

The NATIONAL STRATEGY FORUM REVIEW

An Online National Security Journal Published by
the National Strategy Forum

53 West Jackson Blvd.
Suite 516
Chicago, IL 60604
T: 312.697.1286
F: 312.697.1296
W: www.nationalstrategy.com

IN THIS ISSUE

FEATURE ESSAY

Economic and Industrial Espionage

By *Harvey Rishikof* 2

NSF INSIDER VIEW

Rethinking U.S. National Strategy

By *Richard E. Friedman* 8

Foreign Policy and Defense in the Obama Administration

By *John Allen Williams* 9

The Moment to Decide

By *Frank Schell* 10

Protecting America's Virtual Reality

By *Lauren Bean* 12

Renewing the West

By *Endy Zemenides* 13

KEY REGIONS AT A GLANCE

A Preview of Iran's Upcoming Elections

By *Rami Yelda* 15

Enhancing a Security Dialogue with China

By *Henry Levine* 17

Special Supplement: Non-Lethal Weaponry

19

NATIONAL STRATEGY FORUM REVIEW

PRINT EDITION

SPRING / SUMMER 2009

Letter from the Publisher

Richard E. Friedman, *President*, National Strategy Forum

For many years, the objective of the National Strategy Forum (NSF) has been to provide balanced, nonpartisan, usable information regarding US national strategy and national security. The NSF created an informal "curriculum" based on the Forum monthly lecture series, the National Strategy Forum Review (NSFR) publication, and conferences on emerging national strategy/security issues. The results have been positive -- NSF members are exceptionally well-informed.

The velocity, access, and availability of an enormous amount of information tend to overwhelm careful analysis. Particularly troublesome are some blogs, which are unedited and unscreened, and, frequently, highly partisan. Confusing, inconsistent, misleading and incomplete information interferes with rational analysis. The NSF has adapted to this new milieu.

We seek to provide NSF members with an overview of the national strategy/national security field in summary form, while carefully avoiding superficial treatment. We will continue to adhere to our long-standing principle of "framing the issues," and asking questions rather than answering them. Context will be provided by a wide array of experts in their respective fields.

The major themes that the NSF has focused on are diplomacy, economics, military force, rule of law, strategy, and terrorism. These themes will continue with different emphasis depending upon facts on the ground. It is likely that the economy will receive high priority attention. Strategy will continue to be the glue that ties these interdependent themes together.

NSF members will have a matrix of themes and issues that will assist them in becoming well-informed and well-positioned to discuss these issues with their family, friends, business associates, and civic associates.

The *National Strategy Forum Review* is **now available in electronic format on the National Strategy Forum website**. Please submit your email address to Lillian Murphy, NSF Program Manager (312.697.1286), to ensure you receive future notifications about the NSFR journal issues. If you do not have an email address, the NSF will notify you via regular mail about the online availability of future issues.

Thank you for your continued support.

Economic and Industrial Espionage: Harvey Rishikof

This case (U.S. v. Meng, 2007) highlights the vital importance of protecting the intellectual property and trade secrets not only in Silicon Valley but also for our country's businesses. The alleged economic espionage and theft and export of trade secrets such as these -- visual simulation training software that has military application, no less -- has real consequences that could jeopardize our country's military advantages in the world, in addition to creating substantial financial losses for our businesses which legitimately developed and owned this information. We are grateful to our law enforcement partners for taking swift and appropriate action here, and also want to acknowledge the pivotal role private industry's ready cooperation has in these investigations."

United States Attorney Kevin V. Ryan *

Introduction

Economic or industrial espionage is an old problem. As the current head of the National Counterintelligence Executive (NCIX) under the Director of National Intelligence (DNI), Joel F. Brenner, likes to muse, espionage itself is as old as Joshua reconnoitering the Promised Land, and it will be with us forever.[1] In the Cold War the archetype for technological counterintelligence, as well as industrial espionage, was the American born Russian spy Dr. George Koval's penetration of the Manhattan Project for the atomic bomb.[2] But the paradigm is shifting in the economic era of globalization. The end of the Cold War and the explosion of technology, increased access to computers and the internet, potential profits, poor prosecutorial tools, fear of reporting the theft, and inadequate federal and state laws, have all contributed to the attractiveness of economic espionage.[3] In the words of Bernard Esambert, former Chairman of the Board of the Pasteur Institute, "Today's economic competition is global. The conquest of markets and technologies has replaced former territorial and colonial conquests. We are living in a state of world economic war and this is not just a military metaphor... the companies are training the armies and the unemployed are the casualties." [4]

International commerce and advancing technology have increased the likelihood of and opportunity for economic intelligence and industrial espionage, placing intellectual property and trade secrets at increased risk of appropriation. Consider the iPod, while Apple developed it, its 451 parts are made in several different countries, including Japan, Philippines, Korea, China, and Taiwan.[5] Such outsourcing although efficient and cost effective, leaves Apple open to foreign industrial espionage at critical stages of design. When viewed from the perspective of the NCIX trying to protect economic secrets in a world of shifting boundaries, world supply lines, and spheres of influence, it is a monumental challenge:

Boundaries of every kind are eroding—legally, behaviorally, electronically—in all aspects of our lives: Between the public and private behavior of ordinary people; for example, the sense of dress and decorum appropriate to the home, the street, the office, or houses of worship. Between the public and private—that is, secret—behavior of governments. Between the financing, legal norms, and research activities of public as opposed to private institutions; [and] universities, for instance. Between state and non-state actors and the relative size of the resources they control. Cyber boundaries are also eroding—and not always in ways we like—but simply because we are sometimes helpless to enforce them.[6]

But those in charge are still responsible, and they have to try to craft a response to the new era of globalization, computerization, secrets, and spying. The mission therefore is increasingly difficult and will not go away because the stakes are so high. Our recent economic downturn may only enhance the incentives to increase this type of spying. In the elegant words of Joel Brenner the "intellectual thieves" seem to have the upper hand at the moment. As he recently explained at a public-private sector conference:

The fact is, intellectual thieves are eating our lunch—eating your lunch. The public and private sectors are both leaking badly. I'm not talking about just the pirating of DVDs and movies in Asia. I'm talking about significant technologies that are walking out of our laboratories on electronic disks, walking onto airplanes bound for foreign ports, and re-entering the country as finished products developed by foreign entrepreneurs. In effect, we're buying back our own technology. This is bad enough when we're talking about commercial innovation. But when we're talking about technology with substantial defense applications, we're talking about losses of intellectual capital that in wartime could cost many lives of our fellow citizens. These losses are occurring, and they are occurring in a targeted, systematic manner.

Protecting innovative technology before it can be patented or classified is an urgent task, and it is difficult. If any of us knew how to do it, he'd be very rich, because it's a question of handicapping basic research.[7]

Protecting critical business information is not only a bottom line issue but also may be increasingly a national security issue. Companies however, are fearful of government classification schemes that will hinder innovation and openness. Given this reality and boundary erosion, perhaps it is not surprising that a former head of the French intelligence service in 1994 admitted that his agency spied on U.S. executives abroad and "bugged" first-class seats on Air France to monitor conversations.[8] Moreover, this arena is complicated not only by the fact that the key to our information networks is openness but the information can be transmitted through standard business practices – merger and acquisitions, joint ventures, strategic alliances, and licensing agreements. Therefore, both military friends and foes may be adversaries in the economic arena of espionage. Sometimes the attack is from government-sponsored espionage, other times it is the private illicit acquisition of proprietary information, and sometimes it may be a combination of the two.

