THE DEFENSE MONITOR

The Newsletter of the Center for Defense Information

DROWNING IN DOLLARS   *Straus Military Reform Project Force Structure Series*

$174 Billion Plus-Up Scuttles Navy Ship Acquisition

BY WINSLOW T. WHEELER, STRAUS MILITARY REFORM PROJECT DIRECTOR

IN EARLY 2001, THE PENTAGON anticipated an approximate budget of $900 billion for the Navy and Marines for the period 2001 to 2009.[1] Not counting $95 billion subsequently received for the wars in Iraq and Afghanistan, the Navy/Marine Corps "base" (non-war) budget was increased by $174 billion to $1.074 trillion. The data used for these calculations are displayed in the table on this page.

Did this additional $174 billion reverse a central trend that has plagued the Navy for decades? Did the extra $174 billion stem the receding tide of a shrinking fleet?[2]

The publicly available budget[3] and force structure data for the Navy for the post-World War II period are shown in the table to the right. As clearly shown, the Navy's fleet of active duty combat ships has sharply declined over time. Overall, the fleet is today as small as at any point in the post-World War II period. From a 1953 high of 835 combat ships, it persistently hovers in the 21st century at about 300.

The budget, however, shows a very different story. There have been ups and downs, but the overall trend is for it to increase in "real" dollars.[4] In recent years, the Navy's budget has increased sharply, mostly for expenses not related to the wars in Iraq and Afghanistan. Thus, at significantly increased spending, we have a combat Navy that is as small as it has ever been since World War II.

The existing "plan" is for these

U.S. NAVY & MARINE CORPS ADDITIONAL FUNDING IN THE "BASE" BUDGET [5]

|	2001	2002	2003	2004	2005	2006	2007	2008	2009	Total
2001 "Plan" (extrapolated for 2005-2009)	91.7	90.8	94.1	96.4	98.7	101.6	105.8	108.7	111.9	899.7
Base Budget Requests	92.6	98.7	108.2	114.5	119.2	125.4	127.1	139.5	149.0	1074.2
Base Navy Budget above 2001 Plan	0.9	7.0	14.1	20.1	20.5	23.8	21.3	30.8	37.1	174.5
Total Appropriations (including war funding)	95.5	102.4	124.1	124.3	131.7	143.8	150.3	147.7*	149.0	1168.8
Calculated War Spending	2.9	3.7	15.9	9.8	12.5	18.4	23.2	8.2*	N.A.*	94.6

* The war funding shown for 2008 is incomplete; Congress has not finished action on the president's request for 2008. No war funding for 2009 for the Navy/Marine Corps has yet been specified.

(INSIDE)

NAVY ACTIVE DUTY COMBAT SHIPS with trendline
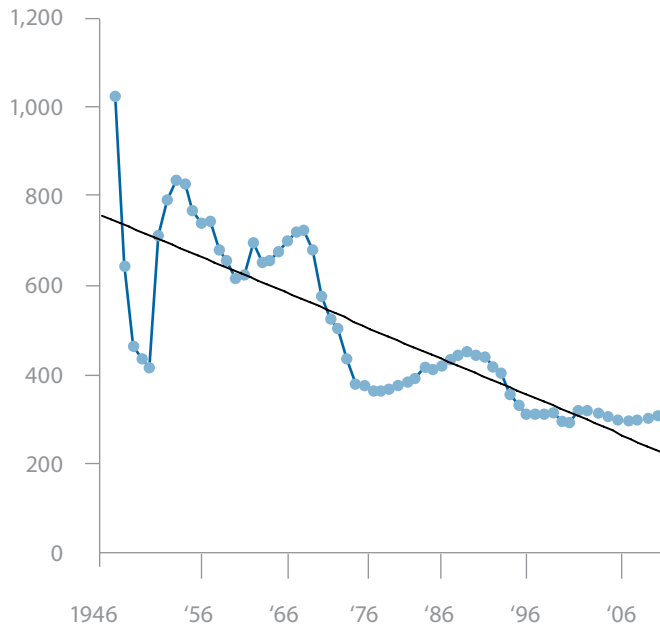
NAVY BUDGET with trendline (Billions, Fiscal Year 2009 Dollars) [6]
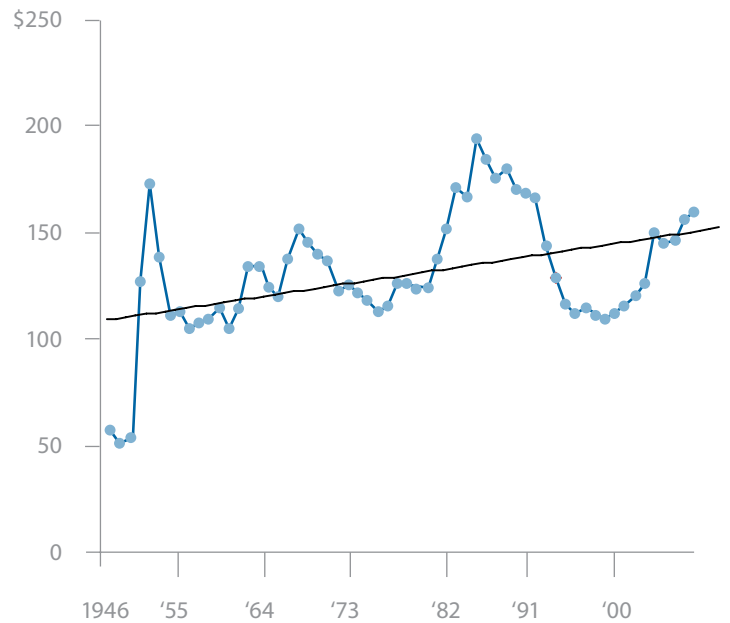
At significantly increased spending, we have a combat Navy that is as small as it has ever been since World War II.

trends to continue. The Navy is seeking higher spending levels while its fleet will remain hovering around 300 ships. As this plan progresses, the average age of the ship inventory will increase.[7]

Today, as it has each year since the mid-1990s, the Navy is seeking to supplement its own budget with "extracurricular" money, mostly in the form of a "wish list" that it eagerly sends to Congress each year after the charade of a "request" for it. Citing the shrunken size of the fleet, the

Navy seeks $7 billion more than it requested in its official budget, $149 billion (an amount well above the Navy's post-World War II average in inflation-adjusted figures). Taking into account the amount by which the 2009 Navy budget has already been increased over and above the extrapolated 2001 plan for 2009, $37.1 billion, it is apparent that the Navy is actually seeking a $44.1 billion "plus-up."

