AIR WAR COLLEGE

AIR UNIVERSITY

WHAT TECHNOLOGIES OR INTEGRATING CONCEPTS ARE NEEDED FOR THE US MILITARY TO COUNTER FUTURE MISSILE THREATS LOOKING OUT TO 2040?

by

Reid Vander Schaaf, Colonel, US Army

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Harry Foster

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

Biography

Colonel Reid Vander Schaaf is assigned to the Air War College, Air University, Maxwell AFB, AL. He has been an Army Acquisition professional for over 11 years with the majority of that time spent working on various missile defense programs. Colonel Vander Schaaf has a Bachelor of Science from the US Military Academy in Aerospace Engineering, Masters degrees from Stanford University in Structural Engineering and Construction Engineering Management, and a PhD from Purdue University resulting from research into system-of-systems engineering.

Abstract

As the United States continues its pivot to the Pacific, the joint force faces a new and menacing threat from massed ballistic and cruise missile attacks against fixed infrastructure of all kinds from airports to ports to power grids. These threats form the centerpiece of the strategy of anti-access/area denial (A2AD). The research conducted here shows that the Department of Defense needs to invest in system-of-systems (SoS) engineering and research so the government can understand how to allocate new system requirements against capabilities that address the needs of the SoS. Research is also required on how to design for positive emergent behavior. The dollars invested in software and SoS research will be useful in domains far beyond missile defense. Another critical goal for future software is its ability to enable and accept technology upgrades and insertion without redesigning entire software spirals. Command and control (C2) software should be designed with the ability to isolate compromised components or networks to protect the SoS by preventing the spread of corrupt data or in response to cyber-attacks. The software needs to allow graceful degradation of the SoS, maximizing available capability based on current circumstances or while the system is under attack.

The US will continue to need interceptors through 2040. This inventory should be scaled to respond to rouge state and non-state actor threats. The key and asymmetric limitation of interceptors is that they are too expensive to fully defeat the thousands of potential enemy missiles. Interceptors will also we needed to supplement the lasers that will be available in this timeframe. Lasers will continue to be limited to see and ground used with large energy sources and heat-sinks. Lasers will also be limited due to weather and countermeasures and should be supplemented by interceptors. Lasers have a potential with us in a few additional generations

beyond the 2040 timeframe of almost completely replacing the need for interceptors. In the meantime, the US must invest in SoS to make the best use of its limited number of interceptors.

Introduction

As the United States continues its pivot to the Pacific, the joint force faces a new and menacing threat from massed ballistic and cruise missile attacks against fixed infrastructure of all kinds from airports to seaports to power grids. These capabilities are the centerpiece of the strategy of anti-access/area denial (A2AD). Pioneered by China, planners can expect this strategy and the guided missile regime that enables it to proliferate by 2040.[1]

To date, countering the guided missile regime has proven difficult with existing US missile defense technology. US interceptors, running $14M per copy, are expensive and may require multiple shots to down a single missile. Moreover, protracted cruise and ballistic missile attacks risk rapidly exhausting the US magazine of missile defense interceptors. Purported panaceas for limited magazines, like directed energy systems, have thus far fallen short when evaluated in operational scenarios. Finally, discrimination of the warhead, the coin of the realm for missile defense, remains difficult with current command and control (C2) approaches.

As the joint force considers its ability to maintain sensor and weapons effects over time in anti-access environments from forward airfields in 2040, it is clear that improving the effectiveness of missile defense is vital. This paper explores ways to do this. It argues that the services and the Missile Defense Agency must adopt a systems-of-systems (SoS) approach to maximize the capability of the current fielded systems and increase flexibility so new systems and system upgrades that expand capabilities can be added rapidly while controlling costs. In particular, C2 systems need to use all available sensor information to discriminate the warhead. A centralized discrimination capability will increase discrimination accuracy, thus requiring fewer interceptors and saving interceptor inventory. A SoS approach will enable graceful degradation as systems are removed or lost.

To explore this SoS approach, this paper begins by discussing the nature of the threat, presenting US capabilities to counter it, and describing some of the limitations of these systems in operational settings. Next, it examines why directed energy, while a beneficial capability, is not a plausible sole solution to the missile defense problem. Finally, it examines how the services can improve the existing architecture to overcome some of its limitations and improve its effectiveness in the A2AD environment. The discussion begins by surveying the threat, US counter-missile capabilities, and some of the limitations of these capabilities.

Thesis

This research paper uses a mix of qualitative and quantitative approaches to determine what technologies or integrating concepts are needed for the US military to counter missile threats looking out to 2040.

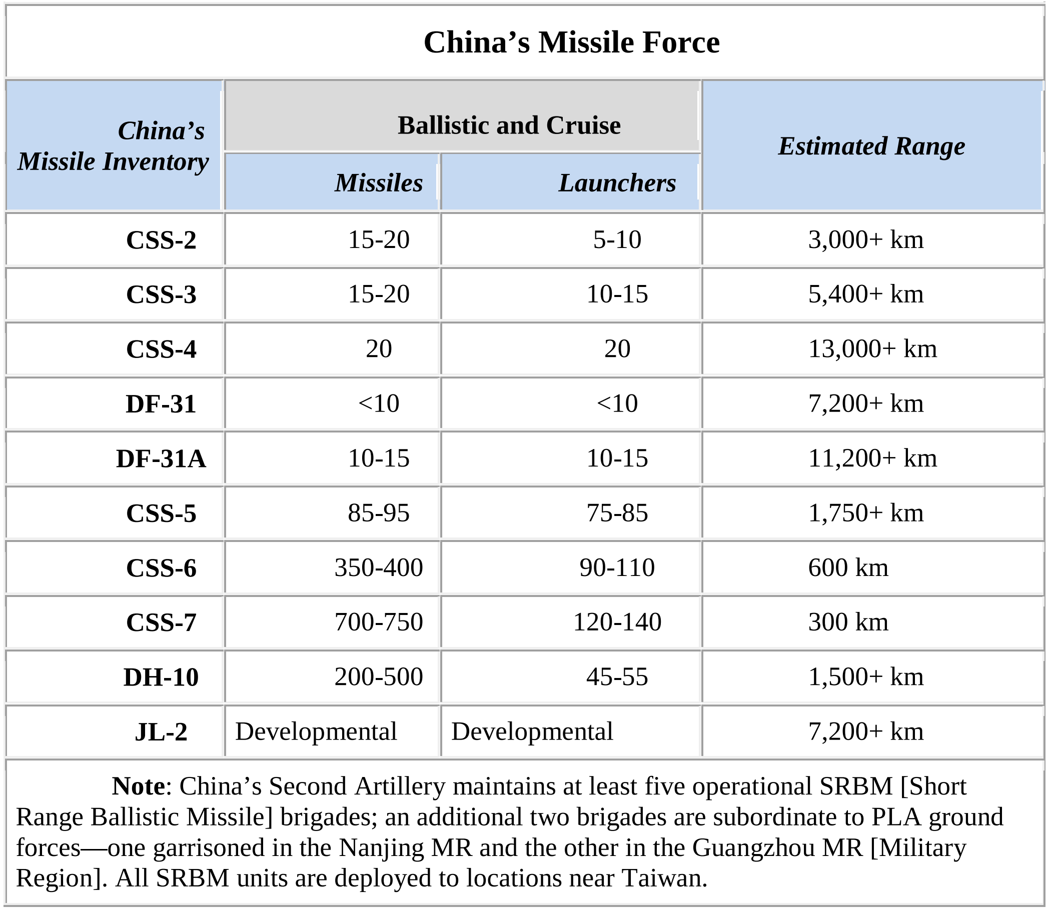
Cruise and Ballistic Missile Threats and US Counter-Missile Capabilities

