
# THE CIP REPORT

CENTER FOR INFRASTRUCTURE PROTECTION VOLUME 7 NUMBER 9

MARCH 2009
TRADE AND INVESTMENT

Fearsome Risks ..... 2
Financial Winners ..... 4
OECD Roundtables ..... 6
Legal Insights ..... 7
Cyber Conflict Perspective ..... 9



Contact: CIPP02@gmu.edu
703.993.4840



This month *The CIP Report* focuses on trade and investment. As our economy experiences some instability, we look at how two different centers at George Mason University are applying research in this area. The Interdisciplinary Center for Economic Science (ICES) and The Terrorism, Transnational Crime and Corruption Center (TraCCC) raise interesting questions about the financial situation

GEORGE MASON UNIVERSITY
School of Law
CENTER for INFRASTRUCTURE PROTECTION

Dr. Carl Johnston from ICES discusses correlated risk and disaster insurance, while Dr. Louise Shelley from TraCCC concentrates on what the outcome of the financial crisis will mean to people and who will benefit in the aftermath. An overview of the Organization for Economic Co-operation and Development's (OECD) roundtables is provided. *Legal Insights* summarizes the changes in the Committee of Foreign Investment in the United States (CFIUS) review process, including the new regulations and guidance. This month *Cyber Conflict Perspectives* discusses global cyber security and information sharing.

Next month we will focus on maritime and port security. We welcome and encourage your ideas and thank you for your support.

Mick Kicklighter
Director, CIP
George Mason University, School of Law

# Fearsome Risks and What We Don't Know About Them

by Carl Johnston, Ph.D., Research Fellow
Interdisciplinary Center for Economic Science (ICES), George Mason University

## Introduction

At ICES, we believe we have to go right back to basics in trying to understand the risks associated with catastrophes with a systematic study to find out what institutions are best suited to insuring against catastrophic losses, including the correlated risks most closely associated with terrorism, war, market collapse, and other disasters. "Correlated risk" refers to those occasions when multiple types of losses occur simultaneously as a result of a single event. For example, fire, flooding, droughts, famines, and plagues are events that can cause widespread catastrophic damage of a single, particular kind. Earthquakes, floods, hurricanes, war, and terrorism can produce combinations of multiple types of catastrophic damage that could be characterized as correlated losses. Indeed, we can define War and Terror as the purposeful effort by one party to maximize an opponent's, real or perceived, risk of massive correlated failure. When you ignite an explosive device in a populated area, everyone's risks of damage from fire, flood, violence, infrastructure failure, and a host of other risks that are usually distinct from each other arise at the same time. Risks in the banking system also increase. How do we account for correlated risks in such a highly interconnected world?

Societies can protect themselves from the economic damage of correlated losses by buying insurance. Insurance is a vital part of defense and disaster preparedness. However, insurance companies encounter difficulty in writing such insurance against correlated failure and making it affordable. Moreover, conventional methods for trading such risks are typically private and consequently lack the depth and liquidity that public markets provide. Efforts to establish public markets in catastrophic risks have not flourished or failed. We propose systematic, basic research into the institutional issues of risk trading and providing insurance against correlated risks with the objective of discovering why previous efforts have failed to flourish and how new attempts based on new basic research might be more productive.

## Risk Insurance Markets

Usually, insurance companies avoid underwriting correlated risks by including riders for natural disasters, war and *force majeure.* This avoids several problems for the insurer: (1) ambiguity of risk — it is difficult to define combinations of risks without over-inflating the definition of the contract; (2) the possibility of pricing the risk too low — correlated risks are harder to price as explained below; and (3) the threat to capital that many correlated risks represent.

A number of disaster insurance providers do exist. Lloyds of London and AIG, for example, have offered various kinds of insurance against catastrophes. These along with giant reinsurance companies use non-public markets in which contracts trade (and the risk is borne) privately between investors, agents, clients, and various intermediaries. Public markets, such as the market for catastrophe bonds, or Cat Bonds, have not been as successful, and leaders in the field cannot easily explain the failure. It may be that some deeper issue involving the nature of public markets keeps the trading of risk instruments out of public view.

