# \*\*Ground CP\*\*

# 1NC- Ground CP

### Text: The United States Federal Government should enhance the Distributed Common Ground System as per the 1NC ISB evidence.

### More sensors are bad- infrastructure such as the DCGS are critical for data integration and dispersion

ISB 8- Intelligence Science Board, Report of the Joint Defense Science Board Intelligence Science Board Task Force on Integrating Sensor-Collected Intelligence, November 2008, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics

The rapid proliferation of sensors both enables and overwhelms the current ISR infrastructure. The number of images and signal intercepts are well beyond the capacity of the existing analyst community so there are huge backlogs for translators and image interpreters and much of the collected data are never reviewed.

Further, decision makers and intelligence analysts have difficulty knowing what information is available. Most collection requests, particularly for sensors beyond the commander’’s control, go to central tasking systems that provide little feedback on whether or when the request will be satisfied. Access to ISR information is equally problematic. Large staffs, often numbering in the thousands, are required in theater to accept and organize data that are broadcast in a bulkdistribution manner. These analysts spend much of their time inefficiently sorting through this volume of information to find the small subset that they believe is relevant to the commander’’s needs rather than interpreting and exploiting the data selected on current needs to create useful information.

The investment made by the Department of Defense and the Intelligence Community over the last decade in creating the infrastructure for network-centric operations provides a way to address many of the problems with ISR data collection and processing. The task force noted recent ISR processing developments, such as the Distributed Common Ground System (DCGS) and RT10, where ISR sensor data are posted to a shared data store along with meta-data to describe them. The meta-data are searchable, allowing users to pull data of interest in a manner similar to Internet searches. We believe that the Defense Department and Intelligence Agencies should take all possible actions to accelerate the transition to this new paradigm leveraging the integrated sensor-collected intelligence architecture as shown in Figure 1.

The key elements of this architecture include assured broadband, ubiquitous communications system and implementation of the Department’’s data strategy, which calls for separation of data and applications and meta-data tagging. The communications2 capability includes two major components –– a terrestrial-based high capacity core built on the Defense Information System Network (DISN) investment (largely through the Global Information Grid –– Bandwidth Expansion (GIG-BE) program) to provide the capability to transfer data from sensors to accessible storage and satellite and airborne links to download sensor data to the core and to 2 While nomenclature is inconsistent, this entire communications system is often referred to as the Global Information Grid provide mobile users access to the ISR data. The meta-data tagging makes the sensor information discoverable by authorized users. The recommended architecture has not only the potential to alleviate the major bottlenecks in the existing ISR process but it also facilitates integrating data from multiple ISR sensors to provide important improvements in sensitivity and detection times, thereby increasing the performance of whatever sensor systems are acquired and deployed.

# Ground CP- Solvency- Sensors/=Solve Data

### Sensors creates intelligence problems- integration is more important

ISB 8- Intelligence Science Board, Report of the Joint Defense Science Board Intelligence Science Board Task Force on Integrating Sensor-Collected Intelligence, November 2008, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics

In this study, the task force took a broad view of what constituted a ““sensor.”” We observed that there are classes of intelligence problems –– such as determining the intent of nations and their leaders, detecting and tracking people, monitoring deeply buried facilities and discovering WMD and its precursor agents –– that may be difficult or impossible for physical sensors due to lack of detectable signatures. In these cases, human intelligence (HUMINT), cyber ISR and other nontraditional techniques will be essential. In information poor situations, where the required sensors do not exist or where access to the target is very limited, the benefits of sensor integration will be hard to achieve. However, if there are relevant physical signals, even if they are very weak, the recommended architecture will improve performance of traditional sensors by enhancing the ability to integrate these data with HUMINT, cyber and other nontraditional information.

# Solvency- Situational Awareness

### DCGS create interoperability and collection of data- leads to enhanced situational awareness

ESRI 9- Esri develops geographic information systems (GIS) solutions that function as an integral component in nearly every type of organization. July 22, 2009 http://www.esri.com/industries/defense/pdfs/air\_force\_dcgs.pdf

The past several years have proved the need for persistent intelligence, surveillance, and reconnaissance (ISR) for U.S. armed forces. They require real-time information to gain decision superiority and dominate the battle space.

The Air Force’s (AF) major ISR system, largely made up of legacy components and known as the Distributed Common Ground System (DCGS), recently struck a major evolutionary milestone. The Electronic System Center’s Intelligence Surveillance and Reconnaissance Integration System Program Office awarded the AF DCGS Block 10.2 upgrade contract to an industry team of major companies led by the Raytheon Corporation. The Synergy of Networkcentric Technologies, GIS, and the Distributed Common Ground System’s Integration Backbone (AF DCGS Block 10.2)

The Raytheon-led team is working shoulder to shoulder with the U.S. Air Force to transform the current tasking, processing, exploitation, and dissemination (TPED)-based DCGS system into the task, post, process, and use (TPPU) model. Current ISR systems feed data into platformcentric “stovepiped” tasking, processing, exploitation, and dissemination systems operating independently of each other. Because of this partitioning, commonality and interoperability are restricted between the services, which limits their ability to operate in a joint and coalition environment. AF DCGS Block 10.2 overcomes these obstacles.

With the introduction of the AF DCGS Block 10.2 DIB capabilities, current intelligence data is posted to the network for immediate use by analysts and war fighters and is integrated with other assets to produce situational awareness of the battle space.

ISR knowledge is presented to users in many ways, primarily through the use of a commercial Web-based architecture and technologies and integration, via the DIB, of multiple intelligence systems into a single, worldwide networkcentric enterprise, thus enabling interoperability and improved collection and delivery of ISR data. AF DCGS Block 10.2 Web-based technologies will transform ISR into an integrated element of DoD command and control systems. The AF DCGS Block 10.2 DIB system’s open architecture was developed so that any node or workstation within the Air Force DCGS organization can share intelligence across a worldwide network

# Solvency- Deterrence / No Link Spending

### Integration can’t be achieved with more sensors-improves net work centric warfare

ISB 8- Intelligence Science Board, Report of the Joint Defense Science Board Intelligence Science Board Task Force on Integrating Sensor-Collected Intelligence, November 2008, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics

The integration of sensor information across multiple sensors is enabled by the net-centric infrastructure of broadband, assured communications. As discussed in the last section, this integration can provide benefits of a significant magnitude to U.S. military forces and the Intelligence Community. However a new architecture must be created before these benefits can be fully realized. Figure 4, Integrated Sensor-Collected Intelligence Architecture, illustrates the required integrated sensor-collected intelligence initiative.

Capabilities enabled by this architecture include leveraging angle diversity, simultaneous looks from different sensors, exploitation of multi-INTs phenomenology, use of machine-to-machine data transfer to decrease cycle times, data driven tasking, and upstream processing of multiINTs. This architecture will also allow significant improvements in the optimum use of human capital.

Useful integration cannot be achieved by increasing the number of sensors alone. The following elements must be incorporated into the architecture: 􀂃 Meta-data. Meta-data is critically important to effect the capabilities desired. Benefit = enhanced situational awareness 10x speed improvement Social Networks (RT10) Benefit = Counters deceit and deception tactics aimed at single Int ~100x improvement in geolocation and detection improvement of 4-8 dB SNR Angle Diversity Benefit = improved detection probability Equivalent􀀃4 dB SNR improvement Upstream Multi-INT Sensor Integration Benefit = improved target tracking convergence 3x to 10x reduction in position error >10x reduction in convergence time Benefit = faster convergence in prosecuting fleeting targets ~10x improvement in geolocation 10x reduction in time Cooperative Target Tracking Passive Geolocation\* \* On-going programs briefed to DSB ISR panel = NCCT and AOIO assured and a low probability of interception communications. 􀂃 Disaggregate. The disaggregating of data from the applications enables significant improvements to apply innovative techniques and to extract more valuable information from sensors. 􀂃 Net-Centric Services Strategy. Complying with net-centric enterprise services facilitates the inclusion of value-added services.

The inclusion of these elements into the architecture is necessary for improved sensor integration. However, since the DoD is pursuing many of these attributes to support net-centric warfare, performance improvements should be available at little or no increase in infrastructure costs.

# Solvency- Data Sharing

### DCGS enables data sharing

ESRI 9- Esri develops geographic information systems (GIS) solutions that function as an integral component in nearly every type of organization. July 22, 2009 http://www.esri.com/industries/defense/pdfs/air\_force\_dcgs.pdf

The AF DCGS 10.2 upgrade of the Air Force ISR DCGS System will enable networkcentric operations using the DCGS Integration Backbone (DIB) for the U.S. armed forces as each service develops its own system.

DIB can trace its lineage from the Chairman’s Joint Vision 2020, Defense Planning Guidance, Quadrennial Defense Review and Service modernization and transformation efforts.

The Department of Defense (DoD) envisions DCGS as a globally integrated, distributed, and collaborative information technology enterprise. AF DCGS Block 10.2 will provide continuous, on-demand intelligence to achieve full-spectrum dominance so that American and Coalition forces can change the mission objectives in hours, minutes, or even seconds. The environment provides physical and electronic distribution of ISR data, processes, and systems.

# \*\*EU CP\*\*

# 1NC- EU CP

### ESA has the capability for enhanced SSA- esa has better sharing and solves barriers inherent in the U.S. military

Ackerman 10- Edward T. Ackerman, Lt Col, Usaf , Us Military, Commercial, and International Cooperation for Improved Space Situational Awareness, 17 February 2010

In the case of international partners, ESA could offer valuable input to improve SSA. Additionally, ESA‟s 18 members49 are all partnered with NATO, indicating a cooperative orientation towards the United States.50 As ESA is already considering its own SSA capability via a network of sensors from ESA countries, establishing an initial shared capability is possible by tying the ESA network together with the SSN. In such a relationship, NASA could provide an initial “pass-through” between the military and ESA, as NASA and ESA already have established agreements and mechanisms for sharing information and providing mutual support.51 This arrangement avoids any USC Title 10 conflicts regarding the military providing support to a foreign country. Next, non-ESA NATO countries and others in US military alliances could be given the opportunity to join if they possessed a contributing SSA capability, such as a sensor site or satellite. Leveraging existing mechanisms for military-to-military sharing of information within the alliance structures, once again mitigates challenges associated with US military support to foreign entities.

# EU CP- Solvency- Implementation

### Political will exists for SSA- space policy requires space surveillance

UNIDIR 6- United Nations Institute for Disarmament Research Building the Architecture for Sustainable Space Security Conference Report 30–31 March 2006

There are very specific requirements regarding the need for information about ground-, air- or sea-based assets and events. Regarding SSA, there is the shared view that it is needed, but specific common requirements for such a complex system, which could lead to necessary measures, are not yet in place. The civilian user seems to be mainly concerned with space debris and space weather, while the military interest seems to focus on “complete” SSA and early warning. Some civilian capabilities (only space debris related) are available in Europe. The military staffs are developing space-related needs for military operations including the need for space surveillance. The definition of a European space policy encompassing both civilian and defence demands requires the definition of a comprehensive SSA system that serves all user communities and takes advantage of the multiple-use character of space systems. In addition, recent technological developments—for instance, small, agile satellites— should be included in the considerations regarding space surveillance.

# EU CP- Solvency- Debris

### ESA has the tech for debris tracking- implementing debris mitigation in the squo

Senechal 7 [Thierry, Policy Manager of the Commission on Banking Technique and Practice at the International Chamber of Commerce Space Debris Pollution: A Convention Proposal, October 26, 2007 http://www.pon.org/downloads/ien16.2.Senechal.pdf]

ESA has a long history in tracking space debris. In 1986, the Director General of ESA created a Space Debris Working Group with the mandate to assess the various issues of space debris. The findings and conclusions are contained in ESA's Report on Space Debris, issued in 1988. In 1989, the ESA Council passed a resolution on space debris where the Agency‘s objectives were formulated as follows: 1) Minimize the creation of space debris; 2) reduce the risk for manned space flight, 3) reduce the risk on ground due to reentry of space objects, 4) reduce the risk for geostationary satellites. ESA‘s Launcher Directorate at ESA Headquarters in Paris also coordinates the implementation of debris mitigation measures for the Arianespace launcher. Over the last few years, ESA developed debris warning systems and mitigation guidelines. Following the publication of NASA mitigation guidelines for orbital debris in 1995, ESA published a Space Debris Mitigation Handbook, issued in 1999, in order to provide technical support to projects in the following areas: Description of the current space debris and meteoroid environment, risk assessment due to debris and meteoroid impacts, future evolution of the space debris population, hyper-velocity impacts and shielding, cost-efficient debris mitigation measures. The Handbook has

already been updated.19

### ESA SSA is capable of detecting debris in LEO

Bobrinsky et al 10 - The Space Situational Awareness Program of the European Space Agency N. Bobrinsky1 and L. Del Monte2 1 ESA/ESOC, Darmstadt, Germany 2 ESA/DG, Paris, France The organization principles of constructing the European system October 14, 2010 http://www.springerlink.com/content/a592j95k5l113715/fulltext.pdf

The solar system is full of natural objects other than the large planets ranging from dust in the micro to mmsize range, to asteroids and comets whose size is of order of several tens of kilometers. The largest aster oids are several hundred kilometers in diameter. The Earth is permanently bombarded with these particles arriving from the Solar System or beyond it. It is estimated that a few tons of material hit the Earth every day. In most cases this is dust which is unable to do any harm, but larger objects can reach the Earth and cause considerable damage. The effect of these collisions in terms of energy release is shown in Table. By now about 5000 NearEarth Objects have been identified. The larger an object, the brighter it is and, therefore, easier to detect. Thus, our knowledge of NEOs is heavily biased towards the larger objects, while many of the smaller but nevertheless dangerous objects are not identified. It is estimated that several hundred thousand objects exist with the size of the Tunguska meteorite. The SSANEO system will be capable of detecting, monitoring, and characterizing NEOs. It will determine the threat to the Earth and its population and issue appropriate warnings. Studies

related to possible mitigation actions will be pursued.

# EU CP- Solvency- A2:Hegemony

### ESA ssa is key to international cooperation

Keplerlaan et al 10- The NearEarth Objects Segment of the European Space Situational Awareness Program G. Drolshagen1, D. Koschny1, and N. Bobrinsky2 1 European Space Agency, ESA/ESTEC, Keplerlaan 1, Postbus 299, 2200 AG Noordwijk, The Netherlands 2 European Space Agency, ESA/ESOC, RobertBoschStr. 5, 64293 Darmstadt, Germany Received January 12, 2010

The SSA–NEO segment will play an important

role in the area of coordination and international

cooperation. Its envisaged tasks and responsibilities

will include the following.

—To provide reliable information for decision

makers, interested parties, and the general public.

—To issue impact risk warnings if required.

—To serve as an interface with the United Nations

and other international bodies on NEO matters.

—To support the development of related policies.

—To support studies and developments of mitiga

tion measures.

—To support joint observational campaigns.

—To coordinate the NEO related activities.

The SSA–NEO segment will also support the

study, design, and potential realization of missions

deflecting asteroids from collision trajectories. Several

feasibility studies have been performed already, e.g.,

the Don Quijote mission by the ESA, which considered

the use of an orbiter and impactor for studying the

deflection of an asteroid [10]. A true asteroid deflec

tion mission can only be performed in close interna

tional collaboration.

### SSA cooperation is critical- causes collaboration

Bobrinsky et al 10 - The Space Situational Awareness Program of the European Space Agency N. Bobrinsky1 and L. Del Monte2 1 ESA/ESOC, Darmstadt, Germany 2 ESA/DG, Paris, France The organization principles of constructing the European system October 14, 2010 http://www.springerlink.com/content/a592j95k5l113715/fulltext.pdf

The international cooperation of the SSA is becoming increasingly important. As a matter of fact, in all the domains of the SSA (Space Surveillance and Tracking, Space Weather, NEOs), contacts, exchange of views, and in some case exchange of data and infor mation are already taking place on a regular basis in various forums, such as: —Bilateral meetings between cooperating Agen cies; and —International workshops and conferences. The European SSA Program itself is based on international collaboration (within Europe) whose first phase aims at federating the existing and available National and European assets. A true and effective cooperation with non Euro pean Space Powers (US, Russia, Japan, China) is cer tainly one of the major challenges facing the SSA Pro gram in the years to come. Several meetings have already taken place with the various competent US institutions. They were mostly targeted at the technical aspects of the project. A swift progress is expected in the near future as soon as the political and administrative aspects of the European SSA System in the data dissemination field will be reg ulated

### ESA SSA is key to effective governance of data

Bobrinsky et al 10 - The Space Situational Awareness Program of the European Space Agency N. Bobrinsky1 and L. Del Monte2 1 ESA/ESOC, Darmstadt, Germany 2 ESA/DG, Paris, France The organization principles of constructing the European system October 14, 2010 http://www.springerlink.com/content/a592j95k5l113715/fulltext.pdf

As stated in the report of the ESA Council in response to the SSA Program Proposal, a well funded and strongly implemented SSA can serve the ambitious goals of Europe to become one of the most dynamic knowledge based societies in the world thus providing a favorable platform for Europe’s institutions, organiza tions, industry and scientists to maintain a leading edge in preserving the sustainable and peaceful exploitation of outer space while reinforcing global safety and security. In adopting the SSA Program and launching its preparatory phase, the European Union and its Mem ber States have recognized the necessity and usefulness for Europe to have at its disposal an independent and well performed SSA System. Such a system will reduce the dependency of Europe on non European Space Pow ers. It will also provide Europe with the capability to defend its critical space, air, and ground assets against the effects of space debris, space weather, and NEOs. Finally, based on an agreed data policy and gover nance scheme currently under discussion, Europe is prepared to share SSA information with other Space Powers, for the benefit of all the interested and coop erating parties

# EU CP- Solvency- Data Integration/Debris

### ESA SSA has the infrastructure of data integration- solves debris and overall networking

Keplerlaan et al 10- The NearEarth Objects Segment of the European Space Situational Awareness Program G. Drolshagen1, D. Koschny1, and N. Bobrinsky2 1 European Space Agency, ESA/ESTEC, Keplerlaan 1, Postbus 299, 2200 AG Noordwijk, The Netherlands 2 European Space Agency, ESA/ESOC, RobertBoschStr. 5, 64293 Darmstadt, Germany Received January 12, 2010

The SSA–NEO segment will play an important

The European SSA–NEO system will be based ini tially on existing facilities and capabilities. Later, ded icated sensors and instruments will be added. Europe has many optical telescopes, located within or outside Europe, and several radars which are suitable for NEO observations. These facilities were originally built for other purposes. For example, the ESA’s Optical Ground Station was built for optical communications with satellites, but it was regularly and successfully used for space debris and more recently for asteroid observations. Numerous national research telescopes exist at various locations and have different apertures. Some of these telescopes can be used on a regular or occasional basis for NEO observations. Many amateur telescopes which could make valuable contributions to this field also should not be forgotten.

Existing European radar facilities were mainly built for military purposes, but some of them can be used on special occasions for NEO observations, as it took place in the past for space debris observations (e.g., the German FGAN and the French GRAVES systems). A unique European NEO asset is the Near Earth Objects–Dynamic Site (NeoDys). The NeoDys sys tem was established in 1998 and is continuously improved [5]. It is a duplicate system whose elements are located at the Universities of Pisa (Italy) and Vall adolid (Spain). Based on astrometric measurements obtained worldwide and collected centrally by the MPC, NeoDys computes NEO orbits and predicts their further motion. It then computes impact risks for NEOs on a regular basis (everyday updates). NeoDys keeps a risk list, and it contains a database with infor mation on all known asteroids and NEOs. The NeoDys website also contains a link to European Asteroid Research Node (EARN) which is a database of physical properties of NEOs [6]. EARN was devel oped by DLR in Berlin and is updated on a regular basis.

Other existing European structures include the Spaceguard facility [7] and the Planetary Database [8]. Spaceguard is an association aimed at the protec tion of the Earth environment against the bombard ment of objects of the Solar System. It maintains a pri ority list of NEO which require additional observa tions. The Planetary Database was originally developed as a source of information on nonspherical gravitational fields of the Solar System’s bodies. It can serve as kernel of a wider database for all NEO infor mation.

# EU CP- A2: Perm

### Duplicate SSA systems will fail

UNIDIR 6- United Nations Institute for Disarmament Research Building the Architecture for Sustainable Space Security Conference Report 30–31 March 2006

 In view of this diverse scenario, there is a need for a coordinated discussion at the European level and initiating an activity aimed at generating a detailed common understanding of needed space surveillance capabilities and at the development of a characterization of SSA, with a mutually accepted requirement list. This activity is based on the assumption that military and civilian interests overlap. In any case, duplication should be avoided and only one space surveillance system should be developed. It is foreseen that a group of experts representing all space surveillance user communities will compile a list of needs as a first step. Considering this list of needs, the already available and planned assets that could support an SSA system will be assessed in order to identify detailed capability gaps. In parallel, architectural/feasibility studies will be conducted to support the identification of user needs and requirements by offering technical solution options, including ground- and space-based components, serving all user communities. The activity should result in a credible programme proposal for the development of a space surveillance system serving national and common interests.

# EU CP- AT: No Tech

### ESA will procure all tech for a SSA

Bobrinsky et al 10 - The Space Situational Awareness Program of the European Space Agency N. Bobrinsky1 and L. Del Monte2 1 ESA/ESOC, Darmstadt, Germany 2 ESA/DG, Paris, France The organization principles of constructing the European system October 14, 2010 http://www.springerlink.com/content/a592j95k5l113715/fulltext.pdf

The architecture of the future European SSA Sys tem will be based, as a result of a progressive integra tion process, on the federation of already existing and available national assets, together with the newly developed and procured elements. The use of existing and available national assets in the construction of a European integrated system is compliant with the principles expressed in the ESP.

The procurement of the elements that will be part of the future European SSA System will be realized in successive phases of the SSA Program, in line with the decisions made by the participating States and alloca tion of corresponding funds.

The European SSA system will be based on the requirements formulated after consultations with the SSA User community. It will offer technical and oper ational responses to the three main segments of SSA: 1) Space Surveillance and Tracking (SST); 2) Space Weather (SWE); and 3) NearEarth Objects (NEO).