Nothing in the Navy's acquisition strategy is reversing the long-term

trend of fewer ships for more money. Even the Navy's new "low-cost" Littoral Combat Ship has roughly doubled in cost in recent years. As yet untested and unproven, both designs for this clearly needed "brownwater" capability have a long way to go before they demonstrate they are cost effective and should be purchased in any numbers beyond two test ships.

The next presidential administration will have to radically change the thinking in Navy shipbuilding, if not Navy acquisition leadership itself, if the long-term negative trends in the fleet's size and cost are to be altered. ∎

1   The budget plan specified in early 2001 for the Navy and Marine Corps extended to 2005. For the years 2006 to 2009, an extrapolation was made, citing the largest increases consistent with the 2001 – 2005 plan.
2   Such negative trends in all the military services have been thoroughly documented. A documentation of them is available in an analysis written in the late 1990s by Franklin C. "Chuck" Spinney in "Death Spiral," available at http://www.d-n-i.net/fcs/defense_death_spiral/contents.htm.
3   Budget data for this period of time that separate the Navy from the Marine Corps, or naval shipbuilding from the Navy's other expenses are not publicly available.
4   Fiscal Year 2009 "constant" dollars.
5   Source: National Defense Budget Estimates, volumes for 2001-2009, Office of the Under Secretary of Defense (Comptroller).
6   Sources: National Defense Budget Estimate for fiscal year 2009 (FY 09), Office of the Under Secretary of Defense (Comptroller), March 2008, and Navy fleet data from annual Department of the Navy Budget Estimates, the Congressional Research Service and Department of Defense Annual Reports.
7   These are the same trends Spinney found in his "Death Spiral" available at http://www.d-n-i.net/fcs/defense_death_spiral/contents.htm.

Information Warfare Relevance to Nuclear Weapons Security

BY ERIC HUNDMAN, CDI SCIENCE FELLOW

CONCERN ABOUT CYBERWAR, cybercrime and cyber-terrorism is increasing around the globe, especially as it relates to nuclear weapons. However, the actual scale of the threat is difficult to gauge and, worse, it is not always clear what terms like "cyberwar" even mean. Fortunately, the Department of Defense (DOD) has developed a useful system that classifies most of the possibilities under the broad rubric of Information Operations (IO). IO activities, in order of increasing relevance to nuclear weapons command and control (NCC), are categorized by the following five core capabilities:

1. military deception,
2. psychological operations,
3. operational security,
4. computer network operations,
5. electronic warfare.

The distinction between the computer network operations and electronic warfare is particularly important: the former involves attacking, defending, or exploiting purely computer-based networks; the latter involves any military action used to deceive or attack the enemy through use of electromagnetic spectrum energy.[1] For the sake of analytical clarity, the scenarios discussed here primarily involve single IO capabilities.

Military Deception (MILDEC)

MILDEC is defined as "actions executed to deliberately mislead adversary military decision makers with regard to friendly military capabilities, thereby causing the adversary to take (or fail to take) specific actions that will contribute to the success of the friendly military operation."[2]

Although the threats MILDEC operations might pose to NCC or early warning systems are not publicly available, they could include deceptive preparations for launch of a nuclear-capable missile, leading to a nuclear alert or to deploying early warning systems poorly (potentially leaving blind spots). Testimony by STRATCOM officials has indicated that they are using information operations – presumably including MILDEC – through the Joint Information Operations Warfare Command (JIOWC) to support strategic deterrence.[3] However, unless combined with computer network operations (CNO) or electronic warfare (EW), MILDEC seems unlikely to pose the strongest IO threat to nuclear weapons security.

Psychological Operations (PSYOP)

PSYOP essentially involves influencing the behavior of governments, organizations, groups, and individuals by selectively conveying information. With regard to nuclear weapons this could include, for instance, falsified messages aimed at relevant officials in the nuclear chain of command. Such vulnerabilities are easy to address, though – for instance, both missile launch crews and other officials often have secure sources of information.[4] Therefore, the risk of this type of information warfare – on its own – threatening the integrity of NCC or early warning systems seems small.

Similar to MILDEC, studies on PSYOP threats to NCC or early warning systems are not obtainable. However, related studies confirm that NCC incorporates consideration of a command and control failure within the system in a crisis,[5] implying heavily that the NCC is structured to defend against many potential PSYOP attacks.

Operational Security (OPSEC)

OPSEC is defined as "a process of identifying information that is critical to friendly operations and which could enable adversaries to attack operational vulnerabilities."[6] Basically, maintaining OPSEC involves restricting knowledge of security loopholes and similar weaknesses.

In one case involving nuclear weapons, this is achieved through several categories of security: for example, any facility judged to be "essential to the direction and continuity of the overall DOE nuclear weapons program" is considered

1   Clay Wilson, Information Operations, Electronic Warfare, and Cyber war: Capabilities and Related Policy Issues, Congressional Research Service, March 20, 2007.
2   Ibid.
3   Statement of General Kevin P. Chilton, Commander, United States Strategic Command, before the Strategic Forces Subcommittee, House Armed Services Committee, on United States Strategic Command, February 27, 2008, http://armedservices.house.gov/pdfs/STRAT022708/Chilton_Testimony022708.pdf.
4   See, e.g., Nathan Hodge and Sharon Weinberger, "The ever-ready nuclear missileer," The Bulletin of Atomic Scientists, vol. 64, no. 3, pp. 14-21, http://www.thebulletin.org/files/064003005.pdf.
5   DSB Task Force on Mission Impact of Foreign Influence on DOD Software, p. 28.
6   CRS Information Operations.