## Issues Concerning Correlated Risk Insurance

Insurance is straightforward. The insurer identifies a risk (for example, that the chance of an event X doing $10 damage to a client is 9% per year). The insurer then writes a policy promising to pay $10 to the client if X occurs, and the insurer charges $.90, which is 9% times $10, plus some overhead charge for the service. Say there are two risks, X and Y, and each has 9% chance of doing $10 damage. The insurer would charge $.90 for each policy,

*(Continued on Page 3)*

**Risks** *(Cont. from 2)*

plus the overhead charge. The client could buy both policies and on average protect himself against both kinds of damage. If the two risks were correlated, however, the insurer would have to charge much more. The likelihood of both risks occurring simultaneously actually declines (0.09*0.09=0.0081). Despite the order-of-magnitude decline in the likelihood of the event, the damage variance could be nearly twice as large as in the non-correlated scenario and insurers price based off of variance rather than average damage. So, insurance premiums rise dramatically whenever correlated risks are present even though the actual likelihood of the correlated events happening at the same time *declines*. Financing such insurance requires capital to increase directly with the variance. There are also standard problems in the insurance business such as lack of geographical dispersion, mispricing of risk through miscalculation, the desire to hold on to a valued client, or investment gains that make cheaper premiums tempting.

**Personal and Impersonal Trade**

Lately, there has been some experimentation in using public, open markets to trade catastrophic risks. Examples include catastrophe bonds, which are bonds issued by insurance companies whose payout is reduced when a covered catastrophic event occurs. Despite many favorable attributes, catastrophe bonds and other instruments remain rare. Most of the trading in catastrophic risks continues to occur in bilateral

formats between insurance companies and re-insurers where well-developed contractual and business relationships facilitate relatively low transaction costs.

One possibility is that open markets do not always function well when trading heterogeneous items where the underlying asset is a potential cost rather than an item of value. Therefore, one might ask: "What is the best institution for trading insurance?" This question has not been systematically studied.

Classical economic literature and the typical economic policy debate typically assume that trade occurs in an impersonal format, that is, where products are homogenous and participants do not know each other. Much of the literature on auction and economic system design focuses on creating algorithms that allow anonymous individuals to collectively discover the value of the items sold on a public (impersonal) exchange with a high degree of efficiency. Impersonal exchange has numerous advantages important to an industrial or post-industrial mass economy. It allows functionality of large market, aggregation of search costs, and some pooling of regulatory benefits.

The focus on impersonal trade has come at the cost of a comparative lack of study of personal exchange, or direct negotiation. Personal trading formats can be as small as markets of one in which, say, a lawyer sets a fee for handling a case for a client. In many cases, the up-front costs of personal trade are much lower than those of impersonal trade. The ability to deal in heterogeneous products is greater and personal traders do not necessarily require government monitoring.

However, personal exchange is by necessity a smaller scale type of business compared to the impersonal market. In an era of Katrina, continental power outages, and 9/11, the small scale of these private markets is a significant problem.

**Research Agenda**

A research agenda in insurance needs to look at two issues:
1) What is the best way of buying and selling instruments based on assets that have a possibility of being worth nothing (as opposed to options where a positive value asset underlies the trade)? Even less studied are markets in which participants agree contractually in advance to cover a significant loss. What are the best institutions for trading *losses*? Are face-to-face personal markets inherently better

*(Continued on Page 10)*

# The Financial Winners of the Current Crisis

by Louise Shelley, Ph.D., Director
Terrorism, Transnational Crime and Corruption Center (TraCCC)
School of Public Policy, George Mason University

In every financial downturn and depression, there are some who benefit in the recovery that follows. The regulations enacted after September 11th did an enormous favor for organized criminals and terrorists. It excluded them from the banking system and financial markets as regulations made it harder for bankers and financiers to take their money. Consequently, the criminals and terrorists were forced to remain in cash. Cash is now king. Therefore, many criminals and terrorists are now cash rich and well positioned to buy up assets and influence at bargain prices. They are the major beneficiaries of this financial crisis.

