F.A.S. ***PUBLIC INTEREST REPORT***

Journal of the Federation of American Scientists (F.A.S.)

Volume 51, Number 4 July/August 1998

Year 2000 Problem and Nuclear Weapons: Apocalypse or Annoyance?

John E. Pike

The inherent and unavoidable unreliability of computers is about to be stressed, to some unknown and unknowable extent, by a seemingly trivial "feature"—the Year 2000 (Y2K) problem. Systems and application programs that use dates to perform calculations, comparisons, or sorting may generate incorrect results working with years after 1999.

America and other countries are dependent on computers for command and control of nuclear weapon operations.

A Two Digit Problem

The problem arises from the use of two digits to represent year data in many computer hardware and software implementations. In the early years of computer development and use, memory costs were high, and processing speed slow, so the use of two digit years (98) versus the full four digit year (1998) seemed like a good idea. It used less memory, which helped maintain acceptable processing speed, and introduced few anomalies at mid-century. Dates were typically represented by the six character date pattern (YYMMDD), and simple arithmetic could use the last two digits of the year, which worked fine as long as the computations did not extend into the next century.

When a computer determined a person's age, for example, it would subtract the two digit year of birth (example: 53 for 1953) from the current two digit date-year (98 for 1998), producing the correct solution (45 years). But, on 01 January 2000, the shortened date-year becomes 00. Now, however, the simple arithmetic process produces an age of minus 45, obviously an incorrect age.

Another date related computer process is date sequencing. The year 00 would incorrectly appear in the sequence of 00, 97, 98, 99. Faulty sequencing may manifest itself in a variety of ways, most of which are unknown and the subject of considerable speculation. Many implementations will treat the data at face value, canceling accounts or disposing of perishable products which are apparently dated to 1900 rather than 2000.

Results of Y2K

Some applications may simply lock up if faulty mathematical logic such as negative numbers are introduced. Other applications may go to default values. Some implementations may continue to perpetuate the data error, compounding the error at each iteration of the date dependent mathematical computation. The results could be seriously damaging to maintaining the integrity of any automated information system.

Any device that contains a microprocessor or a microcontroller dependent on a timing sequence may encounter Y2K problems, as may a variety of software systems. Microcontrollers, which are pervasive in things like stop lights and automatic door locks, are microchips that control events by executing a series of instructions. Microprocessors, found in computers, communications equipment, building security systems, elevators, cash registers, and medical equipment, are microchips that control events by executing a series of instructions based on inputs received, or it makes decisions after processing data.

Fixing the Y2K bug is complicated by the fact that computer hardware, operating system, applications, and interfaces system components are interdependently and inextricably intertwined. Date dependent software may be obscurely buried among millions of other lines of code of varying complexity. So, in order to fix the problem, all the date dependent areas in each system component must be identified and adjusted. Failing to correct even a single incident of code could compromise the entire system.

Nuclear War Implications

The Y2K Problem has attracted growing attention in the computer and commercial sectors, but it is only in recent weeks that the potential implications of this problem for the danger of nuclear war have become public. Because of the secrecy and sensitivity of strategic warfighting systems, there are currently few definitive answers, but many important questions that must be addressed in coming months by the nuclear weapon states.

(Continued on page 3)

FAS FUND

The Federation of American Scientists Fund, founded in 1971, is the 501 (c)(3) tax-deductible research and education arm of FAS.

Frank von Hippel, Chairman **Jeremy J. Stone, President**

The *FAS Public Interest Report* (USPS 188-100) is published bimonthly at 307 Mass. Ave., NE, Washington, D.C. 20002. Annual subscription $25/year. Copyright © 1998 by the Federation of American Scientists.

Periodicals Postage Paid at Washington, D.C.

POSTMASTER: Send address changes to FAS, Public Interest Rep., 307 Massachusetts Avenue, NE, Washington, D.C. 20002.

FAS

Chairman: CARL KAYSEN
Vice Chairman: ROBERT McC. ADAMS
President: JEREMY J. STONE
Secretary: PRISCILLA J. McMILLAN
Treasurer: MICHAEL MANN

The Federation of American Scientists (FAS), founded October 31, 1945 as the Federation of Atomic Scientists by Manhattan Project scientists, engages in research and advocacy on science- and-society issues, especially global security.

Current war and peace issues range from nuclear war to ethnic conflict and from nuclear disarmament to arms sales; sustainable development issues include disease surveillance, climate modification, poverty, food security and environment. FAS also works on human rights of scientists and on reductions in secrecy.

The considerable uncertainties as to the impact of the Y2K problem on society generally are vastly magnified in the nuclear context. Contemplating the probable effects on society generally, prognosticators anticipate that the impact of the Y2K problem will be somewhere between annoying and catastrophic. The range of uncertainty of the impact of Y2K on nuclear weapons is even greater, ranging between barely noticeable and literally apocalyptic.

