AIR WAR COLLEGE

AIR UNIVERSITY

ESTABLISHING MILITARY UTILITY OF NON-TRADITIONAL SENSING

by

Michael R. Borbath, Lt Col, USAFR

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Col Thomas D. McCarthy, PhD, USAF

13 February 2014

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 United States government or the Department of Defense. In accordance with the Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

Biography

Lieutenant Colonel Michael R. Borbath is an Air Force reservist and program manager with the Air Force Scientific Advisory Board Secretariat. He is also President of Borbath, Inc., a technology consulting firm located in Florida. In addition, he is a senior electrical engineer in the photonics department at Harris Corporation located in Melbourne, Florida. His education includes a BS in Electrical Engineering from the University of Florida and a MS in Electrical Engineering from the University of Maryland, College Park.

Lt Col Borbath has more than 20 years of advanced analog and digital communications experience in fiber optics, free space optics, and RF communications. He has extensive experience in systems engineering, program management, project management, and product development. He holds advanced professional certifications in acquisition, cryptology, program management, space, and cyber systems. He also possesses broad intelligence community work experience and extensive international field deployment experience.

Abstract

America's ability to rely on traditional sensing systems providing vital intelligence information from within anti-access / area denial (A2/AD) environments is at risk. Adversaries are hardening their A2/AD defenses by developing capabilities to destroy, deny, degrade, disrupt, and deceive (D5) our traditional sensing systems. Furthermore, traditional sensing systems continue to suffer from an inherent lack of architecture resiliency and interoperability. Perhaps most important, these vital traditional systems will continue to be burdened with skyrocketing lifecycle costs. These three challenges leave our future sensor viability in doubt on modern battlefields and hold at risk our nation's ability to make sufficiently informed and timely national security decisions. To mitigate the risk of unavailable or inadequate traditional sensing systems and networks, thus helping ensure resilient awareness within A2/AD operational environments by the year 2040, the US must seek and exploit proliferative, non-traditional (NT) sensing systems offering military intelligence utility comparable to traditional sensing systems, while simultaneously augmenting the capabilities of traditional sensing and providing redundant backup in order to minimize capability losses if traditional systems are compromised.

This paper first describes the difference between traditional and non-traditional sensing systems. It then gives examples of how commercial companies use non-traditional sensing systems to provide valuable information for themselves and their customers. Next, it explains the construct forming the three necessary sub-systems constituting militarily useful non-traditional sensing systems. Using examples of military applications, this paper describes how the Air Force may similarly use NT sensing systems to provide militarily useful information from within A2/AD environments. Finally, it concludes with some suggestions that would allow the Air Force to harness the strategic benefits from NT sensing.

Introduction

America's ability to rely on traditional sensing systems providing vital intelligence information from within anti-access / area denial (A2/AD) environments is at risk. Adversaries are hardening their A2/AD defenses by developing increasingly potent capabilities to destroy, deny, degrade, disrupt, and deceive (D5) our traditional sensing systems. Furthermore, traditional sensing systems continue to suffer from an inherent lack of architecture resiliency and interoperability. Perhaps most important, these vital traditional systems will continue to be burdened with skyrocketing lifecycle costs. These three challenges leave our future sensor viability in doubt on modern battlefields and hold at risk our nation's ability to make sufficiently informed and timely national security decisions.

Current US strategic guidance mandates that the military credibly maintain its ability to project power into areas from which the military's access and freedom to operate are challenged.[1] The military's power projection capability, though, is based on intelligence, surveillance and reconnaissance (ISR) information from those denied areas. Yet, traditional US sensor and sensing networks are inherently vulnerable to proliferating A2/AD threats and challenges. Moreover, as A2/AD threats mature in sophistication, vulnerabilities of traditional sensing systems may grow faster than their ability to be defended. To continue meeting strategic requirements, the nation's military must incorporate resilient battlefield awareness systems into its overarching intelligence architecture.[2]

Current intelligence, surveillance, and reconnaissance architectures rely heavily on information provided by exquisite yet delicate sensor systems resident in space, air, ground, and submarine environments. For instance, space imaging systems are used for intelligence collection and have unique capabilities to provide selective, high fidelity imagery of physically denied areas. However, they are also very expensive, fragile and vulnerable to adversary D5 actions. Furthermore, space imaging systems suffer from the tyranny of persistence, meaning increased target persistence is offset by often unpalatable acquisition, sustainment, and other lifecycle considerations. Traditional systems such as these are also incapable of rapidly reconstituting their mission presence in response to diverse nation security emergencies.

There is nothing easy about any aspect of building, operating, maintaining and defending these traditional systems to ensure they remain productive in volatile, uncertain, complex and ambiguous environments. Increasingly through 2040 it will be common to see adversaries, in escalatory conflicts, continue to focus their attack strategies using D5 efforts specifically aimed at reducing US sensor utility. For example, direct-to-geosynchronous anti-satellite weapons, electronic warfare, and other asymmetric tactics degrade US sensor persistence jeopardizing battlespace awareness.

Admittedly, work is already underway to make traditional sensing systems more robust, thus offering better overall future military utility and availability. For example, improved link budgets, fractionated architecture implementations, and enhanced autonomy can all help to make the traditional systems more resilient to escalatory D5 threats. However, there is no alternative plan in the grand overarching sensing architecture but to rely on these delicate systems. If these traditional systems cease to provide the intelligence needed by the warfighter, the US may have no alternative means to bridge the gap unless the systems are reconstituted. This inability to bridge the information gap until reconstitution could have severe negative consequences on the military's targeting, force flow, logistics, and national security abilities.[3] These negative consequences are so dire that other awareness options must be considered.

Thesis

To mitigate the risk of unavailable or inadequate traditional sensing systems and networks, thus helping ensure resilient awareness within A2/AD operational environments by the year 2040, the US must seek and exploit proliferative, non-traditional (NT) sensing systems offering military intelligence utility comparable to traditional sensing systems, while simultaneously augmenting the capabilities of traditional sensing and providing redundant backup in order to minimize capability losses if traditional systems are compromised.

What Distinguishes Non-traditional Sensors from Traditional Sensors?