As one can imagine, it is hard to find data in this arena. As one of my old professor's use to say – studying smuggling is hard and potentially dangerous. A measure of the extent of the growing problem is the number of prosecutions for the illegal export of US technology as reported by the 2003 Annual Report on Foreign Economic Collection and Industrial Espionage (FECIE). During fiscal year 2003, US Department of Immigration and Customs Enforcement (ICE) conducted more than 2,000 investigations involving violations of the Arms Export Control Act, International Traffic in Arms Regulations, Export Administration Regulations, International Emergency Economic Powers Act, and the Trading with the Enemy Act. Those investigations resulted in 120 arrests, 75 criminal indictments, and 55 convictions.[9]

According to a survey published in 2007 by the American Society for Industrial Security (ASIS), the financial impact of individual cases of espionage range from less than \$10,000 to more than \$5.5 million per incident, for a cumulative year-end total in the American economy of billions of dollars in losses – to reputation, image, goodwill, competitive advantage, core technology, and profitability.[10] But as we began to recognize in the late 1990s corporations are of strategic interest to the United States on three levels since they: 1) produce classified products for the government; 2) produce dual-use technology used in both the public and private sectors; and 3) are responsible for R&D and the creation of leading-edge technologies critical to maintaining U.S. economic security. Losses at any of these levels could affect U.S. international competitiveness and security.[11] Regardless of the source, the threat to

NSFR EDITORIAL BOARD

RICHARD E. FRIEDMAN
Publisher

LAUREN BEAN, *Editor*

Editorial Board

JOHN ALLEN WILLIAMS
MARILYN DIAMOND
FRANK SCHELL
ENDY ZEMENIDES

The *National Strategy Forum Review* is a quarterly publication of the **National Strategy Forum**, a Chicago not-for-profit, non-partisan US national security research and education institute, www.nationalstrategy.com.

© 2009

National Strategy Forum, Inc.
www.nationalstrategy.com

US interests is real, and the US is extremely vulnerable.

The 2005 Annual Report to Congress on FECIE reported that 108 countries – both friend and foe – were involved in information collection efforts against the United States.[12] China, Russia, and India top the list. The FECIE reports indicate that foreign collectors tend to target dual-use technology, which can be used for both peaceful and military objectives, and military technology. There is no dispute that foreign governments go after trade secrets for the sake of national security advantage. But what is the United States government's role in company v. company warfare? Should investigations be considered a counterintelligence or law enforcement matter? Do these old jurisdictional boundaries and responsibilities still work? What should be a secret, and what is the government's role in making that determination? What can be done to protect US interests?

The critical issue in the new world of commerce is whether one can clarify the differences between economic and industrial counter-espionage and explain why the latter is particularly problematic. To many, governments have long engaged in economic intelligence but have found the need to engage in economic espionage declining as more and more critical information is available through open sources. Industrial espionage, on the other hand, may be becoming the most prevalent form of economic espionage as governments seek industry-related information for the intelligence they need on battlefield capabilities, for design of counter-measures, and for preparation of the battlefield – including how to attack energy grids, and industrial plants important for war-making etc. Industrial espionage involving the theft of trade secrets, perhaps at one time seemed to be able to be restricted to an industrial sphere, but dual use technologies erase what once was an easy distinction as government involvement becomes more prevalent.

Some recent cases --How to balance counterintelligence v. law enforcement?

At the time of the passage of the Economic Espionage Act in 1996 (EEA), 23 to 26 countries were identified as practicing suspicious collection and acquisition activities and 12, in particular, were targeting trade secrets. In particular the technology categories, many of which are dual-use technologies, listed in the Military Critical Technology List published by the DOD were of greatest interest.[13] The FBI had seen the number of cases of suspected economic espionage under investigation in its Economic Counterintelligence Program started in 1994 leap from 400 to 800 cases by 1996. By 2005 the number of countries involved in collection efforts against sensitive and protected US technologies had risen dramatically.

More specifically, the immediate issue is whether the government should be engaged in a back-door industrial policy by determining which industrial products deserve protection with federal dollars. Criterion might be direct relevance to national security, actually threatened industries, or a mixed strategy using a case-by-case approach. Recent cases brought under the EEA are illustrative of the range of potential problems for prosecution under the current charging schemes as the government tries to establish foreign involvement.

If the companies are selected according to their direct relevance to national security (i.e. they have defense contracts) then the contracting process becomes the tool the FBI and others use for building their database of which industries to help—regardless of whether the thief is a foreign government or a competing firm acting on its own. This is, of course, a very defensive posture but allows for a potential marshalling of resources. An example of such a national security case is *United States v. Meng* that involved military technology, computer source code, and economic opportunity.[14]

In 2007, Xiaodong Sheldon Meng, formerly a resident of Beijing, China, and a resident of Cupertino, California, was charged with stealing military combat and commercial simulation software and other materials from his former employer Quantum3D, a company based in San Jose, California. Meng was charged under the EEA with stealing the trade secrets from Quantum3D with the intent that they would be used to benefit the foreign governments of China, Thailand, and Malaysia.

Many of Quantum3D's products were designed primarily for military purposes, including military combat training in simulated real-time conditions during the day and night and the use of advanced infrared (IR), Electro-Optical (EO), and

Night Vision Goggle (NVG) devices. The indictment alleges that Meng stole numerous Quantum3D products, including “viXsen™” and “nVSensor™,” which were used exclusively in military applications and designed for precision training of military fighter pilots in night vision scenarios among other applications. Both “viXsen™” and “nVSensor™” are classified as defense articles on the U.S. Munitions List and cannot be exported outside the United States without an export license.

In 2003 after a number of years of employment, Meng entered into a consulting agreement with Quantum3D in which he would serve as an independent consultant for Quantum3D in Asia. In this capacity he tried to sell sensitive source code to the Malaysian Air Force. In 2004 he severed his relationship with Quantum3D, joined a competitor, and attempted to sell Quantum3D products to the Chinese and Thailand.[15] In essence Meng given his knowledge of the products became the carrier.

Another recent case highlighting the overlap of economic and industrial espionage in the national security area and they type of cases to focus on is the 2007 Chi Mak case. In the Chi Mak case, five members of a southern California family were charged with acting as agents of the People’s Republic of China and with conspiring with each other to export United States defense articles to the People’s Republic of China a violation of the Arms Export Control Act. This technology theft ring focused on acquiring corporate proprietary information and embargoed defense technology related to the propulsion, weapons and electrical systems of U.S. warships. The family, the father a naturalized citizen from China, had pursued a long-term plan of infiltration over years.

Though the object was clear, who sponsored the ring? Chi Mak was a support engineer at L-3 Communications working on navy quiet drive propulsion technology. The espionage effort appears to have been directed by a Chinese academic at a research institute for Southeast Asian affairs at Zhongshan University in Guangzhou, China. The Chi family encrypted the information it was passing back to China into a computer disk that appeared to contain television and sound broadcasts. It was literally embedded in the other data in encrypted form. This effort has all of the earmarks of professional espionage tradecraft and state-directed espionage, with sophisticated control and sophisticated clandestine communications means. The government university in Guangzhou could have been cover for a state-directed espionage effort. However, Chi Mak and his alleged co-conspirators could just as well have been part of a sophisticated economic espionage operation run out of a university research institute. The future plea agreements will perhaps make clear the true nature of the conspiracy.[16]

This “direct relevance” approach would require prioritizing military programs and “tagging” all employees with access to high value products. And as these cases illustrate the targeting countries are not beyond “planting” potential operatives as “sleepers” whose goal is to join critical companies and plot long-term career paths.

