



# National Security Law Report

Volume 19, Number 1 STANDING COMMITTEE ON LAW AND NATIONAL SECURITY Winter 1997

## Ambassador Saito Discusses U.S.-Japan Security Relationship

*His Excellency Kunihiko Saito, Ambassador of Japan to the United States since 1995, addressed a Standing Committee breakfast on December 19, 1996. During nearly four decades of service within the Ministry of Foreign Affairs, Ambassador Saito has served as Director-General of the Treaties Bureau (the equivalent position to the Legal Adviser to the U.S. Department of State), Ambassador to Iran (1989-91) and as Vice-Minister for Foreign Affairs. His prepared remarks follow.*

I am honored to be here to speak to this prestigious organization. This morning I am going to speak about the Japan-U.S. security relationship and the future. People say that the Cold War is over, and I think it's inaccurate. Maybe it is true in Europe, where all countries are trying to become democratic countries with market economies, but the situation in Asia, particularly East Asia, is different. We still have North-South confrontations on the Korean Peninsula. We have tensions over Taiwan. Unfortunately, tensions and uncertainties still exist in these Asian regions.

We believe that the Japan-U.S. security relationship is one of the most important factors in this region. It provides stability, safety, and therefore prosperity to all of the countries of this region.

The presence of United States forces in Japan and in Korea are welcomed by all Asian nations except North Korea. You may say that China has

*Continued on page 2*



*Japanese Ambassador Kunihiko Saito speaks to Standing Committee breakfast group.*

## NSA Director Minihan

### National Security Implications of the Information Age

*On January 16, 1997, the Standing Committee heard from Lieutenant General Kenneth A. Minihan, USAF, the Director of the National Security Agency/Central Security Service (NSA/CSS). A former Air Force Assistant Chief of Staff for Intelligence and Director of the Defense Intelligence Agency, General Minihan has a distinguished military record dating back to the Vietnam war. His prepared remarks follow.*

Thank you for the opportunity today to share my perspectives with you on the single most pressing need of the information age — information systems security.

Information systems security is a key leadership issue for our time. We won the cold war. Now we're transitioning to a new century, a century which holds tremendous potential for far-reaching changes driven by technology. As a law-abiding nation, we will need to accommodate the new realities of the information age within the framework of our laws. Information systems security — or Infosec — will be a primary focus of this effort.

*Continued on page 4*

#### Inside

- 3 Book Review—Weinberger's *Next War*
- 4 Calendar of Events
- 8 CEELI Seeking Public Service Lawyers
- 10 National Security Agenda

## Ambassador Saito . . .

*Continued from page 1*

expressed its concern over Japan-U.S. security ties, and this is true, particularly after the joint declaration issued in April following the summit meeting in Tokyo between President Clinton and Prime Minister Hashimoto. China expressed its "concern" about the Japan-U.S. security treaty. We have since then been trying to explain to China that this treaty is purely of a defensive nature and is not intended against any country. I personally believe that China in a way appreciates a close Japan-U.S. relationship, including Japan-U.S. security ties.

The people in Asian countries, particularly in Korea and China, have serious, vivid memories of what happened in the 1930s and '40s, and they are wary of the possibility of a revival of Japanese militarism. We Japanese feel certain that there is no such possibility, but in the eyes of other Asian peoples, the Japan-U.S. security treaty serves to prevent Japan from going towards the direction of becoming a big military power.

The Japanese public largely supports the Japan-United States security treaty, including the presence of U.S. bases in Japan. According to published polls, usually 60 to 70 percent of the people support U.S.-Japan security ties, including the presence of United States forces in Japan. We realize that without the security umbrella of the United States, our post-war economic recovery would have been impossible.

You may ask, if the Japanese public so firmly supports close security ties with the United States, why were the people of Okinawa so upset when the unfortunate incident of the rape of a young girl occurred last September. This reflects a very complex feeling of the people of Okinawa that has a deep root in their history. Okinawa used to be autonomous before modern times; and, during World War II, Okinawa was the only place in Japan where actual fighting took place, and more than 100,000 people were killed. And Okinawa had to remain under U.S. administration twenty years after Japan regained independence in 1952. Today, 75 percent of U.S. bases are concentrated in the small island which constitutes only one percent of the total area of Japan. So there is a strong sense of being discriminated against, a strong sense of unfairness, and this feeling was stirred up, brought to the surface, by this incident last September.