There is no standardized definition clearly distinguishing traditional from non-traditional sensors. In fact, one organization's non-traditional sensors could be another organization's traditional sensors. For example, the Air Force Intelligence, Surveillance, and Reconnaissance (ISR) Agency still broadly classifies full motion video (FMV) imagery as "non-traditional" even though FMV ISR military capability has been around for over a decade.[4] Often the determination of whether a sensor is traditional or non-traditional depends on the point of view of the particular entity accessing or utilizing the sensors or data. For the purposes of this paper, traditional sensors are operationally defined as those: 1) built and used for (a) specific purpose(s), 2) intentionally connected to a public or private network so that collected sensor data can be further processed or analyzed, 3) controlled and maintained by the owner or agent of the sensors, and 4) having achieved a mature, stable utility in an established architecture.[5]

In contrast, non-traditional sensors may be operationally defined as those sensors: 1) often used for purposes other than for which they were designed, 2) connected to a network but accessed by non-primary actors, 3) not owned or maintained by the non-primary actors, and 4) inherently adaptable to novel applications. Often, these novel applications are not fully known or understood until years later. Sometimes, as NT sensing systems mature, they serve as the foundation from which traditional sensors are developed. This paper will explain first in commercial terms and then using military examples how NT sensing systems are poised to offer better military utility, resiliency, and life-cycle costs compared with their traditional counterparts.

Commercially Driven NT Sensor Capabilities, Proliferation and Exploitation

The density of sensors and sensing systems is rapidly increasing. Everything connected to the Internet or a private network in some way acts as a sensor. Today this ranges from deli scales in grocery stores to smart appliances in homes and mobile computing devices. As widespread as this might seem, we are still in the relative infancy of the information age. Some observers have described this upcoming hyper connectivity as the "Internet of Things (IoT)."[6]

To illustrate this point, today there are over 10 billion devices connected to the Internet. Projections estimate there will be 50 billion by 2020 and perhaps 100 trillion by 2040.[7] Driven mostly by commercial industry, this explosion of mobile and fixed connectivity is helping create a world shaped by ubiquitous sensors with massive amounts of data circulating across public and private networks. From a military perspective, strategists strive to understand what battlespace awareness the military can derive from all of these sensors. To answer this, it is helpful to look at some recent commercial examples of how accessing and interpreting large amounts of data can be useful to the general public.

In a project designed to leverage its pervasive utility in society, Google Corporation used a software model combining pertinent search terms with geographic data from user searches to understand and project the spread of previous epidemics.[8] Google then applied its model to a new regional flu outbreak and was able to quickly and accurately predict where the flu was spreading. Furthermore, the Google information provided these estimations in near real-time instead of the days or weeks the Centers for Disease Control and Prevention (CDC) took to finalize and report their data.[9] Thus, Google was able to produce equivalent results using non-traditional sensing techniques faster than the CDC's traditional sensing capability.

There are thousands of other examples of commercial businesses harnessing widespread sensor information and transforming it into actionable or profitable knowledge. For instance, the commercial sector mines big data to improve its bottom line through better targeted sales, balanced inventories and reduced logistics costs.[10] Financial organizations use NT sensing to adjudicate potentially misleading or false information. For example, if a country that reported a domestic rate of inflation was suspected of using misleading or deliberately falsified calculations, this may be detected by the use of NT sensing. In this situation, information gathered through country-wide, non-traditional sensors may paint an alternative and more realistic representation of the inflation rate.[11] Furthermore, utilizing non-traditional sensors to develop awareness, even with just the sensor metadata, could provide an alternative means to understand complex economic, political and military situations, capabilities and intentions.

Non-traditional Sensing's Requirements Triad

Non-traditional sensing exhibits three fundamental characteristics:

1) Sensor data: shared access to large quantities of data

2) Networks: a way to transfer this data around networks to inform decision makers

3) Processing: smart algorithms to make sense of the enormous amount of data.

It is these three essential ingredients that make up a viable non-traditional sensing architecture. Moreover, all of the pieces in this requirements triad are interdependent, since each informs or is informed by the others to varying degrees. This interrelationship can be visualized in Figure 1.

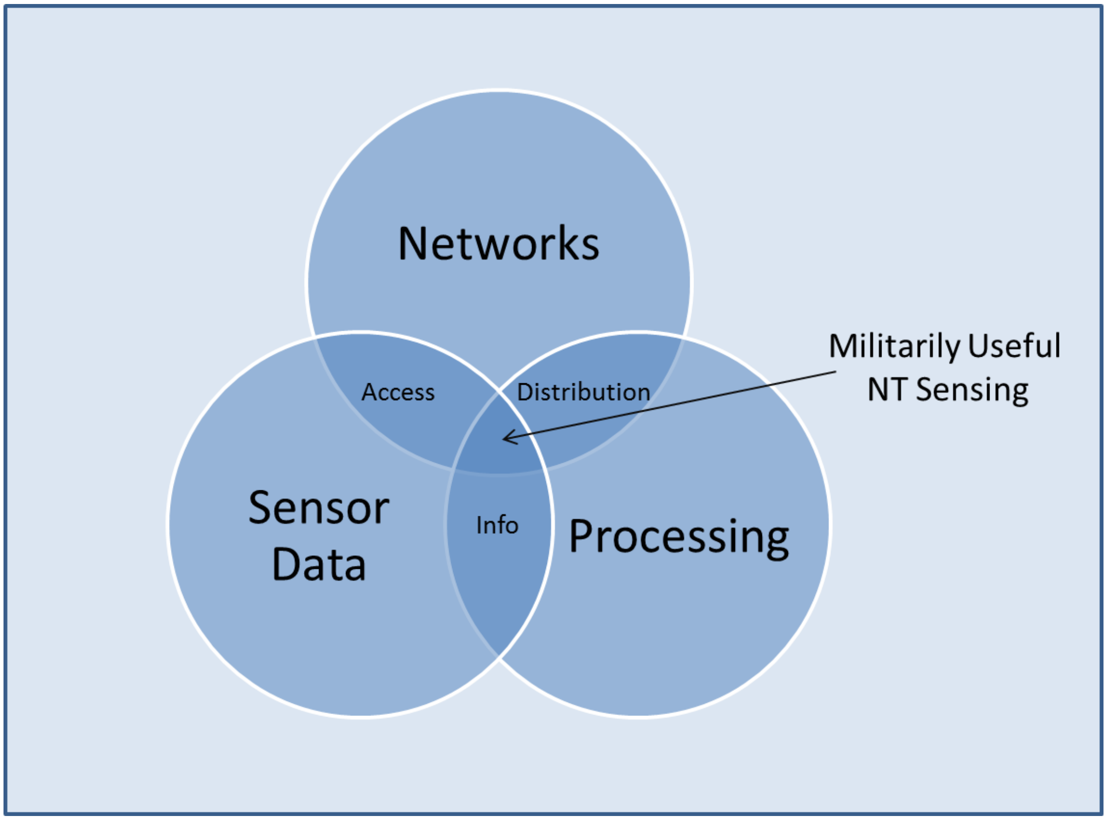

Figure 1: Relationship among NT sensing requirements triad components

As shown in Figure 1, the intersection of sensor data and the networks forms the access piece. The intersection of the processing and networks provides the distribution, or the ways the sensor and weapon system communicate to facilitate the exchange of information. At the center of all of this we find the militarily useful NT sensing. This requirements triad will now be explored in more detail.

