AD8320380

(2)

UNCLASSIFIED/LIMITED

DEFENSE TECHNICAL INFORMATION CENTER

UNCLASSIFIED/LIMITED

DEFENSE INFORMATION SYSTEMS AGENCY
DEFENSE TECHNICAL INFORMATION CENTER
8725 JOHN J. KINGMAN ROAD, SUITE 0944
FORT BELVOIR, VIRGINIA 22060-6218

Policy on the Redistribution of DTIC-Supplied Information

As a condition for obtaining DTIC services, all information received from DTIC that is not clearly marked for public release will be used only to bid or perform work under a U.S. Government contract or grant or for purposes specifically authorized by the U.S. Government agency that is sponsoring access. Further, the information will not be published for profit or in any manner offered for sale.

Non-compliance may result in termination of access and a requirement to return all information obtained from DTIC.

NOTICE

We are pleased to supply this document in response to your request.

The acquisition of technical reports, notes, memorandums, etc. is an active, ongoing program at the **Defense Technical Information Center (DTIC)** that depends, in part, on the efforts and interest of users and contributors.

Therefore, if you know of the existence of any significant reports, etc., that are not in the **DTIC** collection, we would appreciate receiving copies or information related to their sources and availability.

The appropriate regulations are Department of Defense Directive 3200.12, DoD Scientific and Technical Information Program, Department of Defense Directive 5230.24, Distribution Statements on Technical Documents, National Information Standards Organization (NISO) Standard Z39.18-1995, Scientific and Technical Reports - Elements, Organization and Design, Department of Defense 5200.1-R, Information Security Program Regulation.

Our **Acquisitions Branch, DTIC-OCA** will assist in resolving any questions you may have concerning documents to be submitted. Telephone numbers for the office are **(703)767-8040** or **DSN427-8040**. The **Reference and Retrieval Service Branch, DTIC-BRR**, will assist in document identification, ordering and related questions. Telephone numbers for the office are **(703)767-8274** or **DSN424-8274**

DO NOT RETURN THIS DOCUMENT TO DTIC

EACH ACTIVITY IS RESPONSIBLE FOR DESTRUCTION OF THIS DOCUMENT ACCORDING TO APPLICABLE REGULATIONS.

Information Warfare Strategies Seminar I

The Uses of IW Against the US in Wartime

Prepared By The
Strategic Assessment Center
Science Applications International Corporation
September 1998

Prepared for
Contract No. DASW01-95-D-0060 - 19
SAIC Project No. 01-1175-04-7301-002

Strategic Assessment Center
Science Applications International Corporation
Harbour Centre, 2 Eaton Street Suite 506
Hampton, VA 23669

Executive Summary

The OSD/NA sponsored Information Warfare Workshop "The Uses of IW Against the US in Wartime," was held 25-26 June, 1998, and conducted in Hampton, Virginia by the Strategic Assessment Center of SAIC.

The workshop explored the uses of information warfare (IW) against the United States and its allies during wartime. Scenarios were generated by three groups of seminar participants using a red-team approach, and gathered observations and insights about how information warfare might be employed by potential future competitors.

The workshop was conducted by means of three teams, each role-playing a different prospective Red force in the 2020 time-frame. The groups were directed to create two to three information warfare strategies for use against the United States in wartime. To provide background and context, the teams were provided a scenario which described the political, economic, and military events leading to war with the United States. The three scenarios stood alone and were independent of one another. Each Red team was expected to face the full weight of US military resources. To measure this weight, an "intelligence estimate" of the US, 2020 Order of Battle was provided. The workshop had the following characteristics:

- The first red team role-played a near-peer (China-like) competitor, the second team role-played a regional (Iranian-like) competitor, and the third team role-played a transnational/non-state (guerrilla/terrorist) competitor.
- Each team was asked to develop strategies with a focus on the question of why a competitor would use IW to achieve its objectives.
- Strategic issues were not emphasized. The planners were directed to use information warfare in direct support of their theater objectives.
- The teams were asked explicitly to think about the linkage between the "means" of information warfare and the "national ends" pursued by a prospective red force.

A number of issues were raised in the context of the workshop. These included the following:

- **Strategic Perception Management.** Each team focused heavily on creating an international climate conducive to their war aims, especially a policy of attacking US public opinion by creating an impression of "red force legitimacy" in the face of aggressive US actions.
- **Attack US Ability to Have Perfect Battlespace Awareness.** The ability to discriminate and analyze targets and to lessen the effects of fog and friction was seen as a critical, yet vulnerable aspect of US forces in the 2020 time frame.
- **Inflict Damage on High-Value Forces.** The ability to damage or destroy high-value US forces was critical to the campaign. Red challengers generally could not afford to wait for the US to bring its forces to bear in the region, and pursued an aggressive asymmetric area denial campaign.
- **The Limits of Information Warfare.** Even though each red team was directed (by the NCAs) to consider use of IW outside the theater (including in CONUS) to further operational aims in theater, none did so in any significant and coordinated manner, primarily because:
  - no specific gain in theater was perceived.
  - the cost in the area of "Strategic Perception Management" (see above) was seen as excessive.

- IW strategies developed and the capabilities required to carry out a specific strategy are summarized below.

Non-State/Transnational Competitor

I. **IW Logistics Disruption.** Focus on denying the US the ability to sustain its forces already deployed to Venezuela and Columbia, and to delay the deployment of additional forces.

Capabilities

-The ability to use and integrate information technology.

-Significant and timely intelligence capabilities to acquire information on the US logistics infrastructure.

II. **Attack the Individual Soldier.** Attempt to degrade the effectiveness of US forces in the region at the level of the individual soldier.

Capabilities

-Knowledge of US communications systems and their vulnerabilities.

-Ability to scan for and jam electronic communications.

-Ability to use the internet, direct mailing, and research capabilities.

-Computer communications and processing power.

III. **Expand Time and Create Uncertainty.** Strategy directed at the perception that the US must win wars quickly and cleanly, as well as its ability to achieve "topsight" and dominant battlespace awareness.

Capabilities

-Integrating computer network attack and internet psyops at the lowest possible level.

-Use information technology to increase the effectiveness of the guerilla soldier.

Regional Competitor

I. **Islamic Arabian Confederation-Directed Psyops.** Effort to influence opinion within Islamic states against the introduction of US and Western forces to the region.

Capabilities

-Command and Control and operational security.

-Ability to integrate and utilize cultural and academic knowledge.

-Establishment and development of an "Islamic" news network throughout the Middle-East and North Africa.