While many nuclear-related information systems will surely be fixed well in advance of the new millennium, at present this is a conjecture rather than a matter of public record.

Complex Systems Make Compliance Difficult

In principle, the STRATCOM and USSPACECOM operating environments, as well as those of supporting intelligence activities, represent discrete highly-visible mission-critical implementations which are obvious candidates for robust Y2K compliance. In practice, this strategic nuclear warfighting infrastructure is a vast system-of-systems that constitutes the single most complex automated information system currently in existence. In June 1998, Fred Kaplan reported in the Boston Globe that a 1993 test of missile warning systems for Y2K compliance produced a shutdown of the system.

In principle, many Y2K problems should solve themselves through the phase-out of older systems which are most vulnerable to Y2K, and most difficult to fix. Roughly half of DoD's desktop computers, generally those of more recent vintage, have been found to be Y2K compliant. However, in practice, nuclear warfighting commands will enter the new millennium using at least some systems that date to the 1960s. For example, the new Defense Message System (DMS) is being phased in to replace the Automated Digital Network (AUTODIN) which dates to the 1960s, but due to problems with implementation of multi-level security in the new DMS, USSTRATCOM will continue to use the elderly AUTODIN system past the end of the millennium.

What will happen to American nuclear forces on the first day of the new millennium? Probably nothing. The most commonly encountered Y2K glitches will almost certainly consist of minor annoyances for system operators that pose little risk to the rest of the world. And more significant system failures would almost certainly be fail-safe rather than fail-deadly: Y2K is far more likely to prevent missiles from launching when ordered, than to cause missiles to launch themselves un-ordered.

The implausibility of the most compelling scenario—missiles leaping unbidden from their silos the second the new millennium dawns—should not diminish concerns about the risk of accidental nuclear war resulting from the Y2K problem. Complex systems unavoidably display unpredictable emergent properties. The normal vagaries of the Windows 95 operating environment that are the daily torment of desktop computer users are but a dim premonition of the potential for vastly more complex nuclear command and control systems to exhibit "undocumented features."

American strategic command and control systems will experience unprecedented stress during the year 2000, due both to unresolved internal Y2K problems, and Y2K back-contamination from other system interfaces. The precise nature of this stress is difficult to anticipate at this time, and may be difficult to diagnose at the time. Concerns about Y2K will surely complicate the normally challenging fault isolation

Interface Interference

Strategic bombers now assigned to Air Combat Command are largely tasked to perform conventional missions. Along with other forces, these units are now linked through the new Global Command and Control System (GCCS), the automated information system which supports force-wide deliberate and crisis planning. The inherent complexity of these systems and existing interoperability problems may be further complicated by Y2K interface problems. Of the roughly 100 major information systems involved in theater air and missile defense operations, nearly half are not currently certified for interoperability. In March 1998 GAO reported that problems encountered in exercises over the past two years "resulted in the simulated downing of friendly aircraft in one exercise and in the nonengagement of hostile systems in another."

process, as every normal glitch will require the added step of seeking a Y2K explanation. This will introduce new levels of doubt and uncertainty concerning system integrity, both for positive control of nuclear attack forces as well as for strategic intelligence and warning systems.

Y2K Compliance of Other Nuclear States

Providing robust assurance that Y2K will not substantially increase the risk of accidental nuclear war requires not only ensuring American Y2K compliance, but also Y2K compliance of the other nuclear weapons states, and assurances of such Y2K compliance.

The Defense Department is not unaware of the importance of this problem, and in early June 1998 Defense Secretary Cohen met with Russian Defense Minister Sergeyev to address the Y2K problem. Cohen noted that "early warning would be important; what happens in the year 2000 with computers if they suddenly shut down, how would they interpret that and how will they react to that." He also noted that the Russians had stated that "they calibrate their computers differently than we do in the United States, in the West, and they don't foresee a problem."

The core of the Y2K risk derives from the more general nuclear danger under current conditions. Despite a variety of force reduction and detargeting initiatives, most of the world's nuclear forces remain on the hair-trigger alert that is a legacy of Cold War fears of a "bolt-from-the-blue" sneak attack. With the end of the Cold War it has become increasingly apparent that such high alert levels are unwarranted, and are in fact contributory to the risk of accidental or inadvertent nuclear war. Standing down from such high readiness levels is long overdue, and should be a high priority for the nuclear weapons states. While some might suggest that Y2K concerns mandate the immediate de-alerting of nuclear forces, in the real world these arguments are unlikely to move decision makers, though they would almost certainly contribute to public alarm.