Selective regulation of the banking sector and financial markets led us to this ironic situation. Nearly a decade ago, much of the carefully conceived system of regulation of banks, insurance companies, and financial markets was dismantled. Yet, post-Patriot Act regulation tightened control on financial institutions in regards to receipt of criminal and terrorist capital. Bankers and investment houses understood that they faced enormous penalties and loss of reputation if they were caught laundering money. There were, however, very limited costs in engaging in business practices that threatened the international economy — selling sub-prime loans, securitized mortgages, and conducting risky derivatives trading without oversight. Therefore, they followed the perverse logic of existing regulation. Many formerly prudent banks, insurance companies, and financial institutions embarked on high-risk derivatives trading but went to great lengths to exclude suspicious capital. Banks and financiers complained about the administrative burdens attached to the requirement that they "know their client," but despite this, expanded their compliance departments. A new industry of firms emerged to meet this regulatory need of investigating rich potentially harmful clients. Expanded due diligence on clients kept many criminals and terrorists out of established financial institutions, often the very ones now most threatened in the financial crisis. Citigroup had learned earlier the enormous legal and reputational costs for laundering the money of Raul Salinas, the brother of former Mexican President Carlos Salinas.

The fact that organized crime groups were awash in cash was not lost on some in the law enforcement community. In 2007, $205 million in cash was found in a house in Mexico City, guarded by seven people. Its contents were believed to belong to drug cartels. This seizure of bulk cash was the largest, but U.S. law enforcement believe this was a small fraction of the cash moved back to Mexico in fake compartments of trucks, in the tires of cars moved across the border, and on the bodies of thousands of human couriers. In 2008, federal officials seized less than $1 billion of Mexican cartel cash, out of the estimated $18 to $39 billion of drug profits moved annually from the United States to Mexico.

The Mexican criminals are perfectly positioned in the rapidly declining Mexican economy. Migrants are returning home with no prospect of work, criminal violence has created great personal insecurity, and the Mexican state seems fragile. With their enormous cash reserves, Mexican criminals can buy workers, political influence, and depressed assets both home and abroad at bargain prices. In every crisis, some are winners — in the Mexican case it is the criminals.

The cash-rich Mexican criminals are not alone. Fortunately for the mafia, Italian prosecutors understood their opponents all too well. Prosecutors in Palermo could detect mafia forays into stocks and international financial markets. Past experience with seizure of real estate by Italian law enforcement made many mafiosi shy of investing in land and apartments. Consequently,

*(Continued on Page 5)*

**Financial** *(Cont. from 4)*

the mafia remained heavily in cash. In Italy, the liquid assets of the mafia and other key crime groups have placed them at an enormous advantage. With frozen credit markets, individuals seeking credit are often forced to seek loans from the mafia. As always, they are charged usurious rates. Legitimate business people are paying as much as 120 percent annual interest a year to stay afloat. Business is down and a loan from the mafia may be the first step towards mafia acquisition of the business. The mafia is perfectly positioned for growth with an expanding portfolio of businesses to generate cash and through which to launder money. In Italy, as well, the success in keeping organized crime out of financial markets has given them an enormous strategic advantage in this current economic crisis.

In Russia, not all organized criminals have profited. The ruble has fallen a third, the prices for oil and other raw commodities have fallen on world markets and businesses, even some mafia controlled businesses have slowed. Despite this fact, according to official Russian sources, Russians moved $200 billion out of the country between October 2008 and the end of January 2009. Not all is criminal capital but it points to the high liquidity of this highly criminalized economy. Unlike the Mexicans and Italian crime groups who are more often national and regional investors, Russian criminal elites are truly global investors. With their enormous cash reserves parked in safe havens, the Russian investors are poised to go on an international buying spree or to repatriate their cash and buy key assets at fire-sale prices as they did after the ruble collapse in 1998. As in Mexico and Italy, the crime groups will come out stronger from this financial crisis.