# \*\*Commercialization CP\*\*

# Commercialization 1NC

**TEXT: The department of defense should transfer all space situational awareness programs to the commercial satellite communications industry and all data integration from these satellites to the space data association**

**SDA has the ability to integrate data from commercial satellites- effectiveness is only possible without government involvement- large demand for SSA exists**

Committee on the Peaceful Uses of Outer Space 11- Scientific and Technical Subcommittee Forty-eighth session Vienna, 7-18 February 2011 Item 7 of the draft provisional agenda\*Towards Long-term Sustainability of Space Activities: Overcoming the Challenges of Space Debris A Report of the International Interdisciplinary Congress on Space Debris http://www.oosa.unvienna.org/pdf/limited/AC105\_C1\_2011\_CRP14E.pdf

The Space Data Association (SDA) is a non-profit association founded by satellite operators Inmarsat, Intelsat, and SES. SDA’s mandate is to exchange operational data to help ensure safety, provide technical support to improve operational integrity, and share the associated costs.43 The “Space Data Center” provides and shares information among fellow operators regarding satellites under their control. As of January, 2011, the Space Data Center has twenty participating operators and provides safety services for almost 1200 satellites in GEO and 114 satellites in LEO.44 The Data Center is an interactive repository for commercial satellite orbit, manoeuvre, and frequency information. Satellite operators routinely deposit their fleet information into the Data Center and retrieve information from other member operators when necessary. The Data Center allows operators to augment the existing Two Line Element (TLE) data with precision orbit data and manoeuvre plans from the operator’s fleets.

One major shortcoming of the Data Center is that its operators must still rely on governments, and primarily the U.S. Government, to monitor dead satellites and other objects drifting in GEO that could collide with active satellites. In addition, separate tools are necessary to exchange data with each operator. Some operators write their own software tools for monitoring and predicting the close approach of other spacecraft while others contract with third parties for this service. The magnitude of the effort to maintain “space situational awareness” grows quickly as the number of coordinating operators increase. To mitigate this, the SDA has developed tools to automatically translate data between the different formats used by the operators. Unfortunately some operators are not able or willing to participate in close approach monitoring due to lack of resources or capabilities. The SDA Space Data Center is currently being expanded to:

• Develop data sharing relationships with governments and other data providers

to get access to tracking data on space debris;

• Provide collision avoidance manoeuvre planning assistance to operators; and

• More satellite operators.

### COMSATCOM has the ability to provide every deterrence function- 80 percent of DOD satellites are commercial

NSTAC 9- National Security Telecommunications Advisory Committee NSTAC Report to the President on Commercial Satellite Communications Mission Assurance November 2009

In recent years, the commercial satellite communications (COMSATCOM) industry has significantly increased its support to Government users, supplying a wide range of advanced voice, data, and video communications services. The uniquely flexible nature of satellite networks offers mobile communications services, ubiquitous coverage over large geographic areas, and greater access to remote areas or difficult terrain. Satellite networks can quickly provide surge capacity to aide in terrestrial critical infrastructure restoration efforts in the event of an emergency or crisis operation. Meanwhile, U.S. reliance on satellites for military and economic success has grown dramatically in recent years, making protection of space assets a priority. As a result, the need to protect space assets has increased.1 Currently, commercial satellite systems provide over 85 percent of the Department of Defense’s (DoD) global satellite communications (SATCOM), and commercial satellite links are used to operate almost all unmanned aerial vehicles in Afghanistan and Iraq. The DoD also estimated that 80 percent of the satellite communications capacity used for Operation Iraqi Freedom was provided by commercial satellites.2 Figure 1 below depicts the DoD’s increasing expenditures and use of commercial fixed satellite service bandwidth.

Services offered by the commercial satellite industry are critical to maintaining national security and emergency preparedness (NS/EP) communications and mission assurance because satellites: (1) offer primary and back-up communications; (2) facilitate continuity of operations services; (3) offer customers point-to-multipoint communications; (4) serve as an alternative in the event of a terrestrial wireline or wireless network outage; (5) provide restoration services to terrestrial critical telecommunications and utilities (oil, gas, electricity, and water) infrastructure; (6) offer diversified and distributed commercial owner/operator facilities; and (7) reside in an environment that makes assets highly resistant to many natural and terrestrial effects.

Satellite communications are a part of the Nation’s critical infrastructure, identified as such various Executive Orders4 and Presidential Directives,5 that provide key communications capabilities to the Federal Government. See Appendix H for high-level descriptions of the Executive Orders and Presidential Directives that support the requirement to use satellite communications during emergencies and for continuity of Government.

# SDA CP- Government Data Bad- Unreliable

### Private sector is reducing reliance on government data- not updated and lack of precision

Smitham 10- Matthew C. Smitham, Lt Col, USAF, The Need for a Global Space-Traffic-Control Service: an Opportunity for Us Leadership, 17 February 2010 Air War College

Air University

A new US government initiative is also emerging. In 2003, Congress directed the Secretary of Defense to conduct SSA for all US government space systems and as appropriate for commercial and foreign entities (CFE). In response, USAF Space Command made available conjunction analyses via the Space-track.org website to non-governmental entities as a pilot program. As of September 2009, 18 commercial companies, which operate 66 satellites, have signed quid-pro-quo agreements with the US government for conjunction analyses and launch support. In October 2009, USAF Space Command transitioned CFE to US Strategic Command as an operational program. However, high-precision conjunction analyses needed for effective collision avoidance are not universally available. This is limited to high-value satellites (as prioritized by the US military) because it is labor intensive and not automated.

Along with Space-track.org (as part of CFE), several other public-domain services such as HeavensAbove.com and Celestrack.com also publish the space catalog on the internet. Although they provide a valuable service, they are not necessarily providing new data. Essentially, they re-publish the unclassified space catalog provided by the Air Force, the so called “two line element” (TLE) sets. Although available to the world, these TLE sets do not have the requisite accuracy needed for precision conjunction analysis. In fact, the Air Force warns Space-track users to use the data at their own risk.

42 In addition, at least 6,000 objects do not appear in the Space-track catalog because the launching nation could not be identified.43 In an apparent response to this, three of the world’s largest commercial satellite operators—Intelsat, SES and Inmarsat—in a cooperative private venture, created the Space Data Association in November 2009. They expect eight companies to participate in collision avoidance and another 14 companies to be involved in reducing satellite radio-frequency interference. Although they acknowledge the US CFE program has some benefit, they feel compelled to invest their own capital because the “information is not always as precise or up to date—nor is it disseminated as quickly—as it needs to be to protect against close encounters between satellites.” With these restrictions and limitations, the underlying message is users need more accurate data. 44

# SDA CP- Solvency- SSA

### SDA would create the first global effort towards enhanced SSA- SDA is positioned to be an asset to the DOD

Space News 9- Wed, 18 November, 2009 Satellite Operators Solicit Bids To Create Orbital Database By Peter B. de Selding <http://www.spacenews.com/satellite_telecom/091118-satellite-firms-moving-ahead-orbital-database.html>

Three of the world’s largest commercial satellite operators have issued a request for proposals for a company to design and operate a database on satellite positions, planned maneuvers and signal transmissions with a view to reducing the chance of orbital collisions and frequency interference. The three companies — Intelsat, SES and Inmarsat — expect to select a contractor as early as December to create the Space Data Center, to be located at the newly established Space Data Association (SDA) on Britain’s Isle of Man. If it is successful in persuading other satellite operators to overcome their natural hesitation in handing over sensitive corporate operating details, the SDA would become the satellite industry’s first global effort to address the related issues of space situational awareness and signal interference. In bringing together three companies that regularly compete with one another, SDA already has proved it can overcome concerns about the release of proprietary information on satellite beam coverage areas, signal strength and planned in-orbit maneuvers. Washington- and Bermuda-based Intelsat and SES of Luxembourg are the world’s two largest fixed satellite services companies in terms of revenue. Inmarsat of London is the oldest and, by revenue, the largest mobile satellite services operator. Taken together, the three companies operate about 100 satellites in geostationary orbit. SDA Chairman Stewart Sanders, senior vice president for customer service at SES Engineering, said Nov. 17 that several other satellite fleet operators have signaled their intent to join the organization. In an interview, Sanders said the three founders have not sought additional members up to now to minimize legal complications that would slow the creation of the Space Data Center.

“There is a group of about eight operators, including the three founders, that have all indicated they support the project,” Sanders said. “In addition, there is a separate group of about 14 operators that have come together to discuss ways of combating [radio-frequency] interference. By sometime in the first quarter of 2010, you will see other members of SDA.” SDA’s two other directors are Tobias Nassif, Intelsat vice president of satellite operations and engineering, and Ruy Pinto, Inmarsat vice president of satellite and network operations. SDA’s request for bids asks prospective contractors to design a network that is backed up by identical databases on two other continents in addition to the home installation on the Isle of Man. The backup facilities could be nothing more than computer servers placed in operating centers already operated by an SDA member but kept separate, with restricted access. SDA has two broad aims. The first is to provide highly accurate information on where commercial satellites are. General information on satellite locations is already publicly available, in part through the U.S. Defense Department’s Space Surveillance Network of ground sensors. But this information is not always as precise or up to date — nor is it disseminated as quickly — as it needs to be to protect against close encounters between satellites, especially in the more-crowded Earth orbits below the geostationary arc 36,000 kilometers above the equator. The second ambition of SDA is to act as a clearinghouse of information on satellites’ individual radio beams and power levels, and whether owners have encountered signal interference — intentional or otherwise. Unintentional signal interference is viewed as a growing problem in some regions of the world as satellite communications links proliferate. More satellites in orbit means they are operating closer than ever to one another, while widespread adoption of the technology has led to occasionally sloppy satellite-antenna pointing or Earth station maintenance.

The result, satellite operators say, is increased incidence of signal interference that, despite new satellite signal-location technology, is difficult and often expensive to locate. SDA’s request for proposals offers the winning company a five-year contract but does not identify a price range. “We’ll see what responses we get in” and then the member companies will agree on a budget, Sanders said. He said the biggest expense is likely to be not personnel but software. Sanders agreed that to be effective, the SDA will require operators to submit data almost constantly on their satellites’ location, maneuvers and beam locations. “Operators already do this today, but it’s on an informal basis. You call someone you know who knows someone at the company who can get you the needed information,” he said. If SDA grows as its current members hope, it will face the question of whether to feed its data into the U.S. Defense Department’s Space Surveillance Network to improve what today is the world’s de facto satellite-tracking agency. Alternatively, U.S. defense authorities could funnel information to SDA, whose Isle of Man location was selected in part for its perceived independence from any national space power. One Defense Department official said U.S. authorities view SDA positively, and depending on its evolution may one day elect to contribute data to it. It remains to be seen whether satellite operators in China, Russia and India, for example, who in some cases are controlled by their national governments, will join SDA.

# SDA CP-Solvency-Enhanced SSA/Sharing

### Commercial interests are key to overall u.s. government data acquisition

Committee on the Peaceful Uses of Outer Space 11- Scientific and Technical Subcommittee Forty-eighth session Vienna, 7-18 February 2011 Item 7 of the draft provisional agenda\*Towards Long-term Sustainability of Space Activities: Overcoming the Challenges of Space Debris A Report of the International Interdisciplinary Congress on Space Debris http://www.oosa.unvienna.org/pdf/limited/AC105\_C1\_2011\_CRP14E.pdf

Direct the Secretary of Defense to make safety of flight and the preservation of the space environment the leading national security drivers for enhanced space situational awareness efforts. − The U.S. Government has a strong interest in preserving the space environment. Through improved data collection and processing, and close collaboration with industry, the Government can play an important role in encouraging safe and responsible space flight operations and can avoid the creation of unnecessary, dangerous space debris. In particular, DoD should: ο Continue and expand the Commercial and Foreign Entities Program under which the U.S. Government currently shares orbital information with the private sector. In particular, the Secretary of Defense should provide high-accuracy Government data on existing space debris to all space operators and routinely share operational and flight data with commercial service providers. The data exchange between the U.S. Government and commercial operators should be automated to the greatest extent possible, and should include the most accurate, operator-supplied data on satellite locations and planned maneuvers. DoD, in conjunction with commercial operators, should begin to develop common operational protocols for handling routine and emergency situations. ο Augment existing space surveillance capabilities through innovative programs such as hosting Government payloads/sensors on commercial satellites. Every satellite launched into space is potentially a sensor that can help extend the capabilities of an evolved Space Surveillance Network. ο In conjunction with the Secretary of State, begin an international dialogue with other nations on space data sharing with the goal of merging national space catalogs and sensor data to create a more complete view of the space environment.

# SDA CP- Solvency- Security

### Commercial satellites are key to address government short comings- addresses all security shortcomings

Committee on the Peaceful Uses of Outer Space 11- Scientific and Technical Subcommittee Forty-eighth session Vienna, 7-18 February 2011 Item 7 of the draft provisional agenda\*Towards Long-term Sustainability of Space Activities: Overcoming the Challenges of Space Debris A Report of the International Interdisciplinary Congress on Space Debris http://www.oosa.unvienna.org/pdf/limited/AC105\_C1\_2011\_CRP14E.pdf

A State-commercial SSA coordination that results in improved SSA data and conjunction analysis sharing between government (e.g. U.S. JSpOC/CFE program) and commercial entities can be implemented.

Assessment: Neither governments nor commercial entities can have sufficient SSA data by themselves. Each has part of a complementary data set, and both benefit from sharing. Ideally, the most accurate data from government satellite catalogues should be available in real-time to commercial satellite operators in order to support conjunction analysis and collision warning. However, for reasons of national security, States are not likely to share their most detailed information and currently only the United States shares any data at all. One solution to facilitate this type of data-sharing is to address the underlying security dilemmas associated with space situational awareness data via international agreements that inter alia provide for data sharing to support conjunction analysis and collision warning while still protecting national security and data privacy needs. However, the availability of precise, actionable orbit data, called Special Perturbations (or SP) data in the U.S. (as opposed to the less accurate, non-actionable General Perturbations (or GP) data in TLE format), may be questionable.

# SDA CP- Solvency- Data Integration

### SDA is key to global data sharing

Committee on the Peaceful Uses of Outer Space 11- Scientific and Technical Subcommittee Forty-eighth session Vienna, 7-18 February 2011 Item 7 of the draft provisional agenda\*Towards Long-term Sustainability of Space Activities: Overcoming the Challenges of Space Debris A Report of the International Interdisciplinary Congress on Space Debris <http://www.oosa.unvienna.org/pdf/limited/AC105_C1_2011_CRP14E.pdf>

In response to the recognition that better and broader inter-operator information sharing is desirable and to augment the services available from the current TLE-based DoD CFE Program,41 a number of satellite operators recently began a broad dialogue on how to best ensure information sharing within the satellite communications industry. The international satellite community is discussing forming a Space Data Association (SDA), which would be an interactive repository for commercial satellite orbit, maneuver, and payload frequency information. The principal goal of the SDA’s Data Center would be to promote the safety of space operations by encouraging coordination and communication among its operator members. Satellite operators would maintain the most accurate information available on their fleets in the Data Center systems, augment existing TLE data with precise orbit data and maneuver plans from the operator’s fleets, and would retrieve information from other member operators when necessary. The Data Center would also allow operators to: Perform data conversion and reformatting tasks allowing operators to share orbital element and/or ephemeris data42 in different formats; Adopt common usage and definition of terminologies; Develop common operational protocols for handling routine and emergency situations; and Exchange operator personnel contact information and supported data protocols.

# SDA CP- Solvency- Miscalc

### SDA provides information sharing to prevent miscalc

Committee on the Peaceful Uses of Outer Space 11- Scientific and Technical Subcommittee Forty-eighth session Vienna, 7-18 February 2011 Item 7 of the draft provisional agenda\*Towards Long-term Sustainability of Space Activities: Overcoming the Challenges of Space Debris A Report of the International Interdisciplinary Congress on Space Debris <http://www.oosa.unvienna.org/pdf/limited/AC105_C1_2011_CRP14E.pdf>

As the Data Center gains acceptance, it could perform additional functions such as close-approach monitoring tasks currently being conducted by operators. In this phase, operators could augment U.S. Government-provided TLE data with more precise operator-generated data to improve the accuracy of the Data Center’s conjunction monitoring and provide a standardized method and focal point for operators to share information and facilitate communications between satellite operators and U.S. and non-U.S. governments. In the early stages, TLE data from the CFE Program and/or other Government programs would still need to supplement information on non-operational space objects. Additionally, U.S. Government or non-U.S. government support would still be required when precise information is required to conduct avoidance maneuver planning.

Details on the implementation of the Data Center, services to be provided, usage policies, structure of the organization, and by-laws have yet to be determined and would ultimately require agreement among the member operators. The development of a Data Center could provide new visibility and awareness of the space environment, allow satellites to be flown in a safer manner, and reduce the likelihood of an accidental international incident in space.43

### Commercial satellites are key to differentiate between natural phenomenon and actual attacks

Committee on the Peaceful Uses of Outer Space 11- Scientific and Technical Subcommittee Forty-eighth session Vienna, 7-18 February 2011 Item 7 of the draft provisional agenda\*Towards Long-term Sustainability of Space Activities: Overcoming the Challenges of Space Debris A Report of the International Interdisciplinary Congress on Space Debris <http://www.oosa.unvienna.org/pdf/limited/AC105_C1_2011_CRP14E.pdf>

The NSTAC found in response to its questionnaire that the satellite industry utilizes a range of standards-based physical security protection techniques to mitigate against a man-made attack or natural disaster. Satellite NOCs, SOCs, and TT&C ground stations generally maintain 24-hour guarded access, security fencing, external lighting, registration and clearance of visitors, and security cameras to monitor the area to dissuade man-made attacks, including capture of a ground station. To combat the results of natural phenomena, providers employ back-up facilities; construct facilities outside of disaster-prone areas; plan for antenna stow methods or protective procedures; and maintain fire detection, flooding, and de-icing procedures. Most commercial providers also maintain back-up facilities and auxiliary power sources in the event of a man-made attack or natural event. However, auxiliary power availability is limited by on-site fuel availability, generally ranging from a minimum of 24 hours to a maximum of 30 days. Further, facilities are generally not constructed to withstand a nuclear detonation, electromagnetic pulse (EMP) and biological attacks, or radiological fallout. Similar to other facilities, satellite operators have established personnel security procedures including background checks and pre-employment screenings, employee badges, logged entry and exit, and on-site security guards

# SDA CP- Solvency- Reliable DATA

### Commercial satellites with SDA provide reliable SSA

SDA 11- Space Data Center Completes Readiness Review of Full Operational Capability ISLE OF MAN (13 April, 2011)

The Space Data Association (SDA), established by commercial satellite operators to improve the safety and efficiency of space operations, today announced that its Space Data Center has completed its Full Operational Capability (FOC) readiness review. With this milestone, the SDA has determined that the system is ready to be employed and maintained, and FOC operations can begin. The SDA’s main technical adviser and systems developer, Analytical Graphics, Inc. (AGI), completed work on the data center less than a year after winning the contract.

The Space Data Center is an automated space situational awareness system through which satellite operators share operator-owned orbital data. It provides full Conjunction Assessment (CA) capability (assessing the physical proximity of objects in space) and data sharing in support of radio frequency interference (RFI) mitigation. Because participating satellite operators provide the data, it is the most up-to-date information available. The system also converts disparate data to a common format and performs integrity checks on contributed ephemerides, making the information more reliable..

# SDA CP- Solvency- Debris

### Commercial satellites are taking measures to be aware of debris

Committee on the Peaceful Uses of Outer Space 11- Scientific and Technical Subcommittee Forty-eighth session Vienna, 7-18 February 2011 Item 7 of the draft provisional agenda\*Towards Long-term Sustainability of Space Activities: Overcoming the Challenges of Space Debris A Report of the International Interdisciplinary Congress on Space Debris http://www.oosa.unvienna.org/pdf/limited/AC105\_C1\_2011\_CRP14E.pdf

In 2009, a group of commercial satellite operators formed the Space Data Association (SDA), an international non-profit organization to increase the sharing of SSA data and cooperation between satellite operators. In 2010, the SDA’s Space Data Center began initial operations to provide conjunction assessment and collision warning services to participating satellite operators, and in 2011 it is expected to add radio frequency interference mitigation services as well.8 In addition to the actual tracking of objects in Earth orbit, sophisticated software models are also used to statistically represent the space debris population which cannot currently be tracked, generally those objects smaller than 10 centimetres in size. Attempts are made to calibrate and validate the models using specific tracking events, such as beam park experiments,9 and through analysis of recovered space hardware.

# SDA CP- Solvency- Hege

### Commercial satellites are being enhanced to support threat situations

Committee on the Peaceful Uses of Outer Space 11- Scientific and Technical Subcommittee Forty-eighth session Vienna, 7-18 February 2011 Item 7 of the draft provisional agenda\*Towards Long-term Sustainability of Space Activities: Overcoming the Challenges of Space Debris A Report of the International Interdisciplinary Congress on Space Debris http://www.oosa.unvienna.org/pdf/limited/AC105\_C1\_2011\_CRP14E.pdf

Commercial Satellite Industry Innovation

Commercial satellite systems are being enhanced with increased capacity and QoS to better support commercial and Government needs, including national communications systems and NS/EP. Recent deployments of systems with multiple narrow spot beams naturally reduce the effects of harmful RFI and add significantly more capacity. Advanced satellites with onboard processing provide improved connectivity, and reduce end-user reliance on centralized Earth stations; benefits include reduced latency, reduced cost, and more efficient use of terrestrial infrastructure. Additional innovations include systemic threat analysis during design time and implementation of security measures such as hardware-based identity for more robust cybersecurity.

Space Weapons

Due to the geopolitical nature of the satellite industry, the strategic situations in which satellites may be employed, and the availability and/or cost of mitigation capabilities, the commercial satellite industry acknowledges the risk of certain threats but does not attempt to mitigate them (for example, the effects of nuclear detonations, space weapons, and resilience of ground systems to chemical, biological, and radiological hazards). Since the industry can not afford to mitigate these threats, the Government should evaluate whether it should fund mitigation of these threats for critical COMSATCOM satellites and ground facilities used to support NS/EP communications.

# SDA CP- Solvency- Deterrence- Data Security

### The SDA has control over data integration systems- insures protection against attacks

Committee on the Peaceful Uses of Outer Space 11- Scientific and Technical Subcommittee Forty-eighth session Vienna, 7-18 February 2011 Item 7 of the draft provisional agenda\*Towards Long-term Sustainability of Space Activities: Overcoming the Challenges of Space Debris A Report of the International Interdisciplinary Congress on Space Debris http://www.oosa.unvienna.org/pdf/limited/AC105\_C1\_2011\_CRP14E.pdf

To mitigate operations center vulnerabilities, providers have implemented more intrinsic controls around those systems. Malicious actors do not require physical access to the satellite or the terrestrial network components. They require only access to the control center systems, which can occur, for example, via a compromised control center workstation.