Sensor Data

The amount of electronically captured data is accumulating at an almost overwhelming rate. In 2013, the amount of stored extant information in the world was estimated to be between 1 and 4 zettabytes.[12] This amount of data is so large it is about to dwarf the seemingly huge storage capacity of the newly built one million square foot NSA data center in Utah.[13] Some estimates even project the amount of digital data in the world as doubling about every three years.[14] YouTube, for example, has over 800 million monthly users uploading over an hour of video per second.[15] Twitter processes more than 400 million tweets every day.[16] Facebook members click a “like” button or leave a comment nearly 3 billion times per day, creating a digital trail the company can mine to learn about users’ preferences.[17] Even US government organizations such as the National Oceanic and Atmospheric Administration (NOAA) currently generate and collect more than 19 TB of data every day.[18] The massive number of sensors proliferating over the next two decades will serve as the raw material forming the haystack from which the proverbial needles will need to be found.

Networks

The vast accumulating stores of data need to be linked with smart algorithms via an interconnected sensing network. Obviously, not all of the data in the world have military utility, but where these militarily useful data do reside will likely be diversely spread across vast regions of the globe. To transport this data in a timely and selective manner requires high speed terrestrial and satellite transmission capacity.

High speed transmission capabilities between networked sensors and the data centers are expanding rapidly. Driven mainly by commercial business markets, high speed fiber optic communication systems utilizing the latest coherent modulation schemes are poised to provide exponential growth in terrestrial bandwidth capacity. These high speed backbones are shared by both commercial and military users alike, creating both operating opportunities and challenges for military NT sensing. In particular, in order to preserve revenue of both the customers and the network providers, these high speed backbones are fundamentally designed to be resilient and robust to outages. As will be described later in this paper, this resiliency in conjunction with other key aspects will help ensure commercial communications during times of conflict.

Processing

Not surprisingly, the magnitude of data to sift is staggering. Google processes more than 24 petabytes of data per day.[19] However, all of this accumulating data is useless unless actionable intelligence can be extracted from it. Processing is needed to tease out the underlying constructs latent within the data to form associations not previously visible by other means. To do this, intelligent algorithms must combine with fast computing hardware to process and transform raw sensor information into clear knowledge presentable to decision makers. Currently though, there is an insufficient ability to process NT sensor information quickly and efficiently, especially for military sensing purposes. [20] Although NOAA collects 19 TB of data, if left unanalyzed, this data cannot provide NOAA any answers on important topics such as crop management and optimization.[21] All of this automation does not mean taking humans out of the loop, however, but instead elevating them to the top of the decision making process instead of where they are now, which is inefficiently spread across every level.[22]

Exploring Military Utility Non-traditional Sensing

Within the construct of the NT sensing triad (as shown in Figure 1), this section will examine specific examples and applications of militarily relevant sensors, networks and processing capabilities. First, a brief discussion of militarily useful data sensors, most of which are already in the environment today, will serve to demonstrate their ubiquitous and proliferating nature. Second, this paper will explore some of the networks utilized in NT architectures. The remainder of this section will explore processing capabilities and how processing supports current and expected military battlespace awareness applications in an A2/AD environment.

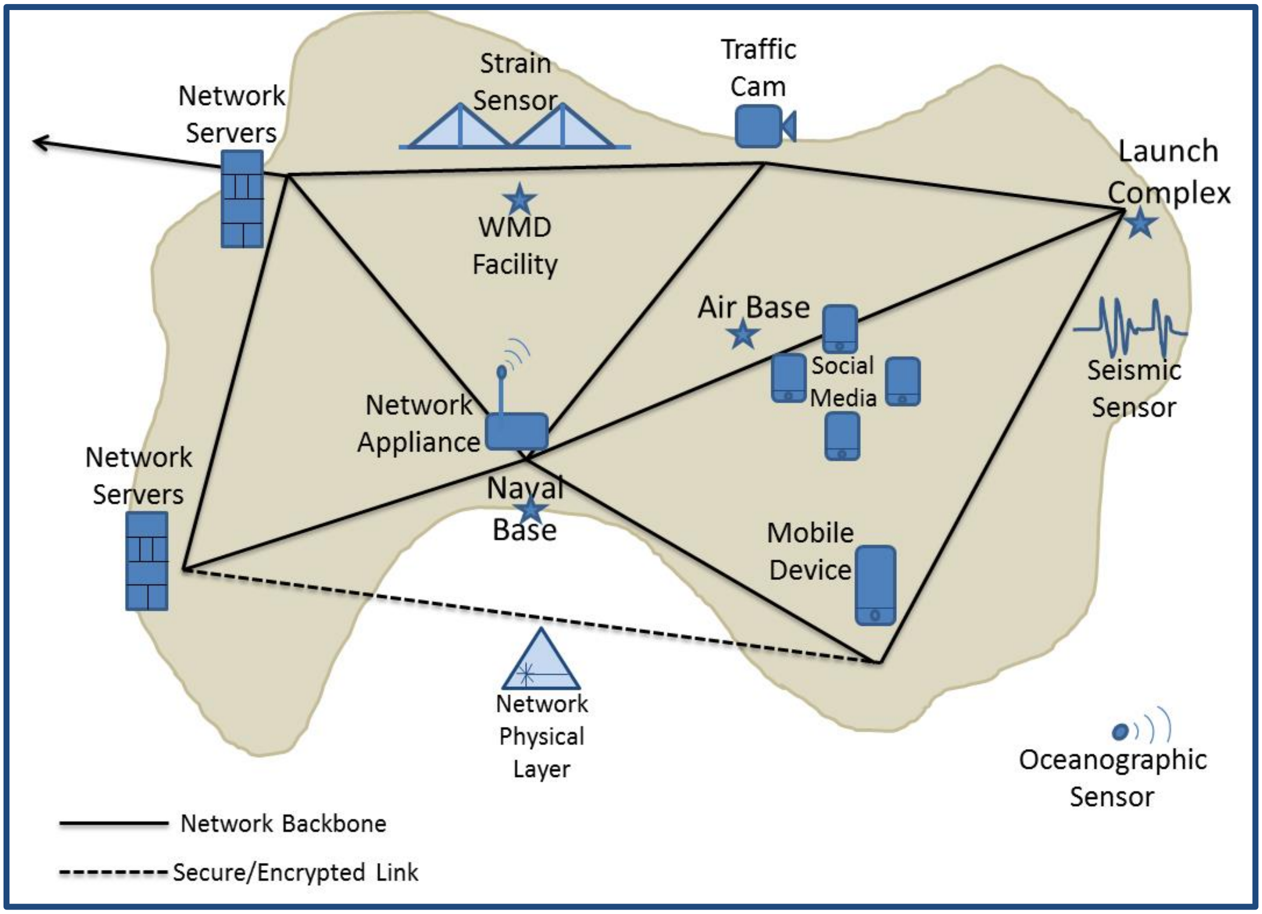

Figure 2: Notional examples of militarily relevant NT sensors and network opportunities within an A2/AD environment (note: processing capability not depicted).