Is there a possible link between cause and effect? Is there a possibility that criminal actors contributed to this world-wide financial crisis in deliberate ways? Their opportunity to benefit is so large, one is ALMOST tempted to ask: Did the financial and mathematical expertise possessed by some powerful crime groups, cause them to engineer this financial crisis through their manipulation of derivatives markets, thereby enhancing the relative wealth of the cash rich crime groups?

One need look no further than Japan to see the impact that organized crime can have on financial markets. Japan, the world's second largest economy, suffered a lost decade in the 1990s. This decade was preceded by a financial situation that has parallels to the United States and the global economy of 2008 — hugely inflated real estate prices, a record high stock market, and banks weighed down by staggering amounts of bad debt.


The Yakuza, Japanese organized crime, were key players in the real estate speculation of the 1980s and an estimated 40% of bad loans were related to yakuza gangs and their front companies. Organized crime could procure these loans because of their powerful links to the banking sector. The Japanese example reveals that organized crime can help bring down a major economy even one as large as that of Japan. However, the Yakuza were not as global as much of contemporary organized crime two decades later. Therefore, when the Japanese economy sank, so did the Yakuza's fortunes. This is a problem not known by many of the truly global transnational crime groups operating today.

What are the lessons of Japan's lost decade, caused in part by the rapacious activities of Yakuza? What are lessons of partial regulation that excluded criminals and terrorists from the banks and financial markets that are tottering today? As we put back the world economic order, we need to consider that illicit actors are not peripheral figures but increasingly key players in the world's financial markets. Moreover, their power is even greater in countries where the state has little capacity to control organized crime. The most extreme case may be Afghanistan, where 80% of the economy, according to the former finance minister, is based

*(Continued on Page 10)*

# OECD Roundtables on Freedom of Investment, National Security and 'Strategic' Industries Encourage International Dialogue and Collaboration

**Introduction**

The challenging mission of the Organization for Economic Co-operation and Development (OECD) International Investment Committee is to foster international cooperation, intergovernmental dialogue and policy analysis germane to the enhancement of international investment. One important element of this committee is the *Freedom of Investment, National Security and 'Strategic' Industries* project. This project, launched in 2006, provides a forum for governments to candidly discuss the management of national security concerns regarding international investment.

The forum promotes interchange through a series of roundtables. The roundtables currently consist of thirty OECD member countries and eleven non-member countries who have subscribed to the *Declaration and Decisions on International Investment and Multinational Enterprises.* Furthermore, external non-member countries are invited to participate. The first roundtable occurred on June 21, 2006 in Paris, France. Six additional roundtables have since been successfully concluded. The tenth roundtable is scheduled for March 26, 2009 in Paris, France.

**The Inaugural and Subsequent Roundtables**

The first roundtable addressed changes in national legislation and national security practices; economic liberalization; and the roles of OECD and international cooperation in limiting protectionism. At the time, France and Germany were experiencing legislative changes. The German Foreign Trade Law was amended to reflect changes in notification requirements for foreign acquisition of sectors included on a "closed list". Similarily, the French "Reform" Law defined "strategic" sectors which required ministerial approval if acquired by foreign investors. Russia and the United States were preparing for impending legislative changes involving national security restrictions on foreign investment.

Subsequent roundtables continued to focus upon changes in national laws and policies that could restrict foreign investment, whether for national security or protectionism purposes. A significant addition to the roundtables was the establishment of a *tour d'horizon*. A *tour d'horizon* is a peer review of recent investment policy developments. This concept, an OECD trademark procedure for international cooperation, has remained a permanent fixture of the roundtables. As the roundtables and peer reviews continued to thrive, noteworthy policy and investment issues such as Sovereign Wealth Funds (SWFs) and energy security emerged. These issues as well as national security concerns have remained essential themes during roundtable discussions.