Alternatively, law enforcement could build a database of those industries actually threatened by foreign governments’ intelligence activities, whether or not the US uses the technology for national security purposes. The rationale here would be: if a foreign government wants the technology, there is national security gain to be had, by definition, in keeping that technology from them. This approach is problematic because of its underlying assumption and because many non-defense firms do not necessarily want the federal government probing their businesses to discover what their R&D involves or interfering in their choices on how to develop, protect or share such technologies.

Such a case was, *United States v. Okamoto and Serizawa*, when Takashi Okamoto, a resident of Japan, and Hiroaki Serizawa, a resident of Kansas, were indicted of stealing trade secrets from the Cleveland Clinic Foundation (CCF). [17] Okamoto and Serizawa conspired to misappropriate from the CCF certain genetic materials called Dioxyribonucleic Acid (DNA) and cell line reagents and constructs which were developed by researchers employed by CCF, with funding provided by the CCF and the National Institutes of Health, to study the genetic cause of and possible treatment for Alzheimer’s. Alzheimer’s affects an estimated 4,000,000 people in the United States alone and is the most common cause of dementia. The pharmaceutical market for this disease is a potentially rich profit center for any company in the field. The Alzheimer’s disease market is forecast to continue to expand significantly over the next ten years. Aided by growing elderly populations, successive product launches have seen global revenues grow at over 35%.[18]

The goal of the conspiracy was to benefit the Institute of Physical and Chemical Research (RIKEN), a quasi-public corporation located in Saitama-Ken, Japan, which received over 94 percent of its operational funding from the Ministry of Science and Technology of the government of Japan. The Brain Science Institute (BSI) of RIKEN was formed in 1997 as a specific initiative of the Ministry of Science and Technology to conduct research in the area of neuroscience, including research into the genetic cause of, and possible treatment for, Alzheimer's Disease

Okamoto and Serizawa had committed economic espionage by stealing, altering and destroying trade secrets that were property of the CCF, specifically, 10 DNA and cell line reagents developed through the efforts and research of researchers employed and funded by the CCF and by a grant from the National Institutes of Health. [19] Okamoto and Serizawa were also charged with transporting, transmitting, and transferring in interstate and foreign commerce, DNA and cell line reagents developed through the efforts of researchers employed and funded by the CCF.[20]

Should law enforcement be focused on lucrative emerging world markets, as in the above case of Okamoto and Serizawa and be using limited resources to protect private companies from losing market share? How can the federal government, given its limited resources, spread itself across such a large canvas? Will corporations want to cooperate with the government?

A third option is to develop a counter intelligence strategy that mixes the two previous approaches and determines, on a case by case basis, whether the efforts at acquisition by a foreign entity represent a national security threat. *United States v. Ye and Zhong*[21] presents such a choice. Fei Ye, and Ming Zhong were arrested at the San Francisco International Airport with stolen trade secret information in their luggage while attempting to board an aircraft bound for China. Ye and Zhong admitted to possessing stolen trade secrets for an integrated circuit design from Sun Microsystems, Inc. and Transmeta Corporation with the intent to benefit the Peoples Republic of China.

Ye and Zhong admitted that they intended to utilize the trade secrets in designing a computer microprocessor that was to be manufactured and marketed by a company that they had established, known as Supervision, Inc. They admitted that Supervision was to have provided a share of any profits made on sales of chips to the City of Hangzhou and the Province of Zhejiang in China, from which Supervision was to receive funding. Mr. Ye and Mr. Zhong also admitted that their company had applied for funding from the National High Technology Research and Development Program of China, commonly known as the "863 Program."

Fei Ye is alleged to have possessed a corporate charter for Hangzhou Zhongtian Microsystems Company Ltd. at his house which states that the joint-venture will raise China's ability to develop super-integrated circuit design and form a powerful capability to compete with worldwide leaders' core development technology and products in the field of integrated circuit design.[22]

The problem here is that, in addition to the issues with the first two previous enforcement approaches raise, the Ye and Zhong case introduces a third: acquiring the expertise within the counter intelligence community to analyze industrial R&D at its most cutting edge. And even if the community were successful in doing this, law enforcement would have to employ a sliding authorization for use of counterintelligence tools (wiretaps, undercover surveillance, etc.) during the investigative process or risk alienating firms it might need to cooperate in an eventual prosecution. Any investigations that did not pan out as espionage would have to be prosecuted as crimes, unless companies decide to drop charges in the interest of pursuing profits instead. But could the corporations count on the federal government or IC to pull back once an interest had been pursued? For some of the proponents of the EEA in 1996, the act was an attempt to pursue this third option, but the infrastructure and groundwork has not materialized to pursue such a nuanced course.

Why these cases are of interest is that they illustrate how difficult counterintelligence is when the focus is the private sector? What were the roles of the firms in each of the cases? Did the company alert law enforcement or the other way around? How were decisions made regarding the use of counterintelligence vs. counter-crime techniques and did internal law enforcement disagreements arise that complicated or slowed down investigations? These important questions demonstrate how difficult pursuing prosecutions in this area.[23]

But if government regulations and enforcement continue to prove ineffective the private sector may be the place where an attempted solution will be looked to, in order to stop having our “lunch eaten.” The questions are: 1) are we willing to pay the price to our privacy and will it work? and, 2) what is a US economic interest and what is a multinational conglomerate interest as it pursues its globalization strategy?

These issues of economic and industrial espionage bleed into other categories of security and competition. Recently Joel Brenner characterized the key three strategic challenges now confronting the counterintelligence community: (1) threats to our cyber networks and opportunities to understand and counter them; (2) acquisition vulnerabilities created by the international nature of our markets; and (3) the need for better collaboration in countering espionage.[24]

A corporate security culture must entail a shift in the traditional notions of privacy.[25] This shift will be a challenge to the previous zone of privacy many of us grew up with. Interestingly, the new generation of “MySpace,” “FaceBook,” and YouTube” employees may approach the new transparent work place with a different appreciation for the new corporate security culture of trade secrets. The government’s responsibility historically has been to concentrate on the espionage side of the national security arena and not be so involved in the industrial, a more private sector field. The private sector paid for its own slackness in lost revenue. Modern technology has helped to erode these two distinct arenas and this has created new burdens for the government. As economic warfare become more industrial based, the distinction between economic and industrial espionage becomes less relevant.