"Class A."[7] Each such facility has a different OPSEC plan that must be continually developed, updated, and tested. Given DOE's historical difficulties when implementing security recommendations, it is probably safe to assume that many of the organizational OPSEC plans are not completely up to date.[8]

Detailed planning procedures governing OPSEC for U.S. nuclear forces are contained in the top secret nuclear annex to the Joint Strategic Capabilities Plan (JSCP).[9] Specifics are classified, but recent versions reportedly incorporate increased flexibility in targeting relocatable and emerging targets that are not specifically addressed in the planning procedures.[10] This type of flexibility may also increase the need for rapid communication and decision making, potentially increasing the danger of OPSEC lapses.

Computer Network Operations (CNO)
CNO encompasses most of the activities referred to using "cyberwar" or "cybersecurity," including but not limited to network surveillance, denial-of-service attacks, computer information theft, and viral attacks. DOD defines CNO generally as including the capability to "(1) attack and disrupt enemy computer networks; (2) defend ... information systems; and (3) exploit enemy computer networks

through intelligence collection."[11]

There are no publicly available reports detailing specific CNO vulnerabilities for NCC systems. However, according to General Cartwright, STRATCOM has so far focused primarily on "network defenses to include firewalls, anti-virus protection, and vulnerability scanning" to fulfill its mission of "planning and directing cyber defense within DOD and conducting cyber attack in support of assigned missions."[12] STRATCOM and the Air Force also reportedly have significant offensive cyber capabilities, including a cyber-SIOP to be launched in the event of hostilities.

Security testing for NCC software appears to be extremely robust, involving meticulous "reverse engineering and thorough manual analysis" at a level rarely performed even for other sensitive DOD systems.[13]

Most importantly, the NCC system is reportedly "air gapped" – physically separated from any other networks – making it, in theory, invulnerable to CNO attacks.[14] However, it is unclear how broadly or effectively such protection is applied, as it was compromised for at least one NCC communications system.[15] In general, air gapped networks often end up sharing connections, power sources,

Matt Inaki, computer network defender coach/trainer of SPAWAR Systems Center San Diego, shows how to monitor the activity of a network during a cyberwar training course at the Space and Naval Warfare Systems Center.

7   Operations Security Program: Guidance for Sub-Contractors," Los Alamos National Laboratory, July 15, 2008, www.lanl.gov/orgs/sup/procurement/php/files/upload_green_docs/subcontractor_guidance.doc.
8   Ibid; Government Accountability Office, DOE Needs to Resolve Significant Issues Before It Fully Meets the New Design Basis Threats, April 2004, http://www.gao.gov/new.items/d04623.pdf.
9   Hans M. Kristensen, "The Joint Strategic Capabilities Plan (JSCP) Nuclear Supplement," The Nuclear Information Project, June 16, 2005, http://www.nukestrat.com/us/jcs/jscp.htm.
10   Ibid.
11   CRS Information Operations.
12   Statement of General James E. Cartwright, Command, United States Strategic Command, before the Strategic Forces Subcommittee, Senate Armed Services Committee on United States Strategic Command, March 28, 2007. Available online at http://www.globalsecurity.org/wmd/library/congress/2007_h/070328-cartwright.pdf.
13   "Findings of the Defense Science Board Task Force on Mission Impact of Foreign Influence on DOD Software."
14   Joshua Green, "The Myth of Cyberterrorism," Washington Monthly, November 2002. Available online at http://www.washingtonmonthly.com/features/2001/0211.green.html.
15   A backdoor was found in the software for the antennas that transmit launch orders to the Trident fleet – they were clearly not air gapped, despite being part of the NCC system: "Unauthorized persons including terrorists may have been able to seize electronic control of shore-based radio transmitters such as the very low frequency facility at Cutler Maine, and actually inject a launch order into the network." Bruce G. Blair, "Increasing Warning and Decision Time ('De-Alerting')," International Conference on Nuclear Disarmament, Oslo, February 26-27, 2008.
16   Philip Coyle, correspondence with the author.
17   Joshua Green, "The Myth of Cyberterrorism."'

or other resources for the sake of convenience or efficiency, all of which decrease network security.[16]

The threat from CNO to NCC is therefore extremely unclear, just as with commercial networks. When discussing commercial vulnerabilities, news reports and government agencies tend to emphasize the vulnerabilities and breaches, from government-sponsored Chinese hackers to significant decreases in satisfactory cybersecurity performance at NNSA sites over the past decade.

But while the economic costs of cyberattacks are clear – on the order of $15 billion worth in 2001[17] – the danger to the actual integrity of critical infrastructure and particularly of military networks is far more uncertain. Even if hackers were able to gain control of a particular system, critical infrastructure systems often require specialized knowledge to operate. Essentially, even if it is possible to break in to a system, a hacker won't necessarily know what he is seeing. And even if attackers are able to gain insider help, power plants or the like are rarely left unsupervised and the intrusion would likely be detected.

In addition, modern critical infrastructure systems are "more flexible and responsive in restoring service than early analysts realized"[18] and "many U.S. counterterrorism experts feel that far-reaching effects from a cyberattack are highly unlikely."[19] Nevertheless, the U.S. government seems insufficiently prepared to recognize and respond to a cyberattack. A 2006 report cited three causes for U.S. unpreparedness: a lack of indicators that would show an attack is underway; a lack of clarity about who is responsible for restoring compromised infrastructure; and a lack of dedicated resources for recovery from cyber attacks.[20]

Given the lack of public information on the vulnerabilities of military networks, it seems reasonable to assume that their weaknesses are smaller than but parallel to those of civilian networks. This is especially true as DOD relies increasingly on commercial technology and software for its increasing information processing needs.

Electronic Warfare (EW)

DOD defines EW as "any military action involving the direction or control of electromagnetic spectrum energy to deceive or attack the enemy."[21] EW is the primary IO vulnerability in NCC and early warning systems because both are dependent on electronic communications that are inherently susceptible to EW.

In theory, both the physical (fiber optics and Ethernet cables, for instance) and wireless (e.g. Very Low Frequency/Low Frequency and Extremely High Frequency) links used by the NCC system to maintain communication are vulnerable to EW techniques such as false launch signals, jamming of radio links, tapping into cables to send false signals, or simply eavesdropping. With regards to the early warning radars, for example, it is theoretically possible to create false radar images even of large targets.[22] In addition, old analog technology is being replaced with newer digital components that may be even more vulnerable to EW techniques.