As "national security" began to incorporate concepts of critical infrastructure protection, governments began reassessing the definitions and categories of industry that may be sensitive to foreign ownership and control. In November 2007, OECD commissioned the Center for Infrastructure Protection (CIP) to draft a white paper for a forthcoming roundtable. The white paper, *Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security*, was co-authored by a senior OECD economist. At that time in the United States, the term 'critical infrastructure' had been receiving additional attention because of changes to the legislation that governed the Committee on Foreign Investment in the United States (CFIUS). The work with OECD drew from four years of CIP research regarding foreign direct investment, particularly the work of CFIUS[1]. The seventh roundtable

*(Continued on Page 11)*

[1] This research included leading and participating in conferences; the publication of a monograph in 2006; the collaborative effort between OECD and CIP; and various articles in past issues of *The CIP Report*. These publications as well as additional information regarding foreign direct investment in critical infrastructure are available on the CIP website at http://cip.gmu.edu/research/CFIUS.php.

Legal Insights

# Committee on Foreign Investment in the United States (CFIUS) Process

by Joe Maltby, JD, Research Associate and Legal Counsel

**Regulations and Guidance Issued**

Foreign investment policies, regulations and laws have endured numerous modifications since the publication of the previous *The CIP Report* dedicated to this issue. The legal landscape has been altered by the amendment of an Executive Order (E.O.); the revision of regulations governing the Committee on Foreign Investment in the United States (CFIUS); and the publication of *Guidance Concerning the National Security Review*. The details and the significance of these documents will be discussed in sequence. (Note: All of these documents can be viewed in full on the CFIUS website, at http://www.treas.gov/offices/international-affairs/cfius/)

**Executive Order 13456 (Amendment of Executive Order 11858)**

In October 2007, the Foreign Investment and National Security Act (FINSA) became effective. Shortly thereafter, in January 2008, President Bush issued a new Executive Order (E.O.) which expanded upon the role of the Executive Branch, particularly the Secretary of the Treasury, in the foreign investment review process. In addition, the E.O. reinforced the commitment of the United States to support foreign investment and clarified CFIUS procedural points. With regards to procedures, the E.O. affirmed that individual members of CFIUS may initiate an inquiry if there are concerns regarding national security; however, discussions with the involved parties must include the lead agency or the Secretary of the Treasury in the absence of an established lead agency. Lastly, the E.O. specified the procedure for situations in which the lead agency or CFIUS enter into a mitigation agreement with parties to a transaction. This procedure includes the production of a written statement that describes the national security risk and addresses the appropriate risk mitigation measures.

**Final Revised Regulations**

In November 2008, the Department of the Treasury issued new regulations pertaining to the foreign investment CFIUS review process. The new regulations, which implement Section 721 of the Defense Production Act of 1950 as amended by FINSA, make significant changes. First, the regulations explicitly encourage prospective parties to contact CFIUS in advance of filing for the purpose of determining if parties have the information necessary for the review process. This practice ensures a more efficient review process; however, there is some concern in Congress that decisions are not conducted through a transparent regulatory process.

Second, the new regulations, which are consistent with the new authority provided by FINSA, require CFIUS to issue penalties for three types of violations: the filing of false statements or omissions; false certifications; and the material breach of a mitigation agreement. The penalties are designed to provide CFIUS with the ability to enforce the mitigation agreements. If there are concerns in the private sector about submitting a review to CFIUS because of the effect the uncertainty has on their stock prices and corporate plans, then adding the possibility of being penalized for statements made in a CFIUS filing may exacerbate this concern. The long-term effects of the penalty provisions remain to be seen.

Third, the new regulations expand upon the FINSA definition of "covered transactions" through clarification of the terms "transaction", "control", "U.S. business", and "foreign person".

