General Marsh Outlines Infrastructure Protection Recommendations

On December 4, 1997, General Thomas Marsh (USAF-Ret.), Chairman of the President's Commission on Critical Infrastructure Protection, addressed a Standing Committee breakfast at the University Club on the work of the Commission. As a former commander of the Air Force Systems Command, General Marsh served as the first chairman of Thiokol Corporation and is currently the chairman of the board of CAE Electronics, Inc. and Converse Government Systems Corporation. The Commission's mandate involves combining governmental and private sector expertise to advise the President on a strategy for protecting and assuring the continued operation of such critical infrastructures as telecommunications, electrical power systems, gas and oil transportation and storage, banking and finance, transportation, water supply systems, emergency services, and continuity of government operations. The text of his remarks follows for the benefit of readers who were unable to be present. —Ed.

Thank you, Paul. Good morning, ladies and gentlemen. It is a pleasure to be here to discuss the work of the President's Commission on Critical Infrastructure Protection. I know that the ABA breakfast meetings are a long-standing tradition here in Washington and I am pleased to have the opportunity to be with you to tell you about the Commission's efforts.

To give you some perspective on the Commission's challenge, imagine, if you will, that:

- the power goes out in the northwest;

Continued on page 2

Snider Discusses Hill Access to Intelligence

by William E. Conner

Despite inclement weather, a full house gathered to hear L. Britt Snider, Special Counsel to the Director of Central Intelligence, discuss the meaning and impact of intelligence sharing with Congress on January 15th at the University Club in Washington, DC. Mr. Snider, a former General Counsel to the Senate Select Committee on Intelligence, former ABA Standing Committee member and current Advisory Committee member, based his remarks upon a monograph he wrote last year for the CIA's Center for the Study of Intelligence.

According to Mr. Snider, providing intelligence information to Congress is one of the least appreciated, yet most important aspects of relations between the legislative and executive branches. Over the last 23 years, since the two Congressional intelligence committees were created, the flow of intelligence to Congress has increased from a trickle to a veritable fire hose, and access to intelligence has expanded beyond just the two intelligence committees.

Continued on page 8
Gen. Marsh...
Continued from page 1

- the 911 system is disrupted in a major city because someone has flooded the phone lines with repeat calls;

- two bridges across the Mississippi are destroyed—bridges that not only carry trucks and trains, but also telephone cables; and

- two Internet service providers in New York City are out of service.

What do we do in such a situation? Who is in charge? Is it merely coincidence, or a concentrated attack? These are the types of questions the Commission has been considering—questions to which there are no easy answers. Questions, we hope, our recommendations will help lay the foundation for answering.

Today I will briefly discuss the Commission, the new vulnerabilities and threats of the cyber age, our key findings, and then summarize our recommendations.

I must admit right up front: our findings, conclusions, and recommendations are very different from what we anticipated—and different from what our stakeholders anticipated. Many thought this was a problem that government alone could resolve in a few easy steps. But during the past year and a half, we concluded that protecting our infrastructures is a public-private undertaking that requires a new partnership, and protecting our infrastructures will take time—and will require long-term efforts and a new way of thinking.

The Commission was established by Executive Order on July 15, 1998. A joint government and private sector endeavor, it was charged to develop a national policy and implementation strategy for protecting our critical infrastructures from physical and cyber threats and assuring their continued operation.

The President identified these eight infrastructures as our national life support system:

- Telecommunications
- Electric Power
- Transportation
- Oil and Gas Delivery and Storage
- Banking and Finance
- Water
- Emergency Services
- Government Services

They are critical in that their incapacity or destruction would have a debilitating impact on the defense and economic security of the United States. Critical infrastructures have long been lucrative targets for anyone wanting to attack another country. Our nation relies on its infrastructures for national security, public welfare, and its economic strength.

Those who would attack the infrastructures would do so to:

- reduce our ability to act in our own interest
- erode public confidence in critical services, or
- reduce American economic competitiveness.

In the Gulf War, as you well know, disabling Iraq's infrastructures was one of the keys to our success—a lesson noted with much interest by many countries around the world.

The Commission was uniquely tailored for the task. Recognizing that the critical infrastructures are largely owned and operated by the private sector, the Commission structure was a joint public-private undertaking.

The Commission was comprised of representatives from both industry and government.

The Steering Committee of senior government officials oversaw the work of the Commission.

Continued on page 4

Paul Schott Stevens
Chairman, Standing Committee on Law and National Security

Holly Stewart McIlhawn
Staff Director

Robert F. Turner
Editor

The National Security Law Report 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 © 1998 American Bar Association. ISSN 0735-2477.
BOOK REVIEW

Arthur I. Cyr,
After the Cold War: American Foreign Policy, Europe, and Asia
pages: 176 price: $40.00

Reviewed by Endy Zemenides

Much intellectual effort has been expended trying to define trends in international politics without resorting to the phrase "post-Cold War." When can we put "post" behind us and agree on what to call the new era? Richard Haass, of the Brookings Institution, has pointed out that it may be impossible to name truly historical political transformations while living through them. Haass asks whether 15th century Florentines ever woke up and thought to themselves, "it’s another great day in the Renaissance."

