THE CIP REPORT

CRITICAL INFRASTRUCTURE PROTECTION PROGRAM VOLUME 6 NUMBER 7

JANUARY 2008
CIP AND LAW

This first issue of *The CIP Report* in 2008 highlights the work of the CIP Program's Law Team, as law research is one of the main focus areas of the CIP Program's core research efforts. Through the Law Team, numerous issues of interest with respect to critical infrastructure protection (CIP) are examined. While articles from the Law Team are frequently included in *The CIP Report* as "legal insights," this month's issue offers a broader look at the array of topics addressed in the CIP Program's law research.

GEORGE MASON UNIVERSITY
School of Law
CRITICAL INFRASTRUCTURE PROTECTION PROGRAM

An article exploring the development of international legal regimes to oversee cyberspace, including the Council of Europe Convention on Cybercrime, is provided. State freedom of information laws and the categorization of sensitive information concerning our Nation's infrastructure are addressed through a discussion of CIP Program participation in a Center for Terrorism Law conference, briefly outlined in the December 2007 issue of *The CIP Report*. The consideration of CIP from both U.S. and international perspectives is further depicted through articles on global partnerships in aviation security and the Spanish Flu, one of three influenza pandemics that impinged on the United States in the 19th century. An in-depth look at the Committee on Foreign Investment in the United States (CFIUS) and brief discussion of a new CFIUS law are also offered. Additionally, this issue features two articles detailing conference proceedings, the first addressing strategic deterrence in cyberspace and, the second, CIP in the States and the state-federal relationship.

Lending to future work, an overview of current and forthcoming Law Team projects is provided. Lastly, with regard to other CIP Program research projects, announcements of the release of a new monograph, *Critical Infrastructure Protection: Elements of Risk*, and of new sector maps are also included in this issue. Additional information and work products are available on our website.

As always, we thank you for your continued support of the CIP Program.

Cyberspace Security: Development of International Legal Regimes

by Timothy P. Clancy, JD, Principal Research Associate for Law

At the recent Association for Enterprise Integration (AFEI) conference on Strategic Cyber Deterrence, several commentators cited the need for developing internationally recognized standards of conduct in cyberspace. General Larry Welch, Director of the Institute for Defense Analyses, and Seymour Goodman, Professor of International Affairs and Computing at the Georgia Institute of Technology, both remarked that such a process will be long and difficult but necessary to reduce the threat of transnational cyber attacks on critical infrastructures.

International legal regimes and treaties are rooted in a system of national sovereignty known as the Westphalian system. Westphalian sovereignty is the core of the concept of the modern nation-state, emphasizing respect for territoriality and the rights of non-interference. It is clear that the Westphalian system of sovereign nations is under severe stress from economic globalization and trade, causing many policy scholars to question its relevance in the 21st century.

Development of international cyberspace conventions and treaties has been slow, despite widespread recognition of international cyber vulnerabilities going back to the 1980s. These concerns have only grown in the 21st century with the proliferation of failed states sheltering organized criminal and terrorist organizations that use the Internet for malicious purposes.

Unique features of the Internet—anonymity, ubiquity, complexity—are often cited as the reasons for the difficulty in constructing international cyber legal regimes. Spanning physical boundaries and national jurisdictions, the uniqueness of cyberspace makes it resistant to government regulation.

The advent of cyberspace has spawned many private legal schemes that cross international boundaries. The most prominent are the Internet Corporation for Assigned Names and Numbers (ICANN) as well as the existing Internet governance structure and the standards and protocols of the Internet. Private legal agreements such as licenses, arbitration and consent agreements are all utilized everyday to regulate and control behavior across the Internet. Communities of users and codes of conduct such as those found in the virtual reality world *Second Life* are an example of this type of private legal ordering.

Some legal scholars such as David Johnson and David Post hold the view that the Internet itself should be described as a sovereign entity with an entirely new legal system addressing individual and property rights.[1] Other the other hand, other American scholars such as Jack Goldsmith have long argued quite persuasively that national regulation of activities in cyberspace is legitimate and feasible from jurisdictional and choice of law perspectives.[2]

Domestic national laws of most nations are used to restrict all types of bad behavior in cyberspace, from ID theft to spamming to computer frauds and extortion. Domestic laws still, and likely always will, hold sway over behavior in cyberspace—creating a new multilateral regime regulating and governing all types of behavior in cyberspace is impractical, likely fruitless and runs contrary to the much of the international law governing other international networks.

Cross-jurisdictional concerns are not limited solely to cyberspace. All types of networks—transportation, energy, health, communications—cross territorial boundaries and

(Continued on Page 17)

[1] Law and Borders - The Rise of Law in Cyberspace, 48 Stanford Law Review, 1367, 1996, David R. Johnson and David G. Post; 'Chaos Prevailing on Every Continent': Towards a New Theory of Decentralized Decision-Making in Complex Systems, 73 Chicago-Kent Law Review, No. 4, p. 1055, 1998, David G. Post and David R. Johnson.
[2] Against Cyberanarchy, 65 University of Chicago Law Review, 1199, Fall 1998, Jack L. Goldsmith, http://cyber.law.harvard.edu/property00/jurisdiction/cyberanarchyedit.html.

State Freedom of Information Laws: Critical Infrastructure Exemptions

By Maeve Dion, JD, Legal Research Associate

In November 2007, the CIP Program participated in a conference entitled *Open Government Law and Practice in a Post-9/11 World.* The conference focused on non-release provisions in state open government laws enacted since the September 11, 2001 terrorist attacks. The conference included the release of a new book detailing changes in state public information laws. A PDF of the book is available here.

The conference was made possible by the Center for Terrorism Law at St. Mary's University School of Law in San Antonio, Texas, and was supported by a 2006 Congressionally-directed Homeland Defense and Civil Support Threat Information Collection grant, administered by the Air Force Research Laboratory. A vital partner in the conference and state law compilation was the Reporters Committee for Freedom of the Press.

Conference panelists commented on various categories of concern, including Critical Infrastructure, Public Health, Cyber Security, Political Structure, and Terrorism Investigations. The CIP Program's Legal Research Associate, Maeve Dion, spoke on the critical infrastructure panel. Printed below are excerpts of her papers, *Protecting Sensitive Information: Critical Infrastructure Protection at the State/Local Level* and *Protecting Sensitive Information: A Private Sector Perspective.* Release of the full papers, as well as those of the other conference panelists, is forthcoming from the Center for Terrorism Law.

What Infrastructure is Critical?

For freedom of information ("FOI") non-disclosure determinations rooted in critical infrastructure protection ("CIP") rationales, the question of what constitutes critical infrastructure ("CI") is often the crux of the debate. Formal governmental definitions of CI can be traced back to the 1996 executive order establishing the President's Commission on Critical Infrastructure Protection.

. . . More recently, in response to the September 11, 2001, terrorist attacks, Congress passed the Critical Infrastructures Protection Act, which defined CI as "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters."

Congress increased the complexity of its CI definition in the Homeland Security Act of 2002, where it differentiated "critical infrastructure" from the term "key resources," which was defined as "publicly or privately controlled resources essential to the minimal operations of the economy and government."

(Continued on Page 4)

Sources for Further Reading:

A Legal Guide to Homeland Security and Emergency Management for State and Local Governments (Ernest B. Abbott & Otto J. Hetzel, eds., 2005).

James W. Conrad, *Protecting Private Security-Related Information from Disclosure by Government Agencies*, 57 Admin. L. Rev. 715 (2005).

Homeland Security Information Sharing Between Government And The Private Sector, Private Sector Information Sharing Task Force, Homeland Security Advisory Council (2005).

Report of the Defense Science Board Task Force on Critical Homeland Infrastructure Protection, United States Department of Defense (January 2007).