Currently, many potential adversaries have more cruise and ballistic missiles for attacking the US than the US has interceptors for defense. The Department of Defense's (DoD) 2010 estimate of China's missile force is shown in Table 1.

In addition, North Korea has up to 200 ballistic missiles[2], Russia has approximately 1,200 nuclear armed intercontinental ballistic missiles (ICBMs)[3], as well as hundreds of short and medium range ballistic missiles, India is estimated to have between 100 and 200 ballistic missiles[4] and Iran is estimated to have up to 400 ballistic missiles[5] of short and medium range.

The number of threat missiles is expected to continue to grow. In the 2040 timeframe, the US can reasonably expect potential adversaries to have arsenals of thousands of missiles of varying capabilities and ranges.

Table 1[6]: Estimate of China's Missile Force



China's Missile Force

China's Missile Inventory	Ballistic and Cruise		*Estimated Range*
	Missiles	*Launchers*	
CSS-2	15-20	5-10	3,000+ km
CSS-3	15-20	10-15	5,400+ km
CSS-4	20	20	13,000+ km
DF-31	<10	<10	7,200+ km
DF-31A	10-15	10-15	11,200+ km
CSS-5	85-95	75-85	1,750+ km
CSS-6	350-400	90-110	600 km
CSS-7	700-750	120-140	300 km
DH-10	200-500	45-55	1,500+ km
JL-2	Developmental	Developmental	7,200+ km

Note: China's Second Artillery maintains at least five operational SRBM [Short Range Ballistic Missile] brigades; an additional two brigades are subordinate to PLA ground forces—one garrisoned in the Nanjing MR and the other in the Guangzhou MR [Military Region]. All SRBM units are deployed to locations near Taiwan.

All potential US adversaries are aware that the US Missile Defense Agency (MDA) and its predecessor organizations has been working for decades to develop interceptor missiles to shoot down the lethal warheads of adversary missiles before they can strike their targets. Therefore, in addition to pursuit of quantity based overmatch, adversaries have added decoys and countermeasure to their missiles to increase the difficulty of US intercepts striking the warhead, the lethal object. The types of countermeasures that might be employed against the US rely on either decoy expendables, such as flares, balloons (infrared (IR), radio-frequency (RF) or both), radar absorbing material, booster fragmentation and other debris, waveform jammers or lasers.[7] All serve to confuse, decoy, overwhelm or degrade the system of systems from striking the lethal object. [8] Individual missiles could carry several to several dozen decoys and countermeasures.[9,10] Since an adversary would have the arsenal to launch raids of 100 cruise and ballistic missiles each carrying decoys and countermeasures, the threat scene US sensors would encounter is incredibly complex. Against this threat, the ability to discriminate the lethal object is critical.

Lasers – a Tremendous Opportunity but No Panacea for Missile Defense

Potential systems and actions that occur in a typical ballistic missile intercept are shown in Figure 1. In this example, a threat missile launch is detected by a space sensor, which then sends a cue to forward based radar, like the SBX or AN/TPY-2. The radar uses the cue to narrow down the region to search for the threat missile. The radar searches, acquires, and tracks the threat objects. Since an individual missile launch will cause dozens to hundreds of objects that the radars will track, the radar tracks the large objects, usually the warhead and the tank. The radar provides an accurate (low uncertainty) track to the weapon platform, in this case an Aegis ship, as well as any discrimination information. The weapons platform launches an interceptor to destroy the warhead.

To build a sufficient quantity of missile interceptors to counter the thousands of threat missiles would be cost prohibitive. In October 2013, the MDA awarded Raytheon a $3B contract to build 216 Standard Missile-3 (SM-3) Block 1B missiles.[11] At approximately $14M each, producing the many thousands of interceptors needed to counter the threat ballistic missile numbers is not affordable.

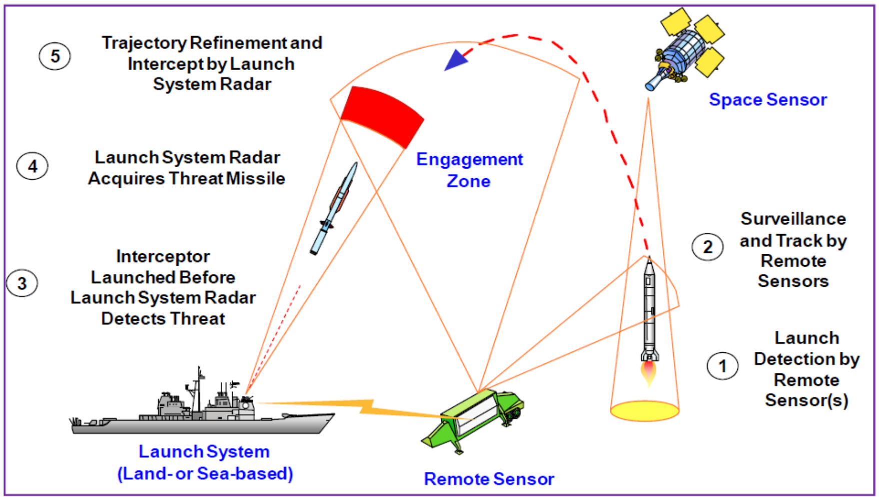

5
Trajectory Refinement and Intercept by Launch System Radar
4
Launch System Radar Acquires Threat Missile
3
Interceptor Launched Before Launch System Radar Detects Threat
Engagement Zone
Space Sensor
2
Surveillance and Track by Remote Sensors
1
Launch Detection by Remote Sensor(s)
Launch System (Land- or Sea-based)
Remote Sensor