The search for the right metaphor to describe geopolitics at the end of the twentieth century need not distract us from important and accessible scholarly projects of a more limited scope. Arthur I. Cyr’s After the Cold War: American Foreign Policy, Europe, and Asia, is one such book. Cyr, who is CEO of the Chicago World Trade Center and a lecturer in international politics at Northwestern University, displays an impressive range of interests and expertise, moving confidently from British politics to the balance of power in Northeast Asia.

Cyr starts from the premise that none of the current worries—militant Islam, China’s growing military might, and so forth—signify the emergence of a new hegemonic conflict. Indeed, the threats to U.S. interests that can be anticipated are likely to call for more subtle and varied responses than Americans were accustomed to during the Cold War. Cyr explains several important conceptual shifts that began before the fall of the Berlin Wall, and although they do not necessarily amount to a new “paradigm,” they have changed the way policymakers and opinion leaders think about the challenges and opportunities that we now face.

Key patterns did emerge in the last years of the Cold War. Cyr argues that one of the Reagan administration’s enduring achievements is sometimes overlooked. The Reagan administration’s philosophical commitment to reducing the government’s scope of responsibilities on the domestic front also had the effect of transforming U.S. foreign policy. By championing the private sector and cutting back government intervention in the U.S. economy, the Reagan administration cleared the way for multinational corporations to compete more aggressively abroad. Combine this with very effective advocacy of trade liberalization, and the Reagan administration can claim credit for helping to set in motion the explosive, export-driven growth of the post-Cold War era. The enormous budget deficits that accompanied the Reagan administration’s tax cuts and defense buildup also shifted power to global capital markets. Arguably, the power of central banks has declined relative to that of the major investment banks that underwrite and trade in government debt.

The volume of currency and debt trading, international investment, and international borrowing has exploded, and private sector capital flows make traditional foreign aid and development assistance funding seem minuscule by comparison. The U.S. Congress has reinforced this perception by downsizing the international operations of foreign policy bureaucracies such as the Agency for International Development and the U.S. Information Agency. The State Department has also felt budgetary pressure. Consulates are being closed, embassy staffs are being reduced, and the Foreign Service cannot post many highly qualified junior officers abroad. Structurally, the United States’ commercial presence is supplanting its military and political presence around the world.

Cyr believes that there are subtle aspects to this shift that serve important U.S. national interests. First, as the three major trading blocs coalesce (East Asia, Europe, Americas) U.S.-based multinational corporations are deterring the threat of regional protectionism. Second, growing foreign investment by U.S. corporations is replacing conventional aid programs. U.S. government backing, in the form of insurance or performance guarantees, offsets some of the risk that U.S.-based multinationals might not otherwise be able to justify to their shareholders. Private sector investment has generated higher rates of growth with less exposure to government corruption in developing countries. Third, and finally, U.S.-based multinationals are proving to be an effective medium of liberal, democratic values in transitional states.

After the Cold War is not a variation on the familiar theme of one set of elites (government officials) exchanging power with another set of elites (international bankers, executives, etc.). On the contrary, Cyr sees a diffusion of power and authority. Increasingly, major decisions are being made by “people operating with great freedom beyond the boundaries of the traditional nation-state.” It is no longer a matter of navigating (or rigging) regulatory

Continued on page 4
Cyr, After the Cold War . . .
Continued from page 1

structures from the top down. Mass media, decentralized information networks, migration, and tourism have undermined the power of the economic and social elites that dominated international affairs in the past. Likewise, public opinion on questions of foreign policy and national security is no longer shaped by a few key "gatekeepers" in prestigious media organizations. A myriad of electronic news media that respond to consumers of news rather than providers of news has taken their place.

Cyr offers quite interesting observations about changing perceptions of cooperative security as well. In the last decade of the Cold War, the prevailing wisdom held that the correlation between economic power and strategic power was becoming tighter and more direct. The arguments over the relative strength or weakness of the Soviet economy echoed from the corridors of the Central Intelligence Agency to the hearing rooms on Capitol Hill. Paul Kennedy's book, The Rise and Fall of Great Powers, put the proposition that richer is mightier in a compelling historical context.