Military Sensor Data Examples

Which NT sensors in an A2/AD environment could the military use to improve battlespace awareness? Figure 2 shows some examples of potential NT sensor systems within an A2/AD environment. This figure also shows that unlike traditional sensing capabilities that are being forced farther and farther out from A2/AD environments because of adversary D5 activities (including airborne or seaborne assets), these NT sensors will continue to remain positioned in key areas denied to many traditional systems. For example, these NT sensors include:

- Fixed and mobile computing devices (e.g. smart phones)
- Strain and flow sensors (e.g. bridges, traffic)
- Seismic sensors (land or sea based)
- Oceanographic sensors
- Social media sites
- Search engine databases
- Exploited computing devices
- Network appliances (e.g. routers, switches, modems)
- Networks (e.g. military, civilian, corporate)

Military Network Examples

How will these NT sensors be accessed? A wide variety of command, control, and communications methods are available depending on the sensor application and the protection level of the sensor. Figure 2 shows some of these network options and opportunities. For example:

- Uncooperative computer-to-computer (C2C) communications (exploits)
- Medium exfiltration (wired, wireless, multi-medium, advanced forwarding)
- Cooperative third parties
- Information brokers or resellers
- Secure, encrypted links
- Implants (C2C, physical, supply chain management)
- Existing intelligence ingress/egress techniques (signals intelligence)

Harnessing the sensing and networking opportunities mentioned above requires advanced and sustained intelligence preparation of the environment (IPoE). However, because the overwhelming focus of ISR for the past 10 years has been on supporting the global war on terrorism and related intelligence needs, the US military’s ability to conduct classical, sustained, persistent IPoE has atrophied.[23] As will be discussed later, NT sensing opportunities will serve to bolster IPoE in A2/AD environments.

Military Processing Examples

In the NT sensing triad, processing addresses the distillation of actionable intelligence from the collected data. To understand what intelligence benefit NT sensing provides the warfighter, it is useful to look at which national security missions stand to benefit from this processed data. Some battlespace awareness benefits are listed below, followed by a more detailed explanation:

- Cyber-attack attribution adjudication
- Augmentation of traditional sensor (e.g. cueing)
- Missile warning and telemetry data
- Special Operations Forces mission enhancement
- Improved munitions effectiveness
- Improved logistics management

Cyber-attack aftermaths are extremely complex events to unravel, especially when attempting to determine attribution. One of the biggest impediments to determining precise attribution is the lack of causal links back to the actual belligerents. This is due to the premeditated circuitous routes through global servers that the attackers use to hide the traceability of their actions. Onerous technical challenges and high costs often prevent the determination of attribution with the certainty required for legal or military action. By utilizing NT sensors in conjunction with processing techniques such as data intensive correlation models and strategically positioned data sensors, cyber-operators can supplement their traditional causal data to clandestinely zero in on the attacker.[24]

Another military example of the use of NT sensing is in the augmentation of cueing for traditional systems. As mentioned earlier, capabilities of traditional systems could be impaired through adversary D5 activities within an A2/AD environment. In situations such as these, augmentation from NT sensors in the A2/AD environment, such as from personal mobile communication systems, would boost the effective of sensor sensitivity and selectivity. For example, information from an NT sensing system could alert a traditional system, such as a partially degraded imaging satellite or a remotely piloted vehicle to take a more detailed look at a region of interest.

In the past, it has proved notoriously difficult to collect missile telemetry data (a type of measurement and signature intelligence or MASINT) such as rocket re-entry signatures from A2/AD environments using traditional sensors. [25] However, a host of NT sensors already in the area of interest can serve to augment these traditional sensors, making collection more effective. Furthermore, situational awareness sensing opportunities could assist combatant commands such as United States European Command with indications and warnings (I&W) that tip off a ramp up to a missile launch.[26] In addition, because of their massive diversity in technical capabilities and high geographic density, NT sensing solutions are poised to overcome some typical traditional sensing challenges such as limited diurnal availability.

NT sensing can also enhance location and identity recognition systems to assist targeted or limited military engagement activities such as those from Special Operations Forces. As in missile warning, the use of NT sensors allows Special Operations to determine intentions, methodologies, decoy validation, and real time exploitation.[27] This would provide a means to supplement more traditional SOF techniques in the areas of activity detection and patterns-of-life determination.[28]

Lastly, augmenting precision guided munitions targeting data with NT sensing improves weapons effectiveness by increasing targeting accuracy and precision.[29] NT sensors located near radio frequency shielded environments and underground bunkers may provide an augmented triangulation of these high value targets. Improved targeting accuracy thereby enables the precision usage of volumetric weapons such as EMP or low yield nuclear weapons. This precision employment can increase the probability of desired effects and thus reduce the overall kill chain timeline and likelihood of collateral damage. Even non-kinetic attacks such as multi-spectral EW effects benefit from the augmentation of NT sensors and enhance the ability to deliver a range of effects on adversary positions.

Military Benefits of NT Sensing over Traditional Sensing

Non-traditional sensing offers several promising advantages to enhance the capabilities of traditional sensing. Three of these advantages are briefly described below:

NT Sensing Networks are Inherently Resilient, Offering Assured Communications

- Unprecedented Prolificacy: Large quantities of commercially driven NT sensors exist in the environment and are under no threat of elimination or complete suppression because of their proliferating, ubiquitous, and highly redundant nature.
- Pervasive connectivity: Because of their interconnected IoT nature, these sensors are thoroughly integrated into commerce and culture thus making it difficult or impossible to disconnect them from the network to which they are linked. This means at least a minimal NT sensing capability or signature is always left behind.
- Improved Error Tolerance: Big data researchers have shown that solution quality or accuracy approaches good enough levels if models with sufficiently large amounts of data are utilized.[30] Thus, because of the rapidly growing quantities of sensors providing data in the future, the non-traditional sensing world offers to be one where "less sophisticated but abundant" has the potential to trump "fewer but pristine."[31]
- Unique Political/Strategic Protections: Consortium-based business models pose Manchester-doctrine-like effects as they begin to inextricably link political, military, and

economic aspects of many host governments.[32] For example, a country's governmental decision calculus to attack part of an NT sensing architecture is more complicated if the targeted country is within the consortium's umbrella organization.