Figure 1. Elements of a Typical Ballistic Missile Engagement[12]

The engagement kill-chain is complex and multiple handovers provide opportunity for error. Could other future weapon systems, lasers for example, change the paradigm by having the ability to shoot every viewable object out of the sky? Laser technology is likely to have become a reality for missile defense by 2040. The US Navy deployed its first Laser Weapon System (LaWS) capable of destroying drones and small attack ships in 2013.[13] The Navy's goal with the next generation of lasers, probably operational in the early 2020s, is to tap into the ship power grid to have mega-watt power free electron lasers capable of shooting down anti-ship missiles and fighters.[14]

The current generation of developmental solid state lasers weigh thousands of pounds and develop kilo-watts of power.[15] By 2040 several orders of magnitude of improvements[16] will occur for the lasers. They will have the ability to kill ballistic and cruise missiles at ranges of hundreds of miles, but these megawatt class lasers[17] will still be confined to ships with nuclear power plants and land locations that offer large power supplies, robust heat sinks, and no limits on size or weight. Thus, the number of lasers available will be relatively small, in the tens rather than hundreds of laser systems.[18]

There are also ways to countermeasure lasers (e.g. lots of small debris particles, spinning the warhead) and weather conditions (e.g. rain, snow, fog) that would significantly limit laser effectiveness. Thus, while lasers would be tremendously beneficial and enable deep magazines, they are not a panacea and do not negate the need to discriminate the lethal object. Since weather, countermeasures, and limitations on the number and ranges will still exist in 2040, there will be a continued need for interceptor missiles. Interceptors will continue to provide defense for the US from ICBMs with long-range exo-atmospheric intercept capability. Interceptors will also supplement regional defense in times that weather conditions limit laser effectiveness.

Identifying the lethal object will maximize the use of the US interceptor missile inventory by increasing the probability of killing the threat warhead and allows for changes in shot doctrine so fewer interceptors are needed per threat missile. Investing in sensors, C2, and discrimination capability has the potential to approximately double the effectiveness (number of intercepts) of the interceptor inventory[19,20] depending on the scenario and with shot doctrine changes. Thus 100 interceptor missiles would be as effective as 200 interceptors today. At approximately $14M per interceptor, this represents a $1.4B savings.

US Missile Defense – A System of Components or a System-of-Systems?

This leads to the question of what is needed to enable the US military to discriminate the lethal objects so weapon systems can target and destroy these lethal objects before they impact US defended areas? The most critical element in potential future conflicts is having and controlling information. The source of most of the information will be from various sensors that will provide data to C2 networks for US decision-makers. The main elements that make up the current US ballistic missile defense system (BMDS) are shown in Figure 2.

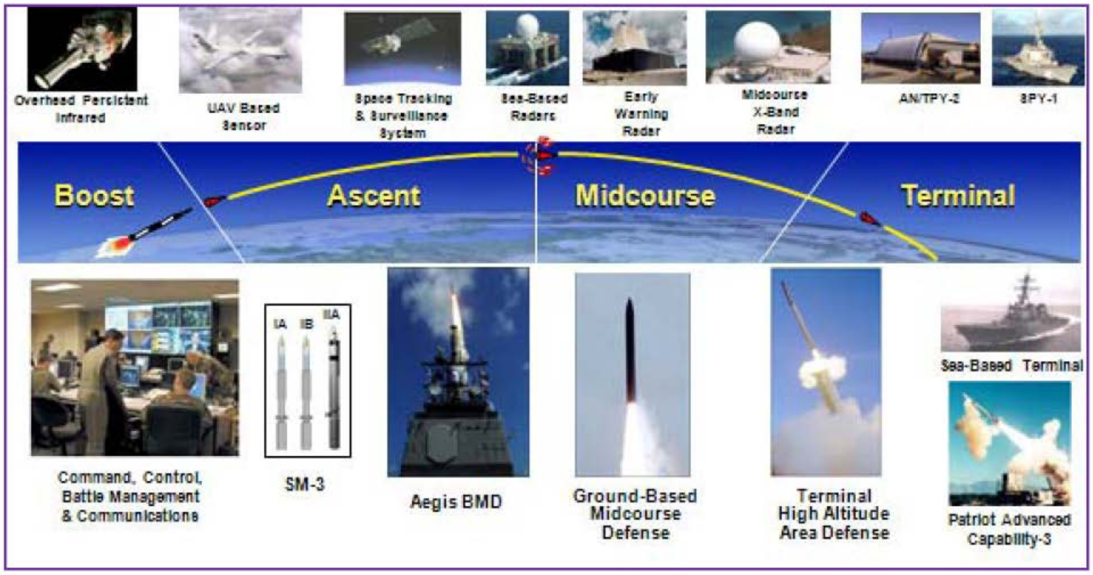

Overhead Persistent Infrared
UAV Based Sensor
Space Tracking & Surveillance System
Sea-Based Radars
Early Warning Radar
Midcourse X-Band Radar
AN/TPY-2
SPY-1
Boost
Ascent
Midcourse
Terminal
Command, Control, Battle Management & Communications
IA
IB
IIA
SM-3
Aegis BMD
Ground-Based Midcourse Defense
Terminal High Altitude Area Defense
Sea-Based Terminal
Patriot Advanced Capability-3

Figure 2. The Ballistic Missile Defense System[21]

First, we need to define what is meant by a SoS. Although there is still no consensus on a formal definition of SoS, Mark Maier[22] has identified five principal characteristics that are useful and widely used in characterizing SoS problems. These guidelines are commonly referred to as Maier's Criteria and are stated as follows:

- Operational Independence of Elements: The elements of the SoS can and do operate independently to serve useful purposes
- Managerial Independence of the Elements: The elements of the SoS are managed and operated independently
- Evolutionary Development: The SoS evolves with the addition, removal and modification of its functions
- Emergent Behavior: The SoS performs functions that none of its elements perform individually through the synergy of its elements
- Geographic Distribution: Components of the SoS are physically distributed and can only readily exchange information, not mass or energy

The US missile defense system meets Maier's definition of a SoS[23]. As depicted in Figure 3, the US missile defense SoS is composed of various sensors, communication paths, and weapons platforms each of which is a stand-alone system with organic capability. The overarching SoS is composed of a variety of radars that have varying capabilities and ranges. These can be integrated with weapon systems, Patriot, THAAD, Aegis, and GMD, to enable a diverse range of capabilities that no individual system (e.g. sensor, missile system) possesses. While each of the individual systems may be designed, developed and used separately, robust software, algorithms, and C2 network could enable each to also be used in concert with other systems. This missile defense SoS would provide information, correlate and fuse data to track air and exo-atmosperic movement, manage multiple concurrent engagements, discriminate warheads, and guide weapon systems to targets.[24]