FOI Laws *(Cont. from 3)*

These definitions are quite broad, and are not further defined in any piece of legislation (although individual agency regulations may provide more specific guidance within their jurisdictions). . . . Therefore, within the realm of national U.S. infrastructure, this is the guidance for determining which assets should be considered critical, and therefore which should receive the focus of federal CIP efforts and CI information protection.

. . . Within the many federal agencies, information may be withheld from public disclosure because the information is deemed Critical Infrastructure Information ("CII"), Sensitive Security Information ("SSI"), or Homeland Security Information ("HSI"). Also, in addition to the more traditional classifications of Top Secret, Secret, and Confidential, information may be labeled For Official Use Only ("FOUO") or Sensitive but Unclassified ("SBU"), and may thus be prohibited from certain transfers or disclosures.

It should be noted that a January 2007 report by a Defense Science Board Task Force (a Department of Defense federal advisory committee) criticized the Department of Homeland Security for its lack of guidance in developing clear, common definitions and common implementation procedures for these many levels of classification, particularly for the SBU category. As the report stated, "the issue of how much information the Federal Government really needs for homeland security, how to protect that information, and how to share it appropriately, were all open questions at the time this Task Force concluded."

And to further complicate the issue, the various information categories can have different definitions not only among federal agencies, but also within different state and local governments. . . . In addition to the federal government, many states have passed their own laws to protect CI and related sensitive information.

The Problem of Perspective

When it comes to applying these labels and state non-disclosure laws on a case-by-case basis in the context of FOI requests, the crux of the security-versus-openness debate is truly a matter of perspective.

. . . When a government entity decides to withhold information -- whether under a CI exemption in a FOI law, or under a law protecting CII or HSI information -- that entity does so on a case-by-case basis, on its own determination regarding both the criticality of the infrastructure and the sensitivity of the information being requested. These determinations may vary greatly among government bodies, depending on each entity's perspective of what is "critical" to that locality or to that specific government.

For example, what is critical to a city may not be critical to the nation, to a region, or even to the respective state. A city government may thus be concerned about protecting systems or assets that are "so vital to the ~~United States~~ *city* that the incapacity or destruction of such systems and assets would have a debilitating impact on security, ~~national~~ *local* economic security, ~~national~~ *local* public health or safety."

Security and public health and safety are inherent responsibilities of government; determinations of the criticality of the infrastructures within a jurisdiction depend on the risk calculations regarding the likelihood of the threat and the weight of the responsibility -- i.e., how great is the potential damage, based upon the level of vulnerability and the type and quantity of damage. If the disclosure of certain information could increase either the likelihood of harm or the consequential damage, the government may decide that one of its responsibilities is to restrict access to that information.

. . . There are several complicating circumstances that a government entity may face when deciding to release information under a FOI request, such as: (1) when the requested information, standing alone, may not be a security threat, but paired with other information, may be deemed a CI threat (i.e., aggregated information); and (2) when the requested information does not endanger infrastructure within that government entity's jurisdiction, but may imperil another jurisdiction's CI.

Thus, in regard to CIP-related state FOI requests, non-disclosure determinations are highly complex and may include decisions as to:

- what is critical to this jurisdiction;
- what is the likelihood of harm if the information is disclosed;
- does this non-sensitive

(Continued on Page 16)

Aviation Security & the International Community

by Colleen Hardy, JD, PhD, Senior Research Associate for Law and Biodefense Studies

A common theme can be seen when examining how the US government works to protect and safeguard a critical infrastructure. The pattern is to incorporate all essential partners associated with the sector and not limiting review and response plans to the US government alone. As is demonstrated across all of the critical infrastructures, it is essential for the US government to collaborate with local and private partners to ensure efficient protection. The transportation sector is an example of a critical infrastructure sector where collaboration and cooperation from the US government and other local partners is especially imperative. However, the aviation sector within the transportation sector calls for the US government to partner with the international community, with special attention to aviation security principles and policies. It is crucial for the US government to work with the international aviation community to ensure aviation security.

While increased global partnership in the aviation sector was greatly amplified after the terrorist attacks on September 11, 2001 and the thwarted terrorist attacks in August 2006 in the United Kingdom, it is not a new phenomenon. In 1944, 52 nations established the International Civil Aviation Organization (ICAO) with the goal to ensure the safe, orderly and economic development of international air transport. Currently, the ICAO consists of 190 State members. The present Strategic Objectives for the period of 2005-2010 include measures to enhance global civil aviation safety and security. The ICAO strives for member States and industry to work closely together to manage their safety initiatives with the ICAO in order to avoid replication and related inefficiencies in the implementation of global safety initiatives.

In February 2002, the ICAO established a Plan of Action for Strengthening Aviation Security in an effort to assist States and industry focus on all forms of aviation security issues. The Plan consists of an audit program to determine the level of implementation of security standards and provides recommendations to correct deficiencies. In the past five years, the ICAO aviation security audit teams conducted a total of 151 audits and were striving to complete audits on all 190 States by the end of 2007.

In November 2007, the President of the Council of the ICAO, Roberto Kobeh Gonzalez, stated the ICAO predicts that in 2025 there could be as many as 4.5 billion airline passengers per year. He reinforced the notion that aviation safety is a shared responsibility and as a result improvements can only be achieved through the leadership of ICAO and the cooperation among all the stakeholders, including airports.

In April 2007, the United States and the European Union reached the first-stage of the Air Transport Agreement. The Agreement establishes an Open-Skies Plus structure between the United States and all 27 EU Member States. Among other things, the Agreement allows every US and every EU airline to fly between every city in the European Union and every city in the United States. It also allows the US and every EU airline to operate without restriction on the number of flights, aircrafts and routes and sets fares according to market demand. The Agreement was developed to promote enhanced cooperation between US and EU aviation matters, especially in security measures. The first stage of the Agreement will go into effect on March 30, 2008.

In October 2007, the Transportation Security Administration (TSA) established a new office, the Office of Global Strategies. According to the TSA, the Office of Global Strategies' mission is to increase security by collaborating with foreign partners and overseas operations affecting the United States. The new office seeks to bolster common strategies on screening liquids, aerosols and gels, implementing advanced technologies and intelligence sharing. In TSA's October 2, 2007 press release, TSA Administrator Kip Hawley stated, "Over the past two years, we have been able to significantly strengthen our relationships with our international transportation security partners through increased communications, information sharing and best practices. The formation of the Office of Global Strategies further represents our commitment to ensuring the highest level of transportation security possible both here in the United States and abroad and illustrates the

(Continued on Page 15)

Foreign Direct Investment in Critical Infrastructure: An Update on the New CFIUS Law

by Maeve Dion, JD, Legal Research Associate

In November 2007, the Organisation for Economic Co-operation and Development ("OECD") asked the CIP Program to draft a white-paper for its *Roundtable on Freedom of Investment, National Security and 'Strategic' Industries* (Paris, Dec. 13, 2007).[1] The whitepaper gave us the opportunity to revisit our work[2] on foreign direct investment in the United States, focusing on national security restrictions and the new law that came into force on October 24, 2007.

Drawing from the OECD work and past CIP Program research, this article will provide an overview of recent Congressional action affecting the Committee on Foreign Investment in the United States ("CFIUS").

National Security-Based Restrictions on Foreign Direct Investment

In regard to perceived threats relating to foreign control of sensitive domestic assets, the United States uses various mechanisms to limit national security risks. For some industries, there may be a complete ban on foreign ownership, such as for nuclear power facilities. In other industries, foreign ownership may be subject to contractual security provisions. Such provisions may be required, for example, in communications licenses per the Federal Communications Commission (which often defers to risk assessments by the intelligence community in its case-by-case determinations). Another example of contractual security provisions is seen in the Department of Defense's ("DoD") use of Special Security Agreements, voting trusts, and proxy agreements, which all work to mitigate concerns of foreign ownership or control of an asset in relation to classified DoD contracts.