II. **ISR Overload.** Attempt to spoof, confuse, and otherwise degrade the ISR systems of the US military.

Capabilities

-Generation of ballistic missile IR plumes, false radar signatures, and transporter/erector/launcher sets.

-False SAM sites and radar signatures.

-False mine/submarine targets.

-Submarine-launched SAMs.

-Parallel communications systems with false SIGINT traffic.

-Ability to corrupt navigation and combat ID systems

III. **EMP Pearl Harbor.** Attempt to inflict damage on high-value US forces by extensive use of advanced EMP/RF weaponry.

Capabilities

-Large numbers of small, man-portable EMP devices.

-Ability to command and control simultaneous attacks throughout the theater.

-Possible use of nuclear EMP detonation in space.

Near-Peer Competitor

I. Global Psyops. Focus on perception management/psychological operations side of Information warfare.

Capabilities

-Ability to engage in and defend against computer network attack.

-Internet broadcasting and "direct advertising" to servicemen and their families.

II. Theater Deception. Attempt to erode the effectiveness of US information systems, which are seen as a center of gravity for future US forces.

Capabilities

-Use of special operations "pirates" in the South China Sea.

-EMP/RF devices on islands and fishing vessels.

Introduction

This seminar, sponsored by the Office of the Secretary of Defense, Office of Net Assessment, is part of its ongoing investigation of the Revolution in Military Affairs (RMA). This seminar was conducted by the Hampton, VA, office of the Strategic Assessment Center of Science Applications International Corporation, and explored the uses of information warfare (IW) against the United States and its allies during wartime. The specific objective of this workshop was to construct a set of plausible strategies (in the form of scenario outlines) for the use of IW against the United States in wartime. Scenarios generated by three groups of seminar participants using a red-team approach garnered further insights about how information warfare might be employed by potential future competitors.

Seminar Objectives

The workshop was conducted by means of three teams, each role-playing a different prospective Red force in the 2020 time frame. The groups were directed to create two to three information warfare strategies for use against the United States in wartime. To provide background and context, the teams were provided a scenario that described the political, economic, and military events leading to war with the United States. The three scenarios were independent of one another. Each Red team was expected to face the full weight of US military resources. To measure this weight, an "intelligence estimate" of the US, 2020 Order of Battle was provided.

A set of research questions and group worksheets were designed to highlight explicit linkages between the "means" of information warfare with the national "ends" as described by the notional political-military command authority. Players were directed to focus their strategies at the operational, rather that strategic-NCA level. Information operations directed at CONUS or any other strategic targets were to be justified in terms of their immediate relevance to the conduct of the war within the theater of operations. In addition, the scenario-building process served to highlight concepts and trends that affect information operations and might merit further analysis.

Seminar Design

Players and Materials

Players were drawn from across US Atlantic Command, operational and staff organizations, other military and government organizations, and private industry. The participants played the role of an Information Warfare Command staff and were tasked to address the operational, rather than strategic-political dimensions of information warfare.

Blue force lists and full text of the scenarios for each group are included in the Read-Ahead package appended to this report (Tabs D through G). Red force lists were intentionally withheld from players to stimulate discussion as to the types of capabilities and force structures that a US competitor would be required to develop from the present to 2020 in order to support a specific IW strategy.

Research Questions

Workshop participants were asked the following questions:

Develop scenarios with an emphasis on the "why" question:

- Why would a U.S. adversary attack a particular IW target with particular IW assets?

Objectives for this seminar include:

- Further exploration of the implications and role of information operations in warfare.
- What objectives might an adversary pursue with information warfare? Why?
- How might an adversary pursue national objectives with information warfare?
- What capabilities would an adversary need to pursue those objectives?
- Identify U.S. targets which are exploitable (or perceived as exploitable) by means of information warfare.
- Identify U.S. targets that might NOT be attacked because of...
  - Impact on own economy.
  - Effect on "neutral" economies.
  - Impact on own ISR
  - Reluctance to escalate conflict.
  - Impact on "world opinion."
- Identify red targets/capability which may need protection from US attacks.

Scenarios

The three scenarios provided had several factors in common:

- A plausible 'story" to take players from the present to a 2020 conflict with the United States.
- Red NCA recognition that force-on-force conflict with the United States was not a viable option.

- Red perceptions that a cleverly designed and quickly executed Information Warfare attack could achieve operational objectives in the short term.

- A primary objective to force US "on station" forces away from red sovereign territory and to prevent resupply/reinforcement.

Scenario 1

The scenario for the first group involved a near-peer (Chinese) competitor to the United States in East Asia. In the scenario, twenty years of dismal economic performance and political unrest in Indonesia contributed to the slow, but accelerating implosion of that country. Attacks on ethnic Chinese in Indonesia and Malaysia, an increase in piracy and lawlessness in the South China Sea, and the need to secure access to oil resources for its growing economy contributed to an increasingly aggressive Chinese presence in the region. Hostilities with the United States were caused by a Chinese declaration of sovereignty over the South China Sea, as well as simultaneous air and seaborne assaults on Malaysia, Indonesia's Natuna island, and the Sultanate of Brunei under the pretext of a NEO, the protection of its nationals, and the need to reestablish order throughout Southeast Asia.

Scenario 2

The scenario for the second group involved a regional competitor in the Middle East. The implosion and partition of Iraq in the last years of the 20th century led to the growth of an Iranian-directed, militant-Islamic state astride the region. Incorporating Iran, parts of Iraq and Syria, Turkmenistan, and allied with Yemen, this state directed its attention to securing the withdrawal of American influence in the Gulf States, and establishing itself as the legitimate hegemon in the region. The New Islamic Republic (NIR) began offensive operations against the Gulf States to secure their acquiescence to its national security and oil production objectives.

Scenario 3

The scenario for the third group was concerned with the Bolivistes, a guerrilla/drug trafficking group in South America and Mexico. Economic collapse, poverty, and drug corruption conspired to erode the traditional interstate and state-government structures there. The US, increasingly dependent on Venezuelan and Colombian oil, was concerned with growing connections between drug producers and nationalist/socialist rebels there. In the midst of the collapse of friendly governments in South and Central America (including Mexico), US forces were introduced into Mexico and the oil-producing regions of Venezuela and Columbia to restore order and limit the advance of the rebel movement.