*(Continued on Page 8)*

**Legal Insights** *(Cont. from 7)*

FINSA defines a "covered transaction" as any merger, acquisition, or takeover by or with a foreign person which may result in foreign control of a U.S. business. The practical definition of "control" is delegated to the new regulations. This term, similar to the definition in previous regulations, is defined as the "ability to exercise certain powers over important matters affecting an entity."[1] In addition, the term "control" is directly associated with the definition of a "foreign person" and "U.S. business". It is imperative that the fundamental definition of "control" is understood as the CFIUS review process is triggered when a prospective transaction may result in foreign "control" of a U.S. business. Limiting the definition of "control" minimizes the flow of foreign investment, while supporting U.S. national security. More specifically, a foreign person does not control an entity if the foreign person holds ten percent or less of the voting interest in the entity and does not intend to exercise control. At this juncture, the regulations have yet to provide exemptions based exclusively on an investment's percent value in a U.S. business. Each transaction is reviewed on a case-by-case basis which allows for the analysis of the complete circumstances and not merely the percentage of ownership.

**Guidance Concerning the National Security Review Conducted by CFIUS**

In December 2008, the Department of the Treasury published guidance regarding the national security review process conducted by CFIUS. While the document is not legally binding, it does provide valuable guidance regarding the purpose of the CFIUS process and the nature of previously reviewed transactions that have presented national security considerations. National security considerations are described as, "facts and circumstances, with respect to a transaction, that have potential national security implications."[2] As described in the guidance, relevant national security considerations are reviewed by CFIUS to determine if the transaction poses a national security risk. A transaction poses a national security risk if, "the foreign person that exercise control over the U.S. business as a result of the transaction might take action that threatens to impair U.S. national security."[3] The review process for analyzing national security risk includes assessment of the foreign person's "capability or intention to exploit or cause harm and whether the nature of the U.S. business, or its relationship to a weakness or shortcoming in a system, entity, or structure, creates susceptibility to impairment of U.S. national security."[4] It is important to note here that not every transaction that presents national security considerations pose a national security risk. National security risk requires the presence of both threat and vulnerability in U.S. national security.

In determining if a transaction poses a national security risk, the definition of "national security" must be understood. Therefore, the guidance refers to the narrow legislative definition of "national security" which includes relevant issues relating to homeland security and its application to critical infrastructure. An example of

*(Continued on Page 12)*

[1] *Regulations Pertaining to Mergers, Acquisitions, and Takeovers by Foreign Persons* available at http://www.ustreas.gov/offices/international-affairs/cfius/docs/CFIUS-Final-Regulations-new.pdf
[2] *Guidance Concerning the National Security Review Conducted by CFIUS* available at http://www.ustreas.gov/offices/international-affairs/cfius/docs/GuidanceFinal_12012008.pdf
[3] *Guidance Concerning the National Security Review Conducted by CFIUS* available at http://www.ustreas.gov/offices/international-affairs/cfius/docs/GuidanceFinal_12012008.pdf
[4] *Guidance Concerning the National Security Review Conducted by CFIUS* available at http://www.ustreas.gov/offices/international-affairs/cfius/docs/GuidanceFinal_12012008.pdf

Cyber Conflict Perspectives

# Global Cyber Security Agenda: NATO and the EU

by Eneken Tikk, M.Jur.

*The investigation and management of cyber incidents is based on sharing and comparing traffic data and server logs, including infrastructure protection (IP) addresses. The countries subjected simultaneously to both the European Union (EU) and NATO organizational frameworks of cyber defense may face difficulties transferring such data to NATO or other nation's authorities as the governing legal view of EU data protection institutions categorizes IP addresses and logs as personal data. While there are legally safe ways to secure evidence and manage cyber incidents, recent trends in EU member states call for attention on the national regulatory level.*

Many countries are part of both NATO and the EU. And many businesses (including cyber/telecom infrastructure owners and operators) must operate in compliance with both EU laws and non-EU regulations (e.g., U.S.). In the context of cyber security there is increasing interrelation of the activities and areas of concern for these two major and influential organizations. Sharing information about cyber incidents is just one of them.