While these examples are specific to their respective industries, all industries are affected by a broad national security-based restriction on foreign mergers, acquisitions, and takeovers. In 1975, President Ford issued an executive order to create the Committee on Foreign Investment in the United States. Under this authority, the inter-agency CFIUS acted as a general investigator and policy advisor. Specifically, CFIUS was responsible for "monitoring the impact of foreign investment in the United States, both direct and portfolio, and for coordinating the implementation of United States policy on such investment." For its first decade, CFIUS had no strong screening power and acted completely at the discretion of the

(Continued on Page 7)

Links to Relevant Documents:

Foreign Investment and National Security Act of 2007, Pub. L. No. 110-49, 121 Stat. 246.

Breakdown (table) of the CFIUS process under the new law (pages 9-10 of this issue of *The CIP Report*).

Public comments regarding forthcoming new CFIUS regulations (following Oct. 2007 public meeting).

Report on U.S. Critical Technology Companies:
Report to Congress on Foreign Acquisitions of and Espionage Activities against U.S. Critical Technology Companies UNCLASSIFIED (Sept. 2007, declassified version of Dec. 2006 report).

[1] The OECD work is ongoing, so the paper is not yet available for distribution. For more information, contact Maeve Dion at mdion@gmu.edu or 703-993-4737.

[2] For a brief review of the CIP Program's work in this area, see http://cipp.gmu.edu/research/CFIUS.php.

CFIUS *(Cont. from 6)*

President. In the 1980s, Congress became increasingly concerned about the potential for foreign economic espionage, particularly in regard to critical technologies. Congress also wanted a stronger mechanism that could actually prevent transactions that posed national security risks. The resulting legislation was the Exon-Florio amendment to Section 721 of the Defense Production Act, passed as part of the Omnibus Trade and Competitiveness Act of 1988. The amended Section 721 authorized the President or his designee to (1) investigate direct foreign investments that might pose national security risks; and (2) suspend or prohibit the transaction, or order divestiture for a completed sale. In January of 1989, President Reagan named CFIUS as the President's designee under Section 721.

A few years later, Congress amended Section 721 to emphasize the concern that a foreign acquirer could be acting on behalf of (or could potentially be controlled by) a foreign government. The legislative changes (1) required a longer period of investigation for such transactions, and (2) attempted to enhance Congressional oversight and transparency by ordering quadrennial reports to track foreign economic espionage and foreign governments' investment strategies in US critical technologies.

In implementing its broad mandate, if CFIUS determined that a proposed transaction posed a national security threat, one of three things usually happened: (1) the foreign acquirer restricted its ownership structure so that "foreign control" of the sensitive asset was not implicated; (2) the foreign acquirer entered into agreements (contracts) with the relevant CFIUS member agency(ies) to mitigate the national security risk by restricting the foreign acquirer's discretion (e.g., in ownership structure, business operations, personnel decisions, etc.); or (3) the parties withdrew their CFIUS notice and either canceled the transaction or delayed it to negotiate changes that would satisfy a subsequent CFIUS review.

This CFIUS process continued for another 15 years without any substantial amendments (mostly just various changes to the membership of CFIUS). While the statute may not have changed, CFIUS reviews evolved to incorporate the changing threat environment. For example, after the terrorist attacks of September 11, 2001, CFIUS reviews of telecommunications transactions became more stringent.

Despite this and similar internal modifications, in recent years Congress became increasingly concerned with various perceived deficiencies in the CFIUS process, as highlighted by specific transactions which received much attention in the media (e.g., IBM - Lenovo, Unocal - CNOOC, Dubai Ports World - P&O Steam Navigation Company, etc.). In response, Congress passed the *Foreign Investment and National Security Act of 2007*, which came into effect on October 24, 2007. A breakdown of how CFIUS works under the new law can be found in the table on pages 9-10. If you are unfamiliar with CFIUS, it may be helpful to review the table before continuing with this article, as the following text primarily addresses only the recent changes to CFIUS.

Recent Changes to CFIUS

The *Foreign Investment and National Security Act of 2007* ("FINSA") significantly changed the text of the relevant US Code (50 U.S.C. App. 2170), and the changes were heralded by much fanfare in the press. However, the new law did not significantly affect the crux of the CFIUS mandate, nor did it make sweeping changes to the underlying risk assessments. Not all of the changes will be discussed in this article -- for example, the new requirements regarding certification by the parties to the transaction, CFIUS certifications to Congress at the end of each review, and non-delegation of certain authorities will not be addressed -- rather, this article will cover some of the main issues that have garnered most of the attention in the last few years.

National Security

The new law specifically states that "national security" includes issues of homeland security and related critical infrastructure concerns. "National security" was not further defined in the statute, leaving it up to CFIUS to apply the definition on a case-by-case basis, pursuant to new CFIUS regulations (forthcoming, no later than the end of April 2008). The phrase "economic security" was not added to the enumerated national security risk assessment factors in FINSA (but the President and CFIUS still have discretion to consider "such other factors as [they] may determine

(Continued on Page 8)

CFIUS *(Cont. from 7)*

to be appropriate, generally or in connection with a specific review or investigation").

Mandatory Investigations

Although the hype surrounding FINSA focused on the new mandatory investigation period for foreign government-controlled transactions and for transactions involving critical infrastructure, both of these mandates have exceptions. These exceptions are so encompassing that they almost overwhelm the "mandate."

For critical infrastructure transactions, the requirement of an investigation only applies if the transaction could impair national security and such potential impairment has not been mitigated. This in effect negates the "mandate" because the critical infrastructure transaction is put back on par with the non-critical infrastructure transactions (see the CFIUS table on pages 9-10 for a breakdown of the CFIUS process).

Further, for both critical infrastructure transactions and foreign government-controlled transactions, FINSA includes a specific exemption from the "mandatory" investigation. If the CFIUS chair and the designated lead CFIUS agency for the transaction jointly determine that the transaction will not impair national security, then no investigation is required. Thus, if a transaction does not pose a risk to national security, then there is no requirement for an additional 45-day investigation, even if the transaction involves critical infrastructure or is a foreign government-controlled transaction.

Note that internal CFIUS procedures, pre-FINSA, followed a consensus rule -- if merely one of the other member agencies called for an investigation, the investigation would occur. Under the new law, Congress has specifically stated that the CFIUS chair and designated lead could jointly veto another agency's call for an investigation. Although such a situation may be unlikely (especially given each agency's respect for the other agencies' national security risk assessments), it is possible under a strict reading of the new law. It will be interesting to see if the new CFIUS regulations address this matter.

Ultimately, though, despite the attention given to the "mandatory" investigations, this discussion may be academic because the phrase "investigation" is a misnomer. The distinction between the 30-day "review" period and subsequent 45-day "investigation" period may in reality be a distinction without a difference, for several reasons. First, many CFIUS reviews begin well before formal notification. Parties to a pending transaction often communicate early with various CFIUS member agencies so that they can anticipate the likely national security requirements and then build the mitigation factors into the transaction agreements. Thus the review may occur over a period of months, not just for 30 days. Second, in practice there may be little difference between the CFIUS activities in the "review" and "investigation" stages. The goal in both is to discover and mitigate potential risks to national security. The CFIUS member agencies use their own internal methods to accomplish this goal, and these methods do not vary just because the process has moved from the 30-day period to an additional 45 days. Therefore, although it has drawn much attention in political and media circles, the "investigation" merely operates as an extended review.