IW Strategies Seminar Attendance List

First Name	Last Name	Organization	Position/Title
Tom	Baldwin	SAIC, SAC, Hampton	Moderator
Jeff	Becker	SAIC, SAC, Hampton	Rapporteur
Tom	Belote	JWAC	Mr.
Rich	Blanchfield	SAIC, SAC, McLean	Moderator
Bill	Brinkmann	USACOM J-28	Capt. USN
Mike	Brown	SAIC, SAC, McLean	Coordinator
Worth	Carter	USACOM JEXP3	Lt. Col. USAF
John	Davis	USACOM J-352C	Lt. Col. USA
Mike	Dziubinski	USACOM J-361	Lt. Col. USAF
Jim	Easterbrooks	USACOM JTASC	LCDR USN
Tammy	Furrow	SAIC, SAC, McLean	Rapporteur
Joe	Gugliotta	SAIC, SAC, McLean	Rapporteur
Mara	Hurwitt	JWFC Concepts Division	Ms.
Kevin	McCrohan	USACOM Joint Res. Unit	Mr.
Perry	Meador	JWFC Concepts Division	Mr.
Bob	Miller	USACOM JTASC	Maj. USAF
Chuck	Nicholson	USACOM J-362B	CDR USN
Barry	Slaughter	USACOM Joint Res. Unit	Mr.
Polly	Spahr	USACOM/NSA	Ms.
Frank	Stech	USACOM Joint Res. Unit	Col. USAR
Jim	Suhr	SAIC, SAC, Hampton	Moderator
Kevin	Van Sloten	USACOM JTASC	CDR USN
Harry	Waters	JWFC Concepts Division	Mr.
Andy	Wilde	JCS J-39	LCDR USN
Jeff	Workman	ACC/DIID	Lt. Col. USAF

Seminar Insights

Although the three teams approached the problem of conducting information warfare against the United States from different perspectives and with differing capabilities, all three red teams reached similar conclusions about the most promising methods.

Strategic Perception Management

First, each team focused heavily on creating an international climate conducive to their war aims. The ability to create an impression of "red force legitimacy" in the face of aggressive US actions, was a constant.

Attack US Ability to Have Perfect Battlespace Awareness

A second information warfare strategy elaborated by each group was an attempt to confuse, delay, and even mislead the US force by attacking its ability to collect, analyze, and understand information. Each team concluded that these ISR functions were a vulnerable aspect of US forces in the 2020 time frame. Teams chose to do this in at least two different ways.

- One team determined to *Stress the ISR System* through deception. In one instance, they built and dispatched hundreds of fake naval mines. Although the team realized the US Navy would be able to discriminate between real and fake mines, they believed that the shear number of "possible" mines would focus commanders' attention, that it would consume valuable time and that it would require the dedication of many different kinds of ISR resources to discriminate real from the fake mines.
- A second team decided to *Stress American forces' intelligence fusion capability.* Realizing that there was very little their side would be able to hide from the US ISR capabilities, they determined that they would make the analysis of that data particularly problematic. By moving forces all over the battlespace and they would make the task of intelligence officers more difficult.

The Limits of Information Warfare

The more advanced and larger the red-team, the less likely the team was to "go strategic" and attack space, and non-military computer systems. Each team weighed the US response to such attacks carefully. For example, the Chinese group never took the fight to space systems, while the Islamic force actively pursued the idea of nuclear detonations in space. The *Boliviste* group planned to attack satellite downlink stations in the United States. The China team did discuss attacking civilian systems in CONUS such as the Social Security payment computers.

Even though each red team was directed (by the NCAs) to consider use of IW outside the theater (including in CONUS) to further operational aims in theater, none did so in any significant and coordinated manner. There were several thought processes causing the rejection of CONUS attacks:

1. There was no linkage to theater objectives
2. There was a feeling that a short-term victory could be achieved in-theater, but

the longer-term reaction of an emotional US public was to be avoided.
3. There was concern about negative effects on red's limited ISR and communications capability.

For example, there were discussions about using Computer Network attack to disrupt the US banking system. The decision not to do so was supported by statements like:

> *Bolivistes*: Much of our strength is in our wealth that is laundered in the US financial system – it would hurt us more than the US.
> *China/NIR*: It would hurt us too, but more importantly, would hurt our friends, allies, and nations neutral in the conflict. Our limited theater objectives will not last long if the entire world is mobilized against us.

The consequence, then, is that each team was cautious about attacking "strategic" targets, either in CONUS or in space. Each team was focused on pursuing limited objectives in the theater of operations, and was concerned that strategic attacks on US assets would probably result in retaliation which would negate any possible advantages of doing so.

Information Warfare Strategies: Non-State/Transnational Competitor

National Command Objectives

The overall objective of the Boliviste campaign in the region is to keep the United States out of the conflict to the greatest extent possible, and to continue operations aimed at seizing control of the states in the region. Sub-objectives included; 1) Attacking US forces currently in the region, and denying their resupply or reinforcement, 2) Indefinitely controlling the flow of oil to the United States from the region, and 3) Denying the ability of US forces in the region the ability to see and understand Boliviste force dispositions or intentions.

Operational-Level Objectives

Operational-level objectives for this scenario included 1) Shaping a favorable international political environment to our overall war aims, 2) Denying the US the ability to influence the outcome of the insurgent's actions in this region. 3) Use of both conventional and IW resources to degrade and destroy assets essential to American power projection, 4) Protecting insurgent military, political and financial assets with information resources, and 5) Protecting Boliviste command, control, and communications resources from degradation or destruction.

Information warfare was to be used as a method to cripple US efforts within the area of insurgent operations, as well as vital resources and supporting infrastructure in CONUS, where prudent and in keeping with political guidance.

INFORMATION WARFARE STRATEGY I:
IW LOGISTICS DISRUPTION CAMPAIGN

Courses of Action

The first strategy by the non-state/transnational group focused on denying the US the ability to sustain its forces already deployed to Venezuela and Columbia, and to delay the deployment of additional forces. The Boliviste movement, as portrayed by the scenario, possessed large cash reserves, and was able to mobilize significant technical

resources in pursuit of their aims. Using a combination of cash bribery and the threat of violence, the Boliviste team attempted to render the civilian infrastructure unreliable and ineffective. Using positive and negative inducements, they attempted to bribe seamen, truck drivers, and rail operators in the region, and also attempted to do the same within the United States near likely staging areas. In this way, critical supplies could become "lost" or damaged. They also considered buying basing rights, ports, railroads, and other infrastructure and legally denying them to US forces. Of course, the US could still physically occupy such assets, but it might serve to slow the momentum of any deployment.