For Further Reading

For more information on Y2K issues, visit the FAS website: http://www.fas.org/2000/y2k
or Dr. Ed Yardeni's CyberEconomics webpage: http://www.yardeni.com/cyber.html

Such public alarm would not be entirely misplaced, as sustaining high alert levels would seem to be directly contributory to the nexus between the Y2K problem and the risk of accidental or inadvertent nuclear war. Initially presenting Y2K glitches would almost certainly have the consequence of rendering information systems inoperable to a greater or lesser extent. But the mandate to sustain very high alert levels could impel system operators to improvise technical implementations and operational procedures. Normally contingency procedures may also in turn manifest Y2K anomalies. System integrity may also face coincidental compromises from a variety of factors, ranging from solar-storm induced communications outages to heightened security due to warnings of terrorist attacks.

Difficult Choices

At this point, operators and commanders may face difficult choices between reducing the overall readiness of nuclear warfighting forces, and making changes in the operational practices of those forces to compensate for degradations in command and control capabilities. Such difficult choices would not be made in isolation, but might simultaneously confront system operators in more than one country, creating complex interactions among partially degraded command and control networks and nuclear warfighting forces. Random events, such as solar storms or sounding rocket launches, could further perturb the situation. In practice, such tightly-coupled interactions are all rather unlikely, given the poor track record of the American intelligence community in monitoring the alert status of Soviet forces during the Cold War. But technological "accidents" seem inexorably to result from seemingly trivial technical problems compounding in unlikely ways to produce surprising and occasionally catastrophic results.

There is obviously considerable potential for public alarm here, whatever the actual underlying risks of Y2K leading to accidental nuclear war. One obvious step would simply be to take all nuclear forces off alert, pending robust resolution of any lingering doubts concerning Y2K compliance. While there are certainly many compelling reasons for de-alerting nuclear forces, it would probably be counterproductive to suggest that the Y2K problem mandates immediate de-alerting as the only prudent step for ensuring that the new millennium dawn with a nuclear apocalypse.

Steps Needed to Address Y2K Issues

Several relatively straightforward steps are clearly called for, both to address the actual potential for the increased risk of accidental nuclear war due to Y2K, and to address potential public concerns.

The first step would be a continuation of Awareness Phase activities to include familiarizing information system operators with likely symptoms of Y2K non-compliance, to reduce the degree of confusion or alarm that may accompany unexpected system performance. Because of the high level of vigilance that currently attends strategic command and control operations, care must be taken to ensure that Y2K-induced glitches are not mistaken for malevolent assaults by adversaries.

The second step would be implementation of robust contingency planning detailing alternate means of fulfilling affected information system missions in the event of a critical failure induced by Y2K problems. These should include defaulting functions to appropriate manual operation if needed. It is exceedingly unlikely that Y2K problems would induce the generation of apparently valid launch authorizations, given the complexity and redundancy of existing launch authorization mechanisms and procedures. Nonetheless, given equally remote likelihood of a "bolt-from-the-blue" sneak attack, a requirement to verbally authenticate apparently valid launch orders would provide an additional risk reduction measure.

The third, and most critical, step would be direction from the National Command Authority that, as a matter of national policy, system operators and commanders should accept reductions in alert status and warfighting readiness pending resolution of Y2K induced problems, rather than attempting to sustain high alert rates through implementing or improvising contingency plans that could contribute to increasing the risk of accidental or inadvertent nuclear war. These are not priorities that can be chosen by commanders on the scene, particularly when faced with puzzling or alarming system failures possibly induced by Y2K problems.

The next step would be the completion of an independent Y2K compliance audit of STRATCOM, USSPACECOM, and supporting intelligence activities. While the full report would surely be highly classified, some portion of the audit and Y2K compliance certification could surely be released to the public, confirming that the American strategic command and control system is Y2K compliant, and that robust measures are in place to counter Y2K interface problems caused by potentially non-compliant American systems.

Y2K Certification from Nuclear States

An American working group, consisting of participants from nuclear weapons agencies and agencies concerned with information assurance issues, should be established to make formal Y2K compliance presentations to all the other nuclear states (declared and otherwise). The focus of these activities would include a rehearsal of the nature of the problem, representations concerning American Y2K compliance initiatives, offers of technical assistance, and a request for reciprocal compliance certification.

Extending Secretary Cohen's initial June meetings, the United States should formally request that all nuclear weapons states implement formal Y2K compliance certification for their nuclear command and control systems. This compliance certification should be validated by some independent entity within each country, consistent with domestic Y2K compliance procedures. The final outcome of this process would be formal public statements by the nuclear weapon states of their Y2K compliance.

None of these initiatives can guarantee the eradication of the millennium bug from nuclear command and control systems, just as there is no guarantee against nuclear war other than the elimination of nuclear weapons. But systematic initiatives taken today could significantly contribute to reducing the risk of accidental nuclear war, and certainly contribute to reducing public anxieties concerning this risk. □

DoD's Five Phase Y2K Plan

Information systems have become increasingly central to military planning and operations across the spectrum of conflict, including nuclear warfighting. The fact that the military is *dependent* on computers does not mean, however, that military computers are *dependable*. During the Cold War computer malfunctions produced false alarms of missile attacks, and during the Gulf War computer malfunctions contributed to the failings of the Patriot anti-missile system. More recently, tests of the new GCCS demonstrated serious flaws in the interfaces between its various distributed components.