To properly protect operations centers, one must implement: (1) physical controls; (2) network layer controls; (3) applications security controls; (4) system-level controls; and (5) redundant or back-up facilities. Proper physical controls include guards, gates, staff background checks, identification (ID) badges, and continued auditing of physical security systems to prevent unauthorized access. Networks that operate across wide areas or in third-party facilities generally employ strong cryptographic controls to ensure the confidentiality and integrity of transmitted and received information. Especially sensitive networks may be “air gapped” and not interconnected at all with other networks. Remote access sessions, when authorized, are carefully secured. Additionally, general systems controls ensure that the correct security countermeasures are in place to stop worms and viruses, and have the proper network access controls including gateways, firewalls, and hardening of systems and network infrastructure so that only authorized personnel are granted access to the network.

Application security controls include authentication and authorization, well-defined operating procedures, and audit controls. Two-factor authentication should be used—not only a log-in and password, but also a token—for entry into the system. Audit controls such as monitoring and logging give authorized personnel visibility into activities that occur throughout that commanding system, and can provide a useful record to develop mitigation strategies to stop future malicious activity. A good log will show who initiated a malicious command, at what time, and through what method. Further, one can write code that allows for visibility into what is happening to the satellite by logging the commands of each person on the network and identifying how an individual affected the satellite.

# SDA CP- Solvency- Deterrence

### Commercial satellites mitigate interruption from radiation- makes it less likely that data is distorted

Committee on the Peaceful Uses of Outer Space 11- Scientific and Technical Subcommittee Forty-eighth session Vienna, 7-18 February 2011 Item 7 of the draft provisional agenda\*Towards Long-term Sustainability of Space Activities: Overcoming the Challenges of Space Debris A Report of the International Interdisciplinary Congress on Space Debris http://www.oosa.unvienna.org/pdf/limited/AC105\_C1\_2011\_CRP14E.pdf

Overall, there are a number of means to mitigate RFI, including user training and certification, identifying and eliminating the interference source, using filters, and grounding and shielding equipment.52 The use of filters and physical shielding may be useful in rejecting strong nearby signals that can be found at satellite terminals, but are ineffective against PI. Terminal operator equipment training and proper system operation is paramount to reducing unintentional RFI.

Traditional communications satellite systems employ large footprints that may cover wide regions or even continents. For this reason, satellite networks may experience RF and uplink interference issues that are greater in geographic scope than those experienced by terrestrial wireless networks. Low-power or infrequent jammers may seek to distort the user’s data in order to reduce effectiveness or trust in the system; this can be difficult to differentiate from unintentional interference. At higher powers, a more overt jammer can saturate key satellite components so that the desired signal is essentially eliminated altogether. Not all military and commercial communications satellite systems are intended to provide complete protection from RFI; robust protection measures remain primarily the domain of certain specialized Government systems such as MILSTAR (Military Strategic and Tactical Relay [satellite]). Satellite systems can employ a combination of antenna beam control (narrow spots, beam steering, or nulling) and spread spectrum techniques to reduce jammer susceptibility. The most effective forms require elaborate antennas and onboard processing, well beyond what can be economically justified in a commercial environment. The Government could enhance commercial satellite mission assurance through targeted funding to implement these measures outside of specialized Government systems.

# SDA CP- A2: Perm- Government Dependence

### SDA exchanges data to ensure operation integrity- however government reliance causes it to fail

Committee on the Peaceful Uses of Outer Space 11- Scientific and Technical Subcommittee Forty-eighth session Vienna, 7-18 February 2011 Item 7 of the draft provisional agenda\*Towards Long-term Sustainability of Space Activities: Overcoming the Challenges of Space Debris A Report of the International Interdisciplinary Congress on Space Debris http://www.oosa.unvienna.org/pdf/limited/AC105\_C1\_2011\_CRP14E.pdf

A commercial “data centre” can be established from which operators can coordinate conjunction analysis and provide collision warnings. Assessment: The international commercial space telecommunication industry is currently experimenting with a commercial Space Data Center run by AGI on behalf of the Space Data Association. Initial reports indicate the data centre is fulfilling its mandate to exchange operation data to ensure safety, technical support to improve operational integrity, and share the associated costs. However, this Center has operational limitations. For example, it relies on the U.S. government and other tracking networks for data on ‘non-active’ satellites and other space..

# SDA CP- A2: Perm- Cost

### The biggest impediment to the SSA network is government involvement

Committee on the Peaceful Uses of Outer Space 11- Scientific and Technical Subcommittee Forty-eighth session Vienna, 7-18 February 2011 Item 7 of the draft provisional agenda\*Towards Long-term Sustainability of Space Activities: Overcoming the Challenges of Space Debris A Report of the International Interdisciplinary Congress on Space Debris http://www.oosa.unvienna.org/pdf/limited/AC105\_C1\_2011\_CRP14E.pdf

A public, open-source, world-wide SSA space objects catalogue and tracking network can be established.

Assessment: An open-source SSA tracking network and catalogue is possible, but faces serious challenges. Foremost among them is financial impact. The majority of SSA tracking is undertaken by government entities. Without the participation of major space-active SSA State governments, an open-source SSA network would have to rely on public and private tracking and analysis. It is possible such an open-source network could be achieved on a limited basis through academic institutions, commercial operators, limited government participation, and/or amateur astronomers. In this context, the maturation of the International Scientific Optical Observation Network (ISON), a collection of more than 20 scientific and academic institutions around the world, bears watching.

# SDA CP- Cyber War Fare NB- Government Systems Susceptible

Government data acquisition is vulnerable to cyber attacks

Smitham 10- Matthew C. Smitham, Lt Col, USAF, The Need for a Global Space-Traffic-Control Service: an Opportunity for Us Leadership, 17 February 2010 Air War College

Air University

Beyond hardware, the US software system is also imperfect and antiquated. In some cases, the Americans are behind Russian mathematical practices to process and predict high-quality space tracks. However, these efforts address mainly data acquisition (see Figure 1), not holistic solutions for space-traffic control.

For example, the US military is still using decades-old astrodynamic techniques to create element sets, mainly because the costs to redesign and recertify its operational systems would be enormous.51 To make up some of this deficit, the Air Force uses the brute force method of over sampling (lots of observations) versus elegant mathematics. In addition, JSpOC until recently was performing conjunction analyses only for priority US satellites, such as manned flights and US defense satellites. After the Iridium-Cosmos collision and renewed interest by Department of Defense senior leaders,52 JSpOC recently upgraded its computational systems to give it the ability to run conjunction analyses for all active satellites within the catalog. However, precision analysis needed for positive collision avoidance is still only on a case-by-case basis because it is labor intensive and not automated.53

# SDA CP- Cyber War Fare NB- Private Solves

### The private sector can establish a healthy network with protection against attacks

Committee on the Peaceful Uses of Outer Space 11- Scientific and Technical Subcommittee Forty-eighth session Vienna, 7-18 February 2011 Item 7 of the draft provisional agenda\*Towards Long-term Sustainability of Space Activities: Overcoming the Challenges of Space Debris A Report of the International Interdisciplinary Congress on Space Debris http://www.oosa.unvienna.org/pdf/limited/AC105\_C1\_2011\_CRP14E.pdf

Finally, the private sector relies on a variety of initiatives to help safeguard the health of the network. In addition to the Data Center initiative discussed above, operators use professional outreach, networks, and publications; collaboration through industry-to-industry and industry-Government working groups; and anti-malware programs and firewalls to protect networks from the threat of cyber attacks. Satellite owners, operators, and manufacturers employ dedicated individuals and teams within their respective organizations that deal specifically with cybersecurity threats. Additionally, many satellite owners and operators maintain redundant or back-up facilities for SOCs, NOCs, and TT&C sites, as discussed above in Section 3.1.3. Backup facilities are regionally diverse, active, and regularly tested to ensure that operators can continue to provide service in the event of a physical or cyber attack

# \*\*Cyber Terror DA\*\*

# Cyber Terror DA- 1NC

### Cyber threats exist to DOD infrastructure in the squo- however, the DOD is experimenting with hardening measures- attacks at attempts have been uncovered

Ginter 7- Lieutenant Colonel Karl Ginter United States Army Dr. Clayton K. S. Chun Project Adviser Space Technology and Network Centric Warfare: a Strategic

Paradox, 30 MAR 2007

The cyber threat to DoD computer networks is real and poses a significant risk to the assured access and availability of critical warfighting systems that are networked into the GIG. 9 While there are malicious network intrusions, hacker attacks, and sabotage threats from within the United States, the great majority of computer network attacks emanate from the United States’ peer military competitors: Russia and China. In 2005, China’s PLA began embedding offensive computer network operations (CNO) into its military exercises, and has incorporated a first strike CNO strategy into its military doctrine, with the intent of achieving electromagnetic dominance in time of conflict. China openly practices military doctrine that combines CNO with electronic warfare, kinetic strikes against C2 and computer network nodes, and virus attacks on enemy battle command systems.31 The PLA also employs its considerable civilian computer expertise from academies, institutes, and IT industries to support PLA operations by conducting hacker attacks, network intrusions, and other forms of cyber warfare.32

Because the DoD has more computers than any other U.S. department or agency—about 5 million worldwide—it’s computers and the networks they traverse are very much exposed to foreign as well as domestic hackers. Consequently, the space control systems and the battlefield systems that are space-enabled are at risk and require hardening. In August 2005, the DoD revealed that it was experiencing nearly 500 attempted intrusions daily, from domestic sources and from the more than 20 nations that possess dedicated computer attack programs— mostly from China, North Korea, and Russia.33 The majority of those attacks used web sites traced to the Chinese province of Guangdong, targeting U.S. military unclassified networks.

The DoD revealed that during a 30-day period in July and August 2005, several large military computer networks, as well as networks of the departments of State, Energy, and Homeland Security were breached and in some cases disabled.34 Similarly, in August and September 2006, cyber attacks on the computer systems of the Department of Commerce forced replacement of hundreds of computers, and lock down of Internet access for one month. A three-year U.S. investigation into the origins of such cyber attacks, code named Titan Rain, confirms that these computer network penetrations are increasingly coming from China.35 Clearly, space-enabled NCW systems, whether C2, intelligence, space and missile warning, or even logistics, invite substantial risk where there is reliance on unclassified computer systems and where critical computer nodes are unprotected.

### Increased military information increases cyberwarfare- adversaries will attack vulnerabilities

### Eriksson and Giacomello 6- Johan Eriksson, Associate Professor of Political Science at Sodertorn, and Giampiero Giacomello,Assistant Professor of International Relations at the Dipartimento di Politica, Istituzioni, Storia, Università di Bologna, The Information Revolution, Security, and International Relations: (IR) Relevant Theory? International Political Science Review / Revue internationale de science politique, Vol.27, No. 3 (Jul., 2006), pp. 221-244 http://www.jstor.org/stable/20445053 .

A study by the National Research Council argues that "Tomorrow's terrorist may be able to do more with a keyboard than with a bomb" (Bendrath, 2001; Denning, 2001a: 282).5 Former US Homeland Security Director Tom Ridge (2002) observed that "Terrorists can sit at one computer connected to one network and can create world havoc - [they] don't necessarily need bombs or explosives to cripple a sector of the economy, or shutdown a power grid." Such rhetorical dramatization is characteristic of the entire discourse on information security and cyber-threats. The common view is that as societies and governments are becoming more reliable with respect to information technology, they are also becoming more vulnerable to all sorts of cyber-threats.

The most cataclysmic dramatization in the literature is that of an "electronic Pearl Harbor" (Bendrath, 2001; Everard, 2000; Forno, 2002; O'Day, 2004; Schwartau, 1997; Smith, 1998).6 According to the "electronic Pearl Harbor" scenario, phone systems could collapse, subway cars suddenly stop, and the money of thousands of people become inaccessible as banks and automatic teller machines stop functioning. In such an apocalyptic vision, overall critical infra structures would be disrupted to the point that society and government would lose the ability to function normally. The evocative image of an "electronic Pearl Harbor" was immediately adopted in the US media and in certain circles of policy makers (Bendrath, 2003). Former Deputy Defense Minister John Hamre argued that "We're facing the possibility of an electronic Pearl Harbor ... There is going to be an electronic attack on this country some time in the future" (CNN, 1997). Some commentators have argued that the "electronic Pearl Harbor" scenario is highly unlikely, and is more about fear-mongering than sober analysis. For example, Denning (2001b) argues that cyber-terrorism, defined as digital attacks causing physical destruction and human deaths, is extremely unlikely.7 Few, if any, cyber-attacks could be characterized as acts of terrorism. Even the US Naval War College, in cooperation with the Gartner Group, concluded that an "electronic Pearl Harbor," although theoretically possible, was highly unlikely: "There are far simpler and less costly ways to attack critical infrastructure, from hoax phone calls to truck bombs and hijacked airliners" (The Economist, 2002: 19). Information operations are seen not merely as a means of improving or complementing physical attack, but as a means of replacing physical destruction with electronic (Denning, 1999; Harshberger and Ochmanek, 1999: 12; O'Day, 2004). Denial-of-service attacks and the defacing of web pages certainly can have material consequences. For firms operating with online transactions, the result can be huge financial losses.8 Nevertheless, the major impact is symbolic and the main effect is humiliation. To a large degree, cyber-attacks are attacks with and against symbols and images. Net-defacing, in particular, is a means for attacking symbols, something which is being done on an everyday basis by "hacktivists" on both sides of the Israeli-Palestinian conflict, the China-Taiwan conflict, and the Protestant-Catholic conflict in Northern Ireland.9

Most observers focus on the transnational and network-based character of cyber-threats (Arquilla and Ronfeldt, 1999, 2001; Deibert and Stein, 2003; Henry and Peartree, 1998; Keohane and Nye, 1998; O'Day, 2004; Pfaltzgraff and Shultz, 1997). ? Adversaries are typically seen as operating in loosely organized networks consisting of relatively independent nodes of individuals, groups, organizations, or even states, capable of quickly assembling and dispersing, even long before an attack has been discovered. In particular, network actors capable of using such means can resort to "asymmetric warfare" (Applegate, 2001; Arquilla and Ronfeldt, 2001; De Borchgrave et al., 2000; Erbschloe, 2001; Herd, 2000; O'Day, 2004; Sofear and Goodman, 2001). Although they might be incapable of engaging states in a conventional military conflict, they can inflict serious damage by attacking and exploiting the vulnerabilities of information systems by resorting to cyber-attacks (Arquilla and Ronfeldt, 1999, 2001; Cordesman, 2002).

The widely acknowledged framing of cyber-threats implies that boundaries are dissolved between the international and the domestic, between civil and military spheres, between the private and public, and between peace and war. If taken seriously, this framing suggests that not only the security of information systems is challenged, but also, and more fundamentally, the sovereignty of states (Everard, 2000; Fountain, 2001; Giacomello, 2005; Giacomello and Mendez, 2001; Rosecrance, 1999). Cyber-threats challenge primarily internal sovereignty (effec tive control of the national territory and of the people living within it), but not necessarily external sovereignty (the formal recognition of independence by other states) (compare Philpott, 2001). At stake are not only the tangible and intangible values of information, but also the ability of governments to control the course of events.

Cyber attacks degrade the overall defense posture- turns the case

Metz 2000- Steven Metz, Research Professor of National Security Affairs in the Strategic Studies Institute, ARMED CONFLICT in the 21st CENTURY: the INFORMATION REVOLUTION and POST-MODERN WARFARE April 2000 http://www.au.af.mil/au/awc/awcgate/ssi/metz\_info\_rev.pdf

Future infrastructure war could take two forms. In one version, strategic information attacks would be used to prepare for or support conventional military operations to weaken an enemy’s ability to mobilize or deploy force. The second possible form would be “stand alone” strategic information warfare. This might take the form of a sustained campaign designed for decisive victory or, more likely, as a series of raids designed to punish or coerce an enemy. Facing a future Iraq or Serbia, for instance, the United States could conceivably use strategic information attacks rather than aerial bombardment, in part because of the belief that such actions would provoke less political opposition. All of this is, however, speculation. Today the technological feasibility, psychological effect, and legal ramifications of strategic information warfare remain unclear.

But should cyberattacks, whether as part of strategic information warfare or as terrorism, become common, the traditional advantage large and rich states hold in armed conflict might erode. Cyberattacks require much less expensive equipment than traditional ones. The necessary skills exist in the civilian information technology world. One of the things that made nation-states the most effective organizations for waging industrial age war was the expense of troops, equipment and supplies. Conventional industrial-age war was expensive and wasteful. Only organizations that could mobilize large amounts of money, flesh, and material could succeed at it. But if it becomes 61 possible to wage war using a handful of computers with internet connections, a vast array of organizations may choose to join the fray. Nonstate organizations could be as effective as states. Private entites might be able to match state armed forces. Private or commercial organizations might even wage information war on each other—cyber “gang wars” played out on servers and network backbones around the world rather than in ghetto alleys.

# Cyber Terror DA- Link Ext- Generic

### Increased SSA information makes us more vulnerable- system crashes become inevitable

Eriksson and Giacomello 6- Johan Eriksson, Associate Professor of Political Science at Sodertorn, and Giampiero Giacomello,Assistant Professor of International Relations at the Dipartimento di Politica, Istituzioni, Storia, Università di Bologna, The Information Revolution, Security, and International Relations: (IR) Relevant Theory? International Political Science Review / Revue internationale de science politique, Vol.27, No. 3 (Jul., 2006), pp. 221-244 http://www.jstor.org/stable/20445053 .

Whether hype or reality, cyber-threats have achieved an indisputable salience in post-cold-war security thinking, particularly among analysts and makers of defense and security policy. Critical infrastructure protection, information warfare, infor mation operations,' information assurance, cyber-terrorism, Revolution in Military Affairs (RMA) , and similar buzzwords are common currency in policy documents, defense bills, and security doctrines of the early 21st century. While conventional forces and military budgets have been generally downsized following the end of the cold war, the new emphasis on information security and cyber-threats are a noteworthy exception. In North America, Europe, Russia, China, and other parts of the world, governments are setting up new units and employing personnel for monitoring, analyzing, and countering the perceived risks and threats of the global network society.

The conception of cyber-threats has grown out of the fear of increased vulnerability and loss of control that presumably is the result of moving from an industrial to an information society (Alberts, 1996a, 1996b; Alberts and Papp, 1997; Henry and Peartree, 1998; O'Day, 2004). Without the development of global computer networks and communications, cyber-threats would be difficult to imagine except as science fiction. Notions of cyber-threats have originated in both the private and public sphere, among military as well as civilian actors. In the business community and within the police, cyber-crime has become a particularly salient threat image. Within the military-bureaucratic establishment, perceived threats have been framed as information warfare, information operations, cyber terrorism, and cyber-war. Among computer scientists, technicians, and network operators, threat images are usually much narrower, with an emphasis on computer network attacks, exploits, and disruptions (implying an adversary) and on structural vulnerabilities such as software conflicts and other bugs which can lead to systems crashes (for example, the Year 2000 or 'Y2K" computer bug). Images of cyber-threats typically involve a very broad range of adversaries and targets, including both state and non-state actors (Campen et al., 1996; Erbschloe, 2001; Furnell, 2002; Henry and Peartree, 1998; Herd, 2000; Khalilzad et al., 1999; O'Day, 2004; Polikanov, 2001; Schwartau, 1996; Yourdon, 2002). States are still typically seen as the single most important type of potential enemy, able to neutralize effectively the critical infrastructures of another country (for example, by shutting down telecommunications), but non-state actors are gaining attention as well.

# Cyber Terror DA- Link Ext- Info. Overload

### An increase in information causes a form of overload that makes us more susceptible to cyber attacks- a smaller footprint strategy is the best deterrent

Simpson 11- Chris Simpson San Diego, CA Associate Professor of Communication at American University “Collective C2 in Multinational Civil-Military Operations” Cyber Security to the Edge: Applying Edge Theory to Cyber Security Operations http://www.dodccrp.org/events/16th\_iccrts\_2011/papers/099.pdf

Information overload is one of the major factors for “fog of war” in cyber warfare. If every organization followed the current rules they would conduct recurring vulnerability scans and this data would be fed into different databases so the chain of command would have a list of 1000’s of vulnerabilities but does this enhance the overall security of the scanned systems if the owners don’t have the tools or manpower to resolve those vulnerabilities? With the amount and com-plexity of this data there is no way for a centralized organization make sense of this. This is ana-logous to telling Platoon commander to defend a street block but instead of letting him deploy his troops he would first have to scan the block for vulnerabilities on a checklist and submit those vulnerabilities to higher HQ. Many of the vulnerabilities on the checklist might not be ap-plicable to the current situation, higher headquarters would asses the listed vulnerabilities them and tell the Platoon Commander which ones to fix. As this data makes its way up the chain of command the enemy disposition is constantly changing and by the time a response is received from upper echelon it may be too late to defend the block. Instead of doing this the Army devel-ops tactics, techniques and procedures (TTPs) for the Platoon Commander to utilize that can be modified based on the local situation.

The attacker has the advantage in cyber warfare, the attacker only needs to know one vulne-rability to gain access to a system while the defender must monitor all vulnerabilities. This ad-vantage is increased when a defender operates in a hierarchical organization and must wait for top down direction to take action. Local units defending their own networks would have a small-er footprint and less data to monitor making it easier to detect attacks.

# Cyber Terror DA- Case Turn

### Inadequate protection leads to more miscalculation and less deterrence

Litvaitis 8- Arturas Litvaitis, graduate of the Joint Command and General Staff Course 2007/2008 of the Baltic Defence College, Challenges of Implementation of the Network Centric Warfare Tenets in Coalition Environment Baltic Security & Defence Review Volume 10, 2008

The main threats to the communication systems are coming from their vulnerabilities to physical attacks (communication nodes and wired communication lines), degradation of network performance (jamming, interference), and unauthorized access (eavesdropping). Computer networks are vulnerable to cyber-attacks such as insertion of malicious software, computer viruses, unauthorized access to the computer-based systems etc. Military communication systems are not an exception, thus are exposed to various attacks as much as civilian ones. It is obvious, that technologies nowadays are spreading very fast, therefore quickly becoming available to our present or potential adversaries too (Alberts, 1996).