One reason for the erosion is that our adversaries have taken such a view, as in the Chinese 863 Program in the Ye and Zhong case. The 863 Program is a funding plan created and operated by the government of the People’s Republic of China, and is also known as the National High Technology Research and Development Program of China. The program was designed by leading PRC scientists to develop and encourage the creation of technology in the PRC and focused on issues such as high technology communications and laser technology, with an emphasis on military applications. The General Armaments Department (“GAD”) of the People’s Liberation Army was responsible for the Army, Navy, and Air Force in the PRC, and oversaw the development of weapons systems used by the PRC. The GAD had a regular role in, and was a major user of, the 863 Program.[26]

This approach is perhaps more understandable in political/economic cultures that encourage state-owned enterprises. In countries where government interests can coincide with corporate interests, or national champions, intelligence agencies can be more easily instructed to assist the private sector. This perhaps explains why France over ten years ago established, the Ecole de Guerre Economique (EGE) or School of Economic Warfare. The founder of the school contends that rather than teaching economic espionage it is more the management of information to develop an economic strategy in the context of conflicts to gain market share.[27] For such state corporate-centric approaches the distinction between fair or unfair business practices can become blurred. Some have contended that the US open competitive market based system and our anti-trust laws combined with our Foreign Corrupt Practices Act has made state sponsored economic espionage a non-starter.[28]

The new Director of National Intelligence has many problems on his plate – Iraq, Afghanistan, the Middle East, China, Pakistan, India etc. How will economic-industrial espionage fair? In Andrew Niccol’s 1997 science fiction film *Gattaca*, set in the near future, the Gattaca Aerospace Corporation has created a totally transparent work place with technology able to manipulate genetic codes and monitor all employee interactions. Although the hero is able to fool the system, the world depicted is a possible modern future that would bring corporate monitoring to one possible logical conclusion. If we do start to travel down this path of a culture of corporate security, future generations will have to judge if the price paid for corporate and national security, so that we stopped having our lunch eaten, was in the end worth the meal.

The views expressed in this article are those of the author and do not reflect the official policy or position of the National Defense University, the National War College, the Department of Defense, or the U.S. Government and the piece has been adapted from a chapter by Rishikof in *Vaults, Mirrors, and Masks: Rediscovering U.S. Counterintelligence* edited by Jennifer E. Sims and Burton Gerber (Georgetown Press 2009). SEE FOOTNOTES ON THE LAST PAGE OF THE JOURNAL, PAGE 21.

Rethinking U.S. National Strategy

Richard E. Friedman

Richard E. Friedman is President of the National Strategy Forum and Publisher of the National Strategy Forum Review.

Ideally, U.S. national strategy should be based on realistic objectives. A strategy that is designed to meet its objectives should include tactics for implementation and an understanding of the strategic objectives of friends, competitors, and adversaries so that foreign policy is not formulated in a vacuum. The ideal execution rarely occurs because putting out fires on a day-to-day basis preempts the energy and resources of policymakers. The following two examples demonstrate this problem.

The battlefield detainee prison at Guantanamo Bay (Gitmo) has become an icon for the belief that the U.S. has avoided the Rule of Law. Closure and release of prisoners from Gitmo raises several difficult issues:

- The release of prisoners may result in acts of terrorism by those who are released. The blame may be placed on government officials.
- Questionable evidence upon which the person was detained or evidence obtained by torture may taint continuing detention and trial.
- There is an unresolved legal issue regarding the appropriate forum for trial: military commissions and rules of evidence, or federal district criminal courts.
- Where to send prisoners after they are released? They may be tortured or killed when they return to their home state.
- What disposition could be made of released prisoners, if there is no state that will accept them?

The Bush II Administration focused on tactics -- what to do with battlefield detainees -- which is a legitimate concern. But it failed to accept the recommendations of legal scholars and civil libertarians regarding alternate methods of providing due process to terrorists. Many advised against the opening and operation of Gitmo.

The second issue that demonstrates the need for a more realistic national strategy is nuclear non-proliferation. The Obama administration has pledged to seek elimination of nuclear weapons under the non-proliferation treaty regime. The U.S. and Russia hold 95 percent of the world's nuclear arsenal. Iran is determined to acquire a nuclear weapon. It is unlikely that North Korea will voluntarily abandon its nuclear weapon program.

The existing nuclear non-proliferation regime is becoming marginal or irrelevant. Sensitive technology is now more available to states and non-state terrorists groups, provided that they can acquire a relatively small amount of fissile material. There is consensus that within the next two decades 30 entities could possess nuclear weapon capability.

There are tangible steps that could be taken to reduce the number of nuclear weapons and strengthen the existing nuclear proliferation regime. However, reduction is far different than elimination of nuclear weapons. Is elimination of nuclear weapons a valid strategic objective or is it a feel good tactic?

U.S. and Russian leaders have no more than 30 minutes to respond to a real nuclear weapon launch or computer warning error. The Bush II administration created a missile warning system (Shield) in Eastern Europe without considering Russia's strategic objective and strong objection.

The Obama administration is now considering eliminating the Shield deployment in Eastern Europe, scheduled for July, 2009. This in return for Russia's commitment to use its leverage to persuade Iran to abandon its nuclear weapon

development program. The Shield could be adapted to address the strategic objectives of both Russia and the U.S. and could protect the interests of both states.

Is the US initiative a tactic or is it a component of a cogent, long-range strategy based on Middle East political stability and the likelihood of Iran abandoning its nuclear program? Could this joint project accelerate the reduction of the U.S. and Russian nuclear arsenals?

The lesson to be learned is that consultation with friends and competitors regarding their strategic objectives could result in realistic and achievable mutual benefits.

Had the Bush II administration consulted with legal experts regarding Gitmo and reflected on the emerging battlefield detainee matter from a strategic perspective the ensuing global condemnation of the US and damage to its leadership image could have been avoided. A grand strategy for the Middle East is more complex because of the interdependence of US oil needs, militant Islamism and terrorism, the potential for an Iranian nuclear weapon and the potential for a nuclear arms race in the region. The ongoing US discussion with Russia regarding Iran's nuclear weapon program may be either a discrete issue, or it may involve Russia's use of its oil and gas to threaten Western Europe and its objective of regaining control of its former Central Asian Republics, including Georgia. Major contemporary events may only be tactical components of strategy.

Foreign and Defense Policy in the Obama Administration

John Allen Williams

John Allen Williams is a member of the National Strategy Forum Review Editorial Board and a Professor of Political Science at Loyola University Chicago and Chair and President of the Inter-University Seminar on Armed Forces and Society.

Early indications are that the Obama administration foreign and defense policies will be more evolutionary than revolutionary. This does not mean that changes are not significant or that they will not, over time, mark significant new directions in policy. Some shifts are already apparent in four areas: the badly misnamed “war on terror,” military personnel and procurement, counterinsurgency operations in Iraq and Afghanistan, and relations with allies – especially Great Britain.

First, President Obama ordered the closure of the detention camp at Guantanamo Bay, Cuba and barred the use of torture, as promised in his campaign. These decisions were the easy ones; more difficult will be finding secure and humane places for the detainees. Some of them are essentially stateless and many are too dangerous to let go.

Other Bush administration security policies are under review, but the Obama administration is not moving as quickly to reverse them as many hoped or feared. Much may be happening below the surface, but there are no early indications of drastic changes in policies toward intelligence collection, in particular.

Second, major changes are underway in the areas of military personnel and procurement. The Army and Marine Corps will be increased in size – a very expensive proposition that will call for cuts elsewhere in defense – to meet the manpower-intensive needs of counterinsurgency operations in Iraq, Afghanistan, and elsewhere. Hardware programs such as the Air Force F-22 “Raptor” fighter are getting a hard look. Perhaps ironically, some of the fighter's strongest supporters are Democratic senators and congressmen who see it as an economic jobs program for their constituents.