In April 1997 the Defense Department issued its Year 2000 Management Plan, which included a five phase approach for addressing the Y2K problem: Awareness, Assessment, Renovation, Validation and Implementation.

Phase Deadlines Not Met

The Awareness Phase is intended to discover the scope of the problem affecting organizations. Before this phase can be exited, all assets need to be inventoried and the hazards associated with them identified. This phase was intended to be completed by March 31, 1998, but as of this date DOD still did not have a complete inventory of systems, or even a consistently applied definition of what constitutes a "system." As of early 1998 the National Reconnaissance Office (NRO) and the National Security Agency (NSA) had not completed their inventory of critical system interfaces.

In the Assessment Phase a determination of asset compliance is made, needs are identified, resources are prioritized, fix actions are planned and contingency actions are developed to handle data exchange issues, lack of data, and bad data. Because of variations, every system must be individually tested to assess compliance. In addition, information systems interface with each other, running the risk that interaction with noncompliant systems can introduce or propagate Y2K errors to otherwise compliant systems.

DoD is still assessing systems, despite the fact that under original plans this phase was supposed to be completed in June 1997. As of early 1998 NRO and NSA had not completed the assessment phase for equipment such as personal computers and telecommunications equipment. The Defense Intelligence Agency and Air Force Intelligence had not completed their assessment of whether their system interfaces were Y2K compliant. The Assessment phase is now intended to be completed by November 30, 1998, by which time systems would be selected to be renovated, replaced, or retired.

The Implementation Phase, scheduled to be completed by December 31, 1998 for mission critical systems and by March 31, 1999 for all other systems, implements the corrective actions planned in the previous phase and all contingency actions are documented. Systems scheduled for repair move to the Renovation Phase. In the final phase, Validation, all systems are tested to assure they will function through January 1, 2000.

GAO Review Finds DoD Lacking

The General Accounting Office has conducted reviews of Y2K activities at DoD, Army, Navy, and Air Force headquarters, three Defense agencies, and three central design activities. GAO concluded that DOD lacks complete and reliable information on systems, interfaces, equipment repairs, and the cost of its correction efforts.

The Defense Department has an inventory of approximately 9,300 systems subject to Y2K compliance evaluation. The Defense Integration Support Tools (DIST) database is the backbone DOD management tool that tracks these systems and their associated 112,000 programs. On February 4, 1998 at the urging of the NSA, DIST was switched from an unclassified implementation to a secure SECRET environment, to protect possible DOD information and weapons systems vulnerabilities caused by Y2K.

As of early 1998 the Defense Department and Navy headquarters did not validate Y2K compliance information received from subordinate components. The Army and Air Force audits disclosed significant discrepancies between reported and actual Y2K compliance. *–JEP* □

Status of DoD Y2K Compliance in Nuclear War-Fighting Systems

The status of Y2K compliance in the American strategic nuclear warfighting community is not presently a matter of public record. There are no unclassified materials that provide a systematic assessment of the status of Y2K efforts, critical intelligence or warning support. at US Strategic Command (STRATCOM) at US Space Command (USSPACECOM), their subordinate components, or other intelligence and communications organizations (such as NRO or NSA).

The extent of this uncertainty, and a glimpse at the current situation in the nuclear arena, is provided by the April 1998 release of the Joint Staff Year 2000 Data file. This compendium of nearly a thousand systems includes 90 associated with USSPACECOM, and another 121 systems associated with STRATCOM. While the basis for inclusion in this database is unclear, it appears to be either highly selective or extremely incomplete, since the inventoried systems associated with intelligence agencies represent only a small fraction of the publicly known systems, which in turn are surely only a very small fraction of the "systems" (however that term might be defined) that pose potential Y2K problems.

STRATCOM Inventories Systems

STRATCOM systems listed in the Joint Staff database range from the Route Analysis and Penetration System (ROPES), the Strategic War Planning System (SWPS), to the Terrain Contour Map (TERCOM) Placement & Evaluation Program. USSPACECOM systems include the Automated Tracking and Monitoring System, the NORAD Forward Automated Reporting System Upgrade, and the Command Center Processing and Display System Replacement. The difficulty of defining what constitutes a "system" and the importance of assessing interfaces between "systems" is apparent in comparing the STRATCOM and USSPACECOM inventories in the Joint Staff database. Many of the USSPACECOM entries correspond to individual operating locations—each tracking radar site is counted as a "system." The STRATCOM inventory apparently consists almost entirely of software modules implemented at USSTRATCOM headquarters. While these differences surely reflect differences in the mission and organization of these two commands, presumably much of the routine administrative functionality of the STRATCOM systems have counterparts at USSPACECOM which are simply not called out in the latter's database inventory.