- Assured Network Communications in Times of Conflict: The previous four factors help ensure the NT sensing architecture, as a whole, is resilient and available during times of conflict. Even if an adversary isolated or inactivated significant portions of networks communications capabilities within its territory, such a move would only serve to isolate them and stymie its highly interconnected diplomatic, informational, military, and economic instruments of power.

NT Sensing Offers Unmatched Sensor Diversity, Flexibility and Confidentiality

- Diversity: Sensors offer wider technical diversity compared with traditional systems, since they leverage market-driven forces of the commercial marketplace.
- Flexibility: The ability to transform their functionality is built into their design and augmented through remote modifications and updates.
- Confidentiality: Adversaries are not likely to ascertain what intelligence is being derived from the sensors in their environments since processing is performed elsewhere.

NT Sensing Economic Advantages

- Lower Lifecycle Costs: Compared with those of traditional systems, the development, installations, operations and maintenance considerations of NT systems are reduced, since these sensors are brought into existence not by the military, but by consumer and industry-driven demand and support.

- Sensor and Network Defense: Sensors are generally welcomed into the environment, and thus they are not at risk of being eliminated, since their primary purpose is to provide information to the sensor owners. Therefore, they do not require military protection.

Strategic Directions to Incorporate NT Sensing into Battlespace Awareness

The NT sensing revolution has already begun. The military must now decide what role it wants to play in harnessing the benefits of NT sensing. This paper advocates that the Air Force take an active role in shaping the future of NT sensing within its own intelligence structure. To do this it must first begin to incorporate NT sensing into the overall joint warfighting intelligence architecture. Second, the Air Force must assess the implications NT sensing has within its future force structure and rebalance the force as necessary to properly accommodate it. Finally, the Air Force needs to capitalize on the ongoing commercial, academic and intelligence community efforts in NT sensing technology to ensure that Air Force needs are represented in this commercially driven environment.

Incorporate NT Sensing Into the Overall Joint Warfighting Intelligence Architecture

1. Understand the benefits and opportunity cost of incorporating NT sensing into current architecture versus remaining solely focused on traditional systems.

Perhaps the biggest factor limiting exploitation of NT sensors is a general lack of awareness of what capabilities NT sensing can bring to the military. Indeed, the technical tools for handling data have already changed dramatically, but our methods and mindsets have been slower to adapt.[33] While commercial industry invests heavily in and focuses on NT sensing or big data mining, the US military appears stymied in its efforts to leverage NT sensors.

To start, the military needs to understand what role NT sensing systems should have within the current intelligence architectures by weighing the advantages NT sensing brings over traditional sensing in an A2/AD environment. For example, since NT sensing system architectures are inherently diverse and resilient, they offer an advantage in solving difficult tactical and intelligence problems. In addition, they are designed to fuse information from large numbers of sources, providing a more complete picture of a situation.[34] Furthermore, because of traditional sensing susceptibility to adversary D5 actions, NT sensing robustness in these same conditions serves to augment military battlespace awareness.

2. Develop trial functional NT sensing capabilities and link them to existing globally networked ISR weapon systems to assess utility and develop concepts of operation.

The Air Force already has relevant and mature traditional sensing systems and architectures in existence today, poised, at least in a basic sense, to incorporate NT sensing. For example, Air Force intelligence exploitation is primarily performed by the Distributed Common Ground System (DCGS), which is a globally networked ISR weapon system.[35] The Air Force could use DCGS or its variants as a platform from which to test out NT sensing systems by augmenting current traditional sensing partner systems. The goal of this trial would be to understand the contribution NT sensing offers for cueing of traditional IMINT systems for improved warfighter battlespace awareness.

3. Develop comprehensive near-, mid-, and far-term NT sensing goals with the assistance of expert panels including warfighter representatives, science boards, government labs, and industry and other stakeholders.

Since NT sensing is expected to touch nearly all aspects of the current joint warfighting intelligence architecture, its successful widespread acceptance will require persistent and genuine involvement from many different intelligence community members as well as support from industry. Comprehensive and realistic near-, mid-, and far-term plans need to be developed that are inclusive and respectful of pertinent stakeholders in the process.

4. Understand the legal enablers, constraints, and opportunities associated with NT sensing.

This paper purposely does not address in significant depth the legal issues associated with NT sensing. However, legal frameworks such as US Code Titles 10, 32, and 50 have always played an important role in shaping intelligence community actions. Specific areas that need clarification with regard to the implementation of NT sensing include the following: What Title 10 and/or 50 organizations can process military NT sensor data? Who will become the DoD's big data cruncher? What are the data storage and retrieval concerns from both domestic and foreign sources?

Assess Implications to the Military Force Structure – Specifically the Air Force

1. Develop a cadre of NT sensing experts within the military.

The Air Force needs to foster subject matter experts knowledgeable across the wide array of systems making up the NT sensing architecture. To develop and retain this essential cadre of NT sensing experts the military needs to incentivize officers pursuing degrees in big data statistical analysis and modeling techniques, including talent who understand the back end technologies: hardware, software, algorithms, and the intelligence networks tying everything together. In addition, the Air Force should support technical exchanges with industry and academia such as through operational fellowships and industry exchange programs with US

National Labs, foreign and domestic academia, and industry.

2. Leverage the skills of military Guard & Reserve members who already possess critical civilian skills in relevant NT sensing technologies.

The Air Force is fortunate to have already within its own force structure Air Force Reserve and Air National Guard members who, in their civilian jobs, have expertise with the hardware and software that form the building blocks of NT sensing systems. These technicians, engineers, scientists, and subject matter experts who already possess many of the critical technical skills needed are prime candidates when forming the force structure and planning cells necessary to support NT sensing.

Capitalize on Ongoing Commercial, Academic and IC Efforts

1. Begin by following the lead of other intelligence community members seeking to understand how NT sensing benefits their missions.

Other intelligence community members such as the Army and Central Intelligence Agency (CIA) have already begun exploring the potential of NT sensing by soliciting contracts to industry.[36] The Defense Advanced Research Projects Agency (DARPA) and US National Labs in cooperation with industry and academia are developing algorithms and tools to prepare for the NT sensing revolution.[37] Unlike in the past when the military was essentially the sole owner and creator of intelligence products from sensor to shooter, in the future the military will switch from a net creator to a net consumer of sensor data. Thus, the military needs to understand and keep pace with advances so that it can influence and leverage the NT sensing marketplace. Through the use of contracts, federal business opportunity announcements, conferences, industry days, and working group participation, the military can proactively and deliberately shape the

NT sensing apparatus for its own purpose.