Military network protection technologies, currently used in the United States and most of the European countries, are based on electronic counter-countermeasures (frequency hopping, spread-spectrum technologies), encryption of communication links, and computer network defence systems like firewalls, intrusion detection systems and anti-virus software. Today, quite an impressive arsenal is available to protect our networks; however, within the multinational environment there are numerous challenges to protect the entire coalition network when it is made of national segments. The first challenge which future coalitions will face is about the different level of technological advance in general, and in the network protection technologies in particular. This issue can be observed currently due to uneven defence expenditures, time-divided defence modernization programmes or diverging priorities. The consequence of this aspect is the inadequate protection of different national networks, which precludes coalition partners with better network protection from connecting their networks to the nations with less protected networks. The second challenge, even among most technical advanced nations, is incompatible national solutions of the network defence. Currently, almost every nation implements its proprietary solution, which is not in favour of passing the necessary information to another nation (Networking Working Group, 2008). When, in static networks, various gateway solutions could be applied, it still would be a challenge to pass the information from one platform, belonging to one nation, to another platform from another nation in a very dynamic environment that Baltic Security & Defence Review Volume 10, 2008 157 a networked coalition is supposed to be. It is simply not possible to predict who is going to talk with whom and, even more, to design working solutions for all possible situations in a net-centric self-synchronizing environment.

# \*\*Politics\*\*

## Plan Unpopular- Data Sharing

### The plan is perceived as a data sharing mechanism- empirically proven this has political ramifications

Weeden 10- Brian Weeden, Technical Advisor for Secure World Foundation, Secure World Foundation Published 1 August 2010, The Norad Experience: Implications for International Space Surveillance Data-Sharing Executive http://swfound.org/media/1817/norad-exec-summ-bw-2010.pdf

A similar situation exists with SSA. Ground-based sensors, particularly phased-array and imaging radars, provide an essential source of SSA data. To provide the necessary spatial coverage, these facilities need to be geographically distributed around the Earth, largely located outside the territorial control of any one country. Although it is theoretically possible for the United States to unilaterally build the network of SSA data sources it requires, it is unlikely to have the fiscal capability to do so in the near future. Leveraging existing data sources and sensors at key locations around the globe, in multiple countries, is a cost-effective way to solve this problem, albeit one that trades economic challenges for political challenges.

3. Planning will far outrun the political will and motivation for actual implementation. Significant political action is only likely to follow precipitating incidents. In the case of NORAD, the Air Interceptor and Warning Plan produced in 1946 contained the basic elements that would become the NORAD warning network, and outlined the essential need to "defend the continent at the perimeter.” However, economic and political constraints largely shelved the plan until the long range nuclear bomber threat finally created the political will for NORAD in 1957 after ten years of procrastination, denial and painful adoption of quickly-superseded half-measures. It was only Soviet testing of an aircraftdeliverable, thermonuclear weapon in advance of prediction that finally drove home the desperate need for NORAD.

The January 2007 Chinese anti-satellite test and the February 2009 first-ever collision between two satellites were both watershed moments that have significantly raised the political awareness of the need for SSA and some level of data sharing.

## Plan Unpopular- EASE

EASE acquisition strategy is unpopular in Congress – use of advance appropriations and lack of detail and vision

DTIC 11 – Defense Technical Information Center, “TITLE III PROCUREMENT,” <http://www.dtic.mil/congressional_budget/pdfs/FY2012_pdfs/HAC_FY2012_PROCUREMENT.pdf>

Over the past five years, the Congress has urged the Department to consider block buys of satellites that were evolved from previous designs. This year the request includes a new proposal for space acquisition called the Evolutionary Acquisition for Space Efficiency (EASE). The Committee is disappointed that the Executive branch developed this concept without input from the Legislative branch. This is especially alarming since the entire space acquisition budget assumes the approval of this latest funding scheme. As a proposed course of action, the theory of EASE has merit, but the implementation details are woefully lacking. There are three main issues that disturb the Committee: the use of advance appropriations, the lack of detail with regards to the Capabilities/Affordability Insertion Program (CAIP), and the lack of vision for what lies beyond the current block buy of Advanced Extremely High Frequency (AEHF) satellites and the Space Based Infrared System (SBIRS) satellites.

The Committee does not approve the acquisition plan using the advance appropriations concept. The Committee understands the funding dilemma but is disappointed that the Department will not dedicate resources to fully fund its space programs, and instead is willing to rely on a budgeting gimmick. Further, there is no clear definition for the funds associated with the CAIP. The Committee is concerned that the concept for evolution of capabilities will be hijacked by the technology enthusiasts within the Department. Therefore, none of the funds appropriated to the CAIP are to be obligated until the Secretary of Defense delivers a technology insertion development plan for the technologies to be pursued for evo-lution onto future increments of the AEHF protected military satellite communications system and the SBIRS missile warning system.

The House of Appropriations Committee is powerful – controls spending

Holly on the Hill 10 – November 12 2010, “Chaffetz headed to Appropriations Committee?,” <http://hollyonthehill.wordpress.com/2010/11/11/chaffetz-headed-to-appropriations-committee/>

The Appropriations committee is widely recognized by political scientists as one of the “power committees,” since it holds the power of the purse. It is one of the exclusive committees of the House, meaning its members typically sit on no other committee. Much of the power of the committee comes from the inherent utility of controlling spending. Its subcommittee chairmen are often called “Cardinals” because of the power they wield over the budget.

Congress hates EASE – assumes availability of advance appropriations and DOD didn’t consult congress on it

Smith 11 – Marcia Smith – writer for Space Policy Online, June 13 2011, “House Approps Markup Will Bring Mostly Bad News for DOD Space Programs, Blast EASE,” <http://spacepolicyonline.com/pages/index.php?option=com_content&view=article&id=1631:house-approps-markup-will-bring-mostly-bad-news-for-dod-space-programs-blast-ease&catid=75:news&Itemid=68>

In a lengthy section beginning on p. 185, the subcommittee sharply criticized DOD's proposed Evolutionary Acquisition for Space

Efficiency ([EASE](http://www.airforce-magazine.com/Features/modernization/Pages/box021611ease.aspx)) acquisition approach to satellite systems.   EASE assumes the availability of advance appropriations instead of the year-by-year appropriations that are typically provided.   The subcommittee said it was "disappointed" that DOD developed EASE without input from Congress and found it "alarming" that DOD based its entire budget request for space programs on Congress accepting EASE.  "The Committee does not approve the acquisition plan using the advance appropriations concept," the subcommittee report states.

## Plan Unpopular- Contractor Backlash

Lockheed Martin has $107 million contract for Space Fence now – switching to an EASE acquisition strategy causes backlash

Space War 11 - Feb 08, 2011, “USAF Awards LockMart Space Fence Radar Contract,”<http://www.spacewar.com/reports/USAF_Awards_LockMart_Space_Fence_Radar_Contract_999.html>

The U.S. Air Force awarded Lockheed Martin a $107 million follow-on contract for the next phase of Space Fence, a program that will increase space situational awareness and enhance safety for both manned and unmanned space operations.

Under the 18-month contract, Lockheed Martin will further develop and prototype its ground-based radar system design in preparation for a final Space Fence production contract next year.

Space Fence will replace the existing Air Force Space Surveillance System, or VHF Fence, which has been in service since the early 1960s. The higher wave frequency of the new Space Fence radars will allow for the detection of much smaller microsatellites and debris than the current systems allow.

"The proliferation of orbital objects, including rocket debris and satellites, threatens our daily use of space-based technology and its valuable services, such as electronic navigation, satellite broadcasting and medical research," said John Morse, Lockheed Martin Space Fence program director.

"Our Space Fence design will provide the Air Force with more time to react to events potentially impacting our space assets and missions - such as collisions with space debris - before they happen."

Space Fence will field two or three high-power, S-band ground-based radars to provide the Air Force with uncued detection, tracking, accurate measurement and cataloging of resident space objects, primarily in low-earth orbit.

The current VHF system is located in the continental U.S., whereas the Space Fence radars will be located at strategic sites around the world to expand global surveillance coverage into the Southern hemisphere.

In June 2009, Lockheed Martin was one of three industry teams awarded a $30 million contract to begin concept development for Space Fence. During the recent system design review phase, the team reduced risks for its solution by prototyping, designing and performing trade studies and analysis of potential system configurations.

The team also conducted site and facility studies and developed net-centric approaches to integrate the new Space Fence with the existing architecture of the Space Surveillance Network.

Lockheed Martin has influence in Congress

SCWIT 04 – Santa Cruz Inspection Team, July 17 2004, “Why Local Activists are Turning their Attention to Lockheed Martin in Bonny Doon,” <http://santacruz.indymedia.org/newswire/display/10275/index.php>

"The world's most powerful corporation, one that literally controls the fate of the earth, is Lockheed Martin." -Helen Caldicott

The World's Most Powerful Corporation

A newly-formed coalition in Santa Cruz is turning its attention to Lockheed Martin, which has a 4000 acre facility in Bonny Doon. Lockheed Martin (L-M) is the world's largest weapons contractor. It invents and develops high-tech war-fighting weapons, markets them to the Pentagon and to Congress, and sells them around the world on the open market. It pollutes the earth, both in the production of weapons and in their use in war. It has been convicted and fined for criminal violations of US law. And yet it has much more say about our government's policies than do ordinary citizens. Lockheed Martin buys access to our government representatives, largely with money it has made from selling weapons to our government, weapons that are both subsidized and paid for with our tax dollars.

Profiteering from War

Just two months after September 11, the Pentagon contracted with Lockheed Martin for 3000 F-35 Joint Strike Fighter Planes, at the cost of 200 billion dollars. This contract has been touted as "the largest defense contract in history." In 2002, L-M received $19 billion in government contracts, including $2 for nuclear weapons. During the build-up before the war with Iraq, L-M boasted a 36% jump in profits, with a 15% increase in military aircraft sales alone. L-M is profiting from the war in Iraq, replenishing weapons for the Defense Department. For instance, L-M recently won contracts worth $109 million for kits that make dumb bombs "smart." L-M is the world's largest arms exporting company. It has sold more than 3000 F-16 combat aircraft around the world. The company also makes the Hellfire missile, "bunker buster" munitions and the massive C-130 transport plane. Developing Weapons of Mass Destruction L-M produces land mines, which kill indiscriminately. It produces weapons made with depleted uranium (DU), which contaminates the soil and the entire food chain. DU is linked to the "Persian Gulf Syndrome" which killed thousands of U.S. veterans, and thousands more Iraqis, after the first Gulf war.

This corporation has an integral role in the US Space Command's plans to wage war in space. L-M produces laser weapons, satellite surveillance equipment, and many components of the Missile Defense ("Star Wars") system. Lockheed Martin is involved in creating a whole new generation of nuclear weapons, which will likely stimulate a renewed nuclear arms race. It is working on nuclear "bunker busters," which are being built not for nuclear deterrence, but as an option for actual use in the War on Terror.

In spite of the fall of the Soviet Union, Lockheed Martin carries on with the nation's only Intercontinental Ballistic Missile program. It builds Trident II nuclear missiles, for use on Trident II Submarines. Components of Trident missiles are being built in Bonny Doon.

Trident II Made in Bonny Doon

There is a Trident II facility on Lockheed Martin in Bonny Doon. When Santa Cruz citizens campaigned against the Trident II program in the early 1980s, the government established a naval base on the grounds of Lockheed Martin in Bonny Doon, and moved the Trident II program onto the naval base. The Bonny Doon Trident II program has been shrouded in secrecy that continues to this day.

Why did Santa Cruzans oppose the program? The Trident II (D5) is a 3-stage missile with a range of 4000 miles. Each Trident II missile carries eight independently-targeted 475 kiloton thermonuclear warheads. Each Trident sub carries 24 of these missiles (192 warheads). Eighteen Trident submarines roam the world's oceans, each with the firepower to destroy an entire continent with nuclear weapons.

Past and current anti-nuclear activists in Santa Cruz say, "Not in my backyard. Not in anybody's backyard." The Trident II program threatens all life on earth. It must be shut down.

Lockheed Martin's Political Influence

Twenty-eight former L-M executives are members of the Bush administration. Lynne Cheney, the wife of the Vice President, is a former member of L-M's Board. Lockheed Martin is headquartered in Bethesda, Maryland, but because it has facilities in all 50 states, it has a "big political footprint." L-M curries favor by contributing to political campaigns at every level. It gave more than $2.2 million in political donations in 2002. Though weapons-industry PACs like L-M favor Republicans to Democrats by a 2 to 1 margin in contributions, they give to both in order to ensure access and influence.

Locally, Lockheed Martin is one of the top 11 campaign contributors to Anna Eshoo (D- 14th District). In the 1998 election cycle, Lockheed Martin was one of the top 5 campaign contributors of Diane Feinstein, contributing $14,500. (These funds come the organization's PAC, its individual members or employees or owners, and those individuals' immediate families.)

Lockheed Martin pays lobbyists to convince the Pentagon that it needs the weapons it has designed, and to persuade members of Congress to approve lucrative weapons contracts that will please voters by bringing jobs to their districts. But L-M does not limit its lobbying efforts to marketing weapons of mass destruction. It also puts its lobbyists to work trying to influence our country's military, foreign, and even domestic policies.

Contributing to the War in Iraq

L-M played a role in developing support for the war in Iraq. Former Lockheed Martin vice-president Bruce Jackson chairs the Coalition for the Liberation of Iraq, which was formed in 2002 promote Bush's plan for war in Iraq. L-M produces many of the weapons used in Afghanistan and Iraq.

Lockheed Martin has political sway – trying to persuade congress to lobby against Obama

Alternet 11 – Online News Service, May 21 2011, “Military Contractors' Secret Sway Over Our Politics -- Does Obama Have the Guts to Make Them Disclose Their Political Spending?,” [http://www.alternet.org/news/151037/military\_contractors'\_secret\_sway\_over\_our\_politics\_--\_does\_obama\_have\_the\_guts\_to\_make\_them\_disclose\_their\_political\_spending](http://www.alternet.org/news/151037/military_contractors%27_secret_sway_over_our_politics_--_does_obama_have_the_guts_to_make_them_disclose_their_political_spending)

President Obama is mulling an executive order to force big government contractors to disclose details of their political spending. Big businesses are already telling their political patrons in Congress to oppose it -- and the pressure is building.

The president should issue the executive order immediately. And he should go even further by banning all political activity by companies receiving more than half their revenues from the U.S. government.

Lockheed Martin, the nation's largest contractor, has already got more than $19 billion in federal contracts so far this year. But we know very little about Lockheed Martin's political spending other than its Political Action Committee contributions. We don't know how much money it gives to the Aerospace Industries Association to lobby for a bigger defense budget.

We don't even know how much Lockheed is giving the U.S. Chamber of Commerce to lobby against Obama's proposed executive order requiring disclosure of its political activities.

# \*\*\*CASE\*\*\*

## \*\*Hegemony\*\*

## Hegemony- Space Not Key

### The only determinant in warfare is manned capabilities and politics- a certain geographic context is irrelevant

Gray 6- Colin S. Gray, Professor of International Politics and Strategic Studies at the University of Reading, England, Recognizing and Understanding Revolutionary Change in Warfare: the Sovereignty of Context February 2006 http://www.strategicstudiesinstitute.army.mil/pdffiles/pub640.pdf

Thus far, this discussion has stressed the challenge in the novelty of the expansion of warfare’s geography. It is necessary, however, to balance that analysis with recognition of some of the more permanent features of the geographical context. Such recognition is vital for our mission because the subject of this enquiry privileges radical change and always threatens to drive into the shadows the more significant contextual elements that change either not at all or only slowly. While certainly it is necessary to attempt to recognize and try to understand revolutionary change in warfare, it is scarcely less important to recognize and understand the constants, or very-slowto- change variables. The latter concern can be controversial. There is a history of the advocates of military revolution claiming that their favored new method of war, exploiting a new geography, would certainly render obsolescent, then obsolete, older concerns tied to the other geographies. This has been the pattern of claims from the submarine, to the aircraft, to the satellite, and now to the computer. Cyberspace, we have been told, not only shrinks space and therefore time, it is effectively beyond geography, it exists everywhere and in a sense, therefore, nowhere.60 If strategic information warfare is the revolution that is coming, who cares about terrestrial geographies! If “command of the nets” is the decisive enabler of victory in future warfare, as Bruce Berkowitz maintains, physical geography cannot fail to suffer a marked demotion in strategic significance.61

Through the several RMAs of the past century, up to and including the current exploitation of the computer, the geographical context has retained features whose importance has scarcely been scratched by revolution. Notwithstanding the marvels of submarines, aircraft, spacecraft, and computers, humans are land animals and, functionally viewed, war is about the control of their will. In the timeless and priceless words of Rear Admiral J. C. Wylie, USN: “The ultimate determinant in war is the man on the scene with the gun.62 This man is the final power in war. He is control.” Military revolutionaries, whether they dream of decisive mechanized maneuver, bombardment from altitude, or electronically triggered mass disruption, should never be permitted to forget Wylie’s maxim. It is perhaps strange to record that in our enthusiasm for novelty, especially for that of a technical kind, we can forget both what war is about as well as who wages it. War is about politics and warfare always is about people, and people inhabit and relate to a geographical context.

## Hegemony- Alt Cause- Geography

### Even if the plan increases first strike capability- adaptability to different geography is still necessary for successful forward presence

Gray 6- Colin S. Gray, Professor of International Politics and Strategic Studies at the University of Reading, England, Recognizing and Understanding Revolutionary Change in Warfare: the Sovereignty of Context February 2006 http://www.strategicstudiesinstitute.army.mil/pdffiles/pub640.pdf

Another more controversial aspect to the salience of physical geography is what we call the geopolitical. It so happens that the arrangements of continents, oceans, and islands is what it is. It is undeniable that changes in warfare, and especially in the technologies of communication, have altered the meaning of geographical distance, and hence time. But there is much, indeed there is very much, of a geopolitical character in warfare’s geographical context that alters hardly at all.63 National geographical location continues to matter greatly. That location literally dictates the necessary balance among a polity’s military instruments, it determines the identity of neighbors, it translates into a distinctive history and culture, and it provides strategic opportunity and carries implicit strategic perils. Despite the wonders of network-centric warfare (NCW) and effects based operations (EBO), there are, and will long remain, significant differences between combat in the jungle, the desert, the mountains, and the city. This is not to suggest that an information-leveraging military transformation will not be able to improve performance in all environments. It is to suggest, though, that a prudent process of transformation must be flexible, adaptable, and ever mindful of the eternal fact that war is not about the enemy’s military defeat, necessary though that usually will be. Instead, war is about persuading the enemy that he is defeated; to repeat, it is about influencing his will.

Warfare is all about human behavior, ours and theirs. Every RMA, actual or mooted, is no more than a means to affect the minds of the people in our gunsights. Those people live in physical geography, and whether we traverse that geography hypersonically or at marching pace is really only a detail. As I have argued elsewhere, all politics is geopolitics and all strategy has to be geostrategy.64 Not everyone is convinced, but I am hopeful that a better appreciation of the enduring significance of geography is achievable.

## Hegemony- Alt Cause- Culture

### Adaption to cultural situations trumps brute force- necessary for successful military operations

Gray 6- Colin S. Gray, Professor of International Politics and Strategic Studies at the University of Reading, England, Recognizing and Understanding Revolutionary Change in Warfare: the Sovereignty of Context February 2006 http://www.strategicstudiesinstitute.army.mil/pdffiles/pub640.pdf

Revolutionary change in warfare may be less important than is revolutionary change in attitudes to war and the military. While the U.S. military establishment has been planning and beginning to implement a revolutionary change in its capabilities for warfare, it probably has been behind the curve in understanding revolutionary change in the social-cultural context of the institution of war. Too much can be made of this argument, as some theorists have demonstrated. However, it is plausible to argue that two revolutions are underway; one in warfare, the subject of the protracted debate over RMA and then transformation; and one in the social-cultural context of war.72 Although war has a constant nature through all periods, attitudes to its legitimacy and to its right conduct have been highly variable. U.S. fighter-bombers happily massacred the German forces who were striving desperately to escape from Normandy through the “Falaise Gap” in August 1944. By contrast, the United States wielded an air arm in 1991 that it felt obliged to rein-in, not that the airmen themselves were enthusiastic, from the historical replay of “Falaise” that was unfolding on the so-called “highway of death” leading north from Kuwait City. Standards of acceptable military behavior vary over time, from conflict to conflict, and sometimes within the same war against different enemies. The reasons are in part politicalpragmatic, as the conduct of war is scrutinized by the media with an immediacy and in a detail that is historically unprecedented.73

This process began as long ago as the 1850s in the Crimea. It was the result of greater public literacy, and hence the demand for more news, the creation of the new profession of war correspondent, the invention of the electric telegraph, and, of course, the slow growth of democratic politics which engendered a sense of public involvement in the country’s strategic ventures and adventures.74

Some theorists today believe that the RMA which is the responsibility of the U.S. defense establishment to effect is really 33 of less significance than is a Revolution in Attitudes towards the Military, or RAM. The future American way(s) of war, singular or plural, will be shaped by the social and cultural context which defines the bounds of acceptable military behavior, as well as by the military-technical opportunities that beckon as a consequence of the exploitation of information technology.

## Hegemony-Turn-Sharing

### SSA makes us more vulnerable- contested environment of space makes our information available

Ackerman 10- Edward T. Ackerman, Lt Col, Usaf , Us Military, Commercial, and International Cooperation for Improved Space Situational Awareness, 17 February 2010

With any endeavor that involves the interests of so many entities, there are bound to be challenges. Separating space‟s national security aspects from the benefits derived through cooperation is one major challenge; other issues include interoperability and legal ramifications. From the military perspective, the primary challenge to a shared SSA capability is the issue of security. Determining who can receive SSA data, what data to release, how to release it, and when to release it are key questions that must be answered. If the US military has information on satellites that requires protection, then vigilance and perhaps discretion in 13 publishing or passing this information must be exercised. In a November 2008 memo, Lt Gen William Shelton, then the commander of Fourteenth Air Force stated, “As space becomes an increasingly contested environment, we must be cautious about disseminating Space Situational Awareness data to unknown recipients.”43 Without proper consideration as to what data is being released and to whom, could in General Shelton‟s words, “potentially provide cueing and/or targeting data to our adversaries.”44

## Hegemony- Turn- Reliance

### SSA leads to dependence- information may not always be available

Ackerman 10- Edward T. Ackerman, Lt Col, Usaf , Us Military, Commercial, and International Cooperation for Improved Space Situational Awareness, 17 February 2010

The systems put in place must employ technical and procedural controls to restrict information as appropriate in order to protect US space assets or employ capabilities in battle against adversaries. However, political concerns could well affect wartime SSA data. For example, SSA could become analogous to GPS, a global utility so highly integrated into everyday life that the thought of limiting its access introduces global economic and worldwide safety concerns. Should SSA end up providing the ubiquitous and unexpected benefits that GPS has, similar ramifications in restricting access may well be felt. Additionally, the US military must be cautious and not develop complete dependencies on external sources for conducting military missions since member provided information may not always be available.