The “don't ask, don't tell” policy restricting the service of open homosexuals in the military is on its way out. The administration is moving slowly in this, however, seeking to build consensus among military leaders to smooth the transition and provide political cover. The change will not be without difficulty, including the sorting out of benefits for domestic partners and interpretations of the Uniform Code of Military Justice (UCMJ). Since the policy is mandated in Title 10, U.S. Code, the president cannot change it by an executive order. It will require congressional action, as well. The most likely result is that the current prohibitions on sexual harassment and sexual assault in the UCMJ will be applied without concern for gender. The domestic partner issue will not be dealt with if it can be avoided, pending more consensus on the issue of

THE NATIONAL STRATEGY FORUM REVIEW

gay marriage. Since the military is a reflection of society, more tolerant societal attitudes will make the adjustment easier, but it will not be without problems. These need to be anticipated and policies developed to deal with them.

Third, the Obama administration is shifting attention and resources from Iraq, where against all odds the war is going reasonably well now, to Afghanistan, where it is not. The administration has a number of highly qualified advisors on counterinsurgency (COIN), and appears to be listening to them – as the Bush administration finally did in late 2006. The strategy of General David Petraeus (now heading the U.S. Central Command, with responsibility for both theaters) and his former deputy General Raymond Odierno (now commander in Iraq) to use forces primarily to protect the people rather than for conventional military operations is firmly in place.

The strategy of trying to “turn” former enemies was successful in Iraq with the “Anbar Awakening” that saw the allegiance of most Sunni tribes switch to the side of the Iraqi government. It will now be tried in Afghanistan, where moderate elements of the Taliban and Taliban supporters will be appealed to, if such can be found. No one seriously believes that the Afghanistan conflict has a military solution, although the military will surely be part of it. The administration realizes that Afghanistan and Pakistan are part of the same problem, with Pakistan the far more serious component. The appointment of Ambassador Richard Holbrooke as a special representative to Afghanistan and Pakistan (the addition of Kashmir issues to his charter being successfully opposed by India) is a sign of this realization.

Fourth, changes on the diplomatic front are underway, some of which may be disquieting. There are early indications of relaxation in our embargo of Cuba (in place since 1962, yet the country is still run by a Castro). This will please farmers and enrage many citizens of Miami. Of more import, because of the relative popularity of the current president compared to his predecessor, this administration is in a better position to make requests of our NATO allies. Among these will be for more help in Afghanistan and taking in some released Guantanamo inmates as the facility shuts down. Given the clamor for this action on their part, it will be an offer more difficult to refuse.

Of possible concern is an apparent reduction in the felt importance by President Obama of the “special relationship” between the U.S. and Great Britain. Assuming, with Oscar Wilde, that “a gentleman is never unintentionally rude,” one wonders along with much of the British press whether several recent actions symbolize a new and lower U.S. priority for that relationship. Prime Minister Gordon Brown’s recent visit was the occasion for several of these, including the lack of a presidential greeting at the airport, no joint Rose Garden press conference, and a dramatically asymmetrical exchange of official gifts. One commentator pointed out that the set of DVDs of great American films presented to the Prime Minister could have been ordered from Netflix. This was in return for a pen holder made from a British ship fighting the slave trade, a sister ship of HMS Resolute, from whose timbers the presidential desk was made in 1880 and presented to the U.S. by Queen Victoria. The earlier return of a bust of Winston Churchill given to George W. Bush after September 11 made many wonder if this was an early sign of a fundamental change. Should President Obama decide to return his desk to the British, as well, that would be a more significant indication that something new is in the wind.

It is important to remember in analyzing an administration so early in its term that apparent policy directions may actually be a result of a new administration settling in and finding its way. Accordingly, not too much should be made of them. Indeed, the apparent snubs to the British may be due to an inexperienced administration overwhelmed by other issues. It is also possible that a new policy on the ethics of gift exchanges, including value limitations, has bled over into the foreign arena. If so, that should have been announced publicly. Policies will evolve, and they will surely provide opportunities for further comments.

The Moment to Decide

Frank Schell

*Frank Schell is a former member of senior management of a major U.S. bank specializing in trade, treasury, and risk management. He serves on the Dean’s International Council of the Harris School of Public Policy Studies at the University of Chicago, and on the editorial board of the National Strategy Forum. His opinion pieces on global affairs and the world economy have appeared in the *Far Eastern Economic Review*, the *Chicago Tribune*, the *American Spectator*, and the *National Strategy Forum Review*.*

“Once to every man and nation comes the moment to decide...”

James Russell Lowell, the American romantic poet, editor of *The Atlantic Monthly* (now *The Atlantic*), and Harvard professor wrote this script for President Obama and the nation – in the mid-19th century. Years later it became part of the Welsh hymn, *Ton-y-Botel*.

There can be no operating manual for a global crisis of unprecedented proportions. But there are already lessons to apply in the way that this economic Pearl Harbor, in the words of Warren Buffet, and the future of the U.S. economy, can henceforth be managed more decisively.

First, the utter severity has been consistently underestimated since early 2007 when HSBC, the largest bank in Europe, took an \$11 BN charge relating in large part to its U.S. subprime portfolio. The implications of this signal were not seen until later that summer, when a \$90 billion contraction in the commercial paper market occurred in August of 2007, which made it difficult for some companies to obtain short term funding. What has transpired since then is beyond the wildest imagination of some of America’s best minds: the unthinkable has already happened in the form of massive government intervention not seen since the Great Depression.

Second, there must be clarity and decisiveness about the rules of engagement – how much force the government is prepared to use as the remedy for financial markets – for private capital to return to the financial sector in particular. Protracted speculation about the future of Citibank and about nationalization in general has in recent months depressed both markets and people everywhere. Well-managed companies and private capital have suffered because of confusion over the limits of government power, the worst possible affliction for credit and capital markets. It is worse than bad news.

Third, government action must be timely, comprehensive, and bold: a 36 percent stake in Citigroup is the third such rescue action for that beleaguered institution but such actions have been incremental. The uncertainty about Citigroup’s future has caused its stock to trade as if it were to be nationalized, also negatively affecting the capital markets in general, particularly stocks in the banking sector.

The confusion started in March of 2008 when the Department of the Treasury assisted in the rescue of Bear Stearns – yet six months later, Lehman Brothers was allowed to fail and AIG, another leader in global finance, was effectively nationalized. To this day, it is really not widely known why there were different remedies for each institution. Like AIG and shortly before it was seized, Fannie Mae and Freddie Mac became wards of the state.

In the mayhem, systemic remedies were applied to maintain liquidity, the functioning of commercial paper markets, and to support the investment banks by granting direct access to the Federal Reserve. The investment banks left standing were converted into commercial banks, viewed as a safer harbor with more regulation.

The \$700 billion Troubled Assets Relief Program, also known as TARP, and more unfortunately as the “Bailout” has also been confusing – a misnomer from inception. When it was enacted in October, the expressed purpose was to acquire illiquid or so-called “toxic assets” from the private sector. Not long thereafter, part of TARP was used for capital injections into selected banks, both weak and strong, irrespective of whether some banks needed or wanted that capital in the form of preferred equity. TARP has also been used as the source of relief for the automobile industry.