2. Capitalize on NT sensing enabling technologies.

The Air Force should partner with industry on technology initiatives such as innovative algorithms, novel data exfiltration methods, large data set statistics, and high performance computing solutions having military utility. In fact, partnering with industry is crucial for the military to understand the array of innovative algorithms behind database search engines mining the voluminous amount of data generated by ubiquitous sensor proliferation.

3. Address technology and policy gaps preventing seamless integration of sensors into intelligence architectures.

There are a number of ongoing internal intelligence community challenges impeding the incorporation of NT sensing. One longstanding challenge has been the myriad of data formats and metadata standards. For example, there is no coordinated approach to provide commonality of full motion video (FMV) data formats across all of the different FMV sources. This issue, combined with the multitude of meta-data standards imbedded within these video standards, means that most FMV systems are unnecessarily non-interoperable. Further complicating efforts are the DoD and military services stove-piped requirements and standards and the resultant struggle to incorporate interoperability.[38] To resolve this, the IC members and stakeholders must agree on interoperability standards and develop long-term strategic efficiencies focused on hardware and software reuse across platforms.

Conclusion

To mitigate the risk of unavailable or inadequate traditional sensing systems and networks, thus helping ensure resilient awareness within A2/AD operational environments by the year 2040, the US must seek and exploit proliferative, non-traditional (NT) sensing systems offering military intelligence utility comparable to traditional sensing systems, while simultaneously augmenting the capabilities of traditional sensing and providing redundant backup in order to minimize capability losses if traditional systems are compromised. Fortunately, due in large part to the combination of commercially driven future sensor, network, and processing developments, by 2040 there could already be sufficient NT sensors and sensing systems to derive intelligence from the information they provide. These sensing systems, if the military chooses to exploit them, have the potential to provide sufficient militarily-suitable intelligence utility by the year 2040.

In the near term, information derived from an NT sensing architecture has the ability to provide good enough sensing information to augment traditional sensors by enhancing their depth and accuracy.[39] Further into the future, these NT sensing systems are poised to completely replace intelligence derived from some traditional sensors. However, unlike some traditional systems that provide military utility immediately upon sensor system activation, deriving meaningful intelligence from NT sensing requires years of investment to mature. The Air Force should start as soon as possible to incorporate NT sensing into its intelligence architecture to preserve adequate battlespace awareness into 2040.

Notes

[1] Secretary of Defense. *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense.* Washington: DoD, 2012, 1-10.

[2] Department of Defense, *Joint Warfighting Science and technology Plan*, US Government Report (Washington, DC: Department of Defense, 2008), 1-15. Battlespace Awareness is the ability to understand dispositions and intentions as well as the characteristics and conditions of the operational environment that bear on national and military decision making. The goal of *Battlespace Awareness* is to provide commanders and warfighters actionable intelligence that will provide the ability to make better decisions through a better understanding of the environment in which they operate, relevant blue force data, and the adversaries they face. *Battlespace Awareness* should bring to bear a constellation of highly responsive sensors (e.g., unattended, human, intrusive, remote), providing persistent, redundant, and tailored coverage of the battlespace. Sources of information will be integrated into models and simulations to facilitate an understanding of the potential impacts of various courses of action.

[3] Challenges inherent in a multipolar world of alliances, WMDs, and terrorism demand the US national command leadership need timely, relevant information.

[4] Col Michael Stevenson, "AFSOC DGS/DCGS ISR Capabilities." (Lecture, LeMay Center, Maxwell AFB, AL, 5 December 2013).

[5] Michael Nowak, Sensors Directorate, Wright Patterson AFB, OH, to the author, e-mail, 18 November 2013.

[6] Kevin Ashton, "That 'Internet of Things' Thing," *RFID Journal*, 22 June 2009, http://www.rfidjournal.com/articles/view?4986 (accessed 5 January 2014).

[7] Cisco Corporation, "Connections Counter: The Internet of Everything in Motion." *www.cisco.com*, 23 October 2013. http://newsroom.cisco.com/feature-content?type=webcontent&articleId=1208342 (accessed 23 October 2013).

[8] Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Boston: Houghton Mifflin Harcourt, 2013), 26.

[9] Ibid., 2.

[10] Jeffrey Sorenson, ""How to Turn Too Much Data Into Just Enough Information." *defensenews.com*,13 December 2013. http://www.c4isrnet.com/article/M5/20131213/C4ISRNET18/312130012/How-turn-too-much-data-into-just-enough-information?odyssey=nav|head (accessed 13 December 2013).

[11] Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Boston: Houghton Mifflin Harcourt, 2013), 42.

[12] Ibid., 9. One zettabyte = one billion terabytes = 10^21 bytes.

[13] Catherine Herridge, "NSA data center front and center in debate over liberty, security and privacy," *FoxNews.com*, 12 April 2013, http://www.foxnews.com/tech/2013/04/12/nsa-data-center-front-and-center-in-debate-over-liberty-security-and-privacy/ (accessed 21 October 2013).

[14] Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution That Will*

Transform How We Live, Work, and Think (Boston: Houghton Mifflin Harcourt, 2013), 9.

[15] Larry Page, “2012 Update fromt the CEO”. *Google Investor Relations Report*, Mountain View: Google, 2012.

[16] Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Boston: Houghton Mifflin Harcourt, 2013), 8.

[17] Ibid., 8.

[18] Nicole Blake Johnson, “NOAA Looks to Business for Big-Data Help.” *DefenseNews.com*, 17 December 2013. http://www.c4isrnet.com/article/M5/20131217/C4ISRNET13/312170019/NOAA-looks-business-big-data-help?odyssey=nav|head (accessed 17 December 2013).

[19] Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Boston: Houghton Mifflin Harcourt, 2013), 8. One petabyte = one thousand terabytes = 10^15 bytes

[20] Vice Admiral Rob Parker et al., “The New Knowledge Network,” US Naval Institute Proceedings, October 2013, 24-29. Some intelligence community (IC) members believe there will be sufficient sensors in the future and thus the challenge will not be in achieving adequate sensor coverage, but in making sense from the data produced by all those disparate sensors.

[21] Ibid. In late 2014, NOAA is planning on releasing an RFI to get industry’s input on what insights it can derive from all that data.

[22] Department of Defense, *Sensor Data Exploitation*, SAB-TR-11-03-NP (Washington, DC: Air Force Scientific Advisory Board, 2011), 1-104.

[23] Lt Col Mack Curry, “Current and Future Gloabal Air Force ISR Operations.” (Lecture, LeMay Center, Maxwell AFB, AL, 5 February 2013).