The United States Government, and my Government too, reacted very quickly and formed a special group to look at the situation in Okinawa and worked hard, particularly under a very strong initiative of

Secretary Perry, and we came to agreement on the second of this month (December 2, 1996), on a wide range of measures to improve the situation in Okinawa, including more than a 20 percent reduction of U.S. bases in Okinawa with the return of one of the two huge air bases in Okinawa. We expect that these measures will greatly improve the situation in Okinawa and will greatly improve the feelings on the part of the people of Okinawa.

Prime Minister Hashimoto came into power in January of (1996), and has been in power for nearly one year, and during that year President Clinton and Prime Minister Hashimoto met five times. I was able to attend all of those five meetings, and they seemed to get along very well together. Most recently, they met in Manila in November, just after both were reelected. Prime Minister Hashimoto was reelected only a few days before he went to meet with President Clinton. They agreed that the Japan-U.S. security relationship continued to be the most important factor for stability and safety of Asia and the Pacific region. Of course, there is a lot of work to be done, we have to work out the details to implement the agreements reached on Okinawa. We are now reviewing our defense guidelines to make the security arrangements more effective, but I think we have made big progress here in 1996.

I would like to mention one additional factor, a positive factor, and that is that Japan is becoming more and more aware of its responsibilities in maintaining peace. Japan has benefited greatly from the prosperity after World War II, and has become a big economic power. People are beginning to realize that we cannot continue to go on harvesting, so to speak, the fruits of peace, while leaving the responsibility of maintaining peace to other countries, particular to the United States. Of course, Japan in the past has been trying to contribute to peace by financial means, but we now believe it is not sufficient

*Continued on page 5*

**Paul Schott Stevens**

*Chairman, Standing Committee on Law and National Security*

**Holly Stewart McMahon**

*Staff Director*

**Robert F. Turner**

*Editor*

The *National Security Law Report*, which is published eight times a year, contains articles concerning the law relating to the security of the Nation and associated topics. The *National Security Law Report* is sponsored by the ABA Standing Committee on Law and National Security. The views expressed in this publication are not necessarily those of the Standing Committee or the American Bar Association. Comments or original articles should be directed to Professor Robert F. Turner, Center for National Security Law, University of Virginia School of Law, 580 Massie Road, Charlottesville, VA 22903-1789.

Copyright © 1997 American Bar Association, ISSN 0736-2773.

## BOOK REVIEW

### *The Next War*

by Caspar Weinberger & Peter Schweizer  
Washington, DC: Regnery Publishing, Inc., 1996  
Pages: 470 Price: \$27.50

Reviewed by Richard E. Friedman

Former Secretary of State Warren Christopher warned in his recent valedictory of "a new isolationism" emerging in Congress. Christopher warned that the Department of State cannot sustain additional budget cuts without jeopardizing America's foreign policy and world leadership. The response by skeptical members of Congress has been to point out that, in this period of fiscal austerity, all government expenditures are being scrutinized and many agencies are making do with less. Both positions are essentially correct.

United States leadership is projected through a combination of diplomacy, economic aid, and military power. The U.S. military budget has been reduced steadily for over ten years. The administration and Congress continually face the same difficult choice: cut readiness or postpone modernization. Neither option is attractive. There is broad consensus that U.S. military capability—readiness today and combat effectiveness tomorrow—is in a prolonged decline.

The United States government has attempted to realize a "peace dividend" in the State Department's budget, just as it has in the Pentagon's budget. U.S. expenditures on foreign aid, foreign affairs agencies, and contributions to international institutions are down 50% in the last decade (adjusted for inflation).