However, all such attacks would require specialized equipment and expertise. VLF communications with submarines, for example, require extremely long antennas (~2.5 miles) in order to broadcast effectively. An attacker would need to procure such equipment in addition to securing the relevant encryption, timing, and location data for intercepts and faked signals. In addition, the NCC and early warning networks were almost certainly developed as proprietary systems; very few people will have expertise in their specific protocols. They will therefore be very difficult to manipulate electronically without insider knowledge. Even if attackers were to use EW means to get inside a system, they wouldn't necessarily be able to interpret the data they would receive, much less manipulate it.

Conclusions

The threat to NCC systems posed by information operations techniques is far from clear, but, to some extent, it will always be a concern and, as attackers become increasingly sophisticated, the threat will increase accordingly. In addition, militaries around the world – especially in the United States – are working vigorously to increase their networking and information processing capabilities; such integration will likely increase their vulnerability to information-based attack techniques. Despite the uncertain nature of the threat, the complexity of this issue merits further careful analysis. ∎

18   James A. Lewis, Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Center for Strategic and International Studies, December 2002. See also Richard Forno, "Shredding the Paper Tiger of Cyberterrorism," Security Focus, September 25, 2002, http://www.securityfocus.com/printable/columnists/111/.
19   Rollins and Wilson, "Terrorist Capabilities," p. 10.
20   Ibid.
21   Wilson, "Information Operations," p. 6.
22   D.J. Fouts et al, "A single-chip false target radar image generator for countering wideband imaging radars," IEEE Journal of Solid-State Circuits, vol. 37, no. 6, June 2002. Abstract at: http://ieeexplore.ieee.org/xpl/freeabs_all.jsp?tp=&arnumber=1004579&isnumber=21689.

U.N. Small Arms Process Back on Track

United States Plays Limited Role

BY JONAH LEFF, CDI RESEARCH ASSISTANT

TWO YEARS AFTER THE FAILED United Nations Review Conference on Small Arms, United Nations member states again met on the issue of small arms. Over 130 states met from July 14-18 for the Biennial Meeting of States (BMS), where states reviewed progress on the implementation of the Programme of Action (PoA), a politically binding agreement agreed to in 2001 that establishes national, regional and global measures to stem the illicit trade in small arms and light weapons. The meeting marked the third BMS meeting; the other two took place in 2003 and 2005.

The BMS focused primarily on three thematic issues: international cooperation, assistance and national capacity-building; stockpile management and surplus disposal; and illicit brokering. Governments also spent one day discussing the implementation of the International Instrument to Enable Sates to Identify and Trace, in a Timely and Reliable Manner, Illicit Small Arms and Light Weapons (also known as the International Tracing Instrument, or ITI). The ITI is a politically binding document established through the PoA in 2005, which enhances international cooperation for the tracing of illicit weapons around the world.

After an arduous week of formal and informal negotiations, which were chaired by Dalius Cekuolis of Lithuania, governments unanimously adopted an outcome document representing the conclusions of the meeting. One hundred thirty-four countries voted in favor of the docu-

ment, while two countries abstained (Iran and Zimbabwe), and 56 countries were not in attendance, including the United States.

The meeting's final report primarily encourages states to uphold their commitments enshrined in the PoA, but also includes some new elements. For example, in the section on international cooperation, assistance and national capacity-building, states agreed to utilize two new mechanisms – a PoA Implementation Support System established by the United Nations Office for Disarmament Affairs (UNODA) as well as a database designed by the United Nations Institute for Disarmament Research (UNIDIR) – to enhance assistance by matching needs with available resources. States also discussed the possibility of establishing a legally binding instrument on brokering in small arms and light weapons, but no timetable or commitment has been determined. In addition, the report's section on stockpile management specifically defines regulations, standards and procedures for managing stockpiles and destroying surplus weapons.

The report also listed concerns voiced by some states that in the past were too controversial: civilian possession of small arms and light weapons; linkages between security, armed violence, development and human rights; ammunition; prohibiting the supply of small arms and light weapons to nonstate actors and terrorists; and transforming the PoA into a legally binding agreement. Although many states called for rec-

ommendations on these issues to be reflected in the report, other states opposed their inclusion. What resulted was weakened language that allows states to remain free from any obligations that did not enjoy consensus.

Although the document was adopted, some states voiced strong opposition to the process. Iran objected to the negotiating procedures throughout the week, calling for a more transparent line-by-line negotiation of the draft outcome document. Iran argued that a "take it or leave it" approach sets an "unjustifiable precedent in the field of disarmament." Indonesia, speaking on behalf of the Non-aligned Movement, agreed that the process had not been ideal, but said it would accept the draft's text. All other states objected to Iran's stance, some calling small arms a "matter of life or death" and stressing the importance of reaching agreement.

Unlike previous U.N. meetings on small arms, the United States was not a factor in the final deliberations. During the small arms Review Conference in 2006, the United States expressed opposition to continuing the small arms process at the international level, claiming that it was an inefficient use of funds and time. The United States, which took part in the 2001, 2003, 2005 and 2006 U.N. meetings and agreed to the PoA in 2001, has some of the strongest laws on regulating the illicit trade in small arms and light weapons. However, rather than continuing multilateral meetings, the United States believes

more practical initiatives should be taken at the national and regional levels to enhance implementation of the PoA. In addition, the United States faces strong opposition to the U.N. process from the National Rifle Association, which has had a large influence on U.S. policy statements and actions throughout the U.N. small arms process. In the end, the United States did not participate in the BMS and only attended the one-day discussion of the ITI.

In addition to governments, over 150 representatives of nongovernmental organizations (NGO) from 36 countries were also in attendance. In addition, over 20 states had NGO representatives serve on their delegations as advisors, demonstrating significant cooperation between governments and civil society. NGOs and intergovernmental organizations (IGO) also held more than 30 side events at the meeting's margins, which included various presentations by members of the International Action Network on Small Arms (IANSA), the launch of the 2008 Small Arms Survey, as well as a rap performance by a former Sudanese child soldier, Emmanuel Jal. Jal was also invited later in the week to perform in front of states – a considerable break in U.N. conventionality – during the NGO presentation at the meeting.