[24] Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Boston: Houghton Mifflin Harcourt, 2013), 66.

[25] LtCol Joshua Lavin, “Geospatial Intelligence (GEOINT) and Measurement and Signature Intelligence (MASINT)” (Lecture, LeMay Center, Maxwell AFB, AL, 19 November 2013).

[26] I&W form the first part of the kill chain followed by Detect – Identify – Track – Assign – Engage – Assess.

[27] Department of Defense, *Sensor Data Exploitation*, SAB-TR-11-03-NP (Washington, DC: Air Force Scientific Advisory Board, 2011), 1-104.

[28] Col Michael Stevenson, “AFSOC DGS/DCGS ISR Capabilities.” (Lecture, LeMay Center, Maxwell AFB, AL, 5 December 2013).

[29] Dr. Aaron Chia Eng Seng, “MASINT: The Intelligence of the Future,” *DSTA Horizons* (2007): 108-120.

[30] Peter Norvig, “The Unreasonable Effectiveness of Data.” *google.com*, 23 September 2011. http://www.youtube.com/watch?v=yvDCzhbjYWs (accessed 1 December 2013).

[31] Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution That Will*

Transform How We Live, Work, and Think (Boston: Houghton Mifflin Harcourt, 2013), 34.

[32] Christopher J. Rusko and Karthika Sasikumar, “India and China: From Trade to Peace,” *Asian Perspective* (Vol. 31, No. 4, 2007): 99-123. The central claim of the Manchester Doctrine is that, as economic interdependence of two or more countries increases, their propensity to engage in war decreases.

[33] Viktor Mayer-Schonberger and Kenneth Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think* (Boston: Houghton Mifflin Harcourt, 2013), 26.

[34] Dr. Aaron Chia Eng Seng, “MASINT: The Intelligence of the Future,” *DSTA Horizons* (Defence Science and Technology Agency, Singapore, 2007): 108-120.

[35] Department of Defense, *Sensor Data Exploitation,* SAB-TR-11-03-NP (Washington, DC: Air Force Scientific Advisory Board, 2011), 1-104.

[36] Julie Bort, “IBM Has Stopped Fighting Amazon’s $600 Million Cloud Deal with the CIA,” *businessinsider.com*, 1 November 2013, http://www.businessinsider.com/ibm-stops-fighting-amazons-cia-deal-2013-11#ixzz2nVljPE94; and Department of Defense, *Support for a multi-touch, common operational picture (COP) able to present time-synchronized, multi-source intelligence (multi-INT) data products, including full motion video, on a three dimensional map,* W904TE-14-R-RCOP (Washington, DC: Army Contracting Command, 2013), 1-54.

[37] Steven P. Brumby et al., “Video Analysis Search Technology (VAST): Human-Like Computer Vision using Depp Sparse Generative Models." (*Los Alamos National Lab Journal*, 201), 1-28.

[38] Department of Defense, *Sensor Data Exploitation,* SAB-TR-11-03-NP (Washington, DC: Air Force Scientific Advisory Board, 2011), 1-104.

[39] National Intelligence Council, *Iran: Nuclear Intentions and Capabilities.* National Intelligence Estimate, Washington: National Intelligence Council, 2007, 1-10.

Bibliography

Air Force Scientific Advisory Board. *Sensor Data Exploitation.* 2011.

Anderson, Chris. "The End of Theory: The Data Deluge Makes the Scientific Method Obsolete." *Wired*, 23 June 2008. http://www.wired.com/science/discoveries/magazine/16-07/pb_theory (accessed 12 December 2013).

Ante, Spencer. "Computer Thumps *Jeopardy* Minds." *wsj.com*, 17 February 2011. http://online.wsj.com/news/articles/SB10001424052748704171004576148974172060658#printMode (accessed 17 February 2011).

Ashton, Kevin. "That 'Internet of Things' Thing." *RFID Journal*, 22 June 2009.

Baker, Bob. *Fiscal Year 2009 President's Budget Request for DoD Science & Technology.* DoD Report, Washington: Deputy Director, Plans and Programs, Office of the Director, Defense Research and Engineering, 2008.

Bort, Julie. "IBM Has Stopped Fighting Amazon's $600 Million Cloud Deal With the CIA." *Business Insider,* 1 November 2013. http://www.businessinsider.com/ibm-stops-fighting-amazons-cia-deal-2013-11#ixzz2nVljPE94 (accessed 13 December 2013).

Brandon, John. "How to Build a Human Brain (with a computer 1000x faster than todays)." *FoxNews.com*, 07 October 2013. http://www.foxnews.com/tech/2013/10/07/how-to-build-human-brain-with- computer/ (accessed 07 October 2013).

Brenner, Joel. *America The Vulnerable.* London: Penguin Books, 2011.

Brumby, Steven P., et al. "Video Analysis Search Technology (VAST): Human-Like Computer Vision using Depp Sparse Generative Models." *Los Alamos National Lab Journal*, 2013.

Carlisle, General Hawk, "U.S. - China Military Relationship Interview by Vago Muradian." AFA Conference, 15 August 2013. http://www.defensenewstv.com/video.php?bctid=2719735994001#/Segments/Innovative+Technology+at+DARPA/57636759001/52684858001/2580164262001 (accessed 19 September 2013).

Cisco Corporation. "Connections Counter: The Internet of Everything in Motion." *www.cisco.com,* 23 October 2013. http://newsroom.cisco.com/feature-content?type=webcontent&articleId=1208342 (accessed 23 October 2013).

Coleman, Kevin. "Our Reliance on Technology Requires Proactive Cyber Defense ." *defensenews.com,* 30 September, 2013. http://www.c4isrnet.com/article/20130930/C4ISRNET07/309300030/Opinion-Our-reliance-technology-requires-proactive-cyber-defense?odyssey=nav (accessed 30 September 2013).

Curry, Lt Col Mack. "Current and Future Gloabal Air Force ISR Operations." (Lecture, LeMay Center, Maxwell AFB, AL, 5 February 2013).

Secretary of Defense. *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense.* Washington: DoD, 2012.

Department of the Air Force. *Audio Exploitation.* FBO Solicitation Number: BAA-11-05-RIKA, AFRL/RIK - Rome: Air Force Materiel Command, 2013.

Department of the Air Force. *Multi-INT Enhanced Exploitation and Analysis Tools (E2AT).* FBO Solicitation Number: BAA-RIK-12-13, AFRL/RIK - Rome: Air Force Materiel Command, 2013.