## Hegemony- Turn- More Sensors

### More sensors lead to information glitches- this causes communication failure

Litvaitis 8- Arturas Litvaitis, graduate of the Joint Command and General Staff Course 2007/2008 of the Baltic Defence College, Challenges of Implementation of the Network Centric Warfare Tenets in Coalition Environment Baltic Security & Defence Review Volume 10, 2008

Col. Alan D. Campen, USAF (Ret.), in his article is sceptical about the practical proof of the NCW concept presented by its proponents: “Probing questions about NCW were raised as early as 1998 and are echoed today by other voices who contend that substantial technology-driven changes in force structure, organization and operational art should be founded on more substantive evidence than can be gained from selectively sampling the scenario-unique sands of the Iraq War. Fixation on battlefield experience in Iraq can mask issues that rival NCW in fuelling the engine of military transformation” (Campen, 2004). He is supported by Greg Grant, whose opinion is that experience in Iraq has proven that less technically advanced adversary can apply time-tested concealment methods and cheat state-of-the-art U.S. sensors. Grant also explains that, in situations when the enemy becomes out of reach of the U.S. sensors’ view or when communication with the sensor is degraded, the enemy position becomes halted on the information system screen because there is no more updating feed from the sensor. In this quite frequent scenario, relevant situational awareness could not be produced (Grant, 2005). The potential danger of specialization of platforms (sensors and actors) could put actors into danger when communications are lost or degraded by the enemy, because in this case actors become blind: “As fighting vehicles - planes, ships, tanks - are connected to the web, they tend to be dumbed down to save money. Why carry a sensor when the same information is available from other sources? But if network access is severed, the vehicles may lack the capacity to autonomously defend themselves.” (Thompson, 2003)

## \*\*Deterrence\*\*

## Nuclear Deterrence Fails- Human Perception

### a) Unreliable- Relies on human perception

### Gray 99- Colin S. Gray, author and professor of international relations and strategic studies at the University of Reading, The Second Nuclear Age Chapter 1: To Confuse Ourselves: Nuclear Fallacies 1999

Deterrence is never reliable, and this general truth applies with particular force today in the second nuclear age. In the most vigorous and rigorous assault to date on the smellier orthodoxies of both expert and popular beliefs about deterrence, Keith B. Payne offers an uncompromising view of the pertinent realities.

In the second nuclear age, several factors are combining to change the strategic environment of effective deterrence policies: the apparent increase in threats posed by rogue states such as Iraq, Iran, Libya, Syria, China, and North Korea; the retraction of US forward-based armed forces; and the proliferation of WMD. Given these features of the second nuclear age, in comparison with the cold war, US deterrence goals will have to be expanded: the list of players to be deterred has to be expanded, as do the types of behavior to be prevented.26

Why is it that deterrence, even nuclear deterrence, is unreliable? Sir Michael Quinlan penetrates to the heart of the matter when he writes: ‘[d]eterrence is a concept for operating upon the thinking of others. It therefore entails some basic presuppositions about that thinking’.27 Deterrence, therefore, is a relational variable; it is an effect upon, or influence over, behaviour, achieved and achievable only with the co-operation of the intended deteree. Deterrence is structurally unreliable for precisely the same leading reason why friction in war cannot be eliminated by wonderful new technologies:28 specifically, there are human beings in the loop for deterrence and for the conduct of strategy in war. An individual policy-maker, or a group of policy-makers, may decide not to be deterred. Literally, there can be no such thing as ‘the deterrent’, nuclear or otherwise.Whether or not a nuclear arsenal deters is a matter for decision by the recipients of would-be deterrent menaces, not by the owners of the putative deterrent.

## Deterrence Fails- Unreliable

### b) Detterence neglects key factors in decision making

Gray 99- Colin S. Gray, author and professor of international relations and strategic studies at the University of Reading, *The Second Nuclear Age*  Chapter 1: To Confuse Ourselves: Nuclear Fallacies 1999

Nothing, repeat nothing, can render intended deterrent effect entirely reliable. Prudent and sensibly fearful policy-makers certainly should be appalled to the point of co-operation by some not-totally-incredible prospect of suffering damage utterly disproportionate to the prospective gains from an adventurous policy. But ‘should’ is not ‘will’, and even if policymakers genuinely are appalled by the risks that they believe they are running, they might decide to run those risks anyway. Western scholars who place confidence in the practice of the theory of stable deterrence are wont to neglect to factor in the political dimension of strength of motivation for inimical behaviour.33 The key problem is that even if every roguish regime in the world is deterrable over every issue concerning which they are contemplating bold moves, there is no way that an American would-be deterrer can be certain that they would know the specific requirements of deterrence for all those cases.

## Deterrence Fails- China

### Deterrence against china fails- no reliable trust

Gray 99- Colin S. Gray, author and professor of international relations and strategic studies at the University of Reading, *The Second Nuclear Age*  Chapter 1: To Confuse Ourselves: Nuclear Fallacies 1999

A United States that, for example, wishes to achieve such deterrent effect in Beijing as may be necessary is entirely uncertain over how much, and over some questions even whether, deterrence is needed. To a significant degree the deterrence needs of the United States vis-á-vis China currently are unknowable. Some readers may be discomforted by such an open-ended argument regarding China, but that open-endedness is the very core of the difficulty that one must recognize. A China hugely in a condition of domestic turmoil is distinctly possible for the next several decades. How the desperately insecure leaders of such a China could be deterred from taking action—in a bid for national unity—over Taiwan, we cannot know reliably, and even those insecure Chinese leaders themselves cannot know reliably. Ultimately, deterrence is like that.

## Deterrence- Turn- Info. Overload

### Sharing and increase information reduces deterrence- reduces interopability

Litvaitis 8- Arturas Litvaitis, graduate of the Joint Command and General Staff Course 2007/2008 of the Baltic Defence College, Challenges of Implementation of the Network Centric Warfare Tenets in Coalition Environment Baltic Security & Defence Review Volume 10, 2008

Aldo Borgu raises a number of conceivable issues related to the practical implementation of Network Centric Warfare. For instance, it would be a challenge to establish a single network across different services and nations. In his opinion, it most probably will be difficult to integrate “network of networks”. Extensive sharing of information has potential danger of information overload and decreased speed of command. On the other hand, access to the same, even high quality, information doesn’t automatically mean that different people will come to similar conclusions. In reverse of a Network Centric Warfare proposition of decentralisation of decision making, there is a great deal of probability that availability of low tactical level information for the highest levels of command may lead to even greater centralization (micro-management). He also points out that different nations have different view and different approach to the network related military concepts, which automatically implies problems with operational and procedural interoperability. Fast technical U.S. advance will even deepen capability gap between the United States and its allies, so Network Centric Operations in coalition may have no common technical basis (Borgu, 2003).

## Deterrence- Turn- Sensors

### SSA is vulnerable to increased amount of threats- more sensors cause information to become less reliable

Ginter 7- Lieutenant Colonel Karl Ginter United States Army Dr. Clayton K. S. Chun Project Adviser, Space Technology and Network Centric Warfare: a Strategic

Paradox, 30 MAR 2007

The network centric warfare (NCW) concept of developing and leveraging information superiority by synchronizing sensors and shooters provides commanders with greater battlespace awareness and greatly enhances the warfighting capabilities for the U.S. military. A remarkable paradox of NCW and its heavy reliance upon space-based assets and technology is that the very capabilities that enable information sharing on the battlefield makes them increasingly vulnerable to a host of emerging threats. The growing network and communications interconnectivity of the GIG, both terrestrial and space, poses enormous risks to our command and control capabilities, information systems, and essential computer operations that enable battle command. These vulnerabilities also impact political and diplomatic means to achieve national security goals.

Some of the key enabling technologies of NCW are the Global Positioning System (GPS), communications satellites (both military and commercial), and our voice and data networks—all placing critical information at the fingertips of the warfighters.1 These systems have inherent vulnerabilities that can, have, and will be exploited by our adversaries. Adversaries such as terrorist cells, organized crime, transnational groups, and nation-states who can not compete militarily or financially with the United States’ robust information technology capabilities are identifying network vulnerabilities and developing relatively inexpensive attack capabilities to exploit these risks.2 Moreover, the proliferation of vast, networked, computer-based capabilities that employ space assets as primary enablers can expect to encounter increased incidence of natural phenomena, human error, and technical failures.

## Deterrence- Turn- Asymmetric Information

### Information availability increases the likelihood for conflict- allows weaker states to predict the outcome of war

### Jackson and Eberle 9- Matthew O. Jackson, William D. Eberle Professor of Economics at Stanford University, Massimo Morelli, Professor of Economics and Political Science at Columbia University, The Reasons for Wars – an Updated Survey, Revised: December 2009 http://www.stanford.edu/~jacksonm/war-overview.pdf

Asymmetries of information can arise from a variety of sources. It could be an asymmetry of information about the relative strengths of the countries either because of differences in what they know about each other's armaments, quality of military personnel and tactics, determination, geography, political climate, or even just about the relative probability of different outcomes.

The possibility of a bargaining failure due to asymmetric information has a solid foundation in economics, and was made very clear in work by Myerson and Satterthwaite (1983). To see the basic insights in the context of war, suppose that there are two countries and one of them, referred to as country A, has unknown strength. In particular, suppose that country A can either be strong or weak with equal probability in the eyes of the other country. Imagine that war involves a relatively small cost, that the victor in a war gains control of all resources, and that war results in one of the two countries conquering the other. Suppose that if country A is strong then it wins a war with probability 3/4 and if it is weak it wins with probability 1/4. So, in order to always avoid a war, an agreement must provide the strong version of country A with at least 3/4 of all resources less the cost of war (in expectation, presuming it maximizes expected payoff).

Now the asymmetry of information enters: a weak version of country A cannot be distinguished from a strong one by country B. Thus if the strong version of country A always gets at least 3/4 of the resources less the cost of war, then since a weak version of the country cannot be distinguished from a strong version by country B, a weak version of country A must also expect at least 3/4 of the total resources less the cost of war, as it can mimic a strong version of the country and get a high payoff without risk of war. This means that country B must get at most 1/4 of all resources plus the cost of war. If the cost of war is low enough, then the country B is better off simply going to war and taking its chances rather than reaching such an unfavorable bargain. This is obviously a highly stylized example, but it encapsulates the difficulties with bargaining in the face of asymmetric information. Generally, it may be difficult for a weak country to pretend to be a strong one, but there can still be some degree of asymmetric information across countries and even lesser asymmetries can make it impossible to find agreements that all parties will agree to in all circumstances.

It is important to note that imperfect information about the opponent's resolve or strength is a source of conflict that does not require any violation of common knowledge of rationality. The above reasoning is such that all the actors are fully rational, understand the setting, and fully comprehend all of its implications. It is also clear that the countries would like to avoid the difficulty. In particular, a strong version of country A would like to be able to distinguish itself from the weak version. If it could credibly demonstrate its strength, that would solve the problem. That is, if strength can be revealed peacefully and credibly (even at some minor cost), then there is a bargain which works as follows: if country A reveals strength, then it gets 3/4 of all resources and if it does not reveal its strength then it is presumed to be weak and only gets 1/4 of all resources. This solves the incentive problem as the weak version of country A can no longer pretend to be strong. Weakness is presumed unless evidence is presented to the contrary. This provides some insight into why countries might be willing to demonstrate arms (for instance publicly testing nuclear devices, holding military parades and exercises in observable settings, and so forth). There might be other settings where hiding strength is advantageous because bargaining is precluded,8 but in settings where binding agreements can be reached there are powerful incentives for the strongest types to reveal their strength to distinguish themselves from weaker types and to cement their bargaining position. Moreover, this is not limited to settings with just two potential strengths. Even with many different gradations of strength, the strongest wants to reveal itself, and then the next strongest will want to reveal itself, and so forth and this then unravels so all but the weakest types want to distinguish themselves. So this is robust to much richer information environments than the example above.

With such asymmetries of information, whether war will occur will depend on the extent to which the private information of individuals can be credibly revealed or not as well as how relevant the private information is to forecasting the outcome of a war. If it is really impossible to fully and credibly reveal information and such information is critical to predicting the outcome of a potential war, it can be that bargaining will fail and war must be expected with at least some probability. An early paper providing a model of war decisions with asymmetrically informed countries, and pointing out that an uninformed country may sometimes have to go to war to avoid bluffing behavior by an informed country, is Brito and Intriligator (1985).

The form of information asymmetry discussed above concerns potential outcomes of a war. A second information-based reason for a bargaining failure is that agents have inconsistent beliefs. For example, it could be that two states each are optimistic and are convinced that they will benefit from a war. In these cases war can erupt, as long as the inconsistency of beliefs is large enough to compensate for the cost of war. For instance, if both parties expect to win a war with a high enough probability, then there would not exist any agreement that avoids war.9 The possibility and examples of wars that are attributed to such miscalculations or errors due to lack of information or to different priors about relative power have been discussed informally by Blainey (1973), Gartzke (1999), Wagner (2000), Smith and Stam (2003), among others.

A third form of information asymmetry concerns incomplete information about the motivations of other agents. Here it is believed that there is some probability that the other actor might be irrational.10 This includes spiraling models such as those discussed in Waltz (1959) and Schelling (1963), and more recently Kydd (1997). These ideas have been elaborated and extended upon by Baliga and Sjöström (2004) and subsequent works. The idea common to these works is that even a small probability of being faced by an armed irrational foe can lead a rational country to arm to some level. In turn, this now means that either a foe who is irrational, or a foe who thinks that I might be irrational will be arming, and this then leads me to arm even more, and this feedback continues to build. Depending on the specifics of the payoffs to arming and potential conflict, it can be that the rational countries each arm to very high levels and are ready to attack first because of the fear that the other side may attack first. In some cases, communication can help overcome this problem, since it can be in both countries’ interests to be known to be rational, but this depends on the specifics of the setting and the type of communication available,as Baliga and Sjöström (2009) show.

## Deterrence- Turn- Generic

### SSA decreases deterrence in the long-term- causes over-reliance

### Metz 2000- Steven Metz, Research Professor of National Security Affairs in the Strategic Studies Institute, ARMED CONFLICT in the 21st CENTURY: the INFORMATION REVOLUTION and POST-MODERN WARFARE April 2000 http://www.au.af.mil/au/awc/awcgate/ssi/metz\_info\_rev.pdf

Other pockets of innovation and creativity exist through the Department of Defense. For instance, the Pentagon’s Office of Net Assessment, which was the birthplace of American thinking on the revolution in military affairs, has developed an Operational Concepts Wargaming Program to explore the ideas outlined in JV 2010. 66 The Defense Science Board has done some useful thinking about a new land-based military unit which reflects the operational preferences and technological capabilities of a postmodern military. This new unit would be light, agile, and potent. It would operate in a distributed and desegregated fashion, utilizing high situational awareness generated by information technology, depending on remote fires, connected by a robust information infrastructure, and supported by precision logistics. 67 Such an organization could provide a rapid intervention capability and prepare the way for heavier units which would arrive later. It would fight for two weeks or less and then either be reinforced or withdrawn. The basic element would be “combat cells” which would make extensive use of unmanned vehicles and robotics, using humans “only when necessary.” They would avoid direct firefights, remaining dispersed most of the time for survivability, massing only to repulse a major attack. Information technology would be central: “A key capability for combat cell mission success is maintaining a local awareness bubble larger than the enemy’s.” 68

Along similar lines, a study group at the Department of Defense’s Center for Advanced Concepts and Technology has explored the concept of “rapid dominance” attained by “shock and awe.” This is a very important attempt to integrate a psychological dimension into mainstream thinking on the revolution in military affairs. The goal is to use a variety of approaches and techniques to control what an adversary perceives, understands, and knows. 69 To do 37 this, a rapid dominance military force must have near total or absolute knowledge and understanding of itself, the adversary, and operational environment; rapidity and timeliness in application; operational brilliance in execution; and near total control and signature management of the operational environment.

It is not clear, though, what effect an inability to attain one or more of these things might have on a postmodern military. While attaining a perfect picture of the battlefield would give the U.S. military great advantages, reliance on this would also be a vulnerability. Might the future U.S. military become so accustomed to the absence of the fog of war that it could not overcome imperfect knowledge when it does occur? As one dimension of the paradoxical logic of strategy, weakness sometimes begets strength and strength sometimes begets weakness. Eventually, this intricate conundrum might erode the battlefield advantage of the American armed forces.

## Deterrence- Turn- Decision Making- Decentralization

### Increased information due to situational awareness leads to decision-making decentralization

### Cotton 5- Lieutenant Colonel Anthony J. Cotton, United States Air Force, Dr. William G. Pierce Project Adviser, Usawc Strategy Research Project Information Technology – Information Overload for Strategic Leaders, 18 March 2005 http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA431929

One of the most difficult problems that confront any commander who has committed his forces in accordance with a well-developed plan is to alter the operation in light of changing circumstances. Sun Tzu recognized the inherent difficulties, both intellectual and physical, and repeatedly emphasized that the nature of war is ceaseless change.30 Information technology is able to rapidly reflect change and provides the ability to display more information into the warfighting process. Ultimately, the strategic level span of control will be expanded and could cause the streamlining of the operational chain of command. Senior leaders thousands of miles away have the capability to make more decisions traditionally left to tactical and operational commanders. This new construct will result in a flatter command structure not currently in place today.

A flatter structure may not always be beneficial. Lieutenant General Michael Short, Joint Forces Air Component Commander during Operation Allied Force shared his frustrations in many public forums. During a panel discussion at the Air Force Association National Symposium in 2000 he brought the point home.

About 45 days into the war, Predator was providing great coverage for us. …we had live Predator video of three tanks moving down the road in Serbia and Kosovo. We had a FAC [Forward Air Controller] overhead and General Clark [Gen. Wesley K. Clark, SACEUR] had the same live Predator video that I had. “Mike, I want you to kill those tanks.” I quickly responded, I had something else in mind, “Boss, I’ll go after that for you.” When shift time came, [Maj. Gen.] Garry Trexler was on the floor, finishing up in the daytime, and Gelwix arrived to take the night shift. I was there because the SACEUR wanted those three tanks killed. We had a weapon school graduate on the phone talking direction to the FAC on the radio. [The] call went something like this: “A lot of interest in killing those tanks, 421. I’d like you to work on it.” “Roger.” Two or three minutes went by, and 421 clearly had not found those tanks. The young major’s voice went up a bit and said, “ComAirSouth, and SACEUR are real interested in killing those tanks. Have you got them yet?” “Negative.” About two more minutes went by and the weapons school graduate played his last card. “General Short really wants those tanks killed.” And a voice came back that I’ve heard in my house for the better part of 30 years and he said, “[expletive deleted], Dad, I can’t see the [expletive deleted] tanks!”

The incident illustrates how information technology can “drag” strategic and operational thinkers into the tactical level. There are other similar lessons throughout history of a narrowing of focus leading to the possible tendency for senior leaders to relive their “frontline fighting days.” 7 Air Force Doctrine Document 1, the USAF capstone doctrine document, highlights the tenet of centralized control with decentralized execution as crucial to the effective application of air and space power. This tenet compliments the principle of unity of command. Decentralized execution of air and space power is the delegation of execution authority to responsible and capable lower level commanders to achieve effective span of control and to foster disciplined initiative, situational responsiveness, and tactical flexibility. However, numerous forces are changing the applicability of that doctrine. U.S. involvement in wars with limited aims, combined with the technology which allows senior commanders to see the common operational picture and view from the cockpit is driving a trend towards the centralization of air power execution. At the same time, the development of NCW can either centralize or decentralize the control and execution of air power. Over centralization of planning and execution by a staff far from the battle can be deleterious. Air Force doctrine actually addresses the temptation towards centralized execution. The following is an excerpt from AFDD-1: Modern communications technology provides a temptation towards increasingly centralized execution of air and space power. Although several recent operations have employed some degrees of centralized execution, such command arrangements will not stand up in a fully stressed, dynamic combat environment, and as such should not become the norm for all air operations. Despite impressive gains in data exploitation and automated decision aids, a single person cannot achieve and maintain detailed situational awareness when fighting a conflict involving many simultaneous engagements taking place throughout a large area. A high level of centralized execution results in a rigid campaign unresponsive to local conditions and lacking in tactical flexibility. For this reason, execution should be decentralized within a command and control architecture that exploits the ability of strike package leaders, air battle managers, forward air controllers, and other front-line commanders to make on-scene decisions during complex, rapidly unfolding operations. Nevertheless, in some situations, there may be valid reasons for execution of specific operations at higher levels, most notably when the JFC (or perhaps even higher authorities) may wish to control strategic effects, even at the sacrifice of tactical efficiency. 31

U.S. Army FM 100-6 adds ”The accuracy, lethality, and range of modern weapons have forced commanders to disperse their formations, decentralizing control and execution. The speed and pervasiveness of data transmission in the Information Age are causing a revolutionary change in the nature of military operations and warfare.