There is no national public constituency for diplomacy per se. Interest groups have their particular concerns—the Israeli-Palestinian peace negotiations, Northern Ireland, humanitarian assistance, and so forth. What is lacking is a broad consensus on the question of whether international leadership is worth the costs to the United States. National strategy, national security, and foreign policy are regarded by many Americans as esoteric matters and the province of bureaucrats and ivory tower visionaries. Polling demonstrates that the American public is uninformed and largely disinterested in American foreign policy objectives. The American foreign policy establishment has not made the case for a renewed investment in diplomacy and aid very effectively. Most Americans do not see the long-term benefits, although many are apprehensive about foreign competition in labor markets (a

further rationale for isolation). Trade policy might be an exception, given that Congress ratified NAFTA despite vocal opposition from economic nationalists. However, the Commerce Department and the U.S. Trade Representative have principal responsibility for trade negotiations and commercial advocacy. The State Department plays a subordinate, albeit important, role.

What explains the paucity of attention to international affairs? The news media are not able to create a demand for international news. In fact, it is quite expensive for the electronic and print media to provide in-depth coverage of foreign affairs. News organizations do not see a return on their investment in maintaining far-flung news bureaus. So, the trend is to present world news in a blink.

In a sense, Members of Congress respond to the same signals. If their constituents do not voice much concern about international affairs, Members of Congress are not going to spend significant capital on foreign policy initiatives. So, there may be no political risk in reducing appropriations for the conduct of diplomacy.

Nevertheless, there certainly are risks associated with de-funding America's capacity to project political and military power around the world. Caspar Weinberger illustrates the risks—vividly—in his fascinating book, *The Next War*. The former Secretary of Defense has devised several scenarios in which the short-term thinking that drives budget decisions today leads to grave crises in the future.

Foreign policymakers and military strategists regularly conduct wargaming exercises. This has been a key part of strategic planning for decades. Built around hypothetical scenarios that include a complex array of variables, wargames call upon participants to assume the role of decision-makers and to live with their decisions as the exercise proceeds. The sessions are valuable experiences for the participants, who sharpen their ability to assimilate information and make tough decisions under time pressure. Wargames also help refine contingency plans for real conflicts and crises.

Mr. Weinberger has structured the book as a series of five hypothetical events in which American interests and security are threatened. The reader has a front row seat to learn, vicariously, how wargames unfold. It is exciting stuff, and there are elements of drama and psychology that lift strategy out of the realm of formal theory.

Mr. Weinberger does not go to Dickensian lengths to develop his characters. There are protagonists and there are villains. They are sketched with an economy of one-liners, and the principal players

*continued on page 4*

## Book Review . . .

*Continued from page 3*

remain constant in each scenario. President St. John is a wimpish, well-born, do-gooder who clearly wishes that he had pursued a career as an investment banker or a golf professional, rather than seek the presidency. He is, however, a two-term president, who serves from 1998-2007. The Secretary of State clearly is in the wrong line of work. The National Security Adviser is a bit uneven, but performs tolerably well. It comes as no surprise that the Secretary of Defense character is all that we can hope for—strong, incisive, resolute, and uncommonly accurate in his evaluations and correct in his decisions.

The first scenario involves an attack by North Korea on South Korea and the expansion of the People's Republic of China's presence in the Pacific region. The second scenario involves Iran's aggression against its neighbors in the region. The third situation involves a meltdown of Mexico's economy and a mass-migration of Mexican citizens across the US-Mexican border. Next, President St. John must deal with the problem of a newly elected, evidently delusional Russian president who believes that he is the Czar incarnate and that theater nuclear weapons are a reasonable way to settle local difficulties. Finally, the United States is confronted with an expansionist Japan's replay of the 1930s and the events preceding Pearl Harbor.

Mr. Weinberger has an agenda. He believes that America has dissipated its strength:

The United States prevailed in all of these [past] conflicts because we could spend our way out of danger. When a threat emerged, we bought time until we were mobilized and able to respond. But that strategy will no longer work. Ballistic missiles and weapons of mass destruction have not only compressed geographical distances, but may also prevent U.S. forces from ever reaching the battlefield. The next war could be over by the time America is fully mobilized.

He claims that the United States' technological superiority is diminishing. The awesome technological prowess that was displayed during the Persian Gulf War was the result of nearly a decade of investment in new weaponry and platforms. Investment in research and development of new military technology is declining, and other states are closing the technology gap. His scenarios illustrate the potential consequences of under-investment in advanced technologies.