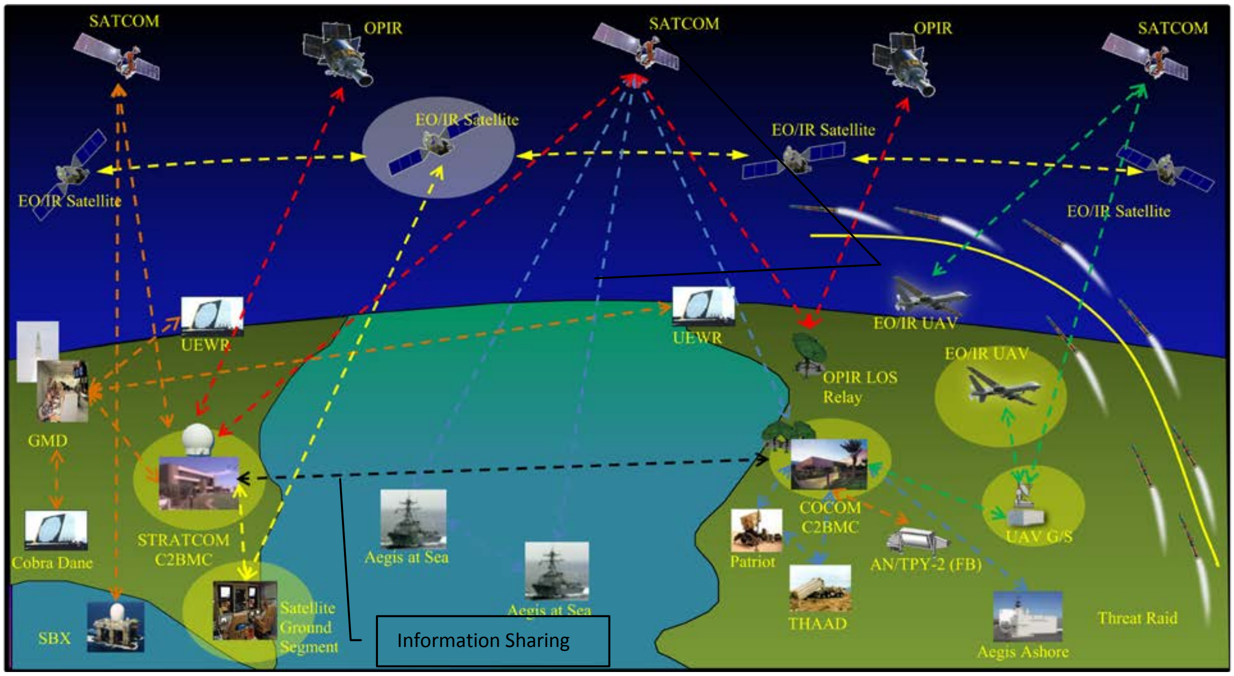


Figure 3. Integrated Missile Defense

Developing a way to design a SoS architecture of sensors, communication paths, and weapons platforms that maximizes the capability of whatever systems the US has at that time is critical. The architecture should be flexible and scalable[25] and able to take advantage of new capabilities as new systems are added. Too often when the US networks its systems together, the result is less than the sum of the capabilities of the individual systems. Additionally, there is evidence that China is working to develop cyber capabilities to “destroy the enemy’s political, economic, and military infrastructure”.[26] A deliberately designed SoS architecture is needed to enable security by defending against cyber attacks, monitoring internal data and functions so intrusions will be rapidly detected, robust so the system is not significantly degraded by the loss of a few component elements, and capable of degrading gracefully if portions of the system are destroyed or compromised.

As stated in the DoD Systems Engineering Guide for Systems of Systems[27], most military systems currently are and in the future will be part of a SoS even if they are not explicitly recognized as such or developed to be part of a SoS. When deployed, the operational commander brings together a mix of systems that are tied together to meet mission objectives. However, the DoD acquisition process was designed to develop independent systems. Most military systems today were created and then evolved without deliberate systems engineering at the SoS level. DoD programs are continuously becoming more and more interdependent, relying on data from one system to operate another. Examples of this are the suite of systems supporting the Air Operations Center (AOC) and the Single Integrated Air Picture (SIAP).

Per Mr. Vince Matrisciano[28], a current problem with the DoD approach to SoS is the SoS objective is often framed in terms of improved capabilities and not as a well-specified technical performance objective. He states that new development systems, particularly sensors, missile and laser weapons platforms, and C2 software will be operationally tied into a SoS, the systems engineering approach must be able to recognize the desired SoS end state capabilities and translate these to the individual program performance requirement at the start of program development.

Dr. Dan DeLaurentis[29], a leading SoS researcher at Purdue University, contends that the goal is to understand the desired operational SoS and then to start new programs that complement and tie seamlessly into the SoS. The state of the art in SoS research is attempting to identify underlying SoS principals that will enable the identification of potential new capabilities for the SoS, so that when new systems with these capabilities are developed and added to the SoS, positive emergent behavior occurs.

An Example – Software and Algorithms for Cyber and Graceful Degradation

Since the SoS will be subject to both physical attacks and cyber attacks it must have the capability to gracefully degrade. This attribute will result in a more robust total capability as well as continue to provide the best available information to both the C2 and the fire control systems. It is probable that all components of the SoS will be attacked by a capable enemy. Sensors, weapons platforms, and communication components like fiber and satellite could be attacked by missiles, direct attacks, or sabotage. Additionally, cyber attacks could be launched to corrupt the information transmitted or received generating false targeting solutions. Denial of service cyber attacks could clog the network bandwidth and prevent critical data from getting through. A cyber attack could also be used to target the infrastructure, take down the internet or even knock out the power grid. [30]

Future US military SoS, which all C2 systems are part of, need to be designed to enable a flexible response to cyber attacks. The C2 software should be able to isolate systems or sections of the SoS as part of a graceful degradation capability. The C2 software needs the ability to constantly compare results from each sensor with the results from data fused across all the sensors within and across phenomenologies to identify data that has potentially been corrupted, intentionally or unintentionally. The system needs the ability to allow the operators to decide to isolate information from systems that are no longer trusted.