Cyr challenges this assumption. Perhaps major industrial democracies such as France, Germany, and Japan are not suited to military responsibilities commensurate with their economic power. Germany and Japan, in particular, observe self-imposed restraints that prevent them from projecting military power abroad. Cyr argues that Britain and South Korea may be as important to the United States in the event of a major regional conflict as Germany or Japan. Germany and Japan may become permanent members of the UN Security Council, and they may pay a large part of the costs incurred by a future U.S.-led military coalition—as they did in the Persian Gulf War. But, countries that have the capability to organize expeditionary forces and stand with the United States diplomatically, such as Britain and South Korea, will be critically important.

Cyr does not resort to the pundits' fashion of phrase-making and summary judgment. What he offers instead is a thoughtful discussion of several transitions that cannot be reduced to a single message or metaphor. This is a style appropriate to the period in which Cyr writes, a period that is not characterized by a single, prolonged crisis, but by an array of challenges and opportunities.

Gen. Marsh . . .
Continued from page 2

guided us through myriad government concerns.

A presidentially-appointed Advisory Committee of key industry leaders provided the unique perspective of owners and operators of the infrastructures.

The Infrastructure Protection Task Force was established at the same time as the Commission to support infrastructure protection until the Commission's recommendations are enacted.

Our approach recognized that most of the infrastructures operate within an existing framework of government policy and regulation. But they are also privately owned competitive enterprises; as such, protection recommendations should not undermine their competitive position. We recognized that any solution would have to be viable in the marketplace as well as the public policy arena. (Incidentally, those of us with long histories in government or the military really need to take this to heart.) Thus we adopted the following guiding principles:

- First, we knew this could not be another Big Government effort. Government must set the example, but it is the owners and operators who are the key to success. They have a strong economic stake in protecting their assets and maximizing customer satisfaction. They understand the infrastructures and know best how to respond to disruptions.

- Second, while we may be undergoing an information revolution, we felt that utilizing the best ideas and processes from current structures and relationships was the proper way to proceed. This means building on existing organizations and relationships as well as fostering voluntary cooperation. Partnership between industry and government will be more effective and efficient than legislation or regulation.

- Finally, this is a long-term effort which requires continuous improvement. We must take action in practical increments. There is no "magic bullet" solution. We must aim not only to protect the infrastructures, but also to enhance them.

Outreach was a cornerstone of our effort. In fact, our conclusions and recommendations result directly from the conversations and meetings we had with more than 6,000 individuals from industry.

Endy Zemenides, a student at the Georgetown University Law Center, was a research assistant with the Chicago-based National Strategy Forum from 1996 to 1997. [AA]
academia, science, technology, the military, and
government.

We held five public meetings around the country, participated in numerous conferences: hosted sim-
ulations, games and focus groups; and increased awareness of this effort through the media and our
website.

In the past, broad oceans and peaceable neigh-
bors provided all the infrastructure protection we
needed. That all changed during the Cold War.
Technology made geography irrelevant. While we
feared attack by bombs and missiles, we knew who
the enemy was and where the attack would origi-
nate.

Computers and electrons change the picture
entirely. Now the capability is widely available at
relatively little cost. This is the “new geography” on
which the Commission focused its efforts—a bor-
derless cyber geography whose major topographi-
cal features are technology and change.

We have long understood physical threats and
vulnerabilities, but not so cyber ones. The fast pace
of technology means we are always running to catch
up in the cyber dimension. Thus the Commission’s
work and our report focus primarily on coping with
the cyber threat. Our foremost concern is the inter-
dependencies presented by the “system of sys-
tems” we rely on for the around the clock delivery of
these critical services.

Furthermore, information that describes our
vulnerabilities is increasingly accessible. Most of it
is unclassified, and much of it is available on the
Internet. We had to be careful in compiling this
information not to provide a handbook for those
who would use it for harmful purposes.

So, who is the threat? The “bad actors,” as I like
to call ‘em, are those with the capability and intent
to do harm. While we have not found a “smoking
keyboard”—that is, we do not know who has the
intent to do harm—we do know a lot about the
capability to do serious damage to these systems.

We characterize capability as a combination of
skills and tools—skills that we’ve found even most
teenagers have, and dangerous tools that are readi-
ly available, even on the Internet. In short, the
opportunity to do harm is expansive and growing.

The bad actors who would use these tools range
from the recreational hacker—who thrives on the
thrill and challenge of breaking into another’s com-
puter—to the national security threat of informa-
tion warriors intent on achieving strategic advan-
tage.

Common to all threats is the insider. In addition
to harnessing technology to protect our infra-
structures, we must pay special attention to insiders—
their trustworthiness and their access to critical
control functions.

The new arsenal of “weapons of mass disruption”
in the cyber world include “Trojan horses,” viruses,
and e-mail attacks used to alter or steal data, or
deny service. These tools recognize neither bor-
ders nor jurisdictions. They can be used anywhere,
anytime, by anyone with the capability, technology,
and intent to do harm. And they offer the advantage
of anonymity.