Critics may contend that Mr. Weinberger's views are alarmist and that wargaming is a polemical

gimmick. The book's strength is that it challenges the reader—it is actually well-grounded in fact. Whatever views the reader may have, the book contributes to the need for a better informed citizenry.

It has been observed that we do not know what to call the present period, so we affix the term "post" to the Cold War era. As we navigate through this period of transition, we still need take our bearings. Caspar Weinberger has pointed out some hazards and identified what he believes is a safer course—even though our destination is only vaguely known.



## Lt. Gen. Minihan . . .

*Continued from page 1*

The compelling need for strong Infosec can be linked to a growing threat against and increasing dependence on our information systems. The traditional geographically-based strategic sanctuary that America has enjoyed for much of our history has been lost as structured and unstructured threats, foreign governments, hackers, cyber-criminals and narco-terrorists all have the tools to disrupt, deny, degrade and attack our national information infrastructure.

Futurists Alvin and Heidi Toffler describe society's evolution in three "waves": agriculture-based, industry-based, and information-based. They maintain that today's leading nations are evolving into information societies. Just as control of industrial technology was key to military and economic power during the past two centuries, control of information technology will be vital in the decades ahead.

The United States has prospered within the first two waves and is certainly on the forefront of the 'third wave'. All of us share a vested interest in ensuring that America leads the information revolution. We must work together as a team to promote American leadership through this time of technological and geopolitical transition. In particular, we must help the nation understand the national security implications of America's journey into cyberspace.

*Continued on page 5*

## Calendar of Events

**May 1—Breakfast Meeting, University Center**  
(Speaker: The Honorable Daniel Fung,  
Solicitor General, Hong Kong)

## Ambassador Saito . . .

*Continued from page 2*

and we are beginning to participate in international efforts to maintain peace by sending armed forces. We have sent forces to Cambodia, Mozambique, Zaire, and now our forces are stationed in the Golan Heights, to be a part of the United Nations Peacekeeping Operation to separate Israeli and Syrian forces.

This has been a good year for the Japan-U.S. relationship, particularly in the security area but also in the economic field where we have reached agreement on a number of important bilateral economic issues. In the security area we have made a lot of progress, and we hope to continue to have such a fruitful and uneventful year in 1997. ABA

---

## Lt. Gen. Minihan . . .

*Continued from page 4*

The term "cyberspace" has a star wars ring to it. Perhaps a way to bring it closer to home is to think of it in biomedical terms. Information has become the life blood of our knowledge-based society, and the networks that distribute it make up the circulatory system that keeps our economy alive and growing. Just as the different organs of the body depend equally on the circulatory system to keep functioning, all of us — the national security community, civil government, and industry — depend equally on our information infrastructure to do our jobs.

Like our circulatory systems, our information infrastructure is under constant attack, and we need an immune system — information systems security — to keep us healthy enough to function. As with the circulatory system, the battle between the attackers and the immune system is dynamic. The attackers grow more powerful and more resistant over time, and the immune system must evolve to keep them under control if we are to stay healthy. If we are to not only survive but have a healthy 21st century, we must take effective preventive measures and develop new methods of treatment to keep our information infrastructure in working order.

Our efforts to build up the immunity of our information infrastructure have met with uneven success so far. For example, consider electronic commerce: inexpensive information technology and widespread networking make electronic commerce possible on a massive scale. However, despite its huge potential, it has grown remarkably slowly, primarily because of the lack of security needed to

enable it to be used with confidence. The internet without security is essentially a vast international party line.

## Conflict in the Information Age

With the emergence of cyberspace, our borders and our boundaries are no longer identical. In the virtual domain our boundaries extend well beyond our shores. Unlike our borders, they are diffuse, constantly changing, and easily penetrated. Our ability to network has far outpaced our ability to protect networks, leaving the data and systems we depend on for military operations, government, and commerce increasingly vulnerable to eavesdropping or attack.