For missile defense, the ideal system has multiple sensors across multiple-phenomenology and fuses data at the measurement level. Advantages of this approach are an improved ability to discriminate and the potential to design a system that both maximizes the SoS capability and can degrade gracefully in terms of the capabilities provided for C2 and to weapons platforms. The fusion of multiple data provides the benefits of non-coherent integration, where measurement accuracy can improve as the square-root of the number of independent measurements. This is true even when the data is from an individual sensor. Independence can be obtained either in time or angular diversity, thus data from multiple sensors that have angular diversity reduce the time needed to collapse track uncertainty ellipses.[31]

Multiple phenomenology sensor coverage provides significant benefits to defeat decoys and countermeasures. Many countermeasures are effective against only one phenomenology type of sensor. An example is chaff, which is effective against radars. Chaff is largely ineffective against infrared (IR) sensors, since the chaff cools quickly. This leads to questions of what type and what quantity of data is needed from each of the individual sensors, and where is the data fused?

As discussed in the SoS section, measurement level data as well as the sensor individual solutions (e.g. tracks, covariance, discrimination results) is preferred. This allows graceful degradation of the SoS. However, this does not imply that full focal plane video is needed or that all measurement data from every item a radar sees should be sent beyond the sensor. Background noise and debris data should be filtered. Even if there is the bandwidth capability to send this data, it should not be sent. This data provides little benefit to improving a centralized solution.

Key steps in intentionally graceful degradation of the missile defense SoS are:

i. Measurement fusion of multiple-phenomenology sensors

ii. Track fusion of multiple-phenomenology sensors

iii. Measurement/track fusion within a phenomenology, then comparison between phenomenology and pick best result to publish

iv. Pick best result from sensors

v. Results from individual sensors directly published to data links

Currently the individual sensors are being upgraded to enable better discrimination at the sensor. Raytheon is upgrading the AN/TPY-2 x-band radar's signal and data processing equipment (SDPE) to "more quickly and accurately discriminate threats from non-threats and enhance radar performance to protect against missile raids".[32]

Command and Control

The US has a hierarchical command-and-control system due to human capacity and span of control. The information is different at each level in the system. Currently a broader perspective and more information is available the higher one sits in the hierarchy. More specific information expertise and awareness of local conditions is understood at lower levels. In 2040, the US command and control will still be hierarchical. It will probably have fewer levels due to the ease of disseminating larger quantities of information to lower levels. Human capacity, however, will still be approximately the same, with possibly some increased ability to handle more data due to a lifetime spent in the increasingly interconnected world.

Previous research has determined that complexity frequently takes the form of hierarchy.[33] This is an expected result when complex systems result from the growth of smaller and simpler systems. Hierarchic systems have some common properties, regardless of their particular content. In a nearly decomposable (interactions between the entities are weak but not negligible) system, the short-run behavior of each entity is approximately independent of the other entities within the system. In the long run, the behavior of any entity depends only in an aggregate way on the other entities.

Decision-makers in complex situations have a continuing need for quantitative methods that enable superior decisions to be made (i.e., effective decision support systems). A command and control system is needed that can task sensors in real time, correlate and fuse data from any and all sensors, discriminate the lethal object, and provide accurate object position and velocity data with low uncertainties to the weapon systems.

Examples of some of the many sensors that will be tied into and providing the data for missile defense are shown at the top of Figure 3. Some examples of various possible message formats and connection paths to get sensor data into the C2 software are shown in the second layer of the figure. These examples are provided to show that various formats of data, various data rates, and data products can be provided from the sensors and successfully used by the C2 software to fuse improved tracks and predicted trajectories.

Algorithm development will continue to be limited to the ability of human developers. It is highly unlikely that an individual algorithm will provide good results against all threats under all conditions, all the time. Thus a suite of algorithms is needed with a method (an example is shown in Figure 4) to pick between the various algorithm results. This algorithm suite also enables a way to insert technology more rapidly than developing an entirely new software spiral.

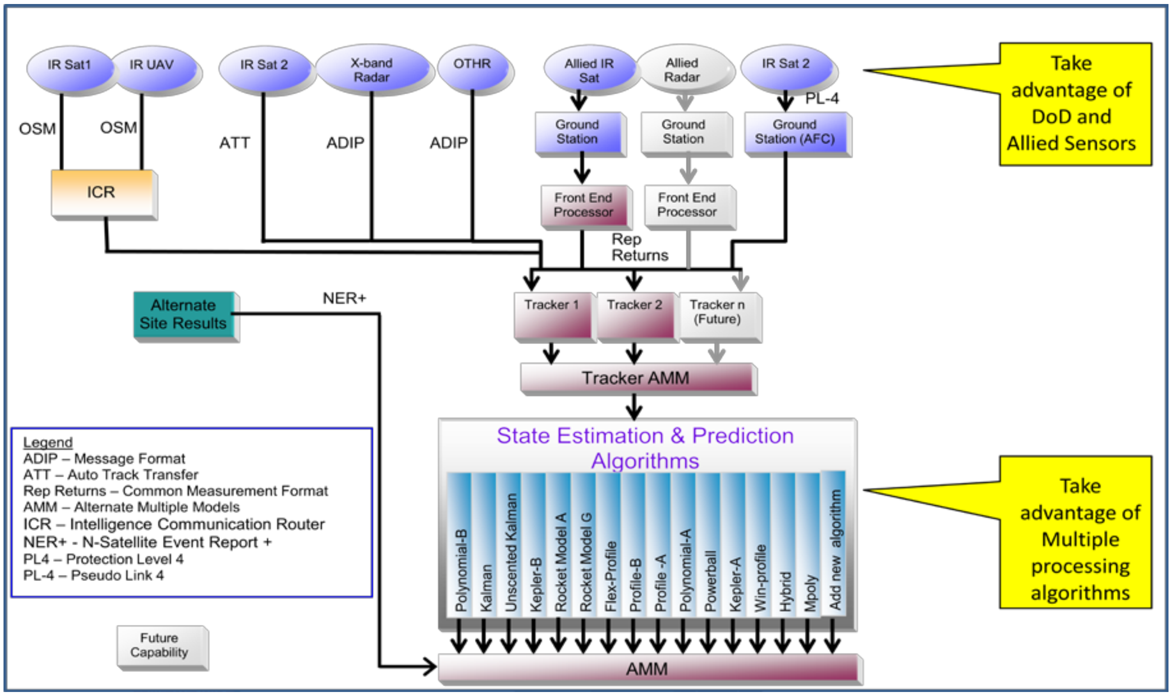


Figure 4. Notional Sensor and Algorithm Architecture

Programmatic and Bureaucratic Limitations

Bureaucratic inertia, programmatic priorities, and budget limitations frequently prevent needed technology investments. An example of this is the unencrypted data links used by the Predator UAV. As early as 1996, an official evaluation had warned about this vulnerability which ranged from image interception to active jamming. In the summer of 2009, US soldiers captured laptops in Iraq contained intercepted Predator video. Militants were being taught to systematically intercept and use video from US UAVs to avoid detection.[34] Thirteen years later, an identified vulnerability had still not been fixed.