Systems Beat Assessment Phase Deadline

Many (but not all) STRATCOM systems are listed as having been certified as compliant with the Assessment Phase of DoD's five-phase compliance effort as of 31 March 1997, a few months prior to DoD's initial goal, and well ahead of the current DoD deadline. USSPACECOM systems were generally certified as compliant with this phase as of 02 October 1997.

As of April 1998, however, essentially no STRATCOM or USSPACECOM systems was reported to have passed the more important, and difficult, subsequent phases of Renovation, Validation or Implementation. The DoD goal for completion of the final Implementation Phase for mission-critical systems is 31 December 1998. If these nuclear warfighting commands have made substantial progress towards this goal, much less the critical intervening Renovation and Validation phases, they had apparently not reported this to the Joint Staff as of nine months prior to deadline. *–JEP* □

Will Federal Agency Systems Meet the Deadline for Y2K?

According to a report by Rep. Horn, Chairman of the House Government, Management, Information and Technology Subcommittee, 10 of the 24 major federal agencies claimed they will be done in time. Mr. Horn observed that based on current rates of progress, some of the remaining agencies will not have their mission-critical systems ready for the year 2000 until: Energy and Labor Departments - 2019, Defense Department - 2012, Transportation Department and Office of Personnel Management - 2010. (*From Dr. Ed Yardeni's website*)

Visit to STRATCOM

At the invitation of its Commander, General Eugene Habiger, a five person FAS delegation visited the Strategic Command (STRATCOM) Headquarters at Offutt Air Force Base in Omaha, Nebraska. While there, FAS received a briefing and, in turn, described the FAS proposal to reduce START levels to 1,000 strategic warheads, while de-MIRVing the U.S. and Russian forces (and securing the de-MIRVing of the forces of Britain and France). This article is based on information received there and elsewhere.

Disarmament and Presidential Guidance

If and when the Russian Duma ratifies START II, the biggest remaining obstacle to further disarmament will lie in the U.S. Presidential guidance for strategic forces, Presidential Decision Directive 60 (PDD60) . Here are outlined, in general terms, what U.S. policy requires of strategic forces. Currently this requires more than 2,000 deployed U.S. nuclear warheads.

This is more than is necessary. For example, notwithstanding the Sino-Soviet split of 1954, and the ability of missiles to be retargeted instantly, the current guidance is interpreted to mean that the United States be able to target both Russia and China *simultaneously*. It also appears to require that the U.S. be able to "dig out" and destroy about 18 highly hardened underground command posts in Russia—even though some of these, at least, would harbor the decision-makers required for negotiations to halt the war.

(L-R) Theodore Hardebeck, Alton Frye, Townsend Hoopes, Eugene Habiger, Jeremy J. Stone, Matthew Bunn, and Charles Ferguson

PDD60 requires that the U.S. target large numbers of Russian military bases as if they were poised, as they once were, to invade Western Europe, instead of being manned now by often unpaid, and sometimes starving, Russian recruits. It requires that the strategic force be able to strike large numbers of Russian industrial targets—making somewhat irrelevant U.S. guidance to avoid metropolitan areas since the metropolitan population would eventually die anyway without survival industry.

New Guidance for Reduced Forces Needed

The current STRATCOM command has told the Administration that it will require new guidance if projected START III levels of 2,000-2,500 are to be reduced. Having watched the force come down from more than 10,000 deployed strategic weapons, no doubt many STRATCOM officials feel that 2,000 warheads at the ready would be a skeleton force, every bit of which is required to maintain "deterrence as we know it."

In fact, however, 2,000 deployed strategic nuclear warheads, even 1,000, is an enormous number, capable of destroying Russia many times over. Since Russia is no longer communist, and lacks both the ideology and the economy to mount a world threat, why are so many U.S. weapons being kept at the ready? Instead, we should mothball them through disarmament with a view to getting Russian forces down in number and off alert—something that is not possible while their weapons are being targeted by us with such effectiveness.

Deterrence as STRATCOM knows it seems to be tied up with the notion of "extended deterrence" which appears on many graphs shown at STRATCOM. Extended deterrence, a term invented by Herman Kahn, was distinguished from ordinary deterrence and was sometimes called by him "Type II" deterrence. According to the theory, an attack upon ones own country could be credibly deterred by threats to reply in kind. But deterrence of an attack upon allies required, for its credibility, being able to substantially disarm the forces of the other side.

Without this ability, the U.S. who initiated a nuclear attack on behalf of an ally, would fear having its own country attacked in response. According to informed officials, the US does not "depend" upon extended deterrence and it will, in any case, "run out at low enough START levels", i.e. at low START levels extended deterrence will cease to be an option.

The proper guidance, today, would embody policy goals of simple deterrence and flexibility. This would require a U.S. strategic force of no more than a few hundred warheads targeted simultaneously on nothing and everything. Based on a revised guidance, which would require less than a year to organize, START could continue a steady decline rather than the leveling off indicated by the current START III goal.