With cyberspace offering new avenues of attack and new requirements for defense, conflict in the information age will be multidimensional. It will extend across both the physical and virtual domains, with events in one domain interacting with events in the other. This environment will be messy and highly ambiguous. Attacks in the virtual domain can take subtle, difficult-to-detect forms. The diffusion of power from nation-states to global and sub-national entities will make identification of adversaries far more difficult. It will become increasingly difficult to answer the questions "Are we under attack, and, if so, by whom?"

Attacks will be difficult to stop using our current geographically-based command structure and traditional weaponry. We will need to modify our principles of strategic and theater operations. We must also recognize that future conflict may involve significant asymmetries in vulnerabilities and combat operations. With its well-developed information infrastructure, America has a lot to lose to information warfare attacks. Many of our potential adversaries have no corresponding infrastructure to hold at risk.

## Mutual Vulnerabilities, Shared Solutions

The nation will increasingly require a safe, trustworthy infrastructure to support virtually all aspects of our national life. Developing this infrastructure is a shared effort because it addresses a shared vulnerability. We are not accustomed to thinking this way. In the past, crime was largely beyond the jurisdiction of the national security community, and strategic security threats were beyond the scope of industry. Today, we're all on the same net, and our requirements and vulnerabilities are

*Continued on page 6*

## Lt. Gen. Minihan . . .

*Continued from page 5*

inextricably intertwined. As a practical matter, it's increasingly difficult to distinguish between a crime and an attack. Regardless of the hacker's motivation, when the net goes down we all go down together.

The White House recently defined a policy initiative that is designed to help foster the shared effort between industry and government needed to bring security to the nation's information infrastructure. Some believe the administration's initiative is about key escrow and export controls, but in the broadest sense the initiative deals with the preparations we must make as a nation to use information technology to its full potential. It transcends the key escrow issue. It focuses on the more fundamental question of key management infrastructure. It is an attempt to create an environment in which an international framework will grow to support the use of strong encryption. I cannot overstress either the importance or the difficulty of moving this initiative from concept to reality.

## Implementing Security

Let's talk about implementing security! To provide security in a networked environment, we will need to resolve a complex and interrelated set of issues pertaining to:

- trust
- scalability
- liability
- availability of service
- public policy

## Trust

Let me give you a baseline on the level of trust in our systems today. According to a survey by Ernst & Young and *Information Week* released in October, 71% of the 1,300 senior information executives surveyed expressed lack of confidence in the security of their computer networks. Over three-quarters had experienced losses within the past two years due to problems with information security, computer viruses, and disaster recovery.

There's a lot more to the issue of trust than a good encryption algorithm. The algorithm gets you perhaps 5% of the way there. Without an effective infrastructure to implement it, an algorithm's value is comparable to that of a bank vault door on a cardboard box.

When I say trust, I mean that you must be willing to bet your company's future not only on the strength of your algorithm but on the integrity of those who:

- Issue the encryption certificates that vouch for your identity and the identity of those you deal with.
- Build the directories that allow others to know how to communicate securely with you.
- Assist you if you believe your encryption key or certificate has been compromised.

Can we build that level of trust into an infrastructure big enough to support electronic commerce on a global basis? Encryption has little chance of being used to its full potential, here or overseas, until a trusted international framework is in place.

## Scalability

Making trust scalable will be a difficult challenge. Many of us have experience building limited segments of infrastructure for a business, a sector, or a part of government. NSA and the Department of Defense have a great deal of experience in building infrastructures for critical functions like nuclear command and control and military operations worldwide. We are currently building the infrastructure to support two million users of the Defense Messaging System to provide e-mail service and browser service to DoD users — but we've yet to tackle tying in support for electronic commerce with the 350,000 vendors who do business with the Department of Defense. The complexity of these efforts pales in comparison with putting together a key management infrastructure for all applications — private, public, and military — in a global networked environment.

Unanswered questions abound in this area. For example:

- Who defines who is a trusted issuer of certificates?
- How do we limit authorities of certificate users?

- Are we ready to certify all users for all applications and all types of transactions?
- Are we ready to cross certify from any nation? All nations?

In order to use certificates with confidence — that is, the way we use paper currency and signed contracts today — we will need to track the authorities of the policy attachments of each certificate globally and with complete trust. How do we scale to a global system while maintaining trust?