We examined the respective roles of the private
sector and the federal government in light of this
new threat. We concluded that the private sector
has a responsibility to protect itself from the local
threats, such as individual hackers and criminals.
And that the federal government has a larger respon-
sibility to protect our citizens from national
security threats. In short, we found that infra-
structure protection is a shared responsibility.

Specifically, the private sector must take pru-
dent measures to protect itself from commonplace
hacker tools. But it turns out, these same tools will
also be used by the terrorist and the information
warrior, so the private sector will also be protecting
itself against terrorist and foreign nation attack,
and hence playing a significant role in national
security.

Therefore, the federal government must assume
responsibility for collecting information about the
tools, the perpetrators, and their intent from all
sources, including the owners and operators of the
infrastructures and must share this information
with the private sector so that industry can take the
necessary protective measures.

In some respects, our most important finding is
that adapting to this new age requires thinking
differently about infrastructure protection. We are
facing a new and different set of national security
challenges as we approach the third millennium.
Specifically, we found that:

- Information sharing is the most immediate
  need.

- Responsibility is shared among owners and
  operators and government.

- The federal government has an important
  role in the new alliance.

- We must develop an analysis and warning
  capability.

- Infrastructure protection requires a focal
  point.

Continued on page 6
The existing legal framework is imperfectly tuned to deal with cyber threats.

Current research and development efforts are inadequate to the task.

Protecting our infrastructures into the Twenty-First Century requires greater understanding of their vulnerabilities and decisive actions to reduce them. After fifteen months of consultation, research, assessment, and deliberation, the Commission's fundamental conclusion is that waiting for disaster is a dangerous strategy. Now is the time to act to protect our future. And this action requires a new partnership to address the risks of protecting our nation's infrastructures.

The Commission's recommendations are the product of much research, discussion, and deliberation. They are founded on shared core principles and are based on fact. They are aimed at improving coordination and establishing roles for infrastructure protection, fostering partnerships among all stakeholders, and coordinating diverse interests.

Our recommendations fall generally into three categories:

- actions the federal government must take;
- actions the owners and operators of the infrastructures must take; and
- actions that require partnership between government and industry.

Most of you here this morning are probably interested, primarily, in the legal initiatives of the Commission. We examined a full range of legal issues relating to protection of the critical infrastructure, and have identified some laws that may be improved to enhance protection, and others that may actually inhibit protective efforts. We examined these authorities with three objectives in mind:

- increasing the effectiveness of government's assurance and protection efforts—particularly the federal government;
- enhancing the private sector's ability to protect itself; and
- enabling effective public-private partnerships where most needed—in areas of joint information sharing and policy formulation.

We examined areas of major federal legislation that traditionally provide for prevention, mitigation, response and recovery in the event of major disasters. We wanted to ensure adequate coverage for the critical infrastructures under the current legislative framework, and to also consider the appropriateness of leveraging these statutes and authorities to address cyber events.

While in many instances it is still too early to know what type of response would be most appropriate to meet public and private needs during a cyber incident, we have proposed studies that would sharpen the focus of these important areas of legislation.

We also looked at the adequacy of current criminal law and procedure. We have made some modest recommendations to, for example, allow the Federal Sentencing Guidelines to better take into account the true harm done by attacks on the critical infrastructures.

We looked at laws that govern the relationship between employers and employees in the critical infrastructures. We found that some employers, with respect to certain highly sensitive positions within the critical infrastructures, want to request from employees certain information similar to that routinely obtained by the federal government when issuing security clearances. We realize this matter involves a delicate balance between security and privacy, and have therefore called for an expert study group, representing a wide range of labor, management, government, and privacy interests, to make recommendations on these security-related issues.

Finally, we looked at ways in which certain laws may actually inhibit the formation of a public-private partnership in crucial areas of information sharing and policy formulation. Some laws, for example, may impede the measured sharing of threat and vulnerability information between government and the owners and operators of the critical infrastructures. Some laws may erect inordinately high barriers to public-private partnerships for dialogues on sensitive matters relating to national security. These impediments need to be carefully considered when structuring such partnerships.

When developing our legal recommendations, we realized that we needed a panorama of existing legal authorities associated with infrastructure assurance; those that may be used to promote or enhance infrastructure assurance, as well as those
that may actually operate in ways that are antithetical to achieving infrastructure assurance objectives. To fill this void, the Commission recruited a team of lawyers to cull through the United States Code, the Code of Federal Regulations, Executive Orders, treaties, select state legislation, and other relevant authorities, and incorporate the results into a legal database. The final product is a database searchable by key word and concept containing over 2,000 entries. We are working to get the database distributed in a limited fashion to federal agencies and Congress on CD-ROM in the next 60 days, and available on the Internet in the next 180 days.