More recently, the focus of TARP and related rescue efforts has returned to acquiring assets of the banking system, potentially guaranteeing certain exposures, and creating a Public-Private Investment Fund to value and acquire the assets. The administration has backed off on setting up a so-called aggregator bank (“bad bank”) as a government controlled entity. There is also the new commitment to use \$50 billion of TARP monies to prevent foreclosures.

The fact is that no one knows what TARP really stands for or what will happen next. TARP is not just about those in trouble – some banking companies that were healthy were forced to accept TARP preferred equity. TARP is about a lot more than assets, as it includes guarantees, equity capital positions, and helping the automobile companies and consumers. And there is the question of whether TARP provides relief by inserting the government into the affairs of private sector firms that did not need or want government assistance and the conditions that come with it.

President Obama should decisively emphasize several principles immediately. First, the President should stress that a well-functioning banking system with the availability of credit is not only essential to the nation’s economic stability and national security but also the first order of business of the Administration. The \$789 billion stimulus plan, job creation,

tax relief, infrastructure development, elimination of pork, homeowner relief, cleaner energy, fuel efficient cars, healthcare reform, income support programs, intervention in the AIG bonuses, the Middle East peace process, and softening of rhetoric toward Russia and Iran should be clearly subordinated now – to fixing the banking system, which is dysfunctional and commands limited confidence.

Further, the President should confirm that for many years, through the Federal Deposit Insurance Corporation (FDIC), there is a proven mechanism for bank interventions that is tantamount to nationalization – this is hardly a new concept. The FDIC will continue to intervene whenever there are banking insolvencies, protecting depositors in the process.

Finally, the President should indicate that acquiring toxic assets, providing liquidity and guarantees, and making selective capital injections are the other principal and continuing instruments of government intervention, as needed.

These directives will clear the air and support the premise of transparency, which the President has stated is a cornerstone of his Administration. Only then will the markets know the extent of government intervention in private markets.

A major unknown is how the public and private sector will collaborate to value the toxic assets. The focus of TARP changed in large part because the Treasury Department found it easier and more timely to take preferred equity positions than to try to establish a price for complicated mortgage backed securities and derivatives. At this writing, a private and public sector collaborative bidding process is now envisioned to determine valuations of toxic assets, and this is a severely needed financial experiment. Opening a more competitive process for private capital to participate is nevertheless a needed financial experiment.

The free market will destroy capital when mistakes are made. But we have also seen the incalculable cost and opportunity cost of indecisiveness and confusion, preventing recovery in the credit and capital markets. It is certain that failing institutions will need to be taken over by the government and sold off in pieces when conditions permit. Shareholders will lose out at that point, but private capital should not be destroyed prior to that because lack of clarity over the role of government.

Colossal irresponsibility in Washington, on Wall Street, and yes, in Hometown U.S.A. has put us into the worst financial mess since the 1930s. This crisis should and must cause reflection on exactly who is entitled to what, if anything. Many countries have their national myths. For the British, it was the destiny of dominion; for the French, the grandeur and glory of la France; and for the Swiss, it is to be a good Swiss. For America, we must assess and decide whether the objective of our society, universal home ownership and the aspirations implied by that, are realistic and affordable.

Protecting America's Virtual Reality

Lauren Bean

Lauren Bean is Editor of the National Strategy Forum Review.

Cyber security represents a major national security challenge with a significant economic vulnerability – the ability of U.S. adversaries to acquire valuable information or data about U.S. strategy, technology, and capability can weaken America's competitive economic advantage.

National security in the virtual environment is receiving due attention after decades of calls by governmental officials and others. The most recent and well-publicized cyber threat posed by the "Conficker" worm, which has infected an estimated 3-12 million Windows PCs was scheduled to activate yesterday, April 1. There are also allegations against China, which it rejects, about an alleged international network of "cyber spies" who have reportedly infiltrated government offices' computers around the world.

Safeguarding the U.S. information and communication infrastructure, which is largely privately-owned and globally operated, is imperative for protecting America's economic strength and its informational integrity. According to a recent report produced by the Center for Strategic and International Studies (CSIS) titled, "Securing Cyberspace for the 44th

Presidency,” “the immediate benefits gained by our opponents are less damaging, however, than is the long-term loss of U.S. economic competitiveness...we are providing them with the ideas and designs to arm themselves and achieve parity...our lack of cybersecurity is steadily eroding this advantage [economic strength].”

The virtual environment is a tool and a weapon used by those seeking to disrupt or incapacitate America’s critical infrastructure, primarily its informational networks. By using the virtual environment, U.S. adversaries seek to collect and exploit valuable data from government and private sector entities. The most significant challenge is posed by foreign military or intelligence entities. In recent years, the Department of Defense, NASA, and the Department of Homeland Security suffered serious cyber intrusions. Last summer, the FBI’s computers were accessed by a foreign entity, and shortly thereafter the White House networks were infiltrated. Cyber attacks on the government computer networks increased by forty percent in 2008 according to the U.S. Computer Emergency Readiness Team (CERT). Cyber crime attacks on private and public sector security entities have resulted in financial losses upwards of \$350,000, according to the 2008 CSI Computer Crime & Security Survey. According the Office of the Director of National Intelligence, China and Russia have the capability to execute large scale cyber attacks or data breaches. Less sophisticated but equally effective is the use of the Internet by hackers, terrorists, or others who seek to exploit the personal identity and financial information of individuals.

President Obama has elevated the need for improved U.S. cyber security to high-priority. However, improving America’s cyber security is not simple – a matrix of conceptual, organizational, legal, and policy components create a significant challenge, particularly for security and legal professionals. Determining who the actors are (state or non-state) and what threats they pose (cyber attack, cyber espionage, cyber intrusion) is complicated by the diffuse nature of the virtual environment. Addressing the threat array requires not only government cooperation (legal, intelligence and law enforcement, in particular), but also the engagement of the private sector and the international community. However, there are complex bureaucratic and legal challenges embedded in both partnerships. There are also prosecutorial difficulties because of an outdated domestic and international legal regime. The need for public support, which is complicated by the difficulty of enhancing security while protecting privacy, makes resolving this problem exceedingly difficult.

Following the issue of cyber security closely will provide substantive insights about U.S. national security. The implications of this important issue are far-reaching, and nearly every individual with access to some form of technology, whether cell phone, laptop, or Blackberry, will be affected. A breach of information, whether by a foreign intelligence agency on the U.S. government, a network of “bot” computers on Microsoft, or a hacker on your personal computer, would alter the established patterns of an information-reliant society.

Renewing the West

Endy Zemenides

Endy Zemenides is a member of the National Strategy Forum Review Editorial Board. He is a partner at Acosta, Kruse & Zemenides, a Chicago law firm.

President Obama’s first major trip overseas takes him to Europe. With his stop in London for the G20, the President visits with a Europe that is a key trading partner with the U.S., and a partner whose assistance is vital if we are to emerge from this global economic crisis. Then to the NATO summit, where he will visit with partners in Europe who have stood with the United States for 60 years in the most successful military alliance in history. Finally, when the President reaches Turkey, he will have reached the edge of Europe, or left Europe altogether (or both in the same country), and realize how much closer Europe is to the most dangerous places in the world than we are.