The management of cross-border cyber conflicts requires extensive and detailed information-sharing among governmental agencies and information infrastructure entities often privately owned. The data of interest comprises not only details about the course of action and background of the incidents but also real-time sharing of IP addresses and logs.

About a year ago, NATO adopted two documents that start to define the management of cyber incidents relevant to national and international security. The cooperative aspect of cyber incident management will require national regulatory action for defining critical information infrastructure and for providing proper legal bases for information exchange between NATO and its member nations.

However, the EU data privacy legal framework may hinder the timely processing and sharing of cyber incident data. Among EU data protection institutions, the governing legal approach is to categorize IP addresses and logs as personal data. This categorization will limit the ability to timely share and process data regarding an ongoing cyber incident. These problems may be improved, but only if EU states take coordinated action on a national regulatory level.

In order to create legal certainty for processing data about cyber incidents, the nature, purpose, and legal effects of the processing of data need to be defined under the national regulatory framework. Also, there should be some level of coordination among the nation states regarding such definition. Otherwise, if the EU member countries diverge too far in their approaches for categorizing logs and IP addresses as personal or not personal, then these different opinions may hamper both operational response and legal proceedings related to cyber incident management.

As international cyber defense laws and policies evolve at both the nation-state and organizational levels, constructive and sophisticated cooperation is needed between EU and NATO and other international organizations to tie the loose ends that may complicate cyber defense measures. ❖

[1] NATO Cyber Defence Concept (MC, 13 March 2008), based on the NATO Cyber Defence Policy (NAC, 20 December 2007).

**Risks** *(Cont. from 3)*

than impersonal markets for these tasks? Can we find a way to extend the size of face-to-face markets in order to cover larger risks?
2) What is the best way of dealing with panic in the market place and restoring trust among participants? Economic damage done as a loss of trust in the market is at least as big a problem as the potential damage done by terrorists themselves. Is there a better way of restoring trust after a fearsome disaster? ❖

**Financial** *(Cont. from 5)*

on illicit trade in drugs, timber, and antiquities. Domination of an economy by crime groups, criminalized warlords, oligarchs, and their state supporters is unfortunately not unique to Afghanistan.

Financial officials working to right the world's economy cannot isolate the problem of criminal capital from their overall strategies to repair financial markets. Nor can we afford to take a single state solution in regards to criminal capital. Federal officials intend to focus on the Mexican cartel's cash to stem their operating capital. This is an important first step, but the problem requires a much more holistic solution that focuses not just on the cash, but on those that facilitate the drug trade and even the high status individuals who launder its money. Moreover, efforts to fight the Mexican drug cartels must not be confined to U.S.-Mexico policy, but must be incorporated into larger efforts to control criminal and terrorist capital in the global economy, particularly in this crisis period.

To ensure that organized crime and terrorists do not benefit even more in this transitional period, we must do more than exclude criminal capital from financial institutions. The international community must try to ensure than criminals do not acquire key assets with their existing wealth or their predatory loans. They must be prevented from cornering the market on key raw commodities which will be in demand when the international community emerges from this global recession. Global economic policies must try to restrict access of crime groups to manpower which can be hired cheaply as desperate and displaced workers are ready to work for anyone, including criminals to survive. We must focus not only on the poor and the vulnerable, but also on restricting the rise of government officials to key positions whose careers have been advanced by criminal capital. The challenge we face from crime groups awash in cash is larger than just the buying power of this money. In this transitional period, this criminal capital will help determine the future allocation of international resources, the deployment of human capital, and the political leadership of key states.

Greater transparency of markets is needed to ensure that criminal capital does not again have a chance to be king. Regulations dismantled must be reinstated. Most important is ensuring that crime groups and criminals do not again have the advantage in international financial markets. Moreover, greater transparency is needed to ensure that sophisticated crime groups cannot bring down financial markets. Without focusing on transnational crime and corruption in the current financial crisis, organized crime groups will emerge even as greater threats in the post-crisis period. ❖

**OECD** *(Cont. from 6)*

discussed these critical infrastructure issues.