Reviewing legal authorities was simply one component of the Commission’s research. We also conducted extensive outreach efforts, where we heard time and again that the owners and operators of the infrastructure need more information about cyber threats. They said that a trusted environment must be built so that they can freely exchange information with each other and with government without fear of regulation, loss of public confidence, incurred liability, or damaged reputation.

The Commission’s legal recommendations lay the foundation for creating a new collaborative environment that includes a two-way exchange of information, not more burdensome regulation. Achieving this legislative change will go a long way toward alleviating private sector concerns—such as protecting proprietary information and ensuring anonymity when necessary—and facilitate the creation of information sharing mechanisms both within industry and between industry and government.

As to other actions the government should take, we recommend specific steps to ensure owners and operators and state and local governments are sufficiently informed and supported to accomplish their infrastructure protection roles, to include:

- Designated federal agencies continuing and expanding the availability of risk assessment services to the private sector and encouraging industry—and assisting when necessary—to develop risk methodologies.

- The U.S. Security Policy Board should study and recommend how best to protect specific private sector information on threats and vulnerabilities to critical infrastructures. And

- The funding for the Nunn-Lugar-Domenici domestic preparedness program should be doubled to expand and accelerate mitigating the effects of weapons of mass destruction attacks.

Key to the success of these initiatives is educating our citizens about the emerging threats and vulnerabilities in the cyber dimension. We must change the way of thinking about technology and the resulting threats and vulnerabilities.

The Commission’s recommendations are aimed at all levels of education, from grammar to graduate school and beyond. They include:

- A series of White House conferences to spur new curricula in computer ethics and intellectual property for elementary and secondary schools.

- A nationwide public awareness campaign, simulations, and round-table discussions to educate the general public as well as industry and government leaders.

- Grants by the National Science Foundation to promote graduate level research and teaching of network security.

- Partnership between the Department of Education and industry to develop curricula and market demand for properly-trained information security technicians and managers.

Infrastructure assurance is a joint responsibility, but the federal government has an unmistakable duty to lead the effort. Clearly, the federal government must lead by example as it exhorts the private sector and state and local governments to raise the level of security of their systems.

The federal government must pursue the tools, practices, and policies required to conduct business in the cyber age. This includes:

- Improving government information security through developing, implementing, and enforcing best practices and standards—and then conducting certification and measures against those standards.

- Working with industry to expedite efforts for alternative information security and encryption key management pilot programs.

- Elevating and formalizing Information Assurance as a foreign intelligence priority.

Continued on page 8
Gen. Marsn . . .

- Recruiting and retaining adequate numbers of law enforcement personnel with cyber skills.
- Conducting a thorough risk assessment of the National Aerospace System and the planned sole reliance on the Global Positioning System.

Federal research and development efforts are inadequate to meet the challenge presented by emerging cyber threats. About $250 million is spent each year on infrastructure assurance-related R&D, of which 60 percent—$150 million—is dedicated to information security. There is very little research supporting a national cyber defense. The Commission believes that real-time detection, identification, and response tools are urgently needed, and we concluded that market forces are currently insufficient to meet these needs.

Thus we recommended doubling federal R&D funding for infrastructure protection to $500 million the first year, with 20 percent increases each year for the next five years. We recommend this funding target such topics as risk management, simulation and modeling, decision support, and early warning and response.

To formulate the public-private partnership necessary for infrastructure protection, we recommend several arrangements for information sharing and policy input. At the policy-making level, we recommend:

- an Office of National Infrastructure Assurance—located within the White House—to serve as the federal government’s focal point for infrastructure protection;
- a National Infrastructure Assurance Council comprised of selected infrastructure CEOs and Cabinet officials to propose policy and advise the President; and
- an Infrastructure Assurance Support Office to support both the Council and the National Office.

At the operational level, we recommend:

- Sector Infrastructure Assurance Coordinators or clearinghouses as focal points within each infrastructure to share information;
- federal Lead Agencies to promote and assist in establishing the sector coordinators;
- an Information Sharing and Analysis Center staffed by both private industry and government to receive and share information about infrastructure intrusions to be located in the private sector; and
- a Warning Center designed to provide operational warning whenever possible of an attack on the infrastructures, either physical or cyber, located within the FBI.

Just as the risks are shared between the public and the private sectors, so will the solutions be found. Our national and economic security has become a shared responsibility—one that will require a new kind of partnership between government and industry—one which encourages information sharing and one which requires the government to lead by example.

For further information about the Commission and to download a copy of its report, go to the Commission’s web site: www.pccip.gov.

Snider on Intelligence . . .
Continued from page 1

Mr. Snider confirmed that the intelligence committees receive many types of finished intelligence products, including publications, briefings, and access to electronic intelligence databases containing archival reports. In 1995, for example, Mr. Snider stated that more than 5,000 finished intelligence reports were furnished to the two intelligence committees, and this figure did not include various daily current intelligence publications available to the committees. Further, other congressional committees with responsibilities in the national security area also receive current intelligence publications and may pick and choose among numerous finished intelligence products they wish to review.