Unfortunately similar decisions are frequently made during the development of C2 software. Open modular software has been a stated goal of US military acquisition for a decade. Large contractors have resisted this since open modular software would allow technology insertion and the ability to update portions of the software without spending for an entire software spiral development. Mr. Cliff Vroonland[35] contends that modular software updates and technology insertion open up the number of players that can compete for the work to small businesses, government laboratories and potentially even universities. He has seen numerous instances where by pricing the open, modular requirement outlandishly high, the large contractors have been able to maneuver government officials into cutting and reducing these requirements. Software updates are slowed since significant funding is needed to update the entire software spiral and many innovative algorithms, techniques and capabilities are not included. Additionally, algorithm funding is often short-changed, resulting in expensive hardware driven by cut-rate software that is not capable of fully using the data produced.

There are a number of programs that currently contend that they have or are developing C2 software in compliance with Modular Open Systems Approach (MOSA) standards or at least best practices. These claims should be tested by asking a few simple questions. Has the program developed and fielded a module of the software separate from paying to update the entire software spiral? Has a software contractor other than the contractor who made the open-modular software developed a new module that was successfully integrated? Has a full and open competition been held to select the contractor to develop a new software module? Even when program offices claim the software they developed is modular and open, the answer to these and similar questions is usually no. If this is the case, where are the cost savings and the ability to increase competition and innovation?

Recommendations

As discussed, the numbers, precision and capabilities of threat missiles continues to grow. The US military faces continued technical, programmatic and bureaucratic challenges in developing new capabilities, and shrinking DoD budgets and growing concern over US budget deficits only serve to exacerbate the challenges. Care must taken in prioritizing available funding to develop US missile defenses. Future uncertainty drives the need for approaches that provide the most flexibility in dealing with a range of potential scenarios. Technologies and programs that provide benefit in more than one DoD domain are also preferred.

Increased Investment Areas

There are four key areas that the DoD needs to invest research funding in now to develop the technologies, understand the complex systems, ensure the C2 data is trustworthy, and set the conditions to take advantages of emerging technology trends. First, the DoD needs to continue to invest in lasers. Lasers are gaining in capability and the next generation of lasers, currently under development by the US Navy, will have operational utility for close-in missile defense. While not sufficient on their own to defend against and defeat large cruise and ballistic missile attacks under all conditions, lasers will provide significant capability by 2040.

Second, increased investments are necessary in SoS engineering expertise, particularly in research to design for positive emergent behavior and for developing systems to address capability gaps in the operational SoS. The ability to design for positive emergent behavior will maximize the capabilities of the fielded SoS. Third, investment is necessary in how to design software for communications that results in resilient and robust SoS C2. This includes ensuring the data on the C2 systems is trustworthy. Watermarking or other methods of verifying that data is still trustworthy are examples of potential research areas. Fourth, the DoD also needs to look at how to add commercial sensor data to C2 software suites for missile defense. Commercial sensor data has the potential to cost effectively extent the sensor coverage of ballistic missile trajectories, which can be thousands of miles. The data could also be used to improve the quality of the tracks and even to help discriminate lethal objects since data from multiple phenomenologies provides significant benefit in identifying the various objects traveling together as a result of a missile launch.

Areas to Maintain

The US will continue to need interceptors, but no significant additional investment is required. While laser use for missile defense will grow, missiles will still be needed to have a robust capability in all weather conditions and to help defeat threat countermeasures. Algorithm development should be deliberately funded and continue with the current research and development (R&D) tools used. Government sponsored small business and University research are excellent methods to initiate the development of algorithms that are and will continue to be needed as technology develops and new sensors become available. Advances in cyber defense should be applied to this domain as it is developed for other applications.

Requirements and Doctrine

Requirements need to be developed that mandate software design that is open, modular and allows for easy technology insertion. Additionally, the software should allow suites of algorithms to be included and updated separately from updates of the entire software spiral. The government needs to ensure that it has the legal rights to all software and algorithms developed to enable and promote maximum future competition. While these requirements are currently known they frequently are not adhered to due to compromises made in program offices as funding and capability development trade-offs take place. Government data rights and modular open software development must not be traded away due to near-term budget short falls. Trading these items away significantly increases future costs and cripples the ability to rapidly insert new capabilities. Future software development should be required to follow these guiding principles.

Further Research Needed

There are several elements needed to enable the US to prevail in future engagements against an enemy with numerous advanced missiles that were not covered in this paper. First, multiple phenomenology sensor coverage of the engagement area is required to enable the correct identification of lethal objects from decoys and countermeasures. Research is needed to determine what types and quantities of these new sensors would be best as well as into how to create the robust and resilient communication networks required to fully leverage them.

Conclusion

The DoD must invest in SoS engineering and research so the government can understand how to allocate new system requirements against capabilities that address the needs of the SoS. Research is also required on how to design for positive emergent behavior. The goal is when systems are added to have 1+1=3 not 1+1=1.2 in terms of end SoS capabilities. The dollars invested in software and system of systems research will be pay benefits in domains far beyond missile defense.

Software development must be open and modular in fact not just in claim. This will save the government money by allowing for modular technology upgrades or insertions thereby reducing the costly expense of updating entire software spirals. It will also increase the ability to compete future developments with the added benefits of increasing innovation and decreasing costs. C2 software also must be designed with the ability to isolate part of the SoS to prevent data corruption or to respond to cyber attacks. The software needs to allow graceful degradation of the SoS, maximizing capability available based on current circumstances or while the system is under attack.

Algorithm development will continue to be a human endeavor and thus a limiting factor. Future software needs to be architected to enable rapid technology insertion. This includes the ability to add new algorithms to an algorithm suite within the software without needing to develop an entirely new software spiral. The goal is to be able to take advantage of new technology development or upgrades by adding the capability when it is available, not after the dollars for a new software spiral can be budgeted and the spiral developed and tested. New algorithms will also need to be added to take advantage of data from new sensors as these sensors become available as well as from ubiquitous commercial sensors.

The US will continue to need interceptors through 2040. This inventory should be scaled to respond to rouge state and non-state actor threats. The key and asymmetric limitation of interceptors is that they are too expensive to fully defeat the thousands of potential enemy missiles. Interceptors will also we needed to supplement the lasers that will be available in this timeframe. Lasers will continue to be limited to see and ground used with large energy sources and heat-sinks. Lasers will also be limited due to weather and countermeasures and should be supplemented by interceptors. Lasers have a potential with us in a few additional generations beyond the 2040 timeframe of almost completely replacing the need for interceptors. In the meantime, the US must invest in SoS to make the best use of its limited number of interceptors.