### Increased information causes commanders to be indefinite about decision making

### Cotton 5- Lieutenant Colonel Anthony J. Cotton, United States Air Force, Dr. William G. Pierce Project Adviser, Usawc Strategy Research Project Information Technology – Information Overload for Strategic Leaders, 18 March 2005 http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA431929

Information overload has flooded our society with a proliferation of “expert opinion.” With the widening pool of elaborate studies and arguments on every side of every question, more expert knowledge has, paradoxically, led to less clarity. This phenomenon is known as 8 “analysis paralysis.”33 The endless analysis is so overwhelming; some experts in the field believe it is becoming difficult to know how and when to decide.34

As discussed above, communication among all echelons will shift dissemination and collection of intelligence, targeting and other data from hierarchical to a non-hierarchical command structure. As the strategic span of control increases, whether through simple e-mail traffic or complex Military Satellite Communications networks, there could be a gravitation to coordinate tactical operations at higher levels. Theoretically, everyone from the White House, the Joint Staff and the Combatant Commander Staffs, down to the tactical level could have access to the same data. Each organization would feel compelled to analyze the information and provide feedback. As we have seen in recent military operations, some operational and tactical level decisions could come from the White House or the Joint Staff. Information technology may unintentionally affect the relationship between echelons by limiting the organization’s initiative, ingenuity, and inventiveness through monitoring by superiors. Retired U.S. Air Force Major General Perry M. Smith, identified initiative, ingenuity and inventiveness as key traits required for military leaders. These traits within our leaders make the

U.S. military a formidable force and anything that adversely affects these traits should not necessarily be considered good for the force.35

Increased theater awareness and the ability to transmit the information pose several problems for subordinate commanders. There is a great fear that senior commanders and staff will second-guess every decision. Will a senior leader allow his or her subordinate commander to operate under their own prerogatives or will he redirect efforts? The outcome will likely be determined by the senior officer’s personality but the fact that higher-level intervention during execution is possible, it may not be desirable.

## Deterrence- Turn- Decision Making

### Information overload makes processing impossible

### Adams 1- Thomas K. Adams, national security consultant based in the Washington DC area. He is a veteran of thirty-four years military service, principally in intelligence and special operations at tactical, operational, and strategic levels from Vietnam to Bosnia, Future Warfare and the Decline of Human Decisionmaking, Parameters, Winter 2001-02, pp. 57-71. http://www.carlisle.army.mil/usawc/Parameters/Articles/01winter/adams.htm

In short, the military systems (including weapons) now on the horizon will be too fast, too small, too numerous, and will create an environment too complex for humans to direct. Furthermore, the proliferation of information-based systems will produce a data overload that will make it difficult or impossible for humans to directly intervene in decisionmaking. This is not a consideration for the remote science-fiction future. Weapons and other military systems already under development will function at increasingly higher levels of complexity and responsibility--and increasingly without meaningful human intervention.

According to the US Army Infantry School, "We intend to transform the Army, all components, into a standard design with internetted C4ISR."[7] And, it is well known that various "digital army" initiatives such as the Land Warrior system and the Force XXI Battle Command Brigade and Below are under way.[8] Likewise, a number of unmanned and semi-autonomous systems are already in wide use, and autonomous systems are in prototype or development.[9] The first operational light-speed weapon, the US Air Force's Yal-1a Attack Laser (also known as ABL or Airborne Laser), is slated for operational readiness by 2003. Others, such as high-power microwave and particle-beam devices, are under development.[10] At Sandia National Laboratories, tiny MEMS (Micro-Electro-Mechanical Systems) already exist in prototype form.[11]

None of this is accidental. For one thing, it is national policy, articulated by former President Bill Clinton as a critical part of the national security strategy.[12] Second, it has been pursued tenaciously by the military despite expense, setbacks, and criticism. Knowledge is seen as the key to "battlefield dominance," and speed is seen as the key to exploiting that knowledge. We have made these two qualities--knowledge (information) and speed--the keystones of planning for the future Army and the other services as well. Army After Next (AAN) forces are expected to need both "linear speed" (speed across the ground) and "angular speed" (the ability to out-think and anticipate) in order to survive and win on future battlefields.[13] Like the chiefs of the other services, General Eric Shinseki, the Army Chief of Staff, has clearly stated that he endorses this concept.[14] It is believed that these qualities--information dominance, combined with speed and agility--will lead to military dominance at all levels of warfare: strategic, operational, and tactical.[15]

Military discussions of advanced warfighting (as opposed to scientific or technical ones) occasionally include the reassurance that there will always be an immediate, direct, and intimate connection between human beings and warfighting. According to the Joint Chiefs of Staff, "The purpose of technology is to equip the man. We must not fall prey to the mistaken notion technology can reduce warfare to simply manning the equipment."[16] As a white paper from the US Army's Training and Doctrine Command (TRADOC) put it, "Autonomous unmanned systems will be fully adaptive to unforeseen changes while remaining completely predictable in mission performance."[17]

We are faced with the prospect of equipment that not only does not require soldiers to operate it, but may be defeated if humans do attempt to exert control in any direct way. It is easy to see a steadily decreasing role for humans in direct combat as the 21st century progresses.

## Deterrence- Turn- Coalition Operations

### NCW decreases coalition readiness- creates gaps with allies

### Cotton 5- Lieutenant Colonel Anthony J. Cotton, United States Air Force, Dr. William G. Pierce Project Adviser, Usawc Strategy Research Project Information Technology – Information Overload for Strategic Leaders, 18 March 2005 http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA431929

Maximized effects of the information age have caused the potential for undesired outcomes within its service component. The stress of information proliferation for senior leaders and the troops they lead are exacerbated when relating to the lack of interoperability of U.S. forces with coalition forces.

Coalitions have become a fundamental tool of United States diplomacy. It has enabled the United States to draw upon other nations’ forces to help face the challenges of “policing” our world. From Operation Desert Shield/Desert Storm, Kosovo to Operation Iraqi Freedom, the United States has relied on its coalition partners to help in either the warfare or peacekeeping segments of any major military intervention. A digitized DOD creates an even greater disparity in capability between the U.S. forces and coalition forces with whom we operate. Our coalition partners do not possess the same resources and integrated systems as the U.S.

Nation states that make up coalitions and alliances face a daunting task. Even our closest allies lack the interoperability to “plug in” to our systems. What happens to nations who want to offer support but lack the resources? European countries have slashed their defense budgets to an average below two per cent of their Gross Domestic Product.43 U.S. spending on defense research and development is four times greater than European counterparts.44 The security 13 implications surrounding the use of NCW architecture present additional challenges to effective coalition operations. NATO has attempted to address the issue of transformation.

In 2002, The Prague Summit launched three key military transformation initiatives: The Prague Capabilities Commitment (PCC), the NATO Response Force and the new NATO Command Structure. The latter creating the NATO Supreme Allied Command Transformation discussed earlier. The PCC directly addresses improved interoperability of forces as well as command, control and information superiority. The September 2002 National Security Strategy articulates the need to “take advantage of the technological opportunities and economies of scale in defense spending…and diminish our vulnerabilities.”45 While numerous areas for improvement have been identified, success will depend on funding. Until then, coalitions and alliances will be unable to contribute equally in high-end operations, worsening the perception of major European partners’ unwillingness to take on their fair share of the world burden.

## Deterrence- Turn- Information Sharing

### Adversaries will take advtange of the information connectedness SSA affords

Metz 2000- Steven Metz, Research Professor of National Security Affairs in the Strategic Studies Institute, ARMED CONFLICT in the 21st CENTURY: the INFORMATION REVOLUTION and POST-MODERN WARFARE April 2000 http://www.au.af.mil/au/awc/awcgate/ssi/metz\_info\_rev.pdf

Interconnectedness also means that future enemies will have a potential constituency within the United States. This is not to imply that émigré communities are automatic breeding grounds for “third columnists.” But immigrants or even native-born children or grandchildren of immigrants can, in some cases, retain a tie to their ethnic homeland which can lead them to lobby for or against American military involvement, as did Serbian Americans during the first stages of the 1999 air campaign. This increases the pressure on American policymakers and military leaders to minimize casualties if the use of force becomes necessary. Émigré communities can also provide logistics and intelligence support for terrorists. Interconnectedness will make protection against terrorism more difficult.

The U.S. Department of Defense and the military services hold that speed, knowledge, and precision will minimize casualties and lead to the rapid resolution of wars, thus minimizing the problems associated with the challenges to the political utility of force. States with fewer intellectual and financial resources than the United States will not have the luxury of using technology as a palliative for the strategic problems associated with interconnectedness and thus must seek other solutions. One such response has been renewed interest in multinational peacekeeping. The idea is that containing or deterring armed conflict limits the chances of full blown war. Some states may turn instead to strategies of passive defense. One of the dilemmas of interconnectedness is that what happens in one place affects many others, but explaining this to mass publics remains difficult. Aggressive states or non-state actors will also have to find ways to transcend the constraints brought on by interconnectedness. Some will rely on proxy conflict, providing surreptitious or, at least, quiet support to insurgents, militias, or terrorists whose activities further the aims of the sponsoring state. Some may attempt hidden or camouflaged aggression, particularly cyberwarfare aimed at the information systems of their enemies. Some—particularly those which find their ambitions blunted by the United States—will turn to political methods, ceding battlefield superiority to the American military while seeking to constrict Washington through legal and political means. America’s military advantages, after all, are not always matched by an equal political and diplomatic superiority.

Because globalization and interconnectedness erode the control which regimes can exercise within their states, those with a shaky hold on power will often seek scapegoats but will sometimes turn to the time-tested method of solidifying internal unity by external aggression as well. Since globalization and interconnectedness raise the political and economic cost of protracted war, regimes which seek to deflect internal discontent through external 18 aggression will probably seek lightening campaigns, seizing something before the international community can reach consensus on intervention. Future actions like the Iraqi seizure of Kuwait are not out of the question, at least for states which believe that the United States cannot or will not stop them. Whether the United States can be deterred from intervention by weapons of mass destruction or terrorism is one of the central questions for the future global security environment.

## Deterrence- No Solvency- Lack of Command and Control

### No solvency for communication

Litvaitis 8- Arturas Litvaitis, graduate of the Joint Command and General Staff Course 2007/2008 of the Baltic Defence College, Challenges of Implementation of the Network Centric Warfare Tenets in Coalition Environment Baltic Security & Defence Review Volume 10, 2008

To realize the main idea of the first Network Centric Warfare tenet, to establish networked forces and improve information sharing, the network services should be available theoretically wherever the operational situation demands; however, robust network connectivity down to the tactical level is still the issue to be addressed in the U.S. armed forces themselves (Tisserand, 2006:B-2). Usually, at the low tactical level, national communications systems can provide only voice communications, which is clearly insufficient for intelligence information distribution, targeting data and higher commander’s intent delivery. The most promising way to provide all necessary types of communications services (voice, data, videoconferencing etc.), is to use satellite communications, but again it is a scarce resource even for the United States, not to talk about the small nations, where national satellite communications are simply not available Baltic Security & Defence Review Volume 10, 2008 153 and services, offered by the commercial providers, are expensive and not always reliable.

## Deterrence- No Solvency- Interoperability

### Gap of interobaility between allies isn’t addressed

Litvaitis 8- Arturas Litvaitis, graduate of the Joint Command and General Staff Course 2007/2008 of the Baltic Defence College, Challenges of Implementation of the Network Centric Warfare Tenets in Coalition Environment Baltic Security & Defence Review Volume 10, 2008

Another significant issue is that today, for multinational operations, the nations are deploying their communications systems which cannot be interconnected due to the use of different protocols, bandwidths and frequencies. Interoperability has been on the list of unresolved issues for a long time, even in those organizations which work hard on achieving interoperability among its members. NATO could serve as a typical example: “The performance of the European armed forces in NATO - or U.S.-led coalition operations, such as in Kosovo, Afghanistan and Iraq, demonstrated clearly the existence of a glaring transatlantic capability gap that has limited the interoperability of multinational forces and the efficiency of coalition war fighting” (Nolin, 2006). Despite the growing trend to build their networks in accordance with commonly agreed military standards, the nations continue to realize their specific national approaches even in those cases when the agreed standards (for instance, NATO STANAG’s) are taken as a basis. Quite a promising direction is the adoption of commercial standards in the military world (Commercial Off-the-Shelf, or COTS, solutions); however, within the industry we can notice a variety of proprietary features, on top of commercial standards, which make network solutions, delivered by different manufacturers, not interoperable, although those solutions are based on the same commercial standard. Lessons learned during multinational military communications and information systems interoperability exercises show that the United States and European nations are still quite away from the “plug and play” level of communications interoperability.

## Deterrence- No Solvency- Bandwidth

### The plan can’t address poor network management

Litvaitis 8- Arturas Litvaitis, graduate of the Joint Command and General Staff Course 2007/2008 of the Baltic Defence College, Challenges of Implementation of the Network Centric Warfare Tenets in Coalition Environment Baltic Security & Defence Review Volume 10, 2008

Having the national networks deployed and getting them interconnected is not the end of the story – usually real operating environment demands the ability to flexibly reconfigure the network, provide increased bandwidth between particular nodes on the network or connect new nodes to the network. Multiple nations, operating in a relatively small area, have diverse requirements for the use of electromagnetic spectrum, necessary for operation of their sensors and wireless communications. This is all about the network management. Taking into account the growing bandwidth demand, it is most likely that opportunities, provided by rather rapidly evolving communications technologies, will be behind the user requirements. Therefore implementation of the net-centric concepts would require an efficient use of network resources, and this is the place, where network management will play its very important role.

Network management within national domains is quite a challenging issue (Donnelly, 2005). However, within the multinational environment, it requires even more effort. First of all, in the recent years, we cannot observe any significant improvement in defining multinational networks’ architecture. For instance, NATO Consultation, Command and Control Board and its sub-committees are working on NATO Information Infrastructure (NII), which is supposed to address the Alliance’s Network Enabled Capabilities architectural issues, but at present stage, it doesn’t seem that architectural developments are turning towards the real netcentric approach. On the contrary, we are still discussing the issue how backbone network, which is supposed to be provided by NATO, will be interconnected with national “appendixes”; therefore hierarchical network architecture is still in place (CNSSC, 2008). Continuing with this approach would not contribute to the construction of flexible and dynamic networks, where a network participant can communicate with any other wherever it is located and whatever nation it belongs to. How can we imagine communication in a hierarchical network between an airborne platform from nation A and a ground-based unit from nation B, when that platform was re-tasked on the spot to accomplish the mission in the airspace over a ground unit, if co-ordination didn’t take place between nations A and B in advance? These issues were already identified during real operations (Hayes, 2004).

## Deterrence- No Solvency- Network Management

### Information exchange doesn’t exist- lack of common network

Litvaitis 8- Arturas Litvaitis, graduate of the Joint Command and General Staff Course 2007/2008 of the Baltic Defence College, Challenges of Implementation of the Network Centric Warfare Tenets in Coalition Environment Baltic Security & Defence Review Volume 10, 2008

Similarly to networking solutions themselves, nations usually have their nation-specific approaches to the network management, consisting of a variety of methods, tools and technical solutions, because there is no multinational consensus how to manage multinational federation of networks, or, in case of the network-centric approach, the single network made of national “pieces”. This happens because we are still thinking in the hierarchical network architectural dimension.

Network, truly supporting net-centric approach, has no centre. In a single nation case, it is possible with current technologies to construct the network, made of self-managed nodes, but there is no commonly agreed technology in place today, supporting management of a multi-domain network, where constitutive elements are based on different technology. To illustrate the situation in an even more realistic way, it should be stressed that nations are usually deploying not a single national network, but a number of networks to support different services (Army, Navy, Air Force), different functional areas (intelligence, logistic, command and control), and different classification domains. Therefore co-ordinated network management doesn’t look very much realistic. “One analysis of CENTCOM operations in Afghanistan and Iraq that year noted that American planners were dealing with more than 84 different coalition networks. … Needless to say, interoperability between this wide variety of networks was extremely variable, and mostly non-existent. As such, information exchange between members of the coalition was often a sluggish affair” (Mitchell, 2006, p. 54).

Inconsistency in national network management solutions could be illustrated by the following example. Informational advantage primarily is facilitated by sharing real-time information among the members of the coalition (Alberts, Papp ed., 2001:258), which in turn can contribute to the achievement of the desired military effects. However, without the coordinated network management, it would be hard to achieve the “identical real-time”, i.e. in the multinational environment, every national domain might have its own “current time”, not necessarily matching with the current time in other nation’s domain. These time differences could produce a vast impact on the quality of certain processes, such as tracking of an adversary’s fast-moving platform by one nation, then sharing track information and expecting the engagement of that platform by another nation.

## A2: SSA Deters Rogue States

### U.S. military poer ensures rising challengers

Gray 99- Colin S. Gray, author and professor of international relations and strategic studies at the University of Reading, *The Second Nuclear Age*  Chapter 1: To Confuse Ourselves: Nuclear Fallacies 1999

This fallacy has two important aspects. First, it misunderstands current conditions, and, second, it all but invites misunderstanding of some chaotically non-linear futures.34 At the level of general deterrence, US military power casts a shadow of global domain over the cunning plans of any and every wouldbe ‘rogue’—or regional ‘aggressor’—in the world. But each would-be regional revisionist polity has to interrogate its specific circumstances, and its understanding of American affairs, to inquire whether that general deterrence has any plausible, let alone probable, relevance to the adventure that it contemplates. Unfortunately for reliability of scholarship, if the general deterrence delivered by the US armed forces has practical effect in immediate deterrence, we are unlikely to know about it.When lines are not drawn in the sand, there are unlikely to be footprints for scholars to photograph.

It is a common failure of the strategic imagination to recognize how difficult it can be to deter those who are truly desperate, those who are overconfident, and those who are fatalistically resigned to submit to ‘History’s command’ or the ‘will of Allah’, and so forth, according to cultural predilection.

35 For most of the time the absence of conditions of acute crisis and war will not be (negative) evidence of the successful functioning of some mechanism for stable deterrence. The leading problems of evidence for scholars are that they cannot know how much dissuasive influence US military power produces for a general deterrence that discourages those would-be aggressors who rule out certain forms of challenge to a US-backed regional order; and they cannot know or discover whether or not a regional power declines to be heroic in face of immediate US deterrence, having first decided to be brave in face of

## A2: Space Key to Defense

### Space is not any more key to defense than any other terrain

Gray and Sheldon 99- DR. COLIN S. GRAY, author and professor of international relations and strategic studies at the University of Reading, and JOHN B. SHELDON, Marshall Institute Fellow, and a visiting professor at the School of Advanced Air and Space Studies, Air University , \*Space Power and the Revolution in Military Affairs A Glass Half Full? AIRPOWER JOURNAL FALL 1999

The technical-tactical challenges that limit the operational and strategic effect of a kind of military power—sea power, airpower, space power—eventually are overcome. This is not to say that geographical environments are created equal; they are not. The land matters most because that is where we live. Space is geographically unique and therefore is distinctive in its technological, tactical, and operational aspects. However, that uniqueness and distinctiveness are of the character of the difference between the sea and the air, between ships and aircraft. In short, it is not obvious that the space environment is technically or tactically any more different from the sea or the air than they are from each other. Space power, space warfare, and the geography of space are not beyond strategy. There is what one can call a “great tradition” of strategic thought that makes sense of military space behavior just as it does of military behavior in the other environments. From Sun Tzu and Thucydides, through Machiavelli, Clausewitz, and Jomini, to John Boyd and Edward Luttwak today, there is a great tradition of strategic speculation that achieves a universal and immortal relevance.20 Strategic theorists cannot help being the product of their time and place—their culture, if you will—but the theorists just cited have each discerned essential features about the nature, not merely the ever-ephemeral character, of war and strategy.

## Deterrence- No Solvency- SSA/= Deterrence

### The plan can’t overcome the inherent fog of war that will always exist- more information doesn’t necessarily translate into superior force

Gray 1- Weapons for Strategic Effect: How Important is Technology? by Colin S. Gray Fellow, Center for Strategy and Technology Air University, 2000-2001 Professor of International Politics and Strategic Studies, University of Reading, England

War is by no means a comprehensively nonlinear event. Criticism even of Admiral Owens for linearity of vision can be overdone. The chaotic possibilities in war are so ripe, the triggering events and players so unpredictable, that it is illusory to think the fog of war can be banished. New technologies, even when intelligently absorbed into a plausible RMA, are not likely to lessen the gamble inherent in war.

Even if we grant the fairly heroic assumption that 40,000 square miles of battlespace truly is transparent to us alone, 43 commanders and politicians still could find many creative ways to snatch strategic defeat from the jaws of what is predicted to be certain military victory. Information usually is useful, but it is not synonymous with power-meaning strategic success properly understood.

For example, in order to stand a chance of winning in Vietnam, USMACV had to be permitted to attempt to effect isolation of the relevant battlespace. This meant that General Westmoreland had to be licensed and armed to fight in the Laotian panhandle so as to close off North Vietnamese access to the South.44 It is not obvious that Admiral Owens’ RMA could have affected the appallingly incompetent decisions on high policy and strategy made by the Kennedy and Johnson Administrations.45 Or, consider the case of the escape of the British Expeditionary Force (BEF) from France and Belgium in May-June 1940. 2000’s-style dominant battlespace knowledge (DBK) would have eased some German anxieties in the last week of May, but would not have precluded fatal operational error. The Fuhrer “halt order” of 24-26 of May froze the panzer divisions in place just as they were about to pre-empt the BEF’s creation of a defensible perimeter around Dunkirk, the last remaining port of evacuation. That order did not stem principally from misinformation. The politically and strategically fatal halt order flowed rather from a combination of Hitler’s willingness to entrust the final destruction of the BEF to Goering’s Luftwaffe, and his, and much of the military high command’s, strong desire to preserve the scarce panzer assets for the impending battle for France.46

Although Hitler’s decision to halt his panzers from 24 to 26 May 1940 was no less erroneous than was the U.S. decision not to defend South Vietnam in Laos, it was a far more excusable mistake. No-one, the British included, expected virtually the whole of the BEF to escape from Dunkirk, Fuhrer Halte Befehl or not. How the United States could allow itself to fight a war wherein the principal enemy effectively was granted sanctuary beyond a long and rugged land frontier, is a mystery to this author. The point in deploying these two illustrations of error is simply to register the claim that the more modern belligerent (in these cases, Germany and the United States), enjoying many strategic advantages in military effectiveness, is capable of snatching defeat from a reasonable prospect for victory.47 That granted, the argument must not be taken too far. Yes, war is a gamble; it is the realm of chance that Clausewitz claimed. Similarly, he was powerfully persuasive when he expounded his theory of friction; the exploration of what it is that distinguishes “real war from war on paper.”48 Lost orders, heavy rains and mud, sick generals (and troops), solar disturbances - the list is endless of the reasons why “[a]ction in war is like movement in a resistant element.”49 However, friction impedes all belligerents and war is not only the realm of chance.