"Critical Infrastructure"

With FINSA, Congress enhanced the definitions section of the CFIUS statute, and included for the first time the phrase "critical infrastructure." However, Congress did not provide a new definition, but rather paraphrased the standard Federal definition (first defined in the USA Patriot Act). FINSA also states that the "critical infrastructure" definition is further subject to CFIUS regulations. It may be interesting to see if the new regulations refine this definition. More likely, practical definition of the term will evolve over time, based upon the case-by-case applications of CFIUS. Helpfully, FINSA includes a requirement that CFIUS publish (no later than the end of April 2008) guidance on the kinds of transactions that implicate national security risks, including those transactions that could involve the risk of a foreign government's control of US critical infrastructure.

Follow-Up & Enforcement

FINSA created new statutory requirements for follow-up and enforcement of CFIUS mitigation agreements (and other CFIUS-required conditions to the transaction) entered into by CFIUS

(Continued on Page 16)

The Committee on Foreign Investment in the United States (CFIUS)

THE PROCESS OF NATIONAL SECURITY REVIEWS AND INVESTIGATIONS
OF FDI-IMPACTED MERGERS, ACQUISITIONS, OR TAKEOVERS

I. Relevant Transactions

- Any merger, transaction, or takeover;

AND • proposed or pending after August 23, 1988;

AND • by or with any foreign person;

AND • which could result in foreign control of any person engaged in US interstate commerce.

II. Preliminary Activity

Parties to a transaction may talk with CFIUS member agencies to determine (1) if their transaction is likely subject to a CFIUS review, and (2) if so, what national security concerns are implicated and what measures could mitigate those concerns. Forthcoming regulations (2008) will provide examples of transactions that have presented national security considerations.

Parties thus (a) can structure their transaction to better satisfy CFIUS demands, (b) will hopefully have a more reliable expectation regarding the timeframe for concluding the transaction, and (c) can better manage communication of the transaction with shareholders and press, to lessen potential detrimental market perceptions and effects.

III. Initiation of Review

EITHER A. Any party to a relevant transaction (pending or already completed) may submit a written notice to CFIUS, identifying the transaction. Regulations describe the content required in the notice.

OR B. Any CFIUS member agency or the US President may:

1. unilaterally initiate review of a relevant transaction;

OR 2. unilaterally re-open review of a transaction that has already undergone CFIUS review ***if*** in the original CFIUS review any party to the transaction (a) submitted false or misleading material, or (b) omitted material information;

OR 3. re-open review of a transaction that has already undergone CFIUS review ***if*** the original CFIUS review resulted in a security agreement or other mitigation measure, and ***all*** of the following apply:

(i). a party to the transaction (or the entity resulting from the transaction) intentionally materially breached the agreement or other mitigation measure;

AND (ii). the breach is certified to CFIUS by the member agency responsible for monitoring and enforcing the agreement or other mitigation measure;

AND (iii). CFIUS determines that there are no other remedies or enforcement mechanisms to address the breach.

IV. Review

Within 30 days of accepting written notification, CFIUS must review the transaction to determine if it affects US national security. The CFIUS member agencies consider (1) factors specified by Congress (and potentially forthcoming in CFIUS regulations), and (2) other factors implicated by the specific transaction being reviewed (a case-by-case assessment).

V. Investigation

If any one of the following three situations apply, CFIUS must (1) conduct an investigation of the transaction (basically an extended review, to last no longer that 45 days from start of investigation), and (2) take necessary actions in relation to the transaction to protect US national security. NOTE: The requirement for investigations of transactions involving "critical infrastructure" only applies if the transaction could impair national security and such potential impairment has not been mitigated -- thus, the factor of "critical infrastructure" does not impose a situation different from non-critical infrastructure transactions. (Further, the exception of C.1. below also applies to critical infrastructure transactions.)

ONLY IF A. The lead CFIUS agency recommends *and* the other CFIUS member agencies concur, that an investigation is needed for further review of the transaction.

OR B. The outcome of the review shows that (a) the transaction threatens to impair US national security *and* (b) the threat was not mitigated during or prior to the review. Traditionally, if only one of the CFIUS member agencies perceives a non-mitigated risk to national security, that one agency's determination is enough to move to the investigation stage.

OR C. [***Unless the exception below is met.***] The outcome of the review shows that the transaction could result in the control of any person engaged in US interstate commerce by a foreign government or entity controlled by or acting on behalf of a foreign government.

EXCEPTION 1. However, if both the Secretary of the US Treasury (the Chairman of CFIUS) and the designated lead CFIUS agency for the transaction jointly determine that the transaction will not impair US national security, then no investigation is required.

VI. Mitigation and Enforcement

A. If the review and/or investigation resulted in (1) modifications to the transaction, and/or (2) security agreements between the CFIUS member agency(ies) and the parties to the transaction (or the entity resulting from the transaction), the designated lead CFIUS agency for this transaction is authorized to monitor and enforce the agreements.

B. If, at the conclusion of the investigation, the transaction is determined to impair US national security, the President may take appropriate action to suspend or prohibit the transaction. The President's determinations and actions are not reviewable in any court of law. The President may direct the US Attorney General to pursue relief, including divestment, in US Federal courts in order to implement and enforce this authority. However, the President may only exercise the authority under this paragraph if ***both*** of the following apply:

ONLY IF A. Based on credible evidence, the President believes that the controlling foreign entity might take action that threatens to impair US national security;

AND B. The President believes that, in relation to the transaction, other provisions of law (excluding the International Emergency Economic Powers Act) do not provide adequate and appropriate authority to protect US national security.

REFERENCES

50 U.S.C. App. 2170. Authority to review certain mergers, acquisitions, and takeovers (as amended by the Foreign Investment and National Security Act of 2007, Pub. L. No. 110-49, 121 Stat. 246).

CFIUS regulations are found at 31 CFR 800 (note that the published regulations are based on old law; new regulations are due by the end of April 2008). Some public comments regarding the forthcoming regulations can be found here.

Strategic Cyber Deterrence

by Timothy P. Clancy, JD, Principal Research Associate for Law

Is the theory of strategic deterrence relevant in cyberspace? Can and should the United States deter a cyber attack through the massive use of force? I attended a November 2007 conference on Strategic Cyber Deterrence[1] sponsored by the Association for Enterprise Integration (AFEI) consisting of international policy scholars, military strategists and technicians that explored these questions.

A product of the Cold War nuclear strategy, *strategic deterrence* refers to the threat by an adversary to inflict unacceptable destruction on a rational enemy in order to prevent similar attacks by the enemy. Strategic deterrence assumes that an adversary's ability to destroy is clearly demonstrated and well understood by the enemy—a notion famously satirized in the movie *Dr. Strangelove* with the secret Doomsday Machine. At its core, strategic deterrence theory is a classical economic equilibrium concept. By applying strategic deterrence theory, a nation-state seeks to impose huge costs and deny substantial benefits to encourage absolute restraint on potential adversaries.

During the Cold War, strategic deterrence represented the core of U.S. military strategy with its emphasis on mutually assured destruction and remains to this day. However, at the November AFEI conference, Professor Richard J. Harknett of the University of Cincinnati noted that the current cyber defense strategy of the United States does not emphasize deterrence but rather focuses on a continuous offensive/defensive strategy that assumes attacks will occur but will be mitigated by a superior U.S. and international response. [2]

Richard Clarke, during his luncheon address to conferees, flatly rejected strategic deterrence as a solution in search of a problem. Clarke contended that concerns over catastrophic cyber terrorism are overblown as most computer attacks fall into two categories, traditional cyber crime or computer espionage, and that these attacks, while on the rise and extremely troubling, do not rise above the nuisance level. Terrorist groups such as Al Qaeda depend on information networks mostly for fundraising and propaganda, not launching destructive attacks. Likewise, organized crime groups depend on the Internet for their cyber crime revenue—fraud, ID theft, etc. Any threat to vulnerable critical infrastructures, Clarke argues, can be solved by governments enforcing proper cybersecurity practices through effective regulation of private sector infrastructure owners and operators.