The outcome of the BMS demonstrated states' rejuvenated commitment to eliminating the illicit trade in small arms and light weapons. The next meeting of states to discuss the PoA will likely take place after January 2009, which provides an opportunity for the next U.S. administration to re-engage the United States in the U.N. small arms process and to continue international progress on this issue. ■

FORGING A SINO-U.S. "GRAND BARGAIN" IN SPACE

BY THERESA HITCHENS, CDI DIRECTOR
AND DAVID CHEN

In Washington's space security community the debate has coalesced around the question of whether the future of Sino-U.S. relations in space should more closely resemble arms control or an arms race – illustrated by the intercepts and destruction of satellites by both nations a year apart. Whatever direction Washington and Beijing take in their nascent military space competition is certain to be followed by other major and emerging space powers.

Unfortunately, the existing trend in both nations is for promoting an offensive space strategy aimed primarily at one another. With a new U.S. administration, whichever candidate enters office will face the challenge of finding viable alternatives to the anti-satellite arms race that lies at the end of the present course, an outcome that would be in neither party's interest. The incoming president might avoid such a security dilemma with China by utilizing the full-range of U.S. soft power, backed by realistic hard-power consequences. This will require the incoming administration to expand its understanding of what constitutes a space issue, and to develop a deeper knowledge of what motivates China's leadership. Using both persuasion and dissuasion to craft a kind of "grand bargain" with China regarding space, the next president may be able to steer Sino-U.S. competition toward trade, economics and sport, rather than military oneupmanship. Accomplishing this would strengthen U.S. national security and international stability in the Pacific region.

The relationship between the U.S. and China will remain a complex one and perhaps the world's most important bilateral relationship in the 21st century. The issue of space security, while only one of many issues of contention, is a high-stakes one that can either stabilize or further destabilize the relationship. A code of conduct establishing clear boundaries delineating the behaviors of responsible stakeholders in space would be an important step toward improving Sino-U.S. ties. By using a two-pronged approach of mitigating U.S. space systems' vulnerability, and negotiating Chinese acceptance of a space code of conduct using incentives like joint space missions and commercial space policy reform, the next president could open a window to avoid an incipient space race with China. Managing such a feat would not only serve peace and stability on Earth and in the heavens, but also it would make a fitting legacy to Nixon's opening of China. ■

Excerpted from: Theresa Hitchens and David Chen, "Forging a Sino-U.S. 'Grand Bargain' in Space," Space Policy 24, no. 3 (August 2008): 128-31.

111 Countries Agree to Cluster Munitions Treaty

BY RACHEL STOHL, SENIOR ANALYST AND JONAH LEFF, RESEARCH ASSISTANT

NEARLY 10 YEARS AFTER the historic Ottawa Landmines Treaty banned an indiscriminate weapon causing tens of thousands of civilian casualties a year, more than 100 countries met in Dublin and agreed to ban another weapon system responsible for immeasurable human suffering. On May 30, 2008, 111 countries agreed to a treaty that bans the use, production, transfer and stockpiling of cluster munitions, and provides survivor assistance and cluster munitions clean-up. The Convention on Cluster Munitions will be opened for signature in December 2008 and will come into force once 30 countries have ratified it.

Cluster munitions are deployed from either the air or ground, scattering bomblets over a wide area on the ground. One of the dangers of cluster munitions is that these submunitions sometimes fail to explode, littering areas with unexploded ordnance. These dud bombs, which are still active, often cause the majority of human casualties. The Cluster Munition Coalition believes 60 percent of those injured by cluster munitions receive their injuries while going about their daily lives, and one-third of these are reportedly children.

Cluster munitions are a global problem, which have affected countries including Afghanistan, Bosnia and Herzegovina, Iraq, Israel, Lebanon and Sudan. These weapons affect civilians disproportionately. The Cluster Munition Coalition has reported that cluster bombs were responsible for more deaths in Kosovo in 1999 and Iraq in 2003 than any other weapon system. According to the Coalition, at least 14 countries have used cluster munitions during conflicts, including Eritrea, Ethiopia, France, Israel, Morocco, the Netherlands, Nigeria, Russia (USSR), Saudi Arabia, Sudan, Tajikistan, the United Kingdom, the United States, and FR Yugoslavia. Hezbollah is the most well known nonstate group to have also used cluster munitions, but they have been used by many other nonstate groups as well.

Although over 100 countries committed to the cluster ban, important producers and users of cluster munitions did not attend the meeting. Russia, China, Israel, Pakistan, India and the United States were not only absent from the meeting, but have publicly opposed the convention.

The treaty prohibits the use, production and transfer of cluster munitions, as well as requires the destruction of all stockpiled cluster munitions. An estimated 76 countries stockpile billions of submunitions, which are produced by at least 34 countries in over 210 varieties. Russia, China and the United States are believed to have stockpiles containing more than a billion cluster munitions alone.

The United States refused to participate in the Dublin meeting, but made its presence felt. Throughout the Oslo Process and the Dublin meeting, the United States lobbied its allies and pressured them not to support the convention. The United States threatened allies that joint operations could be negatively affected by such a treaty and that operations in Iraq and Afghanistan could be affected as well.

U.S. opposition to the Convention on Cluster Munitions is rooted in four motivations. First, the U.S. position is based on the belief that a new convention will jeopardize progress in other international forums. In particular, the United States argues that Protocol V of the Convention on Certain Conventional Weapons (CCW) already addresses all varieties of explosive remnants of war (ERW), including cluster munitions. The United States also believes that cluster munitions should not be singled out from the larger category of ERW, because they could divert attention and resources from other, more deadly ERW. In addition, the United States feels that the CCW should be the forum for any new cluster munition initiatives. However, critics of the U.S. position feel Protocol V, which commits states to clear such ERW from their territories, does not adequately address the humanitarian impacts associated with cluster munitions deployment, targeting requirements and reliability standards.

Second, the United States maintains that cluster munitions remain an effective and necessary weapon of war. The United States argues cluster munitions may in fact cause less collateral damage. Although they haven't been deployed since 2003 in

Iraq, the Pentagon strongly resists giving up cluster munitions. The United States maintains a stockpile containing an estimated 700 million to 1 billion submunitions.

Third, the priority of U.S. policy with regard to cluster munitions is to improve their reliability, not ban them entirely. In 2001, the Department of Defense announced a new policy on submunition reliability that would reduce the failure rate on newly produced submunitions to less than 1 percent (some estimates place current dud rates as high as 15-20 percent).