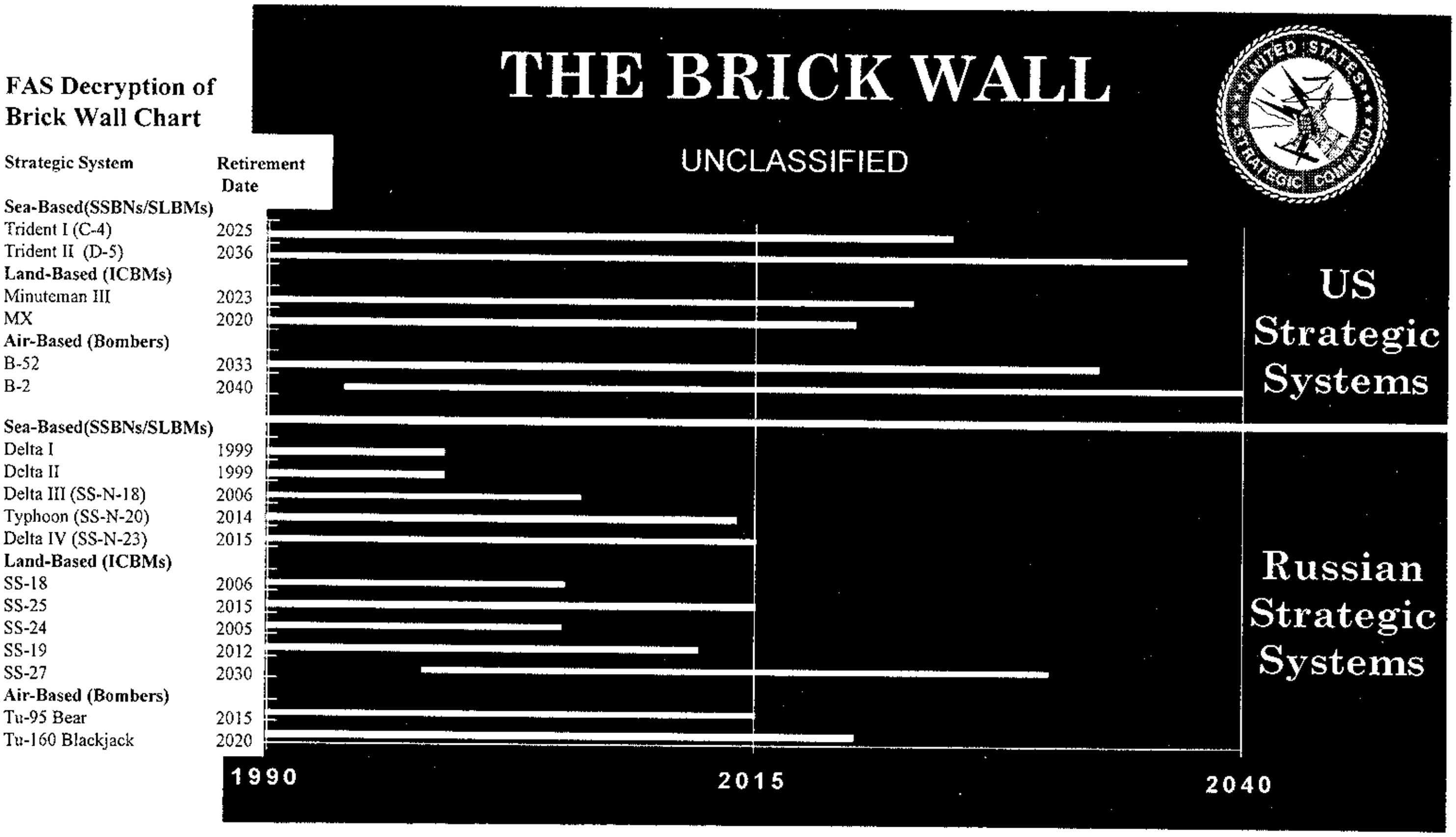
Today, however, with the Russian strategic force in some decline, and our highly accurate Trident submarines poised to attack from off the Norwegian coast, (only 15 minutes of missile flight time), even such an experienced expert as Senator Sam Nunn, former Chairman of the Senate Armed Services Committee, has written that "from the conservative perspective of the Russian military, the only way to preserve Russia's deterrent credibility is to declare—as Russia recently did—its readiness to 'launch on warning'."

Moreover, in the calculations describing the outcome of a U.S. attack, STRATCOM uses the dangerous assumption that any residual Russian missiles will be targeted on U.S. forces rather than on U.S. cities—something that could, in any case, be changed by the Russians quickly in a crisis.

On May 12, for the third time, President Yeltsin referred to the possibility of going far below 2,000 warheads by asserting that START III could see "even deeper cuts—of two or three times" beyond START II's limits of 3,000 to 3,500. We should be willing to go as low as the Russians will. And if it requires changing the current guidance, so much the better. □

Nuclear Arms: Reduction or Replacement?