The significance of the eighth roundtable included announcement of the completion of the OECD *Guidelines for Recipient Country Investment Policies Relating to National Security*. The guidance consists of three sections: general investment policy principles; guidelines for investments implicating national security concerns; and a section pertaining solely to SWFs. The *tour d'horizon* discussed developments in Australia, Canada, Germany, Japan, Brazil, and the United States.

The most recent roundtable, which took place on December 17, 2008, discussed national developments in France, Italy, Germany, United States, and New Zealand during the *tour d'horizon*. In addition, the ninth roundtable continued to discuss national security considerations to investment transactions that may result in foreign-government control of sensitive assets or infrastructures. Two groups within OECD, the Competition Committee and the Working Group on Privatisation and Corporate Governance of State-Owned Assets provided presentations on this topic.

For more information about OECD Roundtables, please access the links in the text box. For more information about CFIUS, please view the United States Department of Treasury website at http://www.ustreas.gov/offices/international-affairs/cfius/. ❖

Links to Relevant Documents:

Roundtable Summary Reports are available electronically on the OECD website at:
http://www.oecd.org/document/25/0,3343,en_2649_34887_42105753_1_1_1_1,00.html

The unclassified version of the OECD *Declaration and Decisions on International Investment and Multinational Enterprises* (November 15, 2000) is available at:
http://www.olis.oecd.org/olis/2000doc.nsf/LinkTo/NT00002BE6/$FILE/00085743.PDF

The unclassified version of *Protection of 'Critical Infrastructure' and the Role of Investment Policies Relating to National Security*, (May 2008) is available at:
http://www.oecd.org/dataoecd/2/41/40700392.pdf

OECD *Complete Guidance* is available in sections at:
http://www.oecd.org/document/19/0,3343,en_2649_34887_41807059_1_1_1_1,00.html

**Legal Insights** *(Cont. from 8)*

national security risk analysis — with regards to the ownership of a particular business or asset — includes investigation into the nature of the asset and its relationship to any weaknesses in other systems, entities, or structures. Therefore, not only will an asset qualify by its very nature, such as a company making missile guidance systems, but it may also qualify by its connection to other systems, such as a transmission company owning lines connecting two major power grids. A company may qualify because it provides essential subcomponents or services to another critical asset, such as subcontractors. Some companies have even qualified as protected national security assets based on their access to classified information or to specific technologies. CFIUS is required to submit a report to Congress annually which contains, among other things, information on the types of transactions CFIUS reviewed.

The guidance also provides a random sampling of the types of transactions that have presented national security considerations during previous CFIUS reviews. The inclusion of examples provides direction to CFIUS as well as to U.S. businesses and foreign persons involved in covered transactions. As previously mentioned, considering that CFIUS encourages parties to undergo an informal review prior to the formal review process, the guidance provides further clarification for both U.S. and international participants which yields a more efficient national security review process.

**CFIUS Annual Report to Congress**

In December 2008, CFIUS released an annual report to Congress. The annual report, mandated by FINSA, includes detailed information about covered transactions that were reviewed and investigated in 2007; potential trends in foreign investment and trends of foreign investment in critical technologies. The annual report replaces the previously-required quadrennial Critical Technologies Reports.

**Conclusion**

It is evident that much has occurred since the publication of the previous *The CIP Report* devoted to the topic of foreign investment. The E.O. amendment, new regulations, and guidance are improving upon an existing trend of producing a more supportive and effective review process. In addition, the consideration of homeland security and critical infrastructure issues in the national security review process also expands the idea of national security to meet our modern threats. However, these are relatively recent changes; therefore, it is difficult to predict their effect upon foreign investment in the United States. ❖

The Center for Infrastructure Protection works in conjunction with James Madison Univerity 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 Center is funded by a grant from the National Institute of Standards and Technology (NIST).

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