Notes

[1] Barry Watts, "The Maturing Revolution in Military Affairs," Washington, DC: Center for Strategic and Budgetary Assessments, (2011).

[2] Office of the Secretary of Defense, "Annual Report to Congress: Military and Security Developments Involving the Democratic People's Republic of Korea 2012." (2012), 15.

[3] National Air and Space Intelligence Center, "Ballistic & Cruise Missile Threat," NASIC-1031-0985-13, http://www.afisr.af.mil/shared/media/document/AFD-130710-054.pdf, (2013), 18.

[4] The Nonproliferation Policy Education Center, "Managing Nuclear Missile Competition Between India, Pakistan, and ?China," http://www.npolicy.org/article_file/Managing-Nuclear-Missile-Competition_260111_1824.pdf, (January 2013), 8.

[5] NTI, "Country Profile Iran: Missile," James Martin Center for Nonproliferation Studies at the Monterey Institute of International Studies, (January 2013) http://www.nti.org/country-profiles/iran/delivery-systems/.

[6] Office of the Secretary of Defense, "Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2010." (2010), 66.

[7] Andrew M. Sessler, John M. Cornwall, Bob Dietz, Steve Fetter, Sherman Frankel, Richard L. Garwin, Kurt Gottfried, Lisbeth Gronlund, George N. Lewis, Theodore A. Postol, and David C. Wright, "Countermeasures: A Technical Evaluation of the Operational Effectiveness of the Planned US National Missile Defense System," Union of Concerned Scientist, MIT Security Studies Program, (April 2000), 39.

[8] Waveform jammers are used to fool homing seekers by providing a confusing signal and either causes the seeker to break lock or to just miss the target. A growing source of jammer energy is lasers. Lasers can also be used to damage the delicate detectors in the seeker. Another countermeasure is sensor dazzlers which provide a veiling glare that is hard for a threat seeker to look through. See Department of Defense techipedia, "Electro-Optical Infrared Sensors." https://www.dodtechipedia.mil/dodwiki/display/techipedia/Electro-Optical+Infrared+Sensors. (Nov 12, 2013).

[9] Andrew M. Sessler et al, "Countermeasures," 42.

[10] Stephen D. Weiner and Sol M. Rocklin, "Discrimination Performance Requirements for Ballistic Missile Defense," The Lincoln Laboratory Journal, Vol. 7, No. 1 (1994), 73.

[11] Geoff Fein, "Raytheon secures USD3 billion contract for SM-3 Block 1B missiles." *IHS Jane's Defense Weekly*, (October 21, 2013).

[12] Department of Defense, "Ballistic Missile Defense Review Report." (February, 2010), 22.

[13] David Szondy, “U.S. Navy to deploy Laser Weapon System on warship,” http://www.gizmag.com/laser-laws/26978/, (April 9, 2013).

[14] Spencer Ackerman, “Watch the Navy’s New Ship-Mounted Laser Cannon Kill a Drone,” *Wired*, http://www.wired.com/dangerroom/2013/04/laser-warfare-system/, (April 8, 2013).

[15] Richard J. Dunn, III, “Operational Implications of Laser Weapons,” 7.

[16] Dave Ahearn, “ORN Laser Power Jumps 10 Fold; Further 10-Fold Leaps Seen,” *Defense Today*, (August 4, 2004), 4.

[17] Richard J. Dunn, III, “Operational Implications of Laser Weapons,” *Analysis Center Papers, Northrop Grumman*, http://www.northropgrumman.com/AboutUs/AnalysisCenter/ Documents/pdfs/Operational_Implications_of_La.pdf , (September 2005), 18.

[18] As example to illustrate the potential of lasers, let us assume it takes one seconds to deliver sufficient energy to destroy the target, and a further three seconds locate and move to a new target (Dunn, 10). This would result in four seconds required per object. For a large raid of one-hundred missiles with one-hundred objects produced per missile, ten-thousand incoming objects would be produced. At five seconds per object, it would take 40,000 seconds to destroy all incoming objects. To further develop this example, assume forty laser systems are available, which results in 1,000 seconds of needed engagement time. Using a typical ballistic missile speed of 5km/s and an effective radar range of 500 km, the available engagement time is 100 seconds, or approximately one-eighth the time needed.

[19] Stephen D. Weiner and Sol M. Rocklin, “Discrimination Performance Requirements for Ballistic Missile Defense,” 81.

[20] Richard J. Dunn, III, “Operational Implications of Laser Weapons,” 18.

[21] Department of Defense, “Ballistic Missile Defense Review Report,” 38.

[22] Mark Maier, “Architecting Principles for Systems-of-Systems.” (http://www.infoed.com/Open/PAPERS/systems.htm, May 24, 2004).

[23] An example of a complex system that is not a SoS is a modern commercial jet aircraft. There are many separate systems (engines, wings, tail section, etc.), that are combined to create the aircraft. Individually, these ‘systems’ are complex and challenging to design, and the resulting aircraft is a very complex system. It is not a SoS because the individual ‘systems’ have no utility separately. All the components must be continually configured to work together to have a functioning aircraft. The missile defense SoS, in contrast, employs individual radar and missile systems to perform their designed mission. Other SoS examples are the commercial air transportation system, the internet, and an ecosystem. Each of these examples has individual systems that operate and are managed separately, and provide utility as an individual system.

When combined with other systems, evolutionary and emergent behavior appears that any individual system lacks.]

[24] Reid Vander Schaaf, “A System-of-Sysem (SoS) Approach for Improved Decision-Making in Infrastructure Project Selection Problems,” (Purdue University PhD Dissertation, May, 2008), 2.

[25] H.C. Lambert and D. Sinno, “Bio-Inspired Resource Management for Multiple-Sensor Target Tracking Systems,” Project Report MD-26, Lincoln Laboratory, Massachusetts Institute of Technology, Lexington, Massachusetts, 2009), 1.

[26] Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare,* (Penguin Press, New York, New York, 2011), 118.

[27] Department of Defense, “Systems Engineering Guide for Systems of Systems,” (Version 1, August 2008).

[28] Vince Matrisciano, information provided by Mr. Matrisciano, vincent.r.matrisciano.civ@mail.mil, (November 2013).

[29] Daniel DeLaurentis, comments during an interview, (Associate Professor, School of Aeronautics and Astronautics, Purdue University, 701 W. Stadium Ave., West Lafayette, IN, December 4, 2013).