There are significant intelligence products that Congress does not receive, however, including the President’s Daily Brief, current intelligence reports compiled for the Secretaries of State and Defense and the Chairman of the Joint Chiefs of Staff, and the tailored reports produced for the National Security Council and other senior administration officials. Generally, Congress does not receive “raw” intelligence reports, which Mr. Snider defined as

Continued on page 11
National Security Resources on the Internet

by Michael N. Schmitt

The following short article was prepared several months ago at the request of the editor, who heard a presentation by Lt. Col. Schmitt to the Oceans and International Law Advisory Committee of the U.S. Naval War College in February 1997. Both because of our limited space and because Internet resources are expanding rapidly, it should be viewed as an introduction rather than a comprehensive guide to the topic. Readers who are aware of other web sites of particular relevance to national security law are invited to bring them to the attention of the Standing Committee for possible mention in future issues.

Ed.

Long considered the province of the socially challenged, the Internet has finally come of age as an indispensable research tool, particularly when dealing with national security issues. Today, failure to "surf the net" when conducting research is at best inefficient; more often it risks missing valuable source material. In an attempt to help alleviate such failings, this article surveys useful sites that novices might find useful in their first forays onto the Internet. Beware, though, that control of material placed on the Internet is de minimis: material can be dated, mistakes are made in loading text, the Internet is often a forum for the less than objective, and, in extreme cases, some miscreants create sites that "spoof" or mimic legitimate organizations. Therefore, a keen sensitivity to caveat emptor is obligatory.

The best place to start is with "host" sites, i.e., those which compile and sort substantive sites into specific topic areas, and provide instant access to them at the click of a mouse. One comprehensive example is the "Social Science Information Gateway" (SOSIG) (www.esrc.bris.ac.uk/roads/cgi/browse.pl). It is organized into broad categories (government, military science, law, etc.) that can be explored by region (World, Europe, UK). The worldwide military science grouping, for instance, contains nearly 100 sites ranging from Jane's to NATO. A particular benefit of SOSIG is a short description of each site prepared by librarians or recognized practitioners that allows one to cull the wheat from the chaff before actually entering individual sites.

A second profitable starting point is "National Security Links" (www.blueriver.net/~wyrm/natsec.html), a site with sources as diverse as the text of the Quadrennial Defense Review and Canada's Lester B. Pearson International Peacekeeping Training Centre. It is particularly rich in military links.

Probably the best single source for the international law aspects of national security is the University of Western Australia's site, "Public International Law" (PIL) (www.law.ecei.uwa.edu.au/intlaw/). Its United Nations section contains links to the UN homepage, which has full text search capability for Security Council and General Assembly resolutions, information on peacekeeping operations, and press releases. PIL's treaty section offers links to virtually all treaty data bases in the field. Especially useful are the Fletcher School's searchable text files of multilateral treaties and a site setting out the current status of treaties deposited with the UN. PIL also connects to a user friendly list of treaty links maintained by the House of Representatives, as well as a number of European and Australian treaty databases. The "war and peace" section is a PIL highlight. It hosts an extensive list of sites, organized into subsections for Chemical/Biological Warfare, Specific Conflicts, NATO, Terrorism, and War Crimes, and a catch-all subsection which includes the first rate International Committee of the Red Cross site. Finally, PIL's international law section has several on-line guides to Internet research, news sources (e.g., the Washington Post and the Economist Archive), and access to government organizations, whereas the general law section has numerous links to legal search engines (programs to search legal resources generally). For additional help in international law, consult the American Society of International Law's superb on-line guide to electronic resources (www.asil.org/resource/home.htm).

The premier host site for government material, "The US Government on the Internet," was developed by the Naval War College Library's Reference Branch. (www.usnwc.edu/nwc/govurl.htm). It offers everything from links to the various branches and individual agencies, to access to government search engines and full text files of documents such as the Supreme Court Reports. As might be expected, its compilation of military sites is unexcelled. The Government Printing Office's "Access Database" (www.access.gpo.gov/su_docs/aces/aces002.html) also gathers an impressive collection of government databases, including the US Code, select Supreme Court Reports, the Budget, Congressional bills and calendars, the Congressional Record and Comptroller General Opinions.

Equally impressive is Congress's site, "Thomas"

Continued on page 10
Schmitt on Internet Resources . . .
Continued from page 9

(thomas.loc.gov); it makes available bills, public laws, the Congressional Record, committee information, historical documents, and connects to sites maintained by the House, Senate, Library of Congress, GAO, and Congressional Budget Office. Additionally, most House committees, including the Committees on International Relations and National Security, have their own sites (www.house.gov/CommitteeWWW.html). These typically include such material as hearing transcripts, committee reports and bills, and activity surveys.