Charles D. Ferguson



FAS Decryption of Brick Wall Chart

Strategic System	Retirement Date
Sea-Based(SSBNs/SLBMs)	
Trident I (C-4)	2025
Trident II (D-5)	2036
Land-Based (ICBMs)	
Minuteman III	2023
MX	2020
Air-Based (Bombers)	
B-52	2033
B-2	2040
Sea-Based(SSBNs/SLBMs)	
Delta I	1999
Delta II	1999
Delta III (SS-N-18)	2006
Typhoon (SS-N-20)	2014
Delta IV (SS-N-23)	2015
Land-Based (ICBMs)	
SS-18	2006
SS-25	2015
SS-24	2005
SS-19	2012
SS-27	2030
Air-Based (Bombers)	
Tu-95 Bear	2015
Tu-160 Blackjack	2020

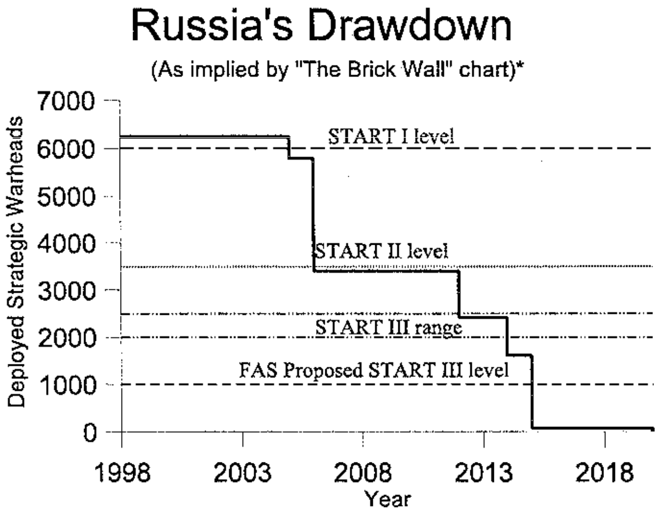
"The Brick Wall" chart above, obtained from the United States Strategic Command (USSTRATCOM), estimates the dates when Russia and the US could lose confidence that their aging nuclear strategic systems will perform reliably within design specifications but does not identify the specific systems. To the left of this chart, FAS decodes the unclassified chart and specifies these systems, based on publicly available, unclassified sources. Unless the START arms control process reduces deployed warhead limits sufficiently, making these expenses unnecessary, each side will be tempted to purchase new systems, costing billions of dollars.

Further using the deciphered "Brick Wall" chart, FAS plots, in a derived "Russia's Drawdown" graph, the number of Russian deployed strategic warheads as a function of time, indicating when these deployed warheads fall below START I, II, and III levels. "The Brick Wall" chart assumptions imply that Russia cannot maintain the START I level beyond 2006, the START II level beyond 2012, the START III range beyond 2014, or the FAS proposed START III level beyond 2015 without purchasing additional missiles, submarines, and bombers.

"The Brick Wall" chart assumptions do not imply strong Russian interest in reducing START III levels, but many analysts would consider these assumptions too optimistic. For instance, Bruce Blair, an American analyst, and Lev Volkov, a Russian analyst, have estimated that 700 to 1,000 deployed warheads seem a likely level by 2007, *even factoring in replacements*. In this case, Russia has incentive to agree to deeper cuts beyond the 1997 Helsinki START III levels. Otherwise, the US and Russia confront a deployed strategic imbalance with various political and strategic implications.

The US also faces tough choices twenty to thirty years from now. For instance, barring further reductions or political and strategic changes, the US will probably replace its most survivable system—the Trident submarine—in the next twenty-five years. Assuming the START II notional force of 14 submarines, the replacement cost would run about $47.6-57.4 billion. (All costs are in constant 1996 dollars.) This immense figure only applies to one leg of the triad. Additionally, the US would likely spend $17 billion to reproduce 500 Minuteman III ICBMs, $3 billion to rebuild 66 B-52H bombers, and $52 billion to replace 20 B-2 bombers.

□



**This graph assumes that all units of each strategic system endure until their retirement date and are not replaced, whereas, in reality, many units will require replacement earlier and may or may not be replaced. Also missiles, bombers and submarines may be kept beyond their service life.*

Kosovo: Unleashing the Diplomatic Sword

Jeremy J. Stone & FAS Council Member Burns H. Weston

Unless something new is added, the ethnic Albanians of Kosovo, inside the Serbian Republic of the former Yugoslavia, may be further brutalized as their ill-armed and amateurish Kosovo Liberation Army (KLA) is crushed by the well-armed and merciless Serbs. The Serbs have even less empathy for the Kosovar Muslims (who are not Slavs) than they had for the Bosnian Muslims (who are) and can be expected to be even crueler in Kosovo. What can be done for the Kosovars?