[30] Joel Brenner in his book *America the Vulnerable* argues that we are moving towards a “transparent world” where information will remain controlled and secret only for a limited amount of time. Information speed, not secrecy will be the critical component in gaining an advantage over opponents. China first started discussing the possibility of using cyber-attacks to paralyze an enemy’s military and financial computer networks twenty-five years ago in 1988, 118.

[31] The sensors and weapon platforms should be integrated by using robust satellite communication (SATCOM) (and fiber when available) to bring elements into the BMDS. Currently there is a teleport gateway used to interconnect elements through the Defense Information Systems Agency (DISA) backbone, and bring data into the Command, Control, Battle Management and Communications (C2BMC) for battle management and situational awareness, with a Cross Domain Solutions (CDS) used to distribute tactical data to additional weapon systems and coalition partners.

[32] Michael Nachshen, “Upgrades boost ballistic missile defense radar’s performance to protect against missile raid.” *Providence Journal*, October 23, 2013.

[33] H.A. Simon, *The Sciences of the Artificial, 3rd Ed,*. MIT Press, Cambridge, MA, (1996), 184.

[34] Joel Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*, 88,89.

[35] Cliff Vroonland, comments during an interview, (Vice President, Missile Defense Business Unit, Archarithms, Inc., 2904 Westcorp Blvd. Suite 101, Huntsville, AL 35805,December 5, 2013).

Bibliography

Ahearn, Dave. "ORN Laser Power Jumps 10 Fold; Further 10-Fold Leaps Seen," *Defense Today*, (4 August 2004).

Ackerman, Spencer. "Watch the Navy's New Ship-Mounted Laser Cannon Kill a Drone," *Wired*, (8 April 2013), http://www.wired.com/dangerroom/2013/04/laser-warfare-system/, (accessed 12 November 2013).

Brenner, J. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfar,* Penguin Press, New York, New York, (2011).

Cannon, S. M. and Cole, R.L. "Designing and Building an LCMC – Blueprint for a High-Performance Organization." *Army AL&T*, (January-March 2006).

Chaturvedi, A., Dolk, D. and Sebastian, H.J. "Agent-Based Simulation and Model Integration." *Workshop on Virtual Environment for Advanced Modeling (VEAM),* Honolulu, HI, (2-3 January 2004).

DeLaurentis, Daniel. Comments during an interview, (Associate Professor, School of Aeronautics and Astronautics, Purdue University, 701 W. Stadium Ave., West Lafayette, IN, 4 December 2013).

Department of Defense. "Ballistic Missile Defense Review Report." (February 2010).

Department of Defense, "Systems Engineering Guide for Systems of Systems," (Version 1, August 2008).

Department of Defense techipedia. "Electro-Optical Infrared Sensors." https://www.dodtechipedia.mil/dodwiki/display/techipedia/Electro-Optical+Infrared+Sensors (accessed 12 Nov 2013).

Dunn, Richard J.III. "Operational Implications of Laser Weapons," *Analysis Center Papers, Northrop Grumman*, (September 2005), http://www.northropgrumman.com/AboutUs/AnalysisCenter/Documents/pdfs/Operational_Implications_of_La.pdf (accessed 17 January 2014).

Lee, C. "AUSA 2013: Boeing to put EO sensor on Phantom Eye for ballistic missile tracking." *IHS Jane's Defense Weekly*, October 21, 2013.

Maier, M. (2004). "Architecting Principles for Systems-of-Systems." (24 May 2004), <http://www.infoed.com/Open/PAPERS/systems.htm> (accessed 5 December 2013).

Vince Matrisciano, information provided by Mr. Matrisciano, vincent.r.matrisciano.civ@mail.mil, (November 2013).

Nachshen, M. (2013). “Upgrades boost ballistic missile defense radar’s performance to protect against missile raid.” *Providence Journal*, October 23, 2013.

National Air and Space Intelligence Center, “Ballistic & Cruise Missile Threat,” NASIC-1031-0985-13,(2013) http://www.afisr.af.mil/shared/media/document/AFD-130710-054.pdf (accessed 4 December 2013).

The Nonproliferation Policy Education Center, “Managing Nuclear Missile Competition Between India, Pakistan, and ?China,” (January 2013), http://www.npolicy.org/article_file/Managing-Nuclear-Missile-Competition_260111_1824.pdf (accessed 27 January 2014).

North, M.J. “Towards Strength and Stability: Agent-Based Modeling of Infrastructure Markets.” *Social Science Computer Review*, Vol. 19, No. 3, (2001).

NTI, “Country Profile Iran: Missile,” James Martin Center for Nonproliferation Studies at the Monterey Institute of International Studies, (January 2013) http://www.nti.org/country-profiles/iran/delivery-systems/ (accessed 27 January 2014).

Office of the Secretary of Defense, “Annual Report to Congress: Military and Security Developments Involving the Democratic People’s Republic of Korea 2012.” (2012).

Rivkin, J.W., and Siggelkow, N. “Balancing Search and Stability: Interdependencies Among Elements of Organizational Design.” *Management Science*, INFORMS Vol. 49, No. 3, (2003).

Simon, H.A. *The Sciences of the Artificial, 3rd Ed.* MIT Press, Cambridge, MA., (1996).

Sessler, Andrew M.; Cornwall, John M.; Dietz, Bob; Fetter, Steve; Frankel, Sherman; Garwin, Richard L.; Gottfried, Kurt; Gronlund, Lisbeth; Lewis, George N.; Postol, Theodore A. and Wright,David C. “Countermeasures: A Technical Evaluation of the Operational Effectiveness of the Planned US National Missile Defense System,” Union of Concerned Scientist, MIT Security Studies Program, (April 2000).

Szondy, David. “U.S. Navy to deploy Laser Weapon System on warship,” (9 April 2013), http://www.gizmag.com/laser-laws/26978/ (accessed 27 November 2013).

Vander Schaaf, Reid. “A System-of-System (SoS) Approach for Improved Decision-Making in Infrastructure Project Selection Problems.” Purdue University PhD Dissertation, (May 2008).

Vroonland, Cliff. Comments during an interview, (Vice President, Missile Defense Business Unit, Archarithms, Inc., 2904 Westcorp Blvd. Suite 101, Huntsville, AL 35805, 5 December 2013).

Watts, Barry. “The Maturing Revolution in Military Affairs,” Washington, DC: Center for Strategic and Budgetary Assessments, (2011).

Weiner, Stephen D. and Rocklin, Sol M. “Discrimination Performance Requirements for Ballistic Missile Defense,” The Lincoln Laboratory Journal, Vol. 7, No. 1 (1994).