The logistics campaign did not attempt to stop every article of materiel from making it to US forces, which was probably not feasible anyway. Rather, the effort concentrated on denying 100% of one or more *critical* type of supply. The cessation of medical supplies, for example, could induce a serious degradation in US war-fighting abilities. Performance in the field might be affected if soldiers discovered that wounds that would be fairly easy to treat in normal times were now life threatening because of lack of supplies.

Guerrilla operations and sabotage campaigns would be focused on cargo terminals, transfer points and specific communications nodes. Targets might also include (depending on the level of security) highly-trained and hard-to-replace operators of logistics systems rather than, or in conjunction with, destruction of the physical infrastructure. Prior to the sabotage campaign, technical computer cadres would be charged with penetrating US computer networks, including routing software and systems, logistics and the TPFDD. While physical attacks on the system took place, penetrated systems would be attacked, by means of viruses and other methods of CNA. Systems, which could not be taken off-line, might have their real-world data corrupted to such an extent that the overall integrity of the system would be in question.

The team also thought it important to attempt to attack US airlift capabilities, by using, for example, shoulder-launched missiles near airbases, and by finding and

attacking any airlift support infrastructure in the region. The combination of simultaneous physical destruction and CNA might compound damage assessments and cause the US to lose track of large amounts of materiel.

In addition to shrinking the size of the logistics pipe, the campaign would attempt to increase demand for supplies through the pipe. Through physical attack, for instance, the Bolivistes would attempt to destroy any bulky or critical items that placed high demands on airlift. By computer Network Attack, , logistics systems could be corrupted with high-priority orders for unneeded items (cold-weather BDUs for example).

Costs/Benefits

The anti-logistics campaign focused on intelligently assessing US logistics needs and using precision-CNA and guerrilla operations to significantly decrease the performance of the system. Although it was hoped that "cascading failures" would be injected by such an operation, the red team took pains to emphasize that information operations would probably not be a silver bullet that would result in a US defeat. Red players thought that significant degradation of the system might be induced, but that red might not be able to locate, or have access to single points of failure.

Although in the scenario, the red force has extensive resources, it was thought that the US would probably spend even more and that by the 2020 time frame that the US would have significant defensive capabilities in this area. Red group members conceded that such attacks would probably be more harassing than decisive, and would be part of a wider overall campaign. The red team thought, however, that extended attrition of US forces and a long-drawn-out conflict that significantly drained its resources would be a useful adjunct and possibly cause the US to lose interest and withdraw from the region over time. The group emphasized the notion that IW resources deployed in this scenario would garner neither quick nor decisive results.

Capabilities Required

The first important capability that the movement would have to develop was the ability to use and integrate information technology. Significant amounts of money could buy the sophisticated technology and weaponry to carry out such tactics. However, the difficulty would lie more in the ability to train and maintain the expert computer operators needed to undertake the CNA portion of the strategy. The dearth of such workers in this highly paid sector of the US economy suggests that recruiting ideologically-motivated and technically proficient information warriors might be a serious bottleneck.

The Bolivistes would also need significant and timely intelligence capabilities to get information on the nature of the US logistics infrastructure.

INFORMATION WARFARE STRATEGY II: ATTACK THE INDIVIDUAL SOLDIER

Courses of Action

The second strategy explored by the transnational team focused on degrading the effectiveness of the individual US soldier. The team noted that such a conflict would be "labor-intensive," in terms of the types of resources that would be required to prosecute a guerilla-type conflict. Therefore, the ability to degrade the effectiveness of the individual soldier would significantly diminish the US ability to fight effectively. First, this strategy involved attacking the morale and motivation of US troops by taking psychological operations into the global information network, including through the internet and electronic mail.

The Bolivistes would set up a web-site in an electronically-open country and post listings of US force deployments and dispositions. Photographs of individual soldiers in-theater could also be posted to the site, with names, family members, addresses in the US, e-mail addresses, and other personal data also included, in online "dossiers." The operation could also include photographs and data about soldiers' family-members and homes in the United States. These photos could also be electronically manipulated to

increase the negative impact on soldiers. An electronic newsletter could be posted to the site, or even e-mailed to soldiers and families with information (both true and false) on individual US soldiers taken captive and killed in action. The ability to capture and use individual e-mail addresses and the use of "targeted marketing" in the information battle might have particularly devastating effects on the morale of US forces. The idea that guerilla forces were watching, reporting and targeting individuals with impunity, coupled with an "online demonstration" of the ability to target and kill a specific individual might have important effects throughout the theater.

The content of an electronic psyop campaign would employ many of the same themes that have been used in opposing US forces before. Red would declare:

- That they had no quarrel with US citizens, only the government that sent them there.
- Press information would be distributed, and press conferences with Boliviste officials would attempt to link the US government with drug trafficking and support of corrupt South American officials. These press conferences would also emphasize the insurgent's "respect for US ideals and people," but that by involving themselves in the region, US forces were bringing the conflict on themselves.
- Using CNN and other media outlets, the "objective" media and its search for "both sides of the story" could also increase the prospective legitimacy of the movement and to send messages to US soldiers that their cause was illegitimate and their leadership misguided.
- A "reverse body count" could be coupled with such a strategy to encourage the idea that the costs of US engagement in the region were higher than the benefits are worth.

Second, the strategy also focused on IW attacks against the electronics and communications of the individual soldier, especially against uncontrolled electronics, cell phones, satellite telephones such as the Iridium system, and lap top computers. Attempts would also be made to jam and spoof GPS signals. In this strategy, the Red team

concentrated its efforts on exploiting the extent to which US forces were dependent on vulnerable communications and navigation technologies, and whether the absence of these technologies would cause small-scale US efforts to "fail catastrophically," or to "fail gracefully." The variety of systems available to individual warfighters was seen as a significant force multiplier, and the ability to interdict and degrade them would serve to increase in insecurity and isolation of US force.

Costs/Benefits

The benefits of this strategy were decreased levels of US morale and a decreased will to fight generated by a psychological assault through information systems. The heavy reliance on communications, control, and navigation systems at the individual level might create vulnerabilities that could be exploited. The strategy aimed to induce militarily significant losses in soldier effectiveness, especially if such failures are not included in training and exercise events. The red team asserted that such a strategy, especially over the long term, could cause a loss of unit cohesion and trust of the chain of command.

Again, the non-state/transnational team emphasized the fact that information operations in this context would not be a silver bullet, but would become more effective the longer the conflict extends in time. IW psychological attacks on individual soldiers would be extremely intelligence-source intensive. The ability to mobilize resources on a scale necessary to significantly degrade the individual soldier might not be cost-effective given the likely amount of protection. Even over the long term, the benefits of such a strategy may be outweighed by the costs.