Fourth, rather than banning cluster munitions, the United States has chosen to address them by spending more money on international cleanup efforts than any other country in the world. The United States has already provided ERW clearance and stockpile destruction assistance to almost 50 different countries and spent over $1.3 billion on ERW and landmine clearance efforts since 1993. The United States has also announced plans to develop a quick reaction force to respond to the humanitarian threats posed by ERW, small arms and light weapons, landmines and man-portable air defense systems (MANPADS).

Although the administration has been consistent in its opposition to an international treaty, Congress has taken a different path. Less than a week after the Dublin meeting concluded, Sens. Dianne Feinstein, D-Calif., Patrick Leahy, D-Vt., and Rep. James P. McGovern, D-Mass., introduced a joint resolution urging the United States to sign onto the Global Convention in December 2008.

This joint resolution reinforces previous congressional efforts on cluster munitions. In 2007, Sens. Feinstein, Leahy, Bernie Sanders, I-Vt., and Bar-bara Mikulski, D-Md., introduced the Cluster Munitions Civilian Protection Act of 2007 (S. 594), which restricts the use and transfer of cluster munitions with higher than a 1 percent failure rate and limits the use of cluster munitions to clearly defined military targets not in the vicinity of civilians. Although stalled in the Senate Committee on Foreign Relations, the bill sent a clear message of Congress's intent on U.S. use of cluster munitions. A similar bill (H.R. 1755) was introduced on the House side and has been referred to the House Armed Services Subcommittee on Readiness.

In addition, within the 2008 Foreign Appropriations bill was a provision (Sec. 695) limiting the sale and transfer of cluster munitions systems that have a 1 percent or lower failure rate and mandating that any country importing U.S. cluster munitions only use them against clearly defined military targets where no civilians are present. President George W. Bush signed the bill into law in December 2007, which in effect results in a one year moratorium on the sale of cluster munitions.

Despite the lack of participation of the United States and others, treaty supporters and advocates have celebrated the convention's creation. And, similar to the Mine Ban Treaty, which lacks signatures from many of the same opponents, it is hoped that states not party to the treaty will comply with its standards. The next U.S. administration may also provide an opportunity for a shift in U.S. cluster munitions policy. One month following the treaty's December 2008 opening for signature, the incoming administration will have the chance to demonstrate a renewed U.S. stance on cluster munitions. The world will be watching. ■

Words Matter

Condemning China's ASAT Test as Illegal

BY EUGENE MARDER, CDI RESEARCH ASSISTANT

CHINA'S JAN. 11, 2007, TEST of an antisatellite (ASAT) weapon left more than just debris in its wake. Destroying its own ailing satellite to demonstrate military capabilities, China prompted worldwide condemnation from other space-faring states. Nations decried the creation of hazardous wreckage that remains in orbit for decades and doubles the threat of collision for existing satellites. They chastised China for moving toward the weaponization of space, while failing to consult with other nations about its plans.

Among these voices, only Japan averred that China had violated international law. As such, the test's most destructive consequence may not be the debris or China's bellicosity, but a significant weakening of international law. Unlike the more immediate effects, this one is reversible, even a year removed. By pointing to the illegality of China's action and defining their expectations for the future, states can reinforce the outer space legal regime and prevent past omissions from setting a dangerous precedent.

The Outer Space Treaty, accepted as international law by all space-faring states, contains multiple provisions applicable to China's test and its surrounding conduct. The most egregious violation is China's lack of international consultations required by Article IX. The article states that if a treaty party has reason to believe that it's   *Words continued on page 10*

The Trouble with NATO

BY MARK BURGESS, DIRECTOR, WSI BRUSSELS

THE RECENT CRISIS IN GEORGIA is only the latest problem to tax NATO. As well as problems with its old enemy, Russia, the alliance's woes in its biggest mission to date continue, causing some to question whether or not it is relevant or needed in today's world. Afghanistan, NATO's first ground shooting war is, by extension, also its most pressing problem. Almost seven years after the U.S. invasion, Afghanistan still totters on the brink of failed statehood, while NATO's first war might yet prove its last.

Rumors of NATO's impending death may be overstated, however failure in Afghanistan will be costly to it as an organization that has sought to reinvent itself since the passing of the Cold War and its original *raison d'être*. The International Security Assistance Force (ISAF) in Afghanistan has become a major element of that reinvention. Yet its problems in Afghanistan give cause for concern as to how effective NATO can hope to be as a fighting force.

NATO's woes in Afghanistan stem partly from the inherent difficulties of counterinsurgency operations. However ISAF is also hindered by the lack of a common strategy among its various national components, as well ›

Words continued from p. 9 outer space activity "would cause potentially harmful interference" with the interests of other parties, it shall undertake consultations before proceeding. China has long known that the destruction of satellites in space contributes to orbital debris. One boon of the otherwise dubious legacy of Cold War arms races is widespread knowledge about the risk of military exercises in space. The United States' deliberate destruction of its Solwind satellite in 1985 created debris that led to the introduction of expensive armor on subsequently launched spacecraft. Nor is the threat of space debris a secret. Satellites frequently change their orbit to avoid objects in space and a few have been decommissioned as a result of collisions. China itself is party to several international organizations recognizing the need to curb space debris proliferation. Knowing full-well the amount of debris that would result from its ASAT test and the potential harmful interference it would cause, China took no steps to engage in the international consultations mandated by the Outer Space Treaty.

Flouting an express provision of a treaty is a patent breach of international law. However, while treaties provide some of the few codified sources of international law, they may be modified based on the subsequent practices of their state parties. Despite evidence of consultations with regard to activities in outer space – information sharing before the crash of a Soviet satellite in Canada and international space monitoring efforts are two examples – some say that the Outer Space Treaty has been rendered moot. Proponents of this theory argue that a lack of calls for consultation during the spate of Cold War ASAT tests was "consistent and general" enough to betray the intent of the states to abdicate Article IX. However, at that time, most states did not recognize the danger of space debris, and many lacked interests in space that could potentially be harmed. Moreover, the perpetrators of the tests were likely hesitant to implicate Article IX in ASAT testing for fear that it may hinder their future efforts to gain a competitive advantage. Their immediate allies would have been equally reluctant to act independently, given the bifurcation and strict allegiances of the bipolar world. No consistent or general intent can be gleaned from these examples.