For a host of reasons, an army, air force, or navy, may have a bad day, but the “better” army, air force, and navy is going to succeed most of the time. Analogy with the NFL is compelling. On any given Sunday’’ any team can beat any other team, but the objectively better teams still win most of their games and make the playoffs.50 War is a gamble because there is a legion of interacting possibilities of disaster, great and small. It would be absurd, though, to argue that war is only a gamble: it is not. Armies that are well led, well trained, well equipped, and - no less important - well guided by policy, will be far more effective strategic instruments. Those deficient in some or all of these respects will not. Better technology should aid military effectiveness, which, in its turn, should improve strategic effectiveness. But even if we ignore the facts that new technology will bring new vulnerabilities as well as advantages, the killer cl8aim against the aspiration for technology to lift the fog of war lies in the scope of the problem. Even though this may be purchased at the near-term cost of less reliability and lower numbers, the strategic problem of effectiveness in war (and in deterrence also) is at least as much a matter of poor political and operational judgment, in the context of a unique enemy with an independent will, as it is of immature technology. Moreover, even when technological innovation is suitably integrated by an RMA, war remains an activity that does not get easier as history moves on.

### SSA can’t fully deter aggressors- they’ll always find a way to bypass tech. superiority

Gray 5- Colin S. Gray, author and professor of international relations and strategic studies at the University of Reading, Transformation and Strategic Surprise, US Army War College, 2005

The third context potentially of importance for strategic surprise is the technological. I will declare boldly, perhaps rashly, that technological surprise is not a likely strategic problem for the U.S. military. The depth, breadth, and consistency of the U.S. commitment to military technological excellence, backed up by a civilian sector technologically of the first rank, all but guarantee against the surprise emergence of a technological shortfall potentially lethal to national security. In fact, the news is even better than that. So many and various are the possible ways in joint warfare, so diverse and complex are today's tools of the military trade, that it would be highly implausible to anticipate strategic disaster for reason of a particular technological failing. That is the good news. The less good news is that the prudent focus for concern is not so much upon new technologies, but rather upon how other countries' or groups' ways of war might chose to employ them. Some American commentators, reasonably, but alas incorrectly, believe that, in its information-led RMA/transformation, the U.S. defense establishment is simply leading the way in the modem way in warfare.5 2 Given the global diffusion of information technology (IT), and given a presumed universal military meaning to common technological knowledge, it should follow that to know the American way is to know the future for all who aspire to master the state of the art in military affairs. Unfortunately, the world does not work like that. The reasons why it does not are both geopolitical and cultural. Geopolitically, America's rivals will pick and choose from the technological menu so as to privilege their unique strategic advantages and hopefully to compensate for their deficiencies. Also, it so happens that there is not and never has been a truly common "grammar" of war.5 3 Different belligerents will have their own views on how a basically common technology should be exploited. An outstanding recent collection of essays on the impact of local culture upon the consequences of the diffusion of technology and ideas offers these cautionary words among its findings: One of the central contributions of this volume is to alert practitioners to be cautious in their expectations that the spread of new military knowledge is easy or straightforward. It cannot be easily controlled, nor held back indefinitely. This is so for several key reasons. First, culture will continue to shape the development and diffusion of military knowledge, producing indigenous adaptations that will be difficult to predict. True emulation is rare, implying that others will probably not leverage the IT-RMA the same way as the United States.'

23

In a small gem of a book, Paul Hirst makes much the same point, only more broadly. He advises that "[w]ar is driven by ideas about how to use weapons and military systems almost as much as it is by technical and organizational changes themselves. Ideas are thus crucial . .. "

To summarize the argument of this section: technology does not pose a significant threat of strategic surprise; rather does the challenge lie in the unexpected uses that other strategic cultures may choose to make of it. Overall, such uses would constitute grave threats to U.S. national security only because of a geopolitical context characterized by notable rivalries. Technology and culture and the strategic surprises to which they might be crucial are strictly dependent variables. They depend upon the political context for their strategic meaning.

## Deterrence- Alt. Cause- Ground-Based

### Even if space assests are secured- attacks on gorund absed systems are a viable option

Ginter 7- Lieutenant Colonel Karl Ginter United States Army Dr. Clayton K. S. Chun Project Adviser Space Technology and Network Centric Warfare: a Strategic

Paradox, 30 MAR 2007

Ground segment attack or sabotage to disrupt space assets is an attractive option to lowtechnology or cash-strapped groups such as terrorists or transnational insurgents. Critical ground control facilities associated with U.S. space systems, both military and civilian, are targets to terrorist cells and foreign special operations forces. While military ground control facilities are located on DoD installations across the world to service the various satellite constellations, as well as provide redundancy for continuity of operations, they also have the added benefit of being operated and secured by military personnel. Commercial ground control facilities in the U.S. and overseas generally don’t have that luxury. Adversaries need only to glean information about which ground facilities are critical to the U.S.—especially those that offer non-redundant vulnerabilities—and where they are located. Unfortunately, many of these facilities are described in open-source reference materials.

Foreign commercial satellite providers present additional vulnerabilities in terms of their satellite ground control facilities and ground control redundancy. Leasing critical warfighting capabilities from a foreign source presents its own risks. Beside the risk of assured access and availability for U.S. forces, the DoD can not oversee what potential adversaries may have access to foreign commercial ground control facilities, nor are these facilities necessarily accorded the same level of physical security as U.S. satellite ground control facilities. Such vulnerabilities at these facilities render them susceptible to unauthorized monitoring or even sabotage of U.S. leased assets. Another inherent risk of using any advanced technology is that failures will occur, and when these failures occur at commercial or foreign ground control facilities, redundant paths for communications circuits and sufficient on-hand bench stock (e.g. spare parts) that maintain continuity of operations are paramount. If the communications architecture is not engineered to be sufficiently robust, allowing both equipment and path redundancy, then the U.S. increases its vulnerability to enemy actions. Not all foreign commercial satellite providers employ a sufficiently redundant ground control capability for continuity or reconstitution in the event of ground system or power failures.

## \*\*Miscalculation\*\*

## Miscalculation- Transparency=/Solve conflict

### Transparency fails- realism proves nations will bypass transparency for security interests

James 7- Marquardt, James J, assistant professor of politics at Lake Forest. College in Illinois, Transparency and Security Competition: Open Skies and America's Cold War Statecraft, 1948–1960. Journal of Cold War Studies, Volume 9, Number 1, Winter 2007, pp. 55-87 (Article)

Realist theory helps to ªll some serious gaps in our thinking about transparency and CBMs as a form of security cooperation. Realists see world politics as inherently conºict-ridden. They claim that the anarchic structure of the international system has a profound effect on state interactions.18 In the absence of a supranational authority that can enforce international rules and punish transgressions, states must rely on their own capabilities to ensure their survival. In this self-help world, states provide for their security through external balancing (the formation of alliances) and internal balancing (the buildup of military forces), or some combination. Because military forces can be used for aggressive as well as defensive purposes, states view each other with considerable fear and suspicion. They normally dismiss each other’s declarations of peaceful intent and focus instead on the ability of others to inºict serious harm. The mutual distrust spawned by this uncertainty exacerbates the security dilemma and sometimes leads to war.

Structural realists highlight the impediments to security cooperation under anarchy—impediments that have important implications for transparency and arms control.19 One such impediment is relative-gains considerations. States’ willingness to cooperate will be affected by their judgments about the likely distribution of gains from cooperation. Efforts to control weaponry are highly unlikely if one state expects that the limits will result in a negative shift in the balance, leaving it relatively worse off than its adversary.20 A second impediment is the concern states have about each other’s compli-ance with international agreements. That cheating is possible and, more importantly, may go undetected, limits the scope of cooperation to situations in which compliance can be easily and closely monitored and defection can be quickly identiªed. The problem with cooperation is that gains considerations and the transparency necessary for effective compliance with agreements work at cross-purposes. Each state seeks to maximize the amount of information it obtains about its potential adversaries and minimize the information it reveals about itself, placing the onus of transparency on its rivals. States’ willingness to open themselves to outside scrutiny rarely satisªes the compliance demands placed on them by others.

## Miscalculation- Transparency/=Solve Miscalc

### Transparency doesn’t build trust- realism means states will always remain cautious about intentions

James 7- Marquardt, James J, assistant professor of politics at Lake Forest. College in Illinois, Transparency and Security Competition: Open Skies and America's Cold War Statecraft, 1948–1960. Journal of Cold War Studies, Volume 9, Number 1, Winter 2007, pp. 55-87 (Article)

Moreover, because states in an anarchic world are wont to assume the worst about each other’s intentions, they must carefully take account of their rivals’ military forces. Hence, structural realists are skeptical about transparency CBMs as a worthwhile form of security cooperation.21 The exchange of information about military matters may help states safely navigate crisis situations and avoid war, but it does not change the fundamental assessments each makes of the external threat environment. Furthermore, even if states are interested in promoting transparency, they do so with an eye toward obtaining strategic advantages over their adversaries. But because other states fear that they will be taken advantage of in this way, they resist their rivals’ self-serving transparency initiatives. Structural realists therefore expect that transparency and CBMs, if agreed to at all, will permit only a very limited degree of outside scrutiny of military matters and will do little if anything to reduce tensions and build trust.Moreover, by producing “winners and losers” in the exchange of information, transparency has implications for the distribution of power.22 Consequently, institutionalized transparency is bound to be limited by states’ caution about the security implications of the disclosure of military information.

## Miscalculation- No Solvency- Culture

### Policymakers will inevitably miscalculate- we don’t fully undertand other countries intentions due to cultural limitations

Cimbala 99- Stephen, Professor of Political Science, Pennsylvania State University Nuclear Crisis Management and Information Warfare From Parameters, Summer 1999, pp. 117-28

The first requirement of successful crisis management is communications transparency. Transparency includes clear signaling and undistorted communications. Signaling refers to the requirement that each side must send its estimate of the situation to the other. It is not necessary for the two sides to have identical or even initially complementary interests. But a sufficient number of correctly sent and received signals are prerequisite to effective transfer of enemy goals and objectives from one side to the other. If signals are poorly sent or misunderstood, steps taken by the sender or receiver may lead to unintended consequences, including miscalculated escalation.

Communications transparency also includes high fidelity communication between adversaries, and within the respective decisionmaking structures of each side. High fidelity communication in a crisis can be distorted by everything that might interfere physically, mechanically, or behaviorally with accurate transmission. Electromagnetic pulses that disrupt communication circuitry or physical destruction of communication networks are obvious examples of impediments to high fidelity communication. Cultural differences that prevent accurate understanding of shared meanings between states can confound deterrence as practiced according to one side's theory. As Keith B. Payne notes, with regard to the potential for deterrence failure in the post-Cold War period:

Unfortunately, our expectations of opponents' behavior frequently are unmet, not because our opponents necessarily are irrational but because we do not understand them--their individual values, goals, determination, and commitments--in the context of the engagement, and therefore we are surprised when their "unreasonable" behavior differs from our expectations.[18]

## Miscalculation- Turn- More Information

### Increased information disrupts communication channels- ensures miscalc.

Cimbala 99- Stephen, Professor of Political Science, Pennsylvania State University Nuclear Crisis Management and Information Warfare From Parameters, Summer 1999, pp. 117-28

Information warfare has the potential to attack or to disrupt successful crisis management on each of the preceding attributes. First, information warfare can muddy the signals being sent from one side to the other in a crisis. This can be done deliberately or inadvertently. Suppose one side plants a virus or worm in the other's communications networks.[24] The virus or worm becomes activated during the crisis and destroys or alters information. The missing or altered information may make it more difficult for the cyber-victim to arrange a military attack. But destroyed or altered information may mislead either side into thinking that its signal has been correctly interpreted when it has not. Thus, side A may intend to signal "resolve" instead of "yield" to its opponent on a particular issue. Side B, misperceiving a "yield" message, may decide to continue its aggression, meeting unexpected resistance and causing a much more dangerous situation to develop.

Infowar can also destroy or disrupt communication channels necessary for successful crisis management. One way infowar can do this is to disrupt communication links between policymakers and military commanders during a period of high threat and severe time pressure. Two kinds of unanticipated problems, from the standpoint of civil-military relations, are possible under these conditions. First, political leaders may have predelegated limited authority for nuclear release or launch under restrictive conditions: only when these few conditions obtain, according to the protocols of predelegation, would military commanders be authorized to employ nuclear weapons distributed within their command. Clogged, destroyed, or disrupted communications could prevent top leaders from knowing that military commanders perceived a situation to be far more desperate, and thus permissive of nuclear initiative, than it really was. For example, during the Cold War, disrupted communications between the US National Command Authority and ballistic missile submarines, once the latter came under attack, could have resulted in a joint decision by submarine officers and crew to launch in the absence of contrary instructions.

### More information increases time pressure- policymakers will be forced to act

Cimbala 99- Stephen, Professor of Political Science, Pennsylvania State University Nuclear Crisis Management and Information Warfare From Parameters, Summer 1999, pp. 117-28

Second, information warfare during a crisis will almost certainly increase the time pressure under which political leaders operate. It may do this literally, or it may affect the perceived time lines within which the policymaking process can make its decisions. Once either side sees parts of its command, control, and communications system being subverted by phony information or extraneous cyber-noise, its sense of panic at the possible loss of military options will be enormous. In the case of US Cold War nuclear war plans, for example, disruption of even portions of the strategic command, control, and communications system could have prevented competent execution of parts of the SIOP (the strategic nuclear war plan). The SIOP depended upon finely orchestrated time-on-target estimates and precise damage expectancies against various classes of targets. Partially misinformed or disinformed networks and communications centers would have led to redundant attacks against the same target sets and, quite possibly, unplanned attacks on friendly military or civilian installations.

### Information reduces routine problem solving- ensures misjudgement

Cimbala 99- Stephen, Professor of Political Science, Pennsylvania State University Nuclear Crisis Management and Information Warfare From Parameters, Summer 1999, pp. 117-28

A third potentially disruptive effect of infowar on nuclear crisis management is that infowar may reduce the search for available alternatives to the few and desperate. Policymakers searching for escapes from crisis denouements need flexible options and creative problem-solving. Victims of information warfare may have a diminished ability to solve problems routinely, let alone creatively, once information networks are filled with flotsam and jetsam. Questions to operators will be poorly posed, and responses (if available at all) will be driven toward the least common denominator of previously programmed standard operating procedures. Retaliatory systems that depend on launch-on-warning instead of survival after riding out an attack are especially vulnerable to reduced time cycles and restricted alternatives:

A well-designed warning system cannot save commanders from misjudging the situation under the constraints of time and information imposed by a posture of launch on warning. Such a posture truncates the decision process too early for iterative estimates to converge on reality. Rapid reaction is inherently unstable because it cuts short the learning time needed to match perception with reality.[25]

## Miscalculation- Turn- Causes Nuclear War

### Information and nuclear deterrence are a dangerous combination- provokes opponents

Cimbala 99- Stephen, Professor of Political Science, Pennsylvania State University Nuclear Crisis Management and Information Warfare From Parameters, Summer 1999, pp. 117-28

The possible combination of information warfare with continuing nuclear deterrence after the Cold War could have unintended by-products, and these may be dangerous for stability. Optimistic expectations about the use of information warfare

to defeat or disrupt opponents on the conventional, high-technology battlefield--in cases where nuclear complications do not figure--may be justified. On the other hand, where the nuclear specter overhangs the decisionmaking process between or among states in conflict, the infowarriors' efforts to obtain dominant battlespace knowledge may provoke the opponent instead of deterring it. One cannot overstate the case that nuclear weapons even after the Cold War remain different in kind, not just in degree, from other forces. Thus interactions between nuclear forces and templates for superiority in battle must always be carefully controlled, and especially so in time of crisis.

## Miscalculation- SSA Isn’t Key

### Increased intelligence doesn’t mean better understanding

Gray 6- Colin S. Gray, Professor of International Politics and Strategic Studies at the University of Reading, England, Recognizing and Understanding Revolutionary Change in Warfare: the Sovereignty of Context February 2006 http://www.strategicstudiesinstitute.army.mil/pdffiles/pub640.pdf

Appreciation of war’s changing technological context is an essential intelligence function, as well as a vital source of inspiration for domestic change. But a common material context across societies does not equate necessarily to a common understanding of the scale, or character, of the change that may be on offer. Recent studies have supported strongly what some of us have long believed or suspected. Different public, strategic, and military cultures, given their unique strategic contexts, exploit, and pick and choose among new technologies according to their own criteria of utility, not in obedience to some presumed universal military logic. If we consider the mechanization RMA(s) of the period 1930-45, for example, it is clear beyond a shadow of a doubt that notwithstanding a tolerably common technological base, each of the principal combatants in World War II developed air and mechanized ground forces along nationally distinctive lines, for reasons that appeared to make sense for each polity’s strategic and military situation.55 There should be little need to highlight the significance of this argument for the mission of our monograph. Many, and probably most, military technologies lend themselves to varied employment, depending on the local military tasks and strategic context and the preferences in operational concepts and organization. Identifying technological trends, no matter how accurately, is no guarantee of a grasp of their meaning. One could make much the same point by observing that superb overhead reconnaissance will provide formidable detail on people and their movement. Unfortunately, that intelligence can tell one nothing at all about what is in their hearts and minds.

## Miscalculation- Turn- Tech Reliance

### Increase information technology causes miscalculation- tech reliance

Gray 6- Colin S. Gray, Professor of International Politics and Strategic Studies at the University of Reading, England, Recognizing and Understanding Revolutionary Change in Warfare: the Sovereignty of Context February 2006 http://www.strategicstudiesinstitute.army.mil/pdffiles/pub640.pdf

Paradoxically, the more firmly an RMA leader, such as the United States with information technology, becomes wedded to a distinctive and arguably revolutionary paradigm of future warfare, the more likely is it to misread the character of military change abroad. It is difficult for a proud and self-confidently dominant military power to accept the notion that there can be more than one contemporary military enlightenment.56 The strategic sin of ethnocentricity is readily revealed. First, other military cultures may not agree with the dominant power’s military logic. Second, those other cultures, even if they appreciate the sense in the RMA leader’s choices, will be bound to make their own decisions on investment in innovation, based upon such local circumstances as distinctive military tasking, affordability, and the need to offset the RMA leader’s putative advantages.57

As the Parthian shot in this discussion, it is worth noting that, despite the contrary claims and implications of dozens of television series, the technological dimension to warfare is very rarely decisive. War is complex and so is its conduct in warfare. Just as its outbreak typically is the product of redundant causation, so its course and outcome, no less typically, is hardly ever plausibly, let alone unarguably, attributable to a technological advantage. It is easy to see why this should be so. Given war’s complexity and the large number of dimensions that are always in play, of which the technological is only one, there are simply too many factors other than the technological which must influence events. This is a long familiar truth. For example, a recent study of Alexander the Great and his way of war concludes that although his army was “a wellarmed force . . . not too much should be made of the technological edge it enjoyed over most of its enemies.”58 The author explains as follows: In the close-order combat of this period [4th century BC], the tactical prowess and morale of the forces was more important to the outcome of battles. Technology does not win wars. Even on those occasions when technology was clearly very significant, for example in the use of siege engines, breaches in the enemy’s defences still had to be exploited by Alexander’s men in face-to-face combat with the enemy. However good Alexander’s instrument was, this outstanding army still had to be led and handled effectively.59

## Miscalculation- Turn- Information Overload

### Increased information makes it impossible to discern good from bad information

Stanovich 8- LtCol Mark Stanovich, USMCR Emergency Readiness and Response Research Center Institute for Security Technology Studies Dartmouth College, “Network-Centric” Emergency Response: The Challenges of Training for a New Command and Control Paradigm” http://www.ists.dartmouth.edu/library/191.pdf

Theoretically, the NCW approach to information sharing should result in pertinent and timely information being provided to the “shooter” when and where he needs it. But experience has proven that when such a massive amount of data is accessible, it becomes nearly impossible to extract what is pertinent from what is peripheral6. The result is “information overload”, a cascade of data that exceeds the finite limits of information that can be processed and acted upon by a human being in a stressful and complex multi-tasking environment. What is new is the potential for inundating all participants with an ever-increasing flow of data masquerading as information because it has been slickly packaged within the common operating picture... …creating strong incentives for all to engage in information overload in an attempt to maintain their bearings in this overly ambitious big picture7. In essence, just as a military “shooter” still needs time to shoot, a responder still needs time to do his job. Such an overload of information prevents him from making timely and effective decisions. This is true for warfighter and emergency responder alike.

After-action feedback and Lessons Learned compiled from Iraq and Afghanistan highlight the problem of information overload and its effects upon operational and tactical command nodes in the conduct of operations. The After-Action Report from the 1st Marine Division in Operation Iraqi Freedom stated bluntly that: Intelligence sources at all levels were inundated with information and data that had little bearing on their mission and intelligence requirements… It seemed that all data, information, and products were being pushed through overburdened communications ports with little thought to who needed what and when they needed it… Too much time and bandwidth is wasted by employing the “information inundation” method.8

Similar observations and complaints from other units and services were common. The Center for Army Lessons Learned (CALL) noted that: At [higher echelons], without the ability to query, the operator had to search reams of information”, and that “Lower echelons can be quickly overwhelmed with information overflow”9.

CALL also remarked that in the theater of operations, intelligence analysis personnel were overloaded with information from all sources, and: …conducted only “minimal analysis” on valuable tactical information provided by Human Intelligence Teams because these personnel reported being so overwhelmed by input that they “don’t have enough time during the day to conduct an analysis”10.

The above observations are equally applicable to an Incident Commander or EOC Commander who is being bombarded with information of varying quality and usefulness in an attempt to gain situational awareness as his/her command responds to an incident or disaster.

### Increased information makes it harder for a commander to know the difference

Stanovich 8- LtCol Mark Stanovich, USMCR Emergency Readiness and Response Research Center Institute for Security Technology Studies Dartmouth College, “Network-Centric” Emergency Response: The Challenges of Training for a New Command and Control Paradigm” http://www.ists.dartmouth.edu/library/191.pdf

When every information source is treated as a collection asset of equal value, as Metcalfe’s Theory would imply, the distinction between evaluated and processed intelligence, and raw, unverifiable information is lost. The latter can often assume the character of rumor and gossip, making it even more difficult for a commander to discern the actual situation. In practice, Metcalfe’s Law has proven significantly overoptimistic regarding the contribution of nodes to the value of the network. 9 Center Network nodes of similar type and usage history flatten the value equation, and some nodes may actually reduce the overall value of the network because of the adding of undesirable elements. Thus, in a “network-centric” concept, all sources of information are not of equal value, and do not contribute equally to overall situational awareness. Some may actually serve to hinder the accuracy of perceptions and the gaining of situational awareness11.