Many other conference speakers noted numerous defects of "classical" Cold War deterrence theory when applied to cyber conflict. Conflict in cyberspace is complicated by a complex, non-linear environment filled with non-state actors, lack of attribution and low barriers of entry for adversaries. Deterrence rests on all players knowing clearly the costs/benefits of certain actions. In a cyber conflict, it is not clear what response the United States would implement or if the U.S. capability could be publicly declared, acknowledged and credibly demonstrated (i.e., nuclear tests).

All presenters agreed that development of attribution or forensic technology—the ability to track and trace back to the source of malicious attack—is critical to any national cyber deterrence strategy. However, as Dr. Ronald Ritchey of Booz Allen Hamilton and others pointed out, attribution technology remains in

(Continued on Page 18)

[1] For the full agenda, see: http://www.afei.org/brochure/8a01/documents/Program31October.pdf.

[2] "Consistent with the objectives of the National Strategy for Homeland Security, the objectives of the National Strategy to Secure Cyberspace are to: Prevent cyber attacks against our critical infrastructures; Reduce our national vulnerabilities to cyber attack; and, Minimize the damage and recovery time from cyber attacks that do occur." [emphasis added] *The National Strategy to Secure Cyberspace,* 2003, pp. 13-14, http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.

The Spanish Flu (1918 - 1919)

by Colleen Hardy, JD, PhD, Senior Research Associate for Law and Biodefense Studies

Many people are aware of the emerging threat of influenza pandemic. However, most people do not know that the United States battled three influenza pandemics during the nineteenth century. The most lethal pandemic was the Spanish Flu which killed several thousands of people in the United States.

The Spanish Flu plagued the United States during the First World War. Outbreaks were reported in North America, Europe, Asia, Africa, Brazil as well as the South Pacific. There are many unanswered questions regarding the Spanish Flu. Many speculate that the uncertainty surrounding the Spanish Flu is due in part to the country being at war as well as the fact that newspapers, magazines and even some parts of the government ignored the pandemic. However, as one author noted if one looks to letters, journals and personal diaries from that time, it is apparent that US citizens were in fact frightened and their lives were drastically affected by the outbreak. Another source speculates the flu did not receive great attention because the devastation came and disappeared quickly, even before the economy was affected.

What is remarkable about the Spanish Flu is the absence of data and information concerning it, especially since it took so many lives. In fact, according to one source, no infection, war or famine has ever been credited with taking so many lives in such a short amount of time as the Spanish Flu did. In fact, the Spanish Flu killed more people in one year than the Black Plague killed in four years.[1] There are disagreements as to the exact number of related deaths, however some state the flu killed over 50 million people. One scholar stated 675,000 Americans died from the flu, which is ten times as many killed in the war.

The first wave of the Spanish Flu emerged in the spring of 1918 in Kansas as well as military camps throughout the United States.[2] Soldiers returning from battle carried the virus back into the United States, which created the second wave. In September 1918, the flu emerged in Boston through ports which received war shipments. The flu also reached San Francisco that September. The war also played a large role in spreading the virus. Men were traveling all over the country to join the military and spread the virus during their journeys. Masses of people went out and celebrated the end of the war in November 1918 and as a result the virus spread once again.

Victims of the Spanish Flu were inflicted with severe pneumonia and fatal pulmonary complications. Patients generally complained of weakness and severe aches in their muscles, backs and joints as well as headaches.[3] Violent coughs, nose bleeds, delirium and high fevers were also common. Another notable fact about this flu is that most of the victims were young individuals. The death rate was highest among individuals between the ages of 15 and 40. Ordinarily, infants, the elderly and those who are chronically ill are amongst the highest death toll for an influenza pandemic.

Unfortunately, doctors and nurses were limited with available treatments for patients. Individuals affected by the flu usually died very quickly. According to the Department of the Navy,[4] the US Navy was forced to rely on quarantine or infectious disease stations to care for its patients. Some cities also enforced quarantine and closed schools, theaters and even churches to prevent the disease from spreading. The Department of Navy depicts one nurse's experience at the Naval Hospital in Illinois in

(Continued on Page 13)

[1] Molly Billings, *The Influenza Pandemic of 1918,* June 1997, available at: http://virus.standford.edu/uda/.

[2] *Id.*

[3] The American Experience, *Influenza 1918, Among the Victims,* available at: http://www.pbs.org/wgbh/amex/influenza/sfeature/victims.html.

[4] Department of the Navy – Naval Historical Center. Influenza of 1918 (Spanish Flu) and the US Navy. Available at: http://www.history.navy.mil/library/online/influenza_main.htm.

Flu *(Cont. from 12)*

1918– Nurse Josie Brown described the gruesome situation and reported that the morgues were completely full with bodies, stacked one on top of another. Nurse Brown also recounted that one could never turn around without seeing a truck loaded with bodies on route to the train station so the bodies could be returned to their homes. There were so many patients to treat, Nurse Brown reported that they did not have enough time to treat them all and most patients would receive hot whisky.[5]

The war greatly impacted the medical community. The majority of doctors and nurses were serving in the military and thus there was a severe shortage of civilian doctors and nurses. According to one report, due to the lack of medical professionals, medical students were asked to help out with the sick patients.[6] Doctors and nurses were commonly victims of the virus as well. The American Red Cross took an active role recruiting volunteers to help care for the sick.

Local governments responded differently to the outbreak of the Spanish Flu. For example, some scholars report that most government officials did not want to cause mass panic and chose instead to either ignore the pandemic or to report there was nothing to worry about. However, in San Francisco a law was passed requiring individuals to wear a mask out in public.[7] If people were caught out in the public not wearing their masks, they would be taken to jail. In Philadelphia, the Department of Health and Charities issued statements informing the public that the illness would not spread beyond military personnel.[8] However, after numerous civilians were reported to be affected by the Spanish Flu, the city closed churches, schools and theaters.

The Spanish Flu only slightly impacted critical infrastructures across the nation. According to one report, a number of trash collectors in San Francisco were taken ill and as a result trash lined the streets.[9] Philadelphia was so overwhelmed with the number of corpses that the local government pleaded to the federal government to supply them with embalmers.[10] One of the biggest problems was the shortage of coffins. One scholar noted infrastructure was not as severely impacted due to the fact that it was less complex than it is today as well as there was less dependence on just-in-time delivery of crucial resources and materials.[11]

There are reports about communities living in extreme fear during this year. Some people were frightened to leave their house or let anyone into their house, even soldiers returning home from the war.[12] As a result, industry, including companies vital to the war effort, was affected by employees not showing up to work. According to one report, almost 50% of one company's workforce stayed home when their town was infected with the flu.

The United States battled two other influenza pandemics during the nineteenth century. The Asian Flu occurred during 1957 and 1958. Close to 70,000 people died in the United States from this outbreak and the mortality rate was highest amongst the elderly. The Hong Kong Flu emerged in the United States in 1968 and killed about 35,000 people.

What have we learned from these pandemics? According to *Avian Influenza: Assessing the Pandemic Threat,* a World Health Organization (WHO) report issued in January 2005, there are several lessons we can learn and use to help prepare for the next influenza pandemic.

(Continued on Page 18)

[5] *Id.*
[6] See Billings, *supra* note 1.
[7] The American Experience, *Influenza 1918, San Francisco*, available at: http://www.pbs.org/wgbh/amex/influenza/sfeature/sanfran.html.
[8] The American Experience, *Influenza 1918, Philadelphia*, available at: http://www.pbs.org/wgbh/amex/influenza/sfeature/philadel.html.
[9] The American Experience, *Influenza 1918, San Francisco*, *supra* note 7.
[10] The American Experience, *Influenza 1918, Philadelphia, supra* note 8.
[11] Dr. Richard Hatchett, *The Effects of Infrastructure and Government,* Pandemic Influenza - Past, Present, Future Workshop, October 17, 2006.
[12] John Barry, *The Effects on Society at Large,* Pandemic Influenza - Past, Present, Future Workshop, October 17, 2006.