Such a campaign would also place a premium on the perceived legitimacy of red aims throughout the world. The red force would have to have significant breadth and depth of international support, and that its quarrel was not with the American people, but with its presence in the region. Red did not consider taking the physical war to US territory in a significant manner, instead, the focus was on attacking US popular opinion at the strategic level—this is how US enemies have been effective in the past.

Information operations against the individual soldier will not, however, provide quick results, although if sustained for a long period of time this strategy may serve to wear down US forces and result in a loss of political support for actions in the region.

Capabilities Required

Besides knowledge of the individual soldier, Red Forces recognized that the most important piece of information they needed was knowledge of US communications systems and their vulnerabilities. Heavy reliance on commercial communications, such as cell and satellite phones would place a premium on the ability to use scanner technology and actively attempt to jam them. In addition, local EMP bursts and other electronic warfare techniques were discussed in attempting to disable electronic systems such as individual computer systems.

The use of the internet and sophisticated direct-mailing with other web-research tools would require a large number of trained and motivated computer operators. Substantial investments in computer processing would be required. However, information warriors of the type described above need not be located in the same place, and may be highly dispersed throughout the world.

INFORMATION WARFARE STRATEGY III: EXPAND TIME AND CREATE UNCERTAINTY

Courses of Action

The third strategy outlined by the non-state/transnational team was directed at both the perception that US wars must decided quickly using overwhelming force, and the specific goal that the US be able to achieve "topsight" and dominant battlespace awareness. The strategy, labeled "expanding time and creating uncertainty," took low-intensity conflict to the information dimension. The US, as in the other scenarios, was materially superior at almost all levels of conflict. However, its forces had several centers of gravity that could be exploited particularly well by the non-state/transnational challenger. These centers included high casualties, a reliance on command and control

systems, sophisticated ISR resources, host nation support structures, basing rights, ports, railroads, lines of communications, and most important of all, time.

US forces could be effectively attacked using "traditional" guerilla means. At the tactical level, the Bolivistes would hit vulnerable US targets and run, hide, and refuse to battle materially superior American forces on its own terms. The focus of this strategy would be to deny the US any sense of gratification on the battlefield. The consensus among red team members was that time was their ally and that the US was generally impatient and could not put up with a long and draining guerilla conflict.

In addition to "expanding time" the team was interested in creating uncertainty about the aims and capabilities of the movement, exaggerating some capabilities, and downgrading important aspects of others. The ISR portion of the Boliviste strategy focused on overloading and blinding US information assets in the region. Group members thought it would be too difficult to directly attack US intelligence capabilities, but that an effective strategy would be to overload and confuse as many of these systems as possible. In addition, the team discussed the encryption of message traffic throughout the region on both critical and "dummy" traffic to further complicate US message gathering and processing assets.

An "online" worldwide hacker contest would be set up, with the Boliviste command offering substantial monetary rewards to those who disrupt or corrupt US military computer systems. The US would be put on an "IW defensive" and have to apply resources to monitor its systems. In addition, the contest could be widely publicized, and the significant "neutral" media stories on such an event possibly generated. Such a strategy may, again, slow the ISR and computer processing advantages on which the US military will come to rely.

Finally, the "creating uncertainty" strategy attempted to horizontally escalate the conflict to Mexico, and across the South American continent in order to dilute US resources. The red players hoped that further instability in the Mexican situation could

serve to relocate the focus of US operations to that region. Attacks on US military bases would attempt to affect the sewer systems, water supply, electricity, and other infrastructure. Such focused targeting of the military bases, and broad publicity of such a strategy, would show that the Bolivistes were not out to hurt American people, but rather their government's interference in the region.

Costs/Benefits

The Red team asserted that the Bolivistes, being a committed, ideological movement, would possibly be less effected than the US by efforts to influence morale, especially over the long term. The attempt to "expand time" plays against a perceived tendency to be unable to sustain military operations over a long period of time against a non-specific and asymmetric enemy. The red team, it was asserted, holds much of the initiative – the red team actively avoided attacking US strengths, and searched for weaknesses. Such a strategy would serve to frustrate the US and deny it a quick and overwhelming victory, a premise on which much of US doctrine and planning is based.

Red's main strength, in this scenario, was their large amounts of cash. Hacker contests and other types of information vandalism are very cheap, and have the potential to wreak havoc disproportionate to their cost. The Boliviste team discussed cost tradeoffs and military effectiveness, an example of this being the race between encryption and decryption technology. If the ability to encrypt communications outpaces decryption processing, heavy encryption (cheap) can tie up US processing and analysis technologies (expensive).

Force Requirements

Force requirements in this scenario are much the same as previous scenarios. Again, such a strategy is predicated on the ability to undertake physical guerilla operations, but this strategy seeks to integrate CNA, and internet psyops at the lowest possible level. The Boliviste would not only carry his grenade and AK-47 into battle, but also his laptop computer and GPS receiver. The increased capabilities that these

technologies give to standing military forces around the world can also contribute to the effectiveness of the guerrilla soldier as well.

Information Warfare Strategies: Regional Competitor

National Command Objectives

Guidance for the NIR team at the operational level included the following: 1) Shaping a favorable international political environment to NIR war aims, 2) Denying the US the ability to influence the outcome of NIR actions in this region, 3) Use of both conventional and IW resources to degrade and destroy assets essential to opposing NIR strategic objectives, 4) Protecting the NIR's military, political and economic assets from interdiction and destruction, and 5) Protecting the NIR's command, control, communications, and surveillance resources from degradation or destruction.

A second NCA objective in support of this effort was to defeat the United States in this region without allowing it to forge an international consensus and military coalition against NIR moves as against Iraq in 1990. The focus of the NIR effort was the isolation of the US from the international community, forcing it to act alone in support of the Gulf States.

Operational-Level Objectives

Information warfare was to be used as a method to achieve these objectives both inside and outside the theater. Attempts to cripple the American effort could be undertaken both within the Persian Gulf region as well as by attacking targets in CONUS including supporting infrastructure where prudent and in keeping with national command objectives.

The operational goal of New Islamic Republic forces in the region was to militarily intimidate the UAE, Qatar, Bahrain, Kuwait, Oman, and Saudi Arabia so that they would acquiesce to NIR political objectives in the region. Missions to support this goal included; 1) Attacking US forces currently in the region, and denying their resupply or reinforcement, 2) Protecting the sovereignty of 12 NM exclusion zones in the Persian Gulf and Arabian Sea 3) indefinitely controlling the flow of traffic through the Strait of

Hormuz, and 4) Denying US forces in the region the ability to see and understand our force dispositions or intentions.