The 2008 presidential campaign focused on many hotspots – Iraq, Afghanistan, Iran, the Israeli/Palestinian conflict, Russia’s incursion into Georgia – and positions were taken on all of those issues. Yet, the “Obama for America” campaign and the new administration – following the tradition of all the post Cold-War presidencies – has not been able to find an overarching structure or an easily identifiable *raison d’être* for American foreign policy. There is no equivalent to the Cold War doctrine of containment in the offing. The last attempt – trying to define American foreign policy in the context of a Global War on Terror – may have unwittingly given breathing space for more long term serious challenges to American

primacy (i.e., China, a resurgent Russia) to assert themselves.

The various challenges to the world order shaped by the U.S. all come from outside what is considered “the West”. This provides tremendous impetus for the U.S. to revisit its relationship with its most reliable partners. No matter what the challenge, it is clear that the U.S. needs Europe in order to manage the new international order. There are at least two compelling reasons for the U.S. to revitalize its oldest alliance, redefine burden sharing within it, and thus renew the West:

We can no longer “go it alone”

The American military is stretched to a point that the Pentagon’s two wars doctrine must be revisited. We are in the midst of a financial crisis that has global ramifications (and in many ways, global roots) and that needs international coordinated action to be overcome. We are a debtor nation, and will remain so for the foreseeable future. While President Obama is popular overseas, the previous Administration’s lack of popularity, combined with the Iraq war, and the recent setbacks suffered by American capitalism have combined to decrease the U.S.’s influence to the lowest point in decades.

This is not your father’s Europe

Or even President Clinton’s for that matter. Although the American foreign policy establishment has not treated Europe as derisively as former Secretary of Defense Donald Rumsfeld (with his distinction of “old Europe vs. new Europe”), but the orientation of American foreign policy leaves one with the impression that Washington looks overseas and sees a European Economic Community and NATO partners, rather than a European Union that may be in fact transforming into a United States of Europe.

Today’s Europe has more people, more wealth, and more votes on every international body than does the U.S. On the security front, it has a 60,000 troop rapid reaction force outside of NATO control, has undertaken several security missions in the last five years, and Javier Solana – the EU’s High Representative for the Common Foreign and Security Policy – is increasingly surrounded by military, rather than civilian, advisors. Europe’s wider and deeper social safety net has allowed it to weather the financial crisis better than the U.S. to date, and to resist the Obama Administration’s pressure for a European stimulus package. It also allows them to reverse their role with Americans in the conversation regarding what is the best way to structure capitalism. Culturally, Europeans study in each other’s universities, and are all glued to their televisions during the annual Eurovision contest. Language is no longer the barrier it once was. Finally, one should not underestimate the political symbolism of European discarding their marks, francs, lira, escudos, drachma, and other currencies in favor of the euro.

France has rejoined NATO military command, but French President Sarkozy continues to identify an autonomous European defense capability as an “absolute priority”. While in the short term this improves capability and stature of NATO, in the long term, it helps modernize French forces (by making them interoperable with American forces) and thus advances an autonomous European defense identity to a great extent.

The United States is still the “indispensable nation”, it just needs stronger partners more than ever before. Europe can be - and should be - that partner. The parameters of that partnership still need to be determined, so the follow up to President Obama’s trip to Europe will be key. There are a few pressing issues where the US and EU differ that should be watched closely:

Dealing with the financial crisis

This will remain an especially significant point of contention well beyond the end of the current crisis. What the EU and US are doing to stimulate their respective economies is but a small part of a much larger picture. A reorganization of the world financial order may be required, and continental Europe will have a much greater say than it did after World War II.

The role of NATO

Americans are committed to a wider role for NATO; Europeans see the future in a European defense identity that

develops autonomously but in parallel to NATO. Now that France has rejoined NATO military command, can those competing visions be reconciled? Can NATO's unwieldy decision making structure survive further expansion of the alliance to countries like Georgia that were never part of Europe? Can Article V of the NATO Treaty (mandating the defense of every NATO member by all NATO allies) survive further expansion; will Americans be willing to risk New York, Frenchmen will to risk Paris, Greeks to risk Athens for the sake of Skopje or Tbilisi?

The "Eastern Question"

Just as the great European powers were focused on the fate of the Ottoman Empire in the 19th century, so does the Western alliance remain fixated on the fate of Turkey. The moment of truth may come quite quickly, as a decision on whether Turkey can continue its accession negotiations with the EU in December.

The US is committed to a Turkey rooted in the West and believes that EU membership is part of that equation. The EU demands that Turkey comply with European standards, and there is some resentment in Europe towards the American push for Turkey's membership, the argument being that the US wants to bring Europe to Turkey rather than Turkey to Europe.

Nonetheless, Turkey faces serious obstacles to its EU membership, the foremost of which is its continued occupation of an EU member state (Cyprus) and its refusal to recognize that state (which puts Turkey in the relatively absurd position of needing the consent of a state it refuses to acknowledge). Fortunately, negotiations between Greek and Turkish Cypriots towards a settlement that will reunify Cyprus are proceeding. Still, there is doubt over whether the Turkish military will allow the Turkish Cypriots to negotiate freely. As long as the occupation of Cyprus continues, European countries that don't want Turkey in the EU for other reasons will have the cover of the Cyprus problem. In the meantime, Turkey's road to Europe runs through Nicosia.

The US needs Europe in order to successfully navigate the challenges in today's world, and Europe needs the US if it aspires to a greater political union with superpower status. What unites the US and Europe is much greater than what separates them. Of the many foreign policy challenges President Obama faces in 2009, perhaps no other one is as important and far ranging consequences as revitalizing the Euro-American/ Western Alliance.

KEY REGIONS AT A GLANCE

A Preview of Iran's Upcoming Elections

Rami Yelda

Rami Yelda is author of A Persian Odyssey: Iran Revisited and a scholar on Iran and Middle East affairs. He is currently working on a forthcoming book.

This year Iran is celebrating the 30th anniversary of the Islamic Revolution that toppled the Shah and replaced him with Ayatollah Seyyed Ruhollah Khomeini. During these 30 years, Iran has been transformed from a corrupt semi-secular state, though friendly with the U.S., into a corrupt and anti-American Islamic theocracy.

The cornerstone of Khomeini's Islamic theocratic regime has been a return to Islamic teachings and also to the belief in the eventual return of Shi'as 12th Imam, who disappeared in a well in Samarra (in Iraq) in 840 AD. Following Khomeini's writings and teachings, the newly formed Islamic Republic was to be ruled by a high-ranking faqih (jurist) known as the "Supreme Leader" who represented the Hidden Imam and was the true ruler of the country with other elected officials playing a lesser role. As expected, Khomeini became the first Supreme Leader. After his death was he succeeded by Ayatollah Seyyed Ali Khameni. It was Khomeini's belief that the U.S., dubbed by him as the "Great Satan" because of its unwavering

support of Israel (seen as the archenemy of Islam and the occupier of the holy Qods, Jerusalem), was to be pestered in any way possible. Taking American diplomats hostage in 1979 and humiliating President Carter marked the beginning of Iran's defiance of the U.S. – a trend that persists today.

In June, 2009, Iranians will elect their next President. The winner of the election will be able to either continue Iran's hostility toward the U.S., or start a meaningful dialogue with America's new administration. This is an election that will have major consequences not only for Iran, but also for the U.S and the world. Since the election of Barack Obama, the Iranian rulers have made guarded and sometimes inconsistent remarks about starting a new relationship with the U.S. It appears the Iranian rulers are trying to make some adjustments in their behavior towards the new American Administration. On the American side, with the Iranian election looming so close, President Obama has taken the proper 'wait-and-see' attitude.