This distraction created by peripheral and irrelevant information often has the effect of slowing the decision-making process, as commanders must process large amounts of obfuscating and sometimes contradictory information. There is a natural tendency in such circumstances to wait until additional, clarifying information is obtained before making a crucial and time-sensitive decision12. This “paralysis by analysis” is often made worse by the decision maker’s perception that a key item of information is sure to be included in the next massive influx of data13.

## Miscalculation- Turn- Decision Making

### Information technology in command structures decreased disaster management

Stanovich 8- LtCol Mark Stanovich, USMCR Emergency Readiness and Response Research Center Institute for Security Technology Studies Dartmouth College, “Network-Centric” Emergency Response: The Challenges of Training for a New Command and Control Paradigm” http://www.ists.dartmouth.edu/library/191.pdf

The infusion of information technology into hierarchical organizations typically reduces the traditional asymmetries of information that define superiorsubordinate relationships.

Empirically, the “flattening” of command hierarchy regarding information availability and distribution may have some positive effects on overall situational awareness. However, a paradigm where all entities potentially have access to all available information can create situations that can be counterproductive to the command and control necessary for coordinated management of resources and response to an incident.

The Incident Command System was developed in the late 1970s as a way of organizing the fight against wildfires in CA that involved thousands of people from hundreds of diverse organizations. The ICS is a structured, intentionally heirarchical command and control model for response to natural and manmade incidents of all sizes and severity, including terrorist attacks14.

NIMS/ICS acknowledges that, in dealing with a complex and dangerous situation, centralized planning and direction is essential for controlling and coordinating efforts, while decentralized execution is necessary to implement the guidance and tasks in the context of local conditions. No single commander can control the detailed actions of such a large number of people and agencies15. The ICS is heavily beaurocratic, formalized and structured, reliant upon policies and plans, rules and instructions.16 But for all its beaurocracy, ICS is designed to allow subordinate organizations to adjust and adapt quickly and easily to deal with changing situations or unforeseen events and circumstances. The ICS retains the strengths (defined command relationships, efficiency, control) of a beaurocratic hierarchy, enabling preplanning in the more predictable aspects of disaster management, but permits the flexibility to foster and encourage a bias for action, and provides leeway for local improvisation to adapt to unforeseen and often volatile conditions17.

## Miscalculation- Turn- SSA

### Increased information changes the command and control structure- reduces the effectiveness of decision making

Stanovich 8- LtCol Mark Stanovich, USMCR Emergency Readiness and Response Research Center Institute for Security Technology Studies Dartmouth College, “Network-Centric” Emergency Response: The Challenges of Training for a New Command and Control Paradigm” http://www.ists.dartmouth.edu/library/191.pdf

The “flattening” of the hierarchical ICS command and control structure resulting from unregulated information infusion could erode the strengths of the Incident Command System’s beaurocratic organization, negating advantages that allow for commanders to leverage a wide range of expertise and experience to provide direction to the efforts of the responders.

The availability of such a plethora of near-real time information often creates the false impression among commanders that they have as solid and accurate a grasp of conditions and situational awareness as the local responders dealing with an incident at the scene. The result of such an illusion often leads a commander to be overcontrolling with his subordinates, imposing significant restrictions on the initiative of subordinate commanders18.

Instead of issuing guidance and allowing his subordinates to leverage their expertise to accomplish their tasks and adapt to changing conditions within that guidance, such a commander is prone to issue overly-detailed directives that are irrelevant or inappropriate for the rapidly-evolving local situation. The infamous Vietnam War parable of President Johnson personally communicating from the White House with Army small-unit leaders in the field while they were in contact with the enemy reminds us that simply because communications are possible, that does not mean they are always a good idea. Such a command and control situation in emergency response is sure to stifle initiative, and will greatly reduce the effectiveness of the efforts of subordinate agencies19.

### Situational awareness causes less unified responses

Stanovich 8- LtCol Mark Stanovich, USMCR Emergency Readiness and Response Research Center Institute for Security Technology Studies Dartmouth College, “Network-Centric” Emergency Response: The Challenges of Training for a New Command and Control Paradigm” http://www.ists.dartmouth.edu/library/191.pdf

An illusory impression of situational awareness can work to the opposite direction, as well. Subordinate commanders, viewing what they perceive as virtually the same information as higher-level commands are seeing, might come to radically different conclusions about courses of action. This can result in a lower-level entity ignoring guidance from higher commands. While ICS allows for and encourages improvisation and adaptation to handle changing situations and conditions, this adjusting must be done within the context of the overall guidance and objectives of the senior Emergency Operations Center (EOC) or Incident Command Center (ICC)20. If the lower entity’s interpretation of events is at odds with that of the higher command, then the risk is of “freelancing” by people acting on their own interpretation (and consequently ignoring the guidance from higher). “Freelancing” is generally defined as illegitimate improvisation that is not working toward the goals of senior Incident Commanders21. It is deviation from higher intent that is both unpredictable and unexpected, and such activity presents serious problems to a unified response effort. At its least damaging, freelancing results in a squandering of effort and resources best used differently, while at its worst, it may create dangers for those who are freelancing and for others involved in the response effort whose actions and safety will be impacted.

## Miscalculation- Turn- Decision Making

### Information causes miscalc - decision maker response

Alberts 96- Dr. David S. Alberts, Director, Directorate of Advanced Concepts, Technologies, and Information Strategies (Actis) National Defense University, Ndu Press Book, The Unintended Consequences of Information Age Technologies, April 1996, http://www.dodccrp.org/events/12th\_ICCRTS/CD/library/html/pdf/Alberts\_Unintended.pdf

The linkages between information quality, distribution, communications patterns, and decision making are complex and diverse. A review of organization theory, group dynamics, information theory, and past research on command and control offers key insights into these linkages and how they function.

First, when information is freely available, role overlap tends to be commonplace. Superiors tend to micromanage, particularly when the stakes are high; there are no higher stakes than combat. Subordinates, however, when provided with the larger picture historically available only to senior commanders, are also likely to second guess decisions made at higher levels and (in richly connected systems) have the information required to undertake initiatives their superiors may find inappropriate. Avoiding this set of counterproductive behaviors and management practices requires doctrine, appropriate organizational structures, self-discipline, and training.

Second, decision making in an information rich environment increasingly means media attention. The pressures of a "fish bowl" environment affect performance in a variety of often adverse ways. Tendencies to overreact, to act quickly, to appear decisive despite limited information, or to "posture" for the media can only be overcome through realistic training and experience.

When decision making becomes a collective process, which tends to occur when several principals have easy access to one another in a situation they all consider important, decisions tend to converge on options that meet group consensus. This "collective wisdom" has been demonstrated in both theoretical and empirical analyses to tend strongly toward risk averse options or poorly thought out "group-think" alternatives. The "brilliant" alternative or innovative approach foreseen by one individual is unlikely to survive this deliberative process. The potential strength of this collective process, which has excelled at solving complex problems such as those at operational and strategic combat levels, can only be achieved by an open approach to command and control decision making and a doctrine that stresses individual innovation and leadership at all levels.

Fully-connected systems also reduce the need for detailed action coordination by commanders because they make available information that would have to be requested from other elements in a classic military information structure. For example, rather than having to request information about the availability of transportation assets or ammunition needed for a combat operation, a line commander will be able to check stock levels directly through the information grid. This can lead to insufficient or ineffective coordination because subject matter experts are not consulted or because more than one command makes plans to use the same asset but none has a clear commitment of asset availability. Industry experience with richly connected systems has shown that collaborative planning and decision aids (which automatically perform coordination tasks and/or pass information between nodes in decision-making structures) are needed to avoid these problems. In addition, "red team" procedures to cross-check decisions can help to ensure adequate, timely coordination.

As generations of military commanders who have become accustomed to the availability of high density and high quality data about the battlefield mature and move into senior command positions, the expectation of near perfect information and the willingness to delay decisions in the expectation of better information will grow. However, the very rapid pace of future battles, as well as the imperatives of turning inside adversary decision loops, will punish procrastination and inaction severely. The commander who waits for near perfect information will be defeated by one who acts on "good enough" information. Doctrine and effective training for commanders must instill the judgement required to differentiate between sufficient and necessary or desirable information.

## Miscalculation- Turn- Information Overload

### Information causes miscalc- gives differing images of the battlespace

Adams 1- Thomas K. Adams, national security consultant based in the Washington DC area. He is a veteran of thirty-four years military service, principally in intelligence and special operations at tactical, operational, and strategic levels from Vietnam to Bosnia, Future Warfare and the Decline of Human Decisionmaking, Parameters, Winter 2001-02, pp. 57-71. http://www.carlisle.army.mil/usawc/Parameters/Articles/01winter/adams.htm

The entry point for automated systems to join the military decisionmaking process is described in abstract form by the so-called "OODA" Loop: observe, orient, decide, and act.[21] For purposes of this discussion, the loop can be seen as beginning with "observation," and indeed there will be a great deal of observation connected with future military organizations.

An enormous amount of attention (and money) has been invested in observation in the form of new surveillance and reconnaissance technology. Development of these capabilities has become increasingly vital with the Army Chief of Staff's 1999 announcement that he plans to field units whose very survival is largely dependent on information collection and advanced information systems.[22] This meshes nicely with the TRADOC view of the future: "The use of multiple, inexpensive unmanned platforms with modular sensor and information-gathering devices provide for an almost unlimited ability to analyze the battlespace. These sensor platforms will be land-based (both mobile and stationary), airborne, and space-based."[23] As explained by Major General John Thomas, commander of the US Army Intelligence Center at Ft. Huachuca, Arizona, this kind of information saturation is essential. The Army's new lightly armored "medium brigades" will have intelligence and sensor assets equivalent to those of a full division. These new brigades are expected to survive by using these assets to avoid the enemy, using superior knowledge, terrain, and agility to remain out of enemy fields of fire. According to General Thomas, "Probably the largest and most exciting area is in robotics so that many of these sensors can be automatically emplaced and maybe even autonomously emplaced."[24]

But victory does not always go the commander with the best observation. It goes to the one that can best process observation into data, data into information, information into orders, and then orders into action. The process is continuous--the results of action are observed, starting the process all over again. The individual functions involved have been enshrined in military jargon as the OODA Loop mentioned above.[25] The notion of mastering this process, "getting inside the enemy's decision loop" (i.e. execute the OODA process more quickly than the enemy) is at the heart of the digital Army and the information warfare concept.

By 2025, speed-of-light engagement will be a common feature of military conflict. Future architectures envision a new array of ground- and space-based sensors, uninhabited combat aerial vehicles (UCAV), and missile defense technologies that will take advantage of directed energy weapons. Air, sea, land, and space forces will be both faster and more agile. Adversaries will take advantage of these characteristics to operate faster than a defender can observe the activity, orient himself, decide how to respond, and act on that decision. The attacker thus places himself "inside" the defender's OODA Loop, destroying an adversary's ability to conduct an active defense.[26]

To master the OODA Loop in this demanding environment, military leaders are pushing hard for the technology to obtain and process more information more rapidly. This push attempts to achieve the core capability of information dominance, "the ability to collect, control, exploit, and defend information while denying an adversary the ability to do the same."[27] From the perspective of an Army organized around automated information systems, the struggle to get inside the enemy decision loop is one of processing power, the ability to move through the loop ever more rapidly.

When improved sensors are coupled with extensive communications links and advanced data-processing, the result is an ever-increasing flow of detailed information. Unfortunately, the explosion of available information inevitably results in information overload and flawed decisionmaking. Human beings commonly deal with this by ignoring much of the inflow, thus negating the purpose of the information systems in the first place. Recent exercises reveal an alarming number of unread messages because of information overload. As the quantity of data rises, the difficulty of preparing and interpreting it for decisionmaking grows. Furthermore, more information, flowing more efficiently, can easily give the commander conflicting perspectives of the battlespace. Soon it becomes obvious that the slowest element in the process is the human decisionmaker. By reducing the human role, the entire system is enhanced.

Automated systems, using some form of artificial intelligence, may be the solution to this difficulty. As an Air Force document asserts: "Unmanned systems will capitalize on artificial intelligence technology gains to be able to assess operational and tactical situations and determine an appropriate course of action. The key to the success of command and control is information. Some of these systems will not only collect data but also have the ability to analyze data and provide recommendations to the commander."[28] Operationally, the difference between "providing" a recommendation and "acting" on a recommendation is merely a software tweak.

Automated systems can certainly reduce the pressure of information saturation and eliminate conflicts, but at a price. Essentially, they do so by creating a series of information "filters" that establish priorities and eliminate marginal data, reconcile the remaining information conflicts, and present a consensus picture of the situation. All of this is invisible to the ultimate consumer, out of his or her control and very likely not well understood. This means that the commander is receiving a picture of the battlefield that is designed to emphasize certain things while de-emphasizing others. Still other factors are omitted entirely.

## \*\*Solvency\*\*

## No Solvency- Data Collection

### Data collection and integration causes in consistent feedback

ISB 8- Intelligence Science Board, Report of the Joint Defense Science Board Intelligence Science Board Task Force on Integrating Sensor-Collected Intelligence, November 2008, Office of the Under Secretary of Defense for Acquisition, Technology, and Logistics

Integration benefits resulting in higher system sensitivity, faster response times, and greater persistence are only possible if multiple sensors, which are currently managed independently operated, are tasked in a coordinated manner. The task force found that, except for a few experimental and technology development programs, current Tactical and National tasking processes do not support the required level of coordination.

One fundamental limitation inhibiting coordination is the lack of collection plan exposure at every level in the collection planning process. If one cannot determine where sensors are and what their system and mission constraints are, one can not begin to determine the feasibility of an integrated collection plan.

Another fundamental limitation is inconsistent feedback on collection assignments and results. The study found that it is frequently the case that an intelligence customer is not able to determine if a request actually resulted in a tasking order, and that the order was executed. Providing transparent processes, facilitated by accessible data, provides the minimum capability to begin coordinating tasking for integration. The task force also found that, even if tasking information was exposed across stove-piped collection systems, the models and tools to allow operators to make informed decisions on logistica l feasibility, cost, expected benefit and desired geometry and timing for coordinated tasking do not exist operationally, and they have been demonstrated only partially in R&D activities. Multi-INT sensor models, anisotropic target models, timely accessible collection meta-data from prior collects, and collection value models, and the analysis tools that use them are needed for operators to develop target-aware multi-INT collection plans across information needs. The required target and sensor models and analysis tools overlap the technology base needed to exploit the resulting collected data.

Sensors are tasked to satisfy collection requirements without passing on the original context of the information requirement that generated the tasking; however, context is needed by collection managers to prioritize and synchronize multiple sensors for a given problem. As a result, too often sensor integration occurs only when multiple sensors have coincidentally (accidentally) collected complementary data, and the results of that collection were serendipitously discovered to provide a benefit.

## No Solvency- Interoperability

### Information gaps between allies cause less intropability in times of war

Litvaitis 8- Arturas Litvaitis, graduate of the Joint Command and General Staff Course 2007/2008 of the Baltic Defence College, Challenges of Implementation of the Network Centric Warfare Tenets in Coalition Environment Baltic Security & Defence Review Volume 10, 2008

Another significant issue is that today, for multinational operations, the nations are deploying their communications systems which cannot be interconnected due to the use of different protocols, bandwidths and frequencies. Interoperability has been on the list of unresolved issues for a long time, even in those organizations which work hard on achieving interoperability among its members. NATO could serve as a typical example: “The performance of the European armed forces in NATO - or U.S.-led coalition operations, such as in Kosovo, Afghanistan and Iraq, demonstrated clearly the existence of a glaring transatlantic capability gap that has limited the interoperability of multinational forces and the efficiency of coalition war fighting” (Nolin, 2006). Despite the growing trend to build their networks in accordance with commonly agreed military standards, the nations continue to realize their specific national approaches even in those cases when the agreed standards (for instance, NATO STANAG’s) are taken as a basis. Quite a promising direction is the adoption of commercial standards in the military world (Commercial Off-the-Shelf, or COTS, solutions); however, within the industry we can notice a variety of proprietary features, on top of commercial standards, which make network solutions, delivered by different manufacturers, not interoperable, although those solutions are based on the same commercial standard. Lessons learned during multinational military communications and information systems interoperability exercises show that the United States and European nations are still quite away from the “plug and play” level of communications interoperability.

## No Solvency- Bandwidth

### Aff cant’t national network coordination- lack fo flexible networks

Litvaitis 8- Arturas Litvaitis, graduate of the Joint Command and General Staff Course 2007/2008 of the Baltic Defence College, Challenges of Implementation of the Network Centric Warfare Tenets in Coalition Environment Baltic Security & Defence Review Volume 10, 2008

Having the national networks deployed and getting them interconnected is not the end of the story – usually real operating environment demands the ability to flexibly reconfigure the network, provide increased bandwidth between particular nodes on the network or connect new nodes to the network. Multiple nations, operating in a relatively small area, have diverse requirements for the use of electromagnetic spectrum, necessary for operation of their sensors and wireless communications. This is all about the network management. Taking into account the growing bandwidth demand, it is most likely that opportunities, provided by rather rapidly evolving communications technologies, will be behind the user requirements. Therefore implementation of the net-centric concepts would require an efficient use of network resources, and this is the place, where network management will play its very important role.

Network management within national domains is quite a challenging issue (Donnelly, 2005). However, within the multinational environment, it requires even more effort. First of all, in the recent years, we cannot observe any significant improvement in defining multinational networks’ architecture. For instance, NATO Consultation, Command and Control Board and its sub-committees are working on NATO Information Infrastructure (NII), which is supposed to address the Alliance’s Network Enabled Capabilities architectural issues, but at present stage, it doesn’t seem that architectural developments are turning towards the real netcentric approach. On the contrary, we are still discussing the issue how backbone network, which is supposed to be provided by NATO, will be interconnected with national “appendixes”; therefore hierarchical network architecture is still in place (CNSSC, 2008). Continuing with this approach would not contribute to the construction of flexible and dynamic networks, where a network participant can communicate with any other wherever it is located and whatever nation it belongs to. How can we imagine communication in a hierarchical network between an airborne platform from nation A and a ground-based unit from nation B, when that platform was re-tasked on the spot to accomplish the mission in the airspace over a ground unit, if co-ordination didn’t take place between nations A and B in advance? These issues were already identified during real operations (Hayes, 2004).

## No Solvency- Network Management

### Network coordination is not a reality- means enahced ssa doesn’t get managed

Litvaitis 8- Arturas Litvaitis, graduate of the Joint Command and General Staff Course 2007/2008 of the Baltic Defence College, Challenges of Implementation of the Network Centric Warfare Tenets in Coalition Environment Baltic Security & Defence Review Volume 10, 2008

Similarly to networking solutions themselves, nations usually have their nation-specific approaches to the network management, consisting of a variety of methods, tools and technical solutions, because there is no multinational consensus how to manage multinational federation of networks, or, in case of the network-centric approach, the single network made of national “pieces”. This happens because we are still thinking in the hierarchical network architectural dimension.

Network, truly supporting net-centric approach, has no centre. In a single nation case, it is possible with current technologies to construct the network, made of self-managed nodes, but there is no commonly agreed technology in place today, supporting management of a multi-domain network, where constitutive elements are based on different technology. To illustrate the situation in an even more realistic way, it should be stressed that nations are usually deploying not a single national network, but a number of networks to support different services (Army, Navy, Air Force), different functional areas (intelligence, logistic, command and control), and different classification domains. Therefore co-ordinated network management doesn’t look very much realistic. “One analysis of CENTCOM operations in Afghanistan and Iraq that year noted that American planners were dealing with more than 84 different coalition networks. … Needless to say, interoperability between this wide variety of networks was extremely variable, and mostly non-existent. As such, information exchange between members of the coalition was often a sluggish affair” (Mitchell, 2006, p. 54).

Inconsistency in national network management solutions could be illustrated by the following example. Informational advantage primarily is facilitated by sharing real-time information among the members of the coalition (Alberts, Papp ed., 2001:258), which in turn can contribute to the achievement of the desired military effects. However, without the coordinated network management, it would be hard to achieve the “identical real-time”, i.e. in the multinational environment, every national domain might have its own “current time”, not necessarily matching with the current time in other nation’s domain. These time differences could produce a vast impact on the quality of certain processes, such as tracking of an adversary’s fast-moving platform by one nation, then sharing track information and expecting the engagement of that platform by another nation.

## No Solvency- Real Time Coordination

### Information decreases deterrence- no solvency mechanism for coordination and integration

Alberts 96- Dr. David S. Alberts, Director, Directorate of Advanced Concepts, Technologies, and Information Strategies (Actis) National Defense University, Ndu Press Book, The Unintended Consequences of Information Age Technologies April 1996 http://www.dodccrp.org/events/12th\_ICCRTS/CD/library/html/pdf/Alberts\_Unintended.pdf

As the global society enters the information age, military operations inevitably have been impacted and transformed. Satellite communications, video conferencing, battlefield facsimile machines, digital communications systems, personal computers, the Global Positioning System, and dozens of other transforming tools are already commonplace. Moreover, DoD has gone from being the driving force in information technology to being a specialty user with a new reliance on commercial-off-the-shelf (COTS) technology in order to acquire and field cost-effective systems. The widespread proliferation of this technology, as well as the increased reliance on COTS, has contributed to a significant increase in our vulnerablity.

The implications of warfare in the information arena are enormous. First, national homelands are not sanctuaries. They can be attacked directly, and potentially anonymously, by foreign powers, criminal organizations, or non-national actors such as ethnic groups, renegade corporations, or zealots of almost any persuasion. Traditional military weapons cannot be inter-posed between the information warfare threat and society.

Second, even where traditional combat conditions exist (hostile military forces face one another in a terrain-defined battlespace), kinetic weapons are only part of the arsenal available to the adversaries. Indeed, electronic espionage and sabotage, psychological warfare attacks delivered via mass media, digital deception, and hacker attacks on the adversaries' command and control systems will be used to neutralize most traditional forces and allow concentration of fire and decisive force at the crucial time and place in the battlespace.

However, warfare in this information age will require enormously complex planning and coordination, very near real time and total situation awareness, decision support systems that filter and fuse information very rapidly and perform simple plan extensions and revisions almost automatically, and massive database and information exchange capabilities to track both friendly and enemy situations as well as rehearse and forecast battlespace dynamics.

This rapidly evolving situation means that the U.S. military must be able to perform the following three fundamental information warfare missions: 1) protect its own information systems, 2) attack and influence the information systems of its adversaries, and 3) leverage U.S. information to gain decisive advantage in a battlespace where national security is threatened.