INFORMATION WARFARE STRATEGY I: IAC PSYOPS

Courses of Action

In the first strategy, the NIR players undertook a significant theater perception management strategy in the early stages of the conflict. The focus of the perception management strategy concentrated heavily on influencing opinion within Islamic states. Failures of the Iraqi attempt at psychological operations in 1990-91 were noted and avoided. NIR players were interested in splitting the coalition by direct action against the regimes in the region, rather than by attacks on Israel, or on American citizens. The strategy was focused on two specific targets. Saudi Arabia was the first target, and as the host-nation for most US forces in the region, was seen as the vital center of gravity for coalition forces. Meanwhile, NIR players also concentrated their effort on splitting the weakest coalition member – Bahrain – to create the impression that momentum was on the side of NIR forces.

The first, and most important element in the perception management campaign as discussed by the NIR players was the development of the "Islamic CNN" and "independent" and "commercial" information channel, which gave the impression of an impartial, but NIR-oriented point of view. The development of an Islamic CNN, which would be in-place and functioning years before the start of the conflict, was critical. Some distance between such a media group and the NIR government would have to be maintained in order to maintain legitimacy. However, the media group (perhaps based in Tehran) would be more easily controlled by the NIR government than western media outlets, and "shaping" stories could be inserted into broadcasts before and during the conflict.

Although it was emphasized by the group leader that psychological operations should only be undertaken in areas which would have immediate positive impact in the theater of operations, the NIR players were convinced that a psychological operations

campaign directed at the "hearts and minds" of Arabs in the region would have immediate and significant effects on the battlefield. First, they emphasized that, in accordance with the scenario, the NIR would have a certain momentum and legitimacy that made historical Iraqi attempts at such an operation pale by comparison. This momentum would be translated into triumphalist rhetoric directed at the Gulf states asserting that "the Muslim world has stood up," and that Muslims themselves, rather than western forces, now had the ability to underwrite and manage stability in the region and act in a forceful manner on the world stage.

Careful attention was paid to the need to be viewed as responsible in the eyes of Muslim, as opposed to American or European populations. Although cultural differences between the Iranians and Arabs were noted, the gulf between them was viewed as narrower than that between Muslim and American/Western attitudes, and thus, highly exploitable by a sophisticated NIR psyops campaign. The psychological aspect of the campaign was specifically geared toward this Western/Arab perceptual gap.

Special forces were to be deployed prior to the crisis in the capital cities of Islamic Arabian Confederation states and Mecca/Medina in order to foment demonstrations, to sabotage military infrastructure, and attack or suppress national command authority structures in the region. In addition, NIR operatives might stage attacks on Arabs (and possibly Arab-Americans) and blame the attacks on US or Israeli forces.

Costs/Benefits

The primary benefit of the perception management strategy is that is very low risk, yet has the potential of seriously undermining the American war effort. Although the US has, and will have a communications and mass media infrastructure that far outstrips that of any possible Mid-East competitor, the cost of building such a system for the region would not be out of the range of a state like the NIR.

Capabilities Required

Several significant capabilities would have to be acquired by 2020 in order for such a strategy to be undertaken. First, C2 and operational security in special operations forces are a key ability that would have to be developed to plan and execute Psyop campaigns. The NIR would also have to be able to integrate and utilize cultural and academic knowledge of the many Iranian students in US over the years in service of the Psyops campaign. In addition, close physical and cultural proximity to the Gulf States would give NIR operatives a significant advantage vis-a-vis similar US psychological operations.

In addition to good cultural and political information, a more robust information architecture would be required. The NIR players thought that the development of a "Persian" or "Islamic" news network able to reach homes throughout the Middle East and North Africa would pay rich dividends in a crisis. Such a service, as well as other NIR-oriented programming could be distributed by direct broadcast throughout the region via a geosynchronous "Islamsat."

INFORMATION WARFARE STRATEGY II: ISR OVERLOAD

Courses of Action

The NIR team focused its second strategy on spoofing, confusing, and otherwise degrading the ISR systems of the US military. The team attempted to generate numerous signatures, some real, most false, in a variety of configurations mimicking ballistic, cruise, and anti-ship missiles, mines and submarines, as well as aircraft strike packages and SAM sites. The analysis, and fusion portions of US systems, were seen as susceptible to overload, and would be the weakest parts of the US military's ability to carry out warfare against a sophisticated enemy in the Middle East. The strategy focused on pre-war analysis of US military commander and NCA concerns and expectations about what such a conflict would look like, and work to actively amplify and exploit those concerns. Such a strategy could seek to create confusion and fog on the part of US commanders about the intentions of the NIR war effort and divert scarce US military resources away from the main effort.

The first, and potentially most attractive aspect of the counter-ISR strategy was the attempt to spoof and overwhelm ballistic missile sensors and defenses in the region. The NIR would develop the capability to generate false ballistic-missile IR plumes, radar signatures, and TEL vehicles. High-fidelity dummies and massive numbers of signatures, intermingled with the real thing could significantly tie up the sensor-fusion and analysis portions of the ISR chain. The benefits of such a strategy would be greater than simply allowing ordinance to reach the target. The true objectives of the NIR could be pursued while scarce analysis resources would be occupied with hunting down weapons peripheral to the main effort.

A second aspect of the ISR strategy involved the generation of large numbers of submarine and mine signatures in the Persian Gulf. Hundreds or thousands of mine targets could be placed throughout the region at the onset of hostilities. In addition, dozens of false submarine contacts would mask the operations of real diesel subs, both in the Gulf and in the Arabian Sea, significantly complicating naval operations in the region. Dummy targets would be seeded with the real thing, possibly allowing a submarine or mine to slip through US detection nets. Immediate results, in the form of US naval forces withdrawing from the Persian Gulf, were anticipated.

A third aspect of the ISR strategy focused on US fears of WMD use. Although the team discounted the actual use of chemical or biological weapons, fears of their use could serve to shift a US commander's focus from carrying out offensive operations, to protecting against such an attack. The team discussed releasing non-lethal amounts of chem/bio agents near ground-based sensors, or in the direction of UAV's. The team also discussed the utility of placing dead animals with obvious signs of chemical poisoning and traces of lethal agents in their bodies near US bases or other high-value US facilities.