CIP and the States: Fall Meeting of the Homeland Security Task Force, National Conference of State Legislatures

by Timothy P. Clancy, JD, Principal Research Associate for Law

The roles and responsibilities of States for protecting the nation's critical infrastructure is often overlooked. Actions and reports by Congress, the federal government and the private sector tend to attract the most attention in the press. However in the end, State governments and localities provide most of the protection for citizens and their infrastructure through traditional police powers.[1]

Under current federal policy, the Department of Homeland Security (DHS) provides significant CIP grant funding to the States and acts as "coordinator-in-chief" for CIP activities among the State, local and tribal governments.[2] The National Infrastructure Protection Plan (NIPP) released by DHS in June 2006 represents the most comprehensive attempt by the federal government to define the roles and responsibilities of the various stakeholders tasked with the complex task of protecting critical infrastructure in the United States. The NIPP calls on State, local and tribal governments to develop and implement a CI/KR protection program as a component of their overarching homeland security programs and provides an integrated risk management framework that States and other stakeholders can utilize to implement a CI/KR protection plan.

From founding of the republic, the domestic security relationship between the States and the federal government has been marked with tensions over federalism. CIP is no exception to this dynamic and, as Maeve Dion's article on State Freedom of Information Laws in this month's edition of *The CIP Report* shows, it is often left to the States and their legislatures to work out the gritty details of balancing competing interests of openness and security.

It is under this backdrop that I gave a presentation to the Homeland Security and Emergency Preparedness Task Force of the National Conference of State Legislatures (NCSL) at its two-day meeting on Critical Infrastructure Protection and the States, the NCSL Fall Forum in Phoenix, Arizona from November 27-28, 2007. The CIP Program was invited by Task Force co-chairs Senator Richard T. Moore (D-Massachusetts) and Senator Thomas J. Wyss (R-Indiana) to give the opening presentation, an overview of CIP issues of interest to the States.

Reflecting the traditional State/federal tension, the Task Force discussed the omission in federal National Response Framework (NRF) of any mention of the role played by state legislatures in emergency response.[3] The Task Force also heard from DHS representatives via teleconference on incorporating the NIPP risk framework within State homeland security plans and Protected Critical Infrastructure Information (PCII). A representative of the Federal Energy Regulatory Commission (FERC) also gave an overview of

(Continued on Page 15)

[1] "State, local, and tribal governments are responsible for implementing the homeland security mission, protecting public safety and welfare, and ensuring the provision of essential services to communities and industries within their jurisdictions." *National Infrastructure Protection Plan*, 2006 Sect. 2.2.4, p. 23.

[2] "Roles and Responsibilities of the Secretary
(12) In carrying out the functions assigned in the Homeland Security Act of 2002, the Secretary shall be responsible for coordinating the overall national effort to enhance the protection of the critical infrastructure and key resources of the United States. The Secretary shall serve as the principal Federal official to lead, integrate, and coordinate implementation of efforts among Federal departments and agencies, State and local governments, and the private sector to protect critical infrastructure and key resources." [emphasis added] *Homeland Security Presidential Directive (HSPD)-7*, Sect. 12, December 17, 2003.

[3] Comment letter on the National Response Framework from the NCSL to the Regulatory and Policy Team DHS/FEMA, October 17, 2007, http://www.ncsl.org/print/terrorism/NRFcomments.pdf.

States *(Cont. from 14)*

the FERC process to certify security procedures at FERC-regulated dams and hydro facilities.

After speaking to several individual Task Force members, it was clear that most of the States (about 20) represented at the meeting were implementing some form of CI/KR protection plan. Also, members were well-versed in the debates over the implementation of PCII and the challenges for States to balance openness with security, several members having drafted model statutes for CIP information sharing within their States.

Apart from PCII, developing effective mechanisms for building trust among key CIP stakeholders was a major concern to the Task Force. The creation of DHS-funded "fusion centers" for information has garnered much attention among many State legislators but confusion over how these fusion centers would integrate with similar yet much larger and better-funded federal centers.

It is no surprise that the members of the NCSL Task Force are extremely savvy on homeland security issues. Many members of the Task Force currently chair their respective State homeland security legislative committees/subcommittees and sit on the various homeland security councils within their States.

Even with the wealth of experience on the Task Force, I came away impressed by members' attention to and interest in CIP issues. Issues such as risk management, interdependencies and information sharing are highly complex, arcane and, at the state level, often overshadowed more pressing concerns of emergency preparedness, response and first responder funding. This is good news as we move from CIP planning to CIP implementation with the release of the NIPP -- much of the activity in the years ahead will be taking place in the States. The CIP Program will be closely monitoring these developments and working with groups like NCSL, the National Governors Association and the Multi-State ISAC to help improve understanding of CIP issues as they relate to the States.

Note: Thank you to Gartner Girthoffer of the NCSL staff and to Senators Moore and Wyss for inviting GMU's CIP Program to meet with the Task Force. ❖

Aviation *(Cont. from 5)*

importance of cooperation with our international partners."

More recently, in November of last year, the members of the European Union, as well as Norway, Switzerland, and Iceland, initiated new security measures related to liquids in carry-on bags in an effort to synchronize with measures established by the United States and Canada in September 2006. According to the TSA, a result of the European Union's new security measures, "approximately half of the world's travelers will be governed by similar security measures." Australia, Japan, Lithuania, Republic of Korea, Hong Kong, and Greece are just a few examples of the 41 nations listed by the TSA who are implementing new security measures to harmonize security at airports. Kip Hawley acknowledged that a strong base of security across the globe is more efficient than having the highest levels of security in only a few select places. Furthermore, he stated that implementing a consistent level of security worldwide will lead to true harmonization. (See http://www.tsa.gov/approach/harmonization.shtm.)

The terrorists behind the September 11, 2001 attacks used airplanes to carry out their attacks. In December 2001, Richard Reid attempted to ignite explosives hidden in his shoes on a flight from Paris to the United States. In August 2006, British authorities arrested several individuals suspected of planning a terrorist attack. The alleged terrorists were plotting to bring liquid explosives onto air planes flying to the United States. Thus, flights coming to and from the United States continue to be a potential target for terrorist activity. As demonstrated above, the United States is not only working with domestic partners but also international partners to protect this essential infrastructure. It is important for the US government to continue collaborating with the international community to ensure the utmost protection and to prevent future attacks. ❖

FOI Laws *(Cont. from 3)*

information become more sensitive when paired with other information;
- what is critical to interconnected and interdependent systems and jurisdictions, and does the release of this information endanger those other constituencies;
- and do any or all of these concerns outweigh our traditional policies of open government?

Further, a state or local government would also have to determine whether the respective CI at issue falls under any federal information-protection laws and regulations, so that even if the state would permit its release, the federal government mandates non-disclosure.

. . . It has only been six years since the 2001 terrorist attacks, and since Congress first defined "critical infrastructure" from a federal perspective. In the immediate aftermath of September 11, 2001, state and local governments responded to an upsurge of security and safety fears. In the intervening years, we have all had to wrangle with the concepts of homeland security and critical infrastructure protection. . . . As more time passes without CI attacks or increases in threats, local governments may reach different conclusions when balancing security versus openness.

Many non-disclosure decisions under FOI laws are challengeable; following the relevant administrative procedures, courts may find that, although the government should be granted deference in its security and safety determinations, withholding of some information is no longer reasonable -- either because the threat environment has changed, or because the subject is not really a matter of "critical infrastructure," "sensitive security," or other security information protection category.

