bailey, The Open Society Paradox: Why the Twenty-First Century Calls for More Openness--Not Less, 1st ed., vol. 1 (Dulles: Brassey's, 2004).

<sup>75</sup> David H. Petraeus, "Fm 3-24: Counterinsurgency," ed. Department of the Army (Department of the Army, 2006).

<sup>76</sup> Colin S. Gray, "The Advantages and Limitations of Air Power," *Explorations in Strategy* (1996).

<sup>&</sup>lt;sup>47</sup> Thomas Hoffman, "Smart Dust," *Computerworld* 37, no. 12 (2003).