The circumstances are different today. The potential harm of space debris is well-known and many nations depend on satellites for essential functions. As some states pursue space weaponization to establish dominance or countervail threats, others should follow Japan's lead in deeming China's lack of consultation illegal. The past may have been forgiving to members of the Outer Space Treaty who ignored the crucial Article IX provisions, but the future will not be. While more pugnacious countries eye space as a strategic battleground for coming wars, the world must show a will to follow the letter and spirit of the Outer Space Treaty and uphold the principles of peaceful cooperation in space. ■

as various degrees of commitment to the mission and sensitivity to domestic politics when it comes to using their troops.

Caveats – limitations on where, how, or when troops can be deployed – have been contentious for some time with some countries, such as the United Kingdom and Canada, feeling they are bearing the brunt of things, with others, including France, Germany and Italy, less inclined to put their forces in harm's way or increase contingents. Such reticence is understandable – when NATO signed on to its expanded mission in Afghanistan many members believed they would be assisting development rather than providing security. Now some troops are facing combat and casualty levels unsurpassed since World War II.

War *a la carte* – such as some NATO countries seem to be fighting in Afghanistan – risks seriously, perhaps even fatally, undermining the principle of collective security and defence that lies at NATO's core. Moves to limit caveats began in recent months and should continue until none remain. They undermine NATO and its mission in Afghanistan.

Additionally, it is worth noting that ISAF is seeking to fix a problem it inherited. The original American invasion quickly overthrew Afghanistan's Taliban government, but ignored the immediate post-conflict phase to a degree that allowed the security situation to deteriorate. This foreshadowed the Bush administration's subsequent mishandling of events in Iraq. It was also made all the more ironic by Washington's dismissal of NATO's historic invocation of its Article V collective security mechanism immediately following the terrorist attacks of Sept. 11, – a rebuttal which was itself damaging to NATO.

Pakistan too must share some blame for the situation in neighboring Afghanistan, with suspicions abounding that elements of the former's intelligence services provide succor and support to the very insurgents they are supposed to be fighting. Meanwhile, Western governments must educate their publics as to the need to be in Afghanistan at all – something the debate over caveats indicates is not happening to the level required.

This may prove difficult at the moment given NATO's other big problem – the crisis in Georgia. Russia's invasion of Georgia and subsequent posturing and recognition of the breakaway Georgian regions of Abkhazia and South Ossetia have left NATO open to charges of impotence. Yet, it is unclear what the alliance, a military organization, can do in this situation. Once again, the contrast with the Cold War is stark.

Some – U.S. presidential hopefuls Barack Obama and John McCain among them – have suggested that efforts to bring Georgia and Ukraine into NATO be expedited. Both countries were denied NATO Membership Actions Plans (MAPs) at the alliance's summit in Bucharest in April this year. In the wake of the Russian invasion of Georgia, suspicion abound that the decision not to issue MAPs gave a green light to Moscow, convincing it the West was weak and disunited when it came to this issue. Indeed, it has been suggested that this may also have encouraged Georgian President Mikheil Saakashvili to take on Russia, convincing him that Europe was and would remain weak when it came to standing up to his giant neighbor on the question of Georgian membership of NATO – a prospect that escalating Russian vio-

lations of Georgian territorial integrity made increasingly unlikely.

Yet, it can also be argued that U.S. President George W. Bush's public call at the 2008 NATO Bucharest Summit for MAPs to be offered to Georgia and Ukraine was ill-advised, ill-executed and ill-timed. For one thing, Bush alienated some NATO allies – notably Germany. He had earlier given them the impression that he would support a compromise solution that stopped short of immediate MAP offers for the two former Soviet states, instead encouraging preparatory work for such a move – possibly in time for NATO's 60th anniversary summit in Berlin in 2009. Bush's altar call in Bucharest also directly contradicted the recently-stated official French position. This did indeed telegraph a picture of Western disunity on the subject to Russia. However, this occurred for no immediately discernible good reason – NATO consensus on what Bush called for was always seen as unlikely – at a time when the opposite appearance was needed and when NATO, as now, had more pressing concerns in Afghanistan. Moreover there were, and remain, questions as to Georgia and Ukraine's eligibility for NATO. Membership of the alliance is unpopular among a large element of the Ukrainian public, while Georgian repression of opposition movements, coupled with the instability in Abkhazia and South Ossetia have long been cited as potential show-stoppers.

Arguments that Russia is stoking unrest in these regions as a means of keeping Georgia out of NATO are not without merit. Yet the fact remains that Tbilisi's behavior has often inflamed rather than ameliorated things. As such, the decision not to offer MAPs at Bucharest was a

defendable one, even if the manner in which it was handled may well have increased Russia's perception of Western weakness, with the current crisis in Georgia partly a result of that.

Now more than ever, there is a need for NATO to put up a front of solidarity and draw the line in the sand it should have drawn in Bucharest, sending the strong message it also should have sent then that Moscow cannot dictate terms to NATO and that the alliance's door will indeed remain open to Georgia and Ukraine. NATO should proceed at a prompt but measured pace on this, especially if it means bringing forward any MAP offers: the Georgian president has already clearly demonstrated the dangers in overreacting to Russian provocations. However, in so doing NATO should better consider and address Russia's concerns with regard to the alliance's post-Cold War expansion, for it is these that arguably underlie the Kremlin's current actions in Georgia.

This expansion was cautioned against by the likes of George Kennan, Thomas Friedman and Michael Mandelbaum, and has been claimed to play on Russian paranoia and humiliation at being the undefeated loser of the Cold War to a degree that is only now becoming apparent. Whatever may be thought of recent Russian actions, their claims of NATO encroachment are not unfounded. Ostensibly, NATO expansion is designed to spread stability and security, however, there are suspicions in some quarters that it is used for power projection by its most powerful member, the United States. More plausibly, it is also claimed that it is being used to contain Russia. Energy security has also been posited as a useful side effect of Georgia and Ukraine joining NATO.