The Executive Branch is similarly well-represented on the Internet. For example, the White House (www.whitehouse.gov) site contains two useful subsites, "The Virtual Library," which posts publicly released documents (e.g., White House documents and executive orders), and "The Briefing Room," containing press releases and links to economic and social statistics. Additionally, the National Security Council has a web site (www.whitehouse.gov/WH/EOP/NSC/html/nsc/home.html), as does the State Department (www.state.gov/). The latter is especially useful as a source for US policy positions; it also provides online versions of both Dispatch and Treaties in Force.

For those interested in intelligence, the CIA web site (www.odci.gov/cia/ciaphome.html) is a find. Among other resources, it has an on-line version of The World Factbook and the Handbook of International Economic Statistics, as well as CIA maps. Likewise, the National Security Agency (www.nsa.gov/8080/) and Defense Intelligence Agency (www.dia.mil/) also maintain sites. Links to these and most other intelligence organizations can be found at www.odci.gov/cia/other_links/wheel/text.html.

Within government, the Department of Defense has the greatest Internet presence. "Defense Link" (www.dtic.dla.mil:80/delfenselink) is the basic site. From it one can access DoD directives and instructions, Defense Fact Files (weapons system descriptions), the President’s Annual Report to Congress, and, for those trying to navigate the maze that is the DoD, the Organization and Functions Guidebook. The Joint Chiefs site is most noteworthy for its "Joint Electronic Library" (www.dtic.mil/doctrine/index.html). JEL contains joint publications, select service publications, and an extensive collection of individual research reports. Expectedly, each of the services possesses a site (www.af.mil; www.army.mil; www.navy.mil; and www.usmc.mil; www.dot.gov/dotinfo/uscg/welcome.html), as do the various war colleges (National Defense University - www.ndu.edu:80; Air University - www.au.af.mil/au.html; Army War College - carlisle-www.army.mil; and Naval War College - www.usnwc.edu/nwc). The latter often offer full text files of their publications and handy links to other organizations involved in national security. Perhaps most importantly, federal government agencies, federal contractors and universities engaged in federally funded research can access the Defense Technical Information Center's holdings (www.dtic.mil/), including thousands of technical reports, R & D summaries, and independent research results by and about the Department of Defense.

Finally, a number of noteworthy organizations outside the US government support web sites relevant to national security. They include NATO (www.nato.int/), the UN (www.un.org/), Rand (www.rand.org/), Brookings (www.brook.edu/), the Heritage Foundation (www.nationalsecurity.org/), the Stimson Center (www.stimson.org/), the Center for Security Studies and Conflict Resolution (www.isn.ethz.ch/index1.htm), UVA’s Center for National Security Law (www.virginia.edu/~cnsi/), the ABA Standing Committee on Law and National Security (http://www.abanet.org/natsecurity/home.html), Duke Law School’s Center on Law, Ethics and National Security (http://www.law.duke.edu/general/program/lens/centralon.html), the US Institute of Peace (www.usip.org/library.html - contains links to most research centers worldwide), the International Institute for Strategic Studies (www.isn.ethz.ch/iiss/iiss/home.htm), the Canadian Forces College (www.cfsc.dnd.ca/), and Cornell University, which has both ICJ opinions (www.law.cornell.edu/icj/) and the US Code (www.law.cornell.edu/uscode/) online. Notably, Yale’s Law Library (eloinore.cis.yale.edu/lawweb/lawlib.htm) not only offers catalog access to their superb collection, but also links to many law journals, law schools, government agencies, and countless NGOs.

Surely countless valuable sites have been excluded in this brief survey; the above simply represent those one former cyberphobe has found beneficial. Hopefully, however, armed with this small sampling even novices should be able to profitably search the net for national security law resources.

Lieutenant Colonel Schmitt is an Air Force JAG officer currently assigned as Professor of International Law, United States Naval War College.
intelligence reporting emanating from a single source and which has not been evaluated for its reliability or significance. On occasion, relevant raw intelligence information may be provided to a congressional committee conducting a special investigation.

Mr. Snider reported that Congress is usually well-satisfied with the intelligence information it receives, in part because Congress can always request a briefing on virtually any subject to deepen its understanding of a particular piece of intelligence. Such briefings are given to committees as a whole, individual members, and to staff. In fact, Mr. Snider noted that nearly every day that Congress is in session, many days when it is not in session, intelligence briefings are being given on the Hill by some element of the intelligence community. According to Mr. Snider, Congress as a whole takes intelligence very seriously and usually regards intelligence as objective, factual, and free of political bias. Although some members of Congress look to intelligence to further their political battles with other members or with the administration, such incidents are the exception and not the rule.