Department of the Army. *Support for a multi-touch, common operational picture (COP) able to present time-synchronized, multi-source intelligence (multi-INT) data products, including full motion video, on a three dimensional map.* FBO Solicitation Number: W904TE-14-R-RCOP, ACC-APG - TAO: Army Contracting Command, 2013.

Deputy Chief of Staff, ISR. *Air Force ISR 2023: Delivering Decision Advantage.* DoD Report, Washington: US Air Force, 2013.

Department of Defense. *Joint Operational Access Concept (JOAC).* DoD Report, Washington: DoD, 2012.

DoD DDR&E. *Joint Warfighting Science and Technology Plan.* Washington: US Govt, 2008.

Galbraith, Amy E., Steven P. Brumby, and Rick Chartrand. "Simulating vision through time: Hierarchical, sparse models of visual cortex for motion imagery." *Los Alamos National Labs Journal*, 2013: 1-8.

Gjelten, Tom. "Are We Moving To A World With More Online Surveillance?" *NPR,*16 October 2013. http://www.npr.org/blogs/parallels/2013/10/16/232181204/are-we-moving-to-a-world-with-more-online-surveillance?sc=ipad&f=1001 (accessed 16 October 2013).

Helland, Pat. "If You Have Too Much Data, then "Good Enough" is Good Enough." *Association for Computing Machinery*, 23 May 2011.

Herridge, Catherine. “NSA data center front and center in debate over liberty, security and privacy.” *FoxNews.com*, 12 April 2013. http://www.foxnews.com/tech/2013/04/12/nsa-data-center-front-and-center-in-debate-over-liberty-security-and-privacy/ (accessed 21 October 2013).

Inglis, John C. *Penn Law's Center for Ethics and Rule of Law Conference.* Penn Law Center, Philadelphia, 22 November 2013.

Johnson, Nicole Blake. "NOAA Looks to Business for Big-Data Help.” *DefenseNews.com,* 17 December 2013. http://www.c4isrnet.com/article/M5/20131217/C4ISRNET13/312170019/NOAA-looks-business-big-data-help?odyssey=nav|head (accessed 17 December 2013).

Kaku, Michio. *Physics of the Future.* New York: Doubleday, 2011.

Kilcullen, David. *The Accidental Guerrilla.* New York: Oxford University Press, 2009.

Lanchester, John. "The Snowden files: why the British public should be worried about GCHQ." *The Guardian,* 3 October 2013. http://www.theguardian.com/world/2013/oct/03/edward-snowden-files-john-lanchester (accessed 3 October 2013).

Lavin, Lt Col Joshua. “Geospatial Intelligence (GEOINT) and Measurement and Signature Intelligence (MASINT)” (Lecture, LeMay Center, Maxwell AFB, AL, 19 November 2013).

Mayer-Schonberger, Viktor, and Kenneth Cukier. *Big Data: A Revolution That Will Transform How We Live, Work, and Think.* Boston: Houghton Mifflin Harcourt, 2013.

McLeary, Paul. "Social Media, Troop Mobility on SOCOM's Radar." *defensenews.com*, 18 October 2013. http://www.c4isrnet.com/article/20131018/C4ISRNET06/310180017/Social-media-troop-mobility-SOCOM-s-radar (accessed 18 October 2013).

Narayanan, Arvind, and Vitaly Shmatikov. "Robust De-anonymization of Large Sparse Datasets." *IEEE Symposium on Security and Privacy.* Oakland, CA: IEEE Computer Society, 2008.

National Intelligence Council. *Iran: Nuclear Intentions and Capabilities.* National Intelligence Estimate, Washington: National Intelligence Council, 2007.

Norvig, Peter. "The Unreasonable Effectiveness of Data." *google.com*, 23 September 2011. http://www.youtube.com/watch?v=yvDCzhbjYWs (accessed 1 December 2013).

Nowak, Michael. *Email Correspondence Related to Traditional Sensing.* Dayton, 18 November 2013.

Nowak, Michael. *The Importance of Trust in a Layered Sensing Construct.* Extended Abstract, Dayton: US Air Force - Sensors Directorate, 2009.

Office of the Chief Scientist of the Air Force. *Technology Horizons: A Vision for Air Force Science and Technology 2010-2030.* Maxwell AFB: Air University Press, 2011.

Page, Larry. "2012 Update fromt the CEO." *Google Investor Relations Report*, Mountain View: Google, 2012.

Parker, Rob, Chuck Michel, Brian Falk, Joe DiRenzo, and Chris Doane. "The New Knowledge Network." *US Naval Institute Proceedings*, October 2013.

Prabhakar, Dr. Arati. "Innovative Technology at DARPA Interview by Vago Muradian." *defensenews.com*, 12 July 2013. http://www.defensenewstv.com/video.php?bctid=2719735994001#/Segments/Innovative+Technology+at+DARPA/57636759001/52684858001/2580164262001 (accessed 10 October 2013).

Rees, Martin. *From Here to Infinity.* New York: W. W. Norton & Company, Inc., 2012.

Richelson, Jeffrey T. "MASINT: The New Kid in Town." *International Journal of Intelligence and CounterIntelligence*. Taylor and Francis, 2001.

Rusko, Christopher, and Karthika Sasikumar. "India and China: From Trade to Peace," *Asian Perspective* (Vol. 31, No. 4, 2007).

Seng, Aaron Chia Eng. "MASINT: The Intelligence of the Future." *DSTA Horizons*. Defence Science and Technology Agency, Singapore, 2007.

Sorenson, Jeffrey. "How to Turn Too Much Data Into Just Enough Information." *defensenews.com,*13 December 2013. http://www.c4isrnet.com/article/M5/20131213/C4ISRNET18/312130012/How-turn-too-much-data-into-just-enough-information?odyssey=nav|head (accessed 13 December 2013).

Stevenson, Colonel Michael. "AFSOC DGS/DCGS ISR Capabilities." (Lecture, LeMay Center, Maxwell AFB, AL, 5 December 2013).

Taigman, Yaniv, and Lior Wolf. “Leveraging Billions of Faces to Overcome Performance Barriers in Unconstrained Face Recognition.” *Face.com*, 2011. http://arxiv.org/abs/1108.1122 (accessed 31 January 2014).

Welsh, Mark A. III. “Invitation to Participate in the Blue Horizons Program for Academic Year 2014.” *Memorandum for AWC and ACSC Students*, Washington: Department of the Air Force, 2013.

Whitwam, Ryan. “Moore’s Law Could Be Saved by Super-Fast Electronics and Photonic tech.” *ExtremeTech.com*, 02 October 2013. http://www.extremetech.com/computing/167866-moores-law-could-be-saved-by-super-fast-electronics-and-photonic-tech (accessed 02 October 2013).