But who will be Iran's next President? Two major candidates are vying for the job: Mahmoud Ahmadinejad, the current president, who is the most conspicuous and wants to be elected for a second term; and Mohammad Bagher Qalibaf, a former military commander and mayor of Tehran.

In the Islamic Republic of Iran, all political elections are rigged. All candidates running for office, no matter how minor, are thoroughly screened by a committee of religious experts and vetted. Devotion to Islam and Shi'ism are the prerequisites. As an example: all candidates' female family members are inspected (sometimes up to three generations) to ensure that they follow the strict rules of hejab and wear chadors (head covering). (Wearing a fashionable headscarf is unacceptable and the candidate will be automatically barred from running.)

Despite what the foreign media says, considering all these factors, Mahmoud Ahmadinejad is a potential loser in the next election. No one doubts that his driving force in life and politics is not the welfare of his compatriots, but is his devotion to the Hidden 12th Imam and to Khomeini's teachings. With his controversial remarks about the Holocaust and his antics in the U.N.'s General Assembly (like seeing a light shining in the hall from the missing 12th Imam and paralyzing all the delegates), he has been an embarrassment to Iranians. Many have wished that he be stopped from leaving the country and projecting an image that does not accurately reflect Iran as a nation.

Economically, Ahmadinejad has been frivolous. He spent the equivalent of \$30 million to build a spectacular mosque on top of a well in Jamkaran (close to Qom) where the Imam was reported to resurface soon. To add some significance to his belief, he held his first cabinet meeting around the well where all his ministers had sat cross-legged and then dropped his government's handwritten agenda down the well to be read and approved by the missing Saint (surmising that during all these centuries, the Arabic-speaking Saint had mastered the Persian language). Ahmadinejad's expensive project and his ridiculous act around the well has been the subject of many jokes in Iran.

When Iran's economy was booming thanks to the high price of oil, Ahmadinejad squandered millions, if not billions, of dollars in Latin American, building roads, ports, dams, hospitals, mosques, etc. Now with the collapse of the global economy and the fall of oil prices, Iran, a mono-economy with 90 percent of its revenues generated from oil, is suffering too. In the good times, Iran collected \$200 billion in three years. For the last several years, Iranians have been complaining about the poor state of the economy: inflation is 24 percent with a high unemployment rate especially among the ever-increasing restive youth.

Sixty independent economists have recently warned about the potential for further deterioration of the government's financial situation. According to them, Iran's budget was planned according to oil prices being pegged at \$60.80. But with the fall of oil prices, there is a serious deficit. To raise funds for the depleted treasury, Ahmadinejad has cancelled subsidies for water and electricity that he had granted to the poor—his main constituents. This has already diminished his popularity. Furthermore, Ahmadinejad has missed several important government meetings in the last several months. Each time, his staff has attributed his absence to "a minor illness."

Another matter hurting the Islamic republic has been American economic sanctions. Whether the regime accepts it or not, Iranians feel the economic noose tightening. With the worldwide economic collapse, Dubai and the rest of the Emirates are not financial sanctuaries for the rich Iranians any longer. Iranian businessmen have to deal with second tier banks in China or Malaysia. Although Ahmadinejad's government has switched the reimbursement of oil payments to the Euro, the U.S. dollar is still king in Iran. With the economic sanctions, it has been easier for Americans to track movements of dollars by the government and Iranian businessmen.

Iran's nuclear aspirations create another chasm. No matter what the financial or diplomatic consequences, Ahmadinejad is adamant about developing a nuclear weapon. The majority of Iranians feel that Iran's primary focus should be to improve the standard of living; they view a nuclear weapon as unnecessary. To them, Iran's nuclear aspirations have only served to isolate Iran from the world community.

Internationally, Ahmadinejad has continued a campaign to irritate “the Great Satan” – the United States. And while he has made new alliances in Latin America, where he has elected to carry out Khomeini's policies (and in the meantime spread Shi'ism), he has also made new adversaries. Hugo Chavez of Venezuela became his main ally in accomplishing his mission, and other Latin American countries such as Bolivia, Ecuador, Nicaragua and Cuba joined later. Yet Iranians consider the Latin American countries to be too geographically distant and too inconsequential for Iran and do not approve of Ahmadinejad's engagement of those countries.

His opponent, Mohammad Bagher Qalibaf, is barely known in the West. He is a serious candidate, and a short introduction is warranted. Qalibaf was born in 1961 in the holy city of Mashhad (in the northeast of Iran, close to the Afghan border). The family had a rug weaving and selling stall in Mashhad's bazaar. (Qali in Persian means “rug” and qalibaf means “rugweaver.”) His father was a Kurd, a descendant of the warlike Kurdish tribes who in the 17th century were forcefully made to leave their ancestral lands in the western Zagros Mountains and settle in Khorasan.

At 19, Qalibaf joined the military and served in the Iran-Iraq war (2000-2008). Because of his heroism and abilities, he was promoted to the rank of major-general. After leaving the military he was assigned to be the Chief of Police Forces. In 2005, he was elected by Tehran's City Council to replace Ahmadinejad who was the mayor of Tehran up to that time, an assignment he was able to fulfill well.

Qalibaf's strongest appeal to Iranians is his brilliant military service. He has added to his popularity by being an able mayor and criticizing Ahmadinejad's squandering of government's funds in Latin America. He has also addressed opening a dialogue with the U.S. and ending the hostilities that have isolated and weakened Iran for the last 30 years. With the genuine popularity that America and Americans have among Iranians, those comments have enhanced his popularity.

Foreigners believe Khamenei is the one who makes all the crucial decisions in Iran. That is not the case. The real power in Iran is the Sepah (Iranian Revolutionary Guard force—IRGC). The Sepah is very strong and very rich. It is a huge military-industrial complex reputed to be worth \$18 billion. Its commander-in-Chief, Mohammad Ali Jafari, is without a doubt the strongest man in the country. Jafari is the real power, and he dictates what Khamenei says. The mullahs know they are in power because of military opposed the Shah. The mullahs know the military leaders can topple them with a coup if they ever decide to.

Overall, Mohammad Bagher Qalibaf has many important qualifications for the Iranian presidency that current President Ahmadinejad lacks: his service in the Iran-Iraq War was commendable; his ties to the powerful military are still strong; he has been a popular mayor; and his comments about a renewed dialogue with the U.S. have made him the strongest candidate for presidency.

Enhancing a Security Dialogue with China

Henry Levine

Henry Levine's twenty-five year government career included assignments at the U.S. Embassy in Beijing, as U.S. Consul General in Shanghai, and as Deputy Assistant Secretary of Commerce for Asia. He is currently a Senior Director with Stonebridge International, a strategic advisory firm in Washington, DC, and Chair of the Intensive China Areas Studies Course at the State Department's Foreign Service Institute. He is a frequent speaker before business groups on U.S.-China economic relations. The views expressed in this article are the author's alone and not necessarily those of any organization with which he is affiliated. Visit the author's blog, “Behind the Curtain: An Insider's Guide to U.S.-China Relations”, visit levinehank.wordpress.com.

Overall, the Bush Administration did a great job on China policy. The Administration's free trade principles helped it steer away from destructive trade actions, to the benefit of Americans