The team also planned to generate massive amounts of false, dummy SIGINT traffic, laden with likely keywords to overload computer processing and analysis and slow the flow of time-sensitive data from sensors to users. Computer network and

communication nodes of no strategic value would appear and generate traffic in the run-up to hostilities, and would be heavily encrypted to further tie up computing resources.

The concept of ISR overload was extended to other systems and focused on creating uncertainty about any and all electronic systems the US was using. Aircraft navigation (TACAN and GPS) might be spoofed and jammed. Combat ID and IFF systems could be corrupted leading to a number of US friendly-fire casualties, either against its own or coalition forces which could be exploited in the psyops campaign. This strategy also included the desire to actually damage or destroy some key US assets. For example, a submarine SAM attack on an AWACS or JSTARS aircraft, or a torpedo/mine hit on a US ship.

Costs/Benefits

Such a strategy would create significant confusion and fog for US commanders, with little cost in terms of escalation.

Capabilities Required

The NIR would need to undertake a comprehensive strategy to classify and target US sensing and processing capabilities and develop specific countermeasures to overload them. A list of possible high-fidelity decoys includes

-The ability to generate Ballistic-Missile IR plumes, false radar signatures, and Transporter/Erector/Launcher sets.

-False SAM sites and radar signatures.

-False mine targets.

-False Submarine contacts.

-Submarine-launched SAMs

In addition, the NIR would need to develop many parallel communication systems and fill them with false SIGINT traffic. Many communications nodes and links should lie dormant until the conflict begins, and simultaneously appear heavily encrypted. To add to the confusion, the NIR should develop an electronic warfare capability and attempt to

corrupt navigation and combat ID systems. Again, the ability to induce doubt as to the reliability of these complex systems could induce caution in US force, cause them to slow their operational tempo, and allow red an opportunity to prevail.

INFORMATION WARFARE STRATEGY [redacted]: EMP PEARL HARBOR

Courses of Action

The third strategy for the NIR team focused on the ability to inflict substantial damage on high-value US forces. The strategy envisioned the extensive use of advanced EMP/RF weaponry to disable US sensor and computer systems, and using the window created by shock and surprise to damage one or more high-value targets in the theater. Ideally, this strategy would take place at a point in time before all US forces deployed to the region. EMP/RF weaponry could be smuggled into Saudi Arabia, or any other gulf state supporting US forces and deployed near its bases and command complexes. The EMP attack would take place throughout the theater simultaneously, and be coordinated with a simultaneous attack by cruise and ballistic missiles, groups of fighter aircraft converging on critical targets, and submarine-launched SAMS against AWACS/JSTARS/ABL. EMP/RF devices would also be deployed against warehouse and storage facilities for spare and replacement electronic equipment.

The team discussed employing EMP/RF weapons against US naval assets by low observable cruise missiles, UAVs, and on "civilian" fishing vessels. Large numbers of SSMs and decoys would be placed in and around the Strait of Hormuz, and would be fired in conjunction with Sub-SAMs against AWACS (see ISR overload above). The confusion caused by the simultaneous loss of electronic equipment and massive attack from the air might result in substantial damage, or even sinking, of high-value naval assets, or at least a fighting withdrawal from the gulf. The NIR players asserted that such a withdrawal would be a substantial victory for the NIR, and damaging or destroying a carrier even more so.

Costs/Benefits

The primary benefit to the EMP pearl harbor strategy is that it was the only way, other than through low-level terrorist-type actions, or wholesale recourse to weapons of mass destruction, that the red force can hope to inflict real damage on US military forces in the field. If done correctly, the shock and surprise of such a coordinated and overwhelming attack could overwhelm the ability to respond.

It was noted that the US would probably use EMP and RF weaponry in the campaign anyway, and thus, to get in the first shot against a force much more dependent on these vulnerable systems could result in significant advantages on the battlefield. On the other hand, there was no consensus on the efficacy of detonating an EMP nuclear weapon in space. The group agreed that it would result in significant damage to US communications and intelligence satellites overhead. However, the team was split as to the response that the US would take in such a situation.

Capabilities Required

The EMP/RF strategy required a substantial investment in the technology over the next twenty years. The physical size of an EMP device was discussed, and it was noted that the ability to develop small (manportable) weapons would enable the NIR to smuggle them across international boundaries before a crisis began. It was noted that operational security was extremely important to this type of operation. Shock and surprise would serve to multiply the effects and create a significant window of opportunity for NIR forces. The ability to coordinate simultaneous attacks throughout the theater of operations by activating tens or hundreds of EMP/RF weapons and launching ballistic and cruise missiles, aircraft, and submarines at a variety of targets, would require a highly effective method of command and control.

Finally, NIR players discussed attacking US satellite intelligence during the initial attack by means of a single nuclear detonation in space. Consensus could not be reached on this issue, but it was noted that the shock of such an attack would substantially multiply the effects of the general attack in-theater. A nuclear attack on space assets had

the advantage of significantly damaging the ability to assess the nature of the overall attack (albeit for a limited time). In addition, there would be no "mushroom cloud," nor American casualties that could be used to justify a nuclear response. The very invisibility to the world community in such an attack would limit the threat of retaliation. Despite these advantages, several NIR players were of the opinion that a nuclear attack on its satellites would guarantee a dramatic US response that would cancel any advantages of such an attack.

This group insisted that heavy damage to US high-profile, high-value forces early in the conflict was critical to winning the war. Psychological operations were useful, but nothing would create the impression of the US losing as much as if it were actually losing. Losses of this sort could push US forces away from the NIR heartland, and force them to fight at a distance.

Near-Peer Competitor: China

National Command Objectives

The players were directed to pursue two primary objectives: First, to project maritime power in Southeast Asia and, second, to prevent the United States from interfering with that power projection. The NCA guidance was such that the campaign should be tailored so as to limit collateral damage to long-term national objectives, such as continuing to increase economic and political development.

National command guidance for the China team included: 1) Shaping a favorable international political environment, 2) Denying the US the ability to influence the outcome of Chinese actions in this region. 3) Protecting Chinese military, political and economic assets, and 4) Protecting China's national and military command, control and communications systems from degradation or destruction.

Operational-Level Objectives

Information warfare was to be used as a method both inside and outside the theater to achieve these objectives. Planning was tasked to relate specific IW objectives to the NCA's campaign goals. Attempts to cripple the American effort could be undertaken both within the Southeast Asian region as well as supporting infrastructure in CONUS where deemed feasible and prudent.