. . . We have a history of using the states as experimental laboratories, where new procedures or laws or policies can be tried out, amended, and refined; very often this approach helps us find the best practices. Perhaps this approach will also prove true in relation to protecting sensitive CI information. If so, rather than calling for a federally-led common CI definition and CIP exemption to FOI laws, we might instead begin a survey of the best practices among state and local FOI-responding offices.

If we look at how these entities make their criticality and risk determinations, not only might such a study be useful for other state and local governments, it might also help us refine our federal practice of protecting CII, SSI, HSI, etc. ❖

CFIUS *(Cont. from 8)*

member agencies and the parties to the transactions. In the past, each CFIUS member agency conducted follow-up and enforcement based upon the respective agency's internal processes -- there was no common procedure, and thus no common tracking mechanism or comprehensive Congressional oversight. Under the new law, CFIUS must use common methods for evaluating compliance with the mitigation agreements. For each transaction, the lead CFIUS agency is required to monitor and enforce the agreement, and to report any future material modifications to all relevant Federal agencies / departments.

Congressional Oversight

The amendments to the CFIUS law also include a number of new provisions that increase Congressional oversight, including:
- Notifications of completed CFIUS reviews;
- Certifications of completed investigations;
- Briefings of specific transactions or mitigation agreements / conditions;
- Detailed annual reports of all reviews and investigations, including comprehensive assessments of possible trends in foreign investment; and
- Annual reports of trends of foreign investment in critical technologies -- specifically, whether there is any coordinated strategy to target critical US technologies, and whether foreign governments are conducting (directly or indirectly) industrial espionage activities targeted at critical US technologies. Note that this had been a quadrennial requirement since the 1988 amendment to the CFIUS law, but only one report had been issued in the period from 1989 - 2005. In the wake of recent Congressional hearings and numerous bills to reform CFIUS, a new critical technolo-

(Continued on Page 21)

Cyberspace Security *(Cont. from 2)*

have posed regulatory and security problems for sovereign nations. Most of these networks have existed since dawn of the modern age and most are privately owned, operated and governed. International standardization bodies and governance structures have been established to improve legal harmonization and arbitrate cross jurisdictional disputes. There are myriad examples including the International Telecommunications Satellite Organization (ITSO) and the International Civil Aviation Organization (ICAO), among others.

The Council of Europe (COE) Convention on Cybercrime[3] is the first and only international treaty dealing specifically with malicious use of international information networks. The Convention was signed in 2001 by the United States and 29 other nations and ratified by the Senate in 2007. Signatory countries agree to establish their own domestic criminal laws to combat cyber crimes such as copyright infringement, computer-related fraud and child pornography and violations of network security such as hacking and spreading of viruses. The Bush Administration has encouraged other countries to become signatories to the Cybercrime Convention.[4]

The Convention does not itself create substantive criminal law offenses or detailed legal procedures. Rather, parties agree to enact domestic laws that criminalize several categories of conduct outlined in the Convention, establish the procedural tools necessary to investigate such crimes under their own national laws and streamline procedures for international law enforcement cooperation.

International agreements like the COE Convention on Cybercrime that promote harmonization of domestic laws and seek to lessen jurisdictional conflicts are likely to gain traction in the years to come. As mentioned previously, there is ample precedent for this type of multilateral agreement regulating activities across other international networks. While no other convention or multilateral agreement regulating behavior in cyberspace is currently under consideration, the International Telecommunications Union (ITU) other international organizations are looking to the COE Convention as a template for future international cyber agreements. ❖

[3] Council of Europe - ETS No. 185 - Convention on Cybercrime, http://conventions.coe.int/Treaty/EN/Treaties/Html/185.
[4] "The United States will encourage other nations to accede to the Council of Europe Convention on Cybercrime or to ensure that their laws and procedures are at least as comprehensive." *The National Strategy to Secure Cyberspace,* 2003, p. 53, http://www.whitehouse.gov/pcipb/cyberspace_strategy.pdf.

Deterrence *(Cont. from 11)*

its infancy and there is little government research investment in this area.

Does this mean deterrence has no place in U.S. cyber security strategy? No, according to Dr. Greg Rattray, a former Air Force officer, cybersecurity consultant and conference presenter. The complex environment of cyberspace makes applying deterrence more difficult but not impossible, Rattray argued. Deterrence is attractive to the United States, he noted, due to its relatively low cost compared with a continuous and escalating game of cyber offense/defense. To make deterrence relevant in the cyber world, new analytical approaches, theory development and focused research on cyber warfare scenarios are needed, Rattray said.

While acknowledging that all cyber threats cannot be deterred,[3] current US cyber policy does leave room for deterrence. The National Strategy to Secure Cyberspace specifically calls for "developing national security programs to deter future cyber threats" [emphasis added].[4] The United States military is eyeing cyberspace as the next domain for conflict similar to the domains of Air, Land, Sea and Space.[5] The United States Air Force has created an independent Cyber Force and has declared that it will fly and fight in Cyberspace.[6]

The offensive capability of the U.S. military is likely to become an important factor in "keeping the peace" in cyberspace. But many questions remain as to how, when and if this capability will be used. In each of the physical domains, a military force can effectively control the battlespace by projecting power. Cyberspace is a mixture of loosely governed transnational networks owned and operated by private companies. It is not clear whether a military could effectively dominate the cyberspace domain and deter cyber threats through overwhelming force where private companies such as Internet Service Providers (ISPs) effectively control the field.

It is clear that deterrence principles—imposing costs, denying benefits and encouraging restraint—are relevant in securing cyberspace and protecting critical infrastructure. Military power alone will not be enough and, indeed, be only part of a multi-pronged integrated strategy that includes law enforcement, diplomatic and economic power to achieve restraint on the part of potential cyber attackers. ❖

Flu *(Cont. from 13)*

For example, the report stated pandemics are extremely unpredictable and there are great variations between the severity, patterns and mortality of each outbreak. The WHO report also noted that it is essential for pandemic preparedness plans to acknowledge the fact that there will be numerous cases at the onset of the pandemic and the potential remains for the number of victims to drastically increase in a short amount of time. In addition, while the potential to help is certainly great, it remains to be seen how vaccines will truly impact a pandemic. Vaccines were used during the Asian and Hong Kong Flu. However, vaccine manufacturers' capability to produce vaccines quickly was severely limited and as a result most vaccines were received too late to have any real impact. Thus, it is important to review lessons learned as well as examine facts, trends and patterns of prior influenza pandemics so that the United States can better prepare and plan for the next outbreak. ❖

[3] "As technology evolves and new systems are introduced, new vulnerabilities emerge. Our strategy cannot be to eliminate all vulnerabilities, or to deter all threats." *The National Strategy to Secure Cyberspace*, 2003, p. 27-28.
[4] Priority II: A National Cyberspace Security Threat and Vulnerability Reduction Program, *The National Strategy to Secure Cyberspace*, 2003, p. 3.
[5] "Cyberspace is a true Domain on a par with Land, Air, Space and Sea is to apply the basic questions of the Principles of War." Remarks of Michael W. Wynne, Secretary of the Air Force delivered to the C4ISR Integration Conference, Crystal City, Va., Nov. 2, 2006, http://www.af.mil/library/speeches/speech.asp?id=283.
[6] "The Mission of the Air Force is to deliver sovereign options for the defense of the United States of America and its global interests-- to fly and fight in Air, Space and Cyberspace." Remarks of Michael W. Wynne, Nov. 2, 2006.

Current Law Research & Forthcoming Projects

Following are some of the projects planned by the CIP Program's "Law Team."