Force is one obvious possibility. In principle, NATO intervention could change the situation, but NATO seems unprepared for decisive intervention. And the prospect of NATO intervention could cause more harm than good if it inspired the Kosovars to a revolt that, in the end, was not supported.

Is there a *diplomatic* threat that could help stimulate constructive negotiations? Consider the threat by some organizations and states of urging self-determination for Kosovo or diplomatic recognition of Kosovo as an independent state. Such a threat might encourage serious negotiations by Serbia on a new autonomy for Kosovo and/or discourage it from outrageous acts of violence. And because of its promise for fulfilling the goals of the Kosovars, it might also encourage the KLA to cease provocative attacks that only stimulate Belgrade's overreaction. Indeed, this cessation could be a condition of those contemplating diplomatic encouragement.

Kosovo the Virtual Republic

History justifies a diplomatic strategy of permitting self-determination in this particular case rather more than in many others. Kosovo, though part of Yugoslavia's Republic of Serbia, had so much autonomy within the Yugoslav Constitution that it had an effective veto in the Yugoslav parliament over Serb actions in Kosovo. Thus Kosovo was, really, in all but name, a republic within the Yugoslav federation, like Slovenia, Croatia, Bosnia and Macedonia. (This autonomy was withdrawn by the Serb authorities in 1989 after the Kosovars sought, no doubt as a route to later secession, just such republic status.) Had it been recognized as such, it would have been accorded, by the international community, the right to secede as all the other Yugoslav republics, except Montenegro, have.

Stone (L) with Ibrahim Rugova

And since the Federal Republic of Yugoslavia has effectively dissolved, reduced from six Republics to two, there is the valid question of whether other constituent parts of Yugoslavia—even if not "republics" but only "autonomous regions"—have the right to self-determination.

The reluctance of nation states to threaten and/or offer recognition to Kosovo stems, at bottom, from self-interest—all nation-states have borders, and many have dissident factions. Russia with its Chechnya, and China with its Tibet and its Taiwan are very sensitive to this issue. And a specific problem exists immediately adjacent to Kosovo, where ethnic Albanians in Macedonia, though unrepressed and living in an uneasy harmony with the other Macedonians, might be encouraged, in time, to try peacefully to separate themselves from Macedonia, probably to join a greater Albania.

Setting Precedents in Diplomacy

Traditional diplomatic practice requires a demonstration of control over territory by those desiring recognition. But this did not prevent the United

States from recognizing Baltic States in exile or the U.N. from continuing to recognize in Cambodia the overthrown Khmer Rouge. Nor did it prevent the German government from initiating recognition of Croatia before Croatia had demonstrated control of its territory.

Indeed, motivating Serbian leaders in its capital, Belgrade, was the rationale used by Germany to other NATO states for its early recognition of the independence of Croatia, viz., that recognition by some would strengthen the hand of those states asking Belgrade to compromise. This reasoning might make even more sense now. And it would help the Kosovar's President, Ibrahim Rugova, who is losing support to the KLA, by showing some kind of light at the end of Rugova's peaceful tunnel.

The international community of 185 states with its rights of recognition is, in effect, the jury in what amounts here to a claim, in a divorce trial, of irreconcilable differences. Perhaps the time has come for them to begin to vote, as a signal of what they think should be done.

How dangerous a precedent would this set? In general, a world in which some, but not all, sovereign states recognize the independence of dissident parts of other states might provide continuing pressure upon repressive states. It might even legitimize external assistance to the dissidents, without producing destabilizing expectations of military intervention.

Accordingly, perhaps the time has come for a conference, resolution, or pronouncement by interested states discussing the conditions under which these states would recognize as only Albania has the claim of independence of Kosovo. This would unleash the diplomatic sword.

□

In the 1998 FAS election for Council, Ruth S. Adams, formerly of the MacArthur Foundation, Harold Feiveson of Princeton University and Gregory van der Vink of the IRIS Consortium were elected replacing Rosemary Chalk, Val Fitch and David Hafemeister. Kenneth Luongo of the Russian-American Nuclear Security Advisory Council (RANSAC) was appointed to the FAS Fund Board.

FAS PUBLIC INTEREST REPORT (202) 546-3300
307 Mass. Ave., N.E., Washington, D.C. 20002
Return Postage Guaranteed
July/August 1998, Volume 51, No. 4

□ I wish to join FAS and receive the newsletter as a full member.
Enclosed is my check for 1998 calendar year dues.

□ $25	□ $75	□ $150	□ $1000	□ $15
Member	Supporting	Patron	Life	Student/Retired

Subscription only: I do not wish to become a member but would like a subscription to:
□ FAS Public Interest Report - $25 for calendar year.

□ Enclosed is my tax deductible contribution of _______ to the FAS Fund.

NAME AND TITLE ______________________________
Please Print

ADDRESS ______________________________

CITY AND STATE ______________________________
Zip

PRIMARY PROFESSIONAL DISCIPLINE ______________________________