The operational goal was to militarily intimidate and defeat Malaysia, the United States, and its regional allies and force them to acquiesce to Chinese political objectives. Missions to support this goal included: 1) Attacking US, Malay, Australian, and allied forces currently in the region and denying their resupply or reinforcement, 2) Protecting the sovereignty of newly declared exclusive economic zones, including the region surrounding occupied Natuna Island and 3) Indefinitely controlling the sea lanes of communication throughout the South China Sea, including the approaches to the Straits of Malacca, and 4) Use of both conventional and IW resources to degrade and destroy assets essential to opposing its war aims.

INFORMATION WARFARE STRATEGY I: GLOBAL PSYOPS

Courses of Action

The group was concerned with portraying China as a hegemon in Southeast Asia, as well as a source of economic and political stability in the region. The group focused principally on the perception management/psychological operations side of IW in the first strategy and chose not to engage the US military overtly but rather, to focus instead on surreptitious computer network attacks, image management, and justification for regional involvement. This strategy focused on nonlethal and covert ways to enhance the legitimacy of the Chinese presence in the region, and to forestall full scale conflict with the United States by creating the perception in the minds of United States citizens (targeted as a significant US center of gravity) that the costs of an adventure in the South China Sea would far outweigh any possible benefit of becoming engaged in the region.

Although hostilities had already begun in this scenario, the China players did not wish to appear aggressive or belligerent, but rather, as a source of stability and legitimate authority in the region. Information warfare resources were focused on shaping a favorable international political environment as well as denying the US the ability to influence Chinese actions in the region.

In this strategy, the Chinese players did not wish to risk (at least early in the conflict) using "conventional and IW resources to destroy and degrade assets," but rather, to degrade the political center of gravity for US forces. The players believed that the wholesale use of IW attacks against US targets was escalatory and counter-productive during the early stages of the conflict. Although such national command concerns were explicitly "above" the operational level, the team was very concerned about the interaction between levels of military action and the region and wider consequences for its interests around the world. The team, in its role as near-peer competitor, found itself in a very "American" predicament – how to aggressively engage in regional conflict, while insulating the conflict from taking a more global and uncontrolled character.

The first course of action considered discussed how to force the US to make cost/benefit decisions in China's favor. The China team focused on transmitting to the US public the idea that involvement in the conflict was more painful than any possible benefits of intervention. In order to do this, the group discussed focusing on the economic potential in the region for US companies and targeting the pro-Chinese business lobby in the US. It was posited that internal pressure in the US against military involvement in the region could be encouraged among business groups in the United States. Business leaders might be convinced that the costs to US corporations of Chinese military and political hegemony would be outweighed by potential economic benefits of a stsbilized region controlled by China.

The group also focused on computer network attack as a method of influencing US perceptions. In the 2020 time-period, software will still come off the shelf, with a portion probably being produced in Taiwan, now a Chinese possession. Computer viruses might be incorporated into the code in commercial off-the-shelf technology to act as "sleepers" to be "awakened" at some future date to instill uncertainty in critical systems. Systems included logistic and transportation systems and other infrastructure components that the US will rely upon to stand up its presence in the region. The ability to instill doubt in critical systems was discussed at length and the conclusion was reached that, even if such systems could be compromised on a small scale, the uncertainty caused by late or misdirected supplies would be an order of magnitude higher than the initial investment in time and resources. Even a small disruption in a critical system could force expensive solutions and complicate the deployment of American resources to the region.

Another focus of the PSYOP campaign was to target US aversion to high casualties. China group members discussed methods to generate and transmit images of body bags being unloaded, as well as other "casualty preparedness" logistics measures, or the "fact" that the military had ordered a very large number of body bags to be shipped to the region. The purpose of such images and reports was to elicit moderating behavior in congress and from the American population. It was hoped that significant reductions in the scope and extent o American war-aims could be generated from such an approach.

A final method of IW psyop the group discussed was an electronic/internet version of "Hanoi Hanna" or "Tokyo Rose." Through means of computer network attack, as well as internet broadcasting, Chinese IW forces would undertake to find the locations of service men and women and send greetings to them including pictures of their location via email. "Live" internet broadcasts, or photographs of ballistic missile attacks on American ships of facilities, real or computer-generated might create significant confusion in a wired society and military. In addition, e-mail messages might be sent to family back home, or, more consequentially, pictures of home and families in CONUS sent to servicemen, particularly those with critical deployment and warfighting jobs.

INFORMATION WARFARE STRATEGY II: THEATER DECEPTION

Courses of Action

In the second scenario, information operations were undertaken in a more overt manner and were aimed at eroding the capabilities of US information systems. The overall objective of information warfare attacks is to induce US forces to question the reliability of information systems to the point where they would shut them off. Players felt that because the US military is dependent on complex information systems, the ability to disable them would represent a considerable force multiplier. Players emphasized that only a small portion of systems need be damaged or corrupted in order to induce doubt. The group concluded that a corruption rate of 25 percent of all information was enough for US commanders to lose confidence in their computer systems and possibly shut them off.

Chinese special operations forces would use pirates covertly to foment uncertainty and disruption in the region. These forces were to be "plausibly deniable" by the Chinese government. The piracy "problem," would be encouraged (and possibly actively directed) by Chinese forces through funding and covert operations. The threat to shipping, commerce and general safety by this force would be highlighted in the media, and contrasted with US claims as the guarantor of security and stability in the South

China Sea. Finally, the PLA navy would "intervene" and apprehend pirate vessels, operations that would be broadcast across the region. The political/psychological aspects of this strategy were extremely important for preparing the battlefield and undoing the US commitment to the region. Again, the team consciously avoided mistakes the Iraqis made in the Gulf War, and wished to garner wider political support for their actions.

A final objective by the China team in this strategy was to create serious uncertainty as to the effectiveness of American forces in the region. This plan was directed not only at the US military, but also at countries in the region that would be counting on US support against Chinese moves. The group emphasized electronic warfare and EMP/RF weaponry as a means to this end. Small vessels or outlying islands could be fitted with a device that emits EMP/RF that "accidentally" render systems on unfriendly vessels unusable. Such a capability would, again, be employed under the guise of preventing pirates from safely navigating the South China Sea. The ability to selectively target commercial and military vessels in the South China Sea with such a device was discussed. Civilian systems, such as Teledesic, however, were specifically excluded from target lists -- once a satellite was targeted, it would be permanently damaged so that non-combatants, as well as one's own ability to use the system would also be affected. These types of unintended consequences and effects were at odds with the overall perception management strategy. Ultimately, the group decided that although the capabilities do not exist now, in the scenario timeline the ability to temporarily affect satellites might become a reality.