## Liability

What happens when something goes wrong — when a user trusts the infrastructure, follows its procedures, and loses information or money? Whose fault is it, and who makes good the loss?

Risk is inherent in networking. With the best of precautions, in a networked environment some risk will remain. With information technology advancing dynamically, today's effective solution will be obsolete tomorrow. The situation is not made easier by the competitive imperatives driving us toward electronic commerce. We cannot wait for the perfect infrastructure to be put in place.

The next stage of electronic commerce takes risk to a new plane. It must protect billions of transactions ranging from simple credit card purchases to large-scale electronic transfers of funds and proprietary information. To use networks we must accept some risk and manage it. Part of risk management will require us to take a hard look at the issue of liability. How do we set limits on liability while maintaining trust?

## Availability

Another challenge is to maintain balance between dependency on networked solutions and availability. Consider the medical community's use of information technology for telemedicine. Applications like these will need the best possible protections against denial of service.

## Public Policy

We are now engaged in a national discussion on how to balance the private interests of individuals and business with the public interests of law enforcement and national security. How we resolve this discussion will shape the infrastructure we build to implement our security solutions. If we overemphasize the public interest, we risk a world with too much government access and too little security. If we overemphasize the private interest, we risk a world with perhaps too many secrets — for example, a world in which terrorists, organized crime, and hackers acquire secure command and control capabilities formerly restricted to advanced military forces. Both of these extremes are unpalatable. We need to strike a balance that provides adequate protection for both individuals and businesses and for society as a whole.

One of the fundamental questions on this issue is whether to provide a key recovery feature in the infrastructure. Key recovery adds complexity to the KMI, and arguments have been advanced to support proceeding without it. There are, however, three very good reasons for designing it into the infrastructure.

First, key recovery is good business practice. It protects information from loss by allowing users to regain access to their encrypted data when encryption keys are lost or corrupted. Key recovery is analogous to systems administrators recovering forgotten passwords or maintaining spare door and desk keys for emergency use.

This goes back to the trust issue. By helping to ensure the availability of information and systems, key recovery can increase the level of trust in the security system.

Second, key recovery makes it possible for law enforcement, with proper authorization, to be able to access the keys. This is an essential component of a solution that protects the public interest. There is a clear societal interest in preventing cyberspace from developing into a sanctuary for global, instantaneous, and secure control of operations for criminals, terrorists, and rogue nations.

*Continued on page 8*




*Lt. Gen. Kenneth A. Minihan spoke at the Standing Committee's January 16th breakfast at the University Club.*

## CEELI Seeking Public Service Lawyers

The Central and East European Law Initiative (CEELI), a public service project of the American Bar Association, is seeking experienced attorneys to serve in a variety of capacities, including as liaisons in Commercial Law, Criminal Law, Leasing, Banking, Bankruptcy, and Environmental Law; and they are also in need of experts on Alternative Dispute Resolution, Court Administration, and the Rule of Law. Applicants should have several years of relevant professional experience, strong interpersonal skills, and ideally knowledge of the region and language skills. Individuals selected will be expected to spend from a few weeks to a year or more in Central or Eastern Europe, and will receive a variety of benefits (including travel expenses, housing allowance, insurance, and a modest living stipend).

This is a good program and a wonderful opportunity to make a difference in an important transitional region of the world.

For further information on these or other opportunities, contact CEELI at 1 (800) 98CEELI, or (202) 662-1754; or by fax at (202) 662-1597. 

### Lt. Gen. Minihan . . .

*Continued from page 7*

Finally, key recovery may prove essential in making encryption scalable on an international basis. We are not the only country wrestling with the public safety implications of unbreakable cryptography. France, Israel, and Russia recently imposed import and domestic use restrictions. Several Asian, South American, and African countries have had similar restrictions in place for years. Others may impose them as strong cryptography proliferates.

The European Union and other confederations are considering key recovery-based KMIs. The world's major standards bodies are designing future standards so that key recovery can be accommodated. International standards and protocols for key recovery may prove essential in heading off national restrictions, establishing a broad export market for cryptography, and establishing an infrastructure acceptable for general international use. This would accelerate the realization of the promise of information technology, and that would be in everyone's interest.

### Zones of Cooperation

Working in partnership, government and industry together need to build up the infrastructure needed to sustain and strengthen information security for America. I wish to emphasize that the infrastructure will be built by industry as a commercial venture. This task is huge. Collaboration among many partners will be essential if we are to establish a key management infrastructure that promotes the use of encryption worldwide.

Protecting the infrastructure falls into a broad middle zone along a spectrum that ranges from the security practices of individual organizations to large-scale military operations directed by the government for the national defense. This is a zone of mutual vulnerability, shared responsibility, and potential cooperation for industry and government. We should seek cooperative engagement in the areas of standards, technology, and collaboration on vulnerabilities.

The standards we develop must enable our infrastructure to meet five key requirements. These include confidentiality through encryption, verification of data integrity, authentication of originators, proof of participation by parties to a transaction, and availability of service on demand. These features are equally key to network operations in support of electronic commerce, vital public services, and national security. We need mutually agreed upon technical standards and operating protocols, comparable to building codes and traffic regulations, to ensure that the infrastructure is sound, that it will permit interoperability, and that anomalous activity on the net can be identified and isolated. If you'll let me use the term speeders, the government needs to set the standards to regulate the speeders — the speed limits, the lane widths, the no passing zones.

The National Security Agency has made major changes in its approach to this issue. We are working with industry to develop the infrastructure, and as it comes on line we are prepared to support relaxation of export controls. We have to work



together to make our own system work. After we have agreed among ourselves we can begin to work on bilateral encryption policy agreements with other countries.

In the area of technology the key focus will be the technical development of the public key infrastructure. The technical solutions we develop together must help the U.S. information technology industry maintain global technological leadership and dominant market share, provide for scalability and interoperability, and permit access for law enforcement. A strong key management infrastructure is essential, but it can be based on a voluntary system of commercial certificate authorities operating within prescribed policy and performance guidelines.

In the area of vulnerabilities, key areas for cooperation are vulnerability analysis and warning. These activities will be crucial to preventing surprise. Much of the information needed for these efforts, however, is held closely by industry, which withholds information on vulnerabilities and losses to prevent further exploitation and to avoid shaking the confidence of investors and customers. Industry and government need to explore how this information can be shared among all who need it without adversely affecting the competitiveness of individual companies or industrial sectors.

### Conclusion

Summarizing, the scale of networking in the United States and the degree to which we rely on information technology to carry out essential functions make us highly vulnerable to network-based

attacks. Working in partnership, government and industry together need to build up an infrastructure that promotes American competitiveness, protects government and private sector information and systems, and denies covert use of cyberspace to criminals, terrorists, and hostile nations.

I'd like to return in closing to the biomedical analogy I touched on earlier. There are two ways to protect your health from disease. One is to stick close to home and never go anywhere where unfamiliar diseases might lurk. For those who dream of going forward boldly, this is not an option.

A hundred years ago, the visionaries who built the Panama Canal took on a yellow fever-ridden jungle and won. Today, those who seek to realize the full potential that information technology holds for us must move into a cyberspace full of electronic versions of yellow fever. We must develop the encryption policies and techniques needed to immunize our system against them, and build up a robust information infrastructure that can flourish in the sometimes dangerous environment of cyberspace.

The National Security Agency has a key role to play in both these efforts. However, we cannot fulfill this vision alone. First, the technologies needed to do the job are to a growing degree no longer controlled by government. Second, in the information age to be connected to anything is to be connected to everything. All of us will stand or fall together. We need to work together. It's a clear choice and a tough choice, and it's yours to make—to develop a road map for a cooperative approach to these issues. ABA

## Standing Committee on Law and National Security

*Chairman:* Paul Schott Stevens

*Members:* E. E. Anderson, Zoë Baird, Stewart Baker, Kenneth C. Bass III, Russell J. Bruemmer, L. Christine Healey, Philip B. Heymann, Elizabeth R. Rindskopf, Jeffrey H. Smith, Edwin D. Williamson

*Advisory Committee Chair:* Richard E. Friedman

*Staff Director:* Holly Stewart McMahon

740 15th St., NW

Washington, D.C. 20005-1009

(202) 662-1035

fax (202) 662-1032

e-mail: [natsecurity@abanet.org](mailto:natsecurity@abanet.org)

web page: <http://www.abanet.org/natsecurity>

# ***The National Security Agenda . . . .***

by Daniel Richard

**Senate Consents to Ratification of Chemical Arms Ban Before April Deadline**—On April 24, by a bipartisan vote of 74-26 (including all 45 Democrats and 29 Republicans), the Senate consented to the ratification of the 1993 Chemical Weapons Convention, which prohibits the production or development of chemical weapons and requires parties to destroy existing stockpiles within 10 years. Among many concessions made to secure the necessary two-thirds majority, the Administration accepted 28 of 33 conditions offered by Senate Foreign Relations Committee Chairman Jesse Helms, agreed to submit modifications in two existing arms control treaties for Senate consideration (the definition of short-range missile defenses under the 1972 ABM Treaty and the so-called “flank agreement” modifying the Conventional Forces in Europe [CFE] treaty), and reportedly agreed to Republican demands concerning UN reform and State Department reorganization as well. The five Helms Amendments which were debated on the Senate floor—four of which were regarded as “killer amendments” that would have blocked U.S. ratification—were defeated.

**President Ratifies CWC Treaty, Praising U.S.-Japan Partnership**—Only hours after the Senate gave its consent, on April 25th President Clinton signed the instrument of ratification to the Chemical Weapons Convention and sent it off to the United Nations. By acting before the treaty went into force on April 29th, he assured the United States a seat on the governing body responsible for establishing the rules and administering the accord. The United States became the 75th State to ratify the treaty, which was signed by 164 countries. The White House signing ceremony occurred during a visit by Japanese Prime Minister Ryutaro Hashimoto (focused in part upon consolidating U.S. military bases in Okinawa), and during subsequent press remarks President Clinton referred to Japan and the United States as “the world’s two strongest democracies” and characterized their security alliance as “the cornerstone of peace and stability in the Asia Pacific Region.”

**Russian Duma Delays Action on CWC**—Shortly after President Clinton ratified the Chemical Weapons Convention, the State Department called upon Russia—the only other State which acknowledges possessing chemical weapons—to “step up to the plate” and quickly ratify. Arguing that Russia lacks the financial resources (an estimated \$5 billion) to destroy its estimated 40,000-ton stockpile of chemical weapons, a spokesman for the Russian parliament announced that the treaty would not be considered before the fall.

**White House, Senate Reach Compromise Over Mexican Drug Certification**—The Clinton Administration reached a compromise with Senate leaders that watered down a proposed resolution (S.J.Res. 21) that would have reversed the President’s certification of Mexico in the war against drugs. The House narrowly passed a bill (H.J. Res. 58) that would have decertified Mexico should they not meet certain requirements within 90 days of the bills enactment. By reaching a successful compromise with the Senate, the White House avoided having to veto an anti-Mexico piece of legislation one month before the President is scheduled to visit Mexico City. Congressional critics have pointed to the recent arrest of Mexico’s top drug fighter on corruption charges and the escape of a leading drug-money launderer as evidence of Mexico’s unwillingness to cooperate fully with the United States. Nonetheless, the Administration has stated it is convinced of Mexican President Zedillo’s commitment toward the war on drugs and that the President intended to veto S.J. Res. 21 if the Administration and the Senate were unable to reach an agreement.

**NATO Expansion Questions Begin Reaching the Hill**—Although the Executive Branch has been working on NATO expansion issues for the past two years, legislators have only recently begun to question the cost and consequence of expanding NATO into Eastern Europe. On February 24, the Administration revealed its projected costs for NATO expansion that fall much lower than estimates provided by the Congressional Budget Office and the RAND Corporation. Although there has been little congressional response to these figures, the discrepancies could prove crucial if the costs for NATO expansion start rising. Additionally, Congressional leaders are starting to review how the Administration is going to placate Russia after expanding NATO eastward. Although a Senate vote is at least one year away, some Senators claim that the Administration may offer Russia too much in return for their acceptance of NATO enlargement. 