With regard to the role of intelligence in decisionmaking, Mr. Snider reminded his audience that intelligence pertains to only one aspect of a larger picture. Intelligence does not, for example, encompass U.S. capabilities for dealing with a particular problem. It does not reveal diplomatic initiatives that may be underway, and it does not take into account U.S. public opinion or political imperatives. Interestingly, Mr. Snider stated that Congress typically gives more weight to intelligence as a factor in decisionmaking than do policymakers in the Executive branch.

He asserted that widespread congressional access to intelligence information produces some special problems for intelligence agencies. Given the number of intelligence briefings, often it is simply impossible to coordinate or even to inform policymakers that certain intelligence matters are being briefed to Congress. Many times the intelligence briefers are unaware that their briefing may run counter to a policymaker’s decision, of which intelligence was only one of many factors. As a result, policymakers often expend considerable time and effort responding to congressional inquiries arising from such briefings. Yet, if the policymaker is excluded from this process, the intelligence agencies run the risk of alienating the customers they principally serve, and may lose their ability to influence the policymaker. On the other hand, a particular member of Congress may take a dim view of an intelligence agency if the intelligence upon which the member relied proves wrong, particularly in a controversial issue.

Despite the complications produced by intelligence sharing among the executive and legislative branches, Mr. Snider concluded that intelligence

Standing Committee on Law and National Security

Chairman: Paul Schott Stevens
Advisory Committee Chair: Richard E. Friedman
Board of Governors Liaison: Thomas Susman
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
web page: http://www.abanet.org/natsecurity

Continued on page 12
The National Security Agenda . . .

by Daniel Richard

Senator Calls for More Efforts to Curb the Spread of WMD Technology - Senator Thad Cochran (R-Miss)—Chairman of the International Security, Proliferation and Federal Services Subcommittee of the Senate Governmental Affairs Committee—stated on 12 January that the Clinton Administration should step up efforts to prevent “rogue” nations from possessing Weapons of Mass Destruction (WMD) technology. The subcommittee recently issued a report called “The Proliferation Primer” which found that China is a major supplier of WMD technology and that Russia is providing Iran some missile technology. In response to these assertions, Senator Cochran has suggested that the US should speed up its deployment of an anti-missile defense system—notwithstanding the limitations imposed by the 1972 ABM Treaty. The Clinton Administration has renewed an executive order emphasizing the threat posed to US national security by the proliferation of nuclear, chemical and biological weapons, but has resisted deciding on the deployment of a missile defense system until 1999.

Federal Judge Criticizes State Department’s Visa Policy - United States Federal Judge Stanley Sporkin has challenged the State Department’s criteria for issuing visas by ruling in a recent court case that the State department’s visa policies in Brazil were “offensive” and “improper.” The case originated from a grievance filed by former State Department Counselor officer Robert E. Olsen against the State Department for dismissing him on grounds that he failed to carry out his duties as a counselor officer. According to Olsen, he refused to follow the Sao Paulo visa guidelines because they allegedly relied on discriminatory ethnic profiles. The State Department has rejected these allegations and continues to argue that “no applicant is refused a non-immigrant visa application on account of his or her ethnicity or nationality.” Nevertheless this ruling challenges the State Department’s use of profiles in embassies and consulates around the world. Moreover, it could set an important legal precedent by granting judicial review over the visa granting process instead of leaving the establishment of visa criteria as an exclusively administrative or political matter.

Israel, US Begin to Discuss Restructuring Financial Aid - According to Israeli press reports, Israel’s Finance Minister Ya’aqov Ne’eman is coming to Washington in January 1998 to meet with Congressional leaders and Clinton Administration officials to discuss the phasing out of $1.2 billion in annual economic aid starting in October 1999. In a 1998 speech before Congress, Israeli Prime Minister Netanyahu stated that he would work to reduce Israel’s dependence on US aid. Press reporting suggests that Netanyahu may now be seeking to follow up on this pledge to offset growing sentiment on Capitol Hill to reduce the foreign aid budget and to limit criticism leveled at his government that it is stalling the peace process. Although many observers have stated that congressional support for Israel is as strong as ever, there have been recent tensions between some Congressional leaders and Israel over the delay in extraditing a Maryland teenager and the initial refusal by Israel in 1997 to provide Jordan with $100 million in financial assistance.

Snider on Intelligence . . .
Continued from page 11
sharing helps to bridge the gap between the branches, and provides firm footing for positive dialogue on national security and foreign affairs matters. Until Congress, the Executive, and the Intelligence Community adopt “rules of the road” to avoid some of the common pitfalls and sources of friction, the problems inherent in sharing secrets with Congress, like most interactions between the branches, will be resolved in the rough and tumble process of politics.

Mr. Conner is a former naval intelligence officer now in private law practice in Washington, DC.