Experimental Neuroeconomic Research and Critical Infrastructure Decision-Making

Realistic threat-based, scenario-based tabletop exercises are central to any strategy of critical infrastructure protection. Currently development of these exercises is more of an art than science, but new advances in human cognition, complex game theory and experimental economics can shed light on the CI decision-making process and hopefully lead to improvements in exercise development. Unique to George Mason University is laboratory research of Dr. Kevin McCabe on neuroeconomic subjects and collection of human cognitive data on functional brain activity during decision-making. This year, the CIP Program will be working with Dr. McCabe on applying the results of his research to critical infrastructure protection. For more information, contact Tim Clancy at tclancy@gmu.edu or 703-993-9605.

International Law and Cyber Conflict / Defense

Most of the literature in the field of cyber conflict has been authored by a select, core group of researchers with specific cyber expertise. This project will (1) evaluate those arguments, and (2) provide a non-cyber expert's analysis of how International Law and US Constitutional law inform the debates regarding sovereignty and security/defense in the cyber realm. This project will survey the existing literature on cyber conflict/defense and will provide an analysis of the problems and proposed remedies. A renowned scholar of International Law and US Constitutional Law will then critique these arguments and will add his own legal analysis and observations, with the goal of crafting a journal-quality law review article. For more information, contact Maeve Dion at mdion@gmu.edu or 703-993-4737.

Updates on the Committee on Foreign Investment in the United States ("CFIUS")

As part of our ongoing work in this area, we will provide a review of the new CFIUS regulations once they are released (by statute, no later than the end of April 2008). Also, upon completion of the current project for the *OECD Investment Committee's Roundtable on Freedom of Investment, National Security, and 'Strategic' Industries*, we will release the publicly-distributable materials. For more information, contact Maeve Dion at mdion@gmu.edu or 703-993-4737.

Critical Assessment: Cyberpower and Critical Infrastructure Protection

The CIP Program is writing this chapter of a book from National Defense University Press, forthcoming in 2008. For more information, contact Maeve Dion at mdion@gmu.edu or 703-993-4737.

Legal Liabilities of Internet-based Port Scanning

Network scanning activities help improve computer security, but the legal framework for such activities is far from clear. This project assesses the judicial opinions and legislation (domestic and international) that may affect legal liability for port scanning operations. The goal is to develop a law review article that shows how such liabilities affect the vulnerabilities of our computer systems and interdependent critical infrastructures. For more information, contact Maeve Dion at mdion@gmu.edu or 703-993-4737. ❖

Release of Monograph on Critical Infrastructure Protection and Risk

As efforts to better protect our Nation's infrastructure advance, the term *risk* is being increasingly used in discussions on homeland security. To promote a greater understanding of risk and how it relates to critical infrastructure protection (CIP), the CIP Program recently released a monograph entitled *Critical Infrastructure Protection: Elements of Risk*. The monograph consists of seven papers addressing numerous topics associated with risk, including the definition of risk, assessment methodologies, and strategic approaches to risk management. A brief overview of each paper is provided below.

In *Security Risk Management: Implementing a National Framework for Success in the Post-9/11 World*, Edward Jopeck and Kerry Thomas of the Security Analysis and Risk Management Association (SARMA) address the need for a national strategy for security risk management, particularly taking into consideration the promotion of a risk-based approach to CIP and limited progress made in developing relevant collaborative public-private efforts. The paper outlines detailed suggestions for enhancing security risk management.

Geoffrey French of CENTRA Technology, Inc. addresses terrorism and threat analysis in *Intelligence Analysis for Strategic Risk Assessments*, affording readers information on the first component of risk, threat. The author discusses how threat information contributes to strategic terrorism risk assessments and provides an in-depth look at the varying types of analysis, noting that the use of certain types may be more beneficial than others when managing and mitigating risk.

In *The Meaning of Vulnerability in the Context of Critical Infrastructure Protection*, William McGill and Bilal Ayyub of the University of Maryland explore ways to measure vulnerability, the second component of risk, and provide an operational definition for the term. The paper describes how probability impacts vulnerability assessment, thus risk assessment, and features mathematical expressions that detail two categories of vulnerability, protection vulnerability and response vulnerability.

Todd White of the Phoenix Police Department / Arizona Counter Terrorism Information Center and Samuel Ariaratnam and Kraig Knutson of Arizona State University provide an example of a state's approach to CIP in *Vulnerability Assessment of Arizona's Critical Infrastructure*. Highlighting the vulnerability assessment methodology used by the State of Arizona, the authors describe Arizona's terrorism prevention program and address issues such as data collection, training, layered screening for site evaluation, protection measures, and infrastructure design standards.

Managing Risk in Critical Infrastructures Using Network Modeling by Thomas Mackin of California Polytechnic State University and Rudy Darken and Ted Lewis of the Naval Postgraduate School explores the use of network analysis in a risk-based approach to CIP, specifically through the use of critical node analysis. The authors use an example from the Energy Sector to illustrate how critical node analysis plays an important role in the identification and prioritization of critical infrastructure.

In *Same Words, Different Meanings: The Need for Uniformity of Language and Lexicon in Security Analysis and Risk Management*, Andrew Harter of SRA International, Inc. discusses the need for a common lexicon in the field of security analysis and risk management. The author examines the development of voluntary consensus standards for a common lexicon and delineates the process for creating such standards, demonstrating one way of addressing the lack of consistently and commonly used terminology.

Robert Liscouski of Centurion Holdings, LLC and Nir Kossovsky of Steel City Re, LLC focus on the need for improved corporate security risk management practices in the final paper of the monograph, *The Intangible Value of Security in a Volatile Global Economy*. In discussing enterprise risk management and the notion of security as an intangible asset, the authors provide examples of the impact risk has on business practices and offer valuable guidance stemming from the efforts of the Intangible Asset Finance Society's Security Risk Management Committee.

The monograph is available on the CIP Program website at http://cipp.gmu.edu/research/CIP_Risk_Monograph.php.

CFIUS *(Cont. from 16)*

gies report was sent to Congress in January 2007, in the midst of debate regarding the FINSA amendments. (Click here to view the unclassified version of this report.)

Note: This article only provides a brief overview of CFIUS issues related to the new statutory amendments. The CIP Program is conducting ongoing work in this field, and we hope to publicly release some of our new work later this year. ❖

CIP Program Website Features Additional Sector Maps

As work continues on the CIP Program's Sector Mapping Project, first introduced in the October 2007 issue of The CIP Report, additional maps have been finalized and made publicly available. Each map developed by Program staff visualizes a particular critical infrastructure and key resource (CI/KR) sector or sub-sector.

Information contained in the interactive Mindjet maps addresses how each sector is structured, identifies assets and key stakeholders, offers statistics on sector components as well as sector economics, and more. By visually organizing this information, users can better understand the scope of the various sectors and view collated data from an array of public sources, including the Sector-Specific Plans drafted to accompany the National Infrastructure Protection Plan.

The sector maps now featured on the CIP Program's website (http://cipp.gmu.edu/research/SectorMappingProject.php) are:

- Banking and Finance;
- Nuclear;
- Oil and Natural Gas; and
- Water.

As new maps are finalized, they will be posted to the website and available for download.

The CIP Program works in conjunction with James Madison University and seeks to fully integrate the disciplines of law, policy, and technology for enhancing the security of cyber-networks, physical systems, and economic processes supporting the Nation's critical infrastructure. The CIP Program is funded by a grant from The National Institute of Standards and Technology (NIST).

The CIP Report is published by Zeichner Risk Analytics, LLC (ZRA) on behalf of the CIP Program. ZRA is the leading provider of risk and security governance knowledge for senior business and government professionals. ZRA's vision is to be a consistent and reliable source of strategic and operational intelligence to support core business processes, functions, and assurance goals.

If you would like to be added to the distribution list for *The CIP Report*, please click on this link: http://listserv.gmu.edu/cgi-bin/wa?SUBED1=cipp-report-l&A=1