None of this is to suggest that Russia is somehow blameless or should not be held accountable for its aggression in Georgia. Nor, it is worth restating, should it be given some sort of veto over NATO enlargement. However, the consequences of such enlargement may be different now than they once were. Heightened Russian assertiveness contrasts with the divisions within NATO. Russia is not a world superpower anymore. But it is still a regional one that, absent any balancing that came with the Cold War threat of mutually assured destruction, may well feel increasingly tempted and able to call the West's bluff. As such, NATO should be prepared to follow through on any

Russia is not a world superpower anymore. But it is still a regional one.

commitments made to new or potential members.

That it is in some ways questionable if NATO would have engaged in a full-scale war with Russia over Georgia – even if the latter had been an alliance member – is something Moscow is doubtlessly well aware of. Poland, which *is* an alliance member, certainly seems to put little trust in Article 5 of NATO's Charter, as the recent deal to station U.S. missile defense components within its borders illustrates. Warsaw's main motivation appeared to be obtaining the security guarantees that come with having American troops on Polish soil, an entangling alliance being considered to provide sounder security guarantees than NATO, or at the very least pursued as an insurance policy.

Recent events in Georgia require

urgent action from NATO. However, the shadow of Afghanistan and NATO's fight there still looms large. It is the more pressing emergency and should be treated as such. That said, NATO clearly also needs an internal debate to come up with consensus as to what enlargement is for – security sector reform, containing Russia, or both, as well as criteria for candidature and benchmarks for eventual membership.

The development of an energy security policy that leaves it less dependent on Russian gas and oil supplies, and therefore less constrained as to what actions it can take in the face of Russian belligerence such as has been witnessed in Georgia, will also leave NATO better equipped to navigate a geostrategic environment that is much more uncertain than that of the Cold War. Wider attempts to finally take nuclear weapons out of international relations are also needed more than ever with East-West confrontation once again rearing its head.

Yet, as the Georgia crisis continues it is also worth considering that Russia is far from the global superpower it once was. With a defense budget a little over one-tenth of America's and an economy one-fourteenth the size, Russia lacks the resources to bedevil the West on the scale that the old Soviet Union could – even if it would be folly to forget that the nuclear genie cannot easily be put back into the bottle. None of this is to suggest that Russia is a sheep in wolf's clothing; however its scope for mischief may be more limited than current fears suggest. That should give the West some degree of relief, and give NATO some breathing space, as it seeks to cope with its "new" old enemy and the more immediate problem of fixing Afghanistan. ■

Score One for Sanity

Cutting Funding for New Nuclear Weapons

BY VICTORIA SAMSON, CDI SENIOR ANALYST

Sen. Barack Obama, D-Ill., and Sen. John McCain, R-Ariz., have stated that they would support working toward global elimination of nuclear weapons.

THIS SUMMER SAW A WELCOME victory for the arms control community when Congress decidedly cut funding for the Reliable Replacement Warhead (RRW). With this move, it is hoped that the United States won't add to its thousands of nuclear weapons left over from the Cold War, but will instead work to get its nuclear monkey off its back.

Both the House and the Senate appropriations committees refused to allow the $10 million asked by the White House for the RRW program in the fiscal year 2009 budget request. This is the second year Congress hasn't appropriated funding for the RRW, indicating the heavy amount of suspicion with which Congress regards the program.

The RRW has been touted as a way in which to ensure that the U.S. nuclear weapons arsenal is still safe and usable. Since the United States has voluntarily refused to explode a nuclear weapon during testing since 1992, proponents of the RRW argue that we cannot be sure that U.S. nuclear weapons would work as planned. They are wrong.

The name "Reliable Replacement Warhead" is a misnomer. The U.S. nuclear arsenal is already extremely reliable, due to the extensive testing held before 1992. Yes, answer supporters of the RRW, but these weapons are getting older by the day. How can we know if they'll age gracefully? The United States already has an extremely successful program in place to ascertain how its nuclear weapons are faring without testing them. As it turns out, they're doing very well – even better than the designers had hoped for or anticipated. And if they weren't, Congress and the president would be informed of that, as they receive annual certifications as to the safety of the U.S. stockpile.

What's dangerous about the RRW is that it feasibly would require the United States to break with its 16-year moratorium on testing in order to determine if the new weapon design of the RRW was indeed reliable. And if the United States establishes a precedent for making nuclear testing acceptable, then other countries could follow, or at least use it as a validation for future nuclear tests (none of the official nuclear weapons states has held a nuclear test since 1996). "Do as I say, not as I do" doesn't work very well as a tenet for U.S. foreign policy.

At a time when the United States is understandably alarmed about other countries establishing military nuclear programs, it is hard to justify why the U.S. not only still thinks it needs thousands of nuclear weapons, but is fighting to retain its gargantuan complex of nuclear weapons laboratories. The National Nuclear Security Administration, charged with the responsibility for the U.S. nuclear arsenal, is struggling to convince Congress that it should not be overhauled even though its duties have changed.

Of course, another major factor is who will be residing in the White House come January. Of the two presumptive nominees for the presidency, Sen. Barack Obama, D-Ill., has come out against the RRW, while Sen. John McCain, R-Ariz., hasn't indicated how he feels about the program. But both candidates have stated that they would support reducing the size of the U.S. nuclear arsenal and working toward global elimination of nuclear weapons. With a world free of nuclear weapons, arguing over the RRW – or any new nuclear weapon – would be a moot point, and, more importantly, we would all be much safer. ■

The design of the RRW was once hinted by the Lawrence Livermore National Laboratory to be based on the above pictured design of the W89 nuclear warhead, which was test fired during the 1980s.

CARBON **eco-ink** NEUTRAL **ecoprinted**

To sign-up for weekly e-mail updates, send an e-mail to INFO@WORLDSECURITYINSTITUTE.ORG.

THE DEFENSE MONITOR

The Center for Defense Information conducts in-depth research on the social, economic, environmental, political and military components of international security. CDI aims to educate the public and inform policymakers on challenges of security policy, strategy, operations, weapon systems and defense budgeting, and to produce creative solutions to them. The Center for Defense Information is a division of the World Security Institute.

WWW.CDI.ORG

© Copyright 2008 by the Center for Defense Information. The Center encourages quotation and reprinting of any of the material, provided the Center is credited. The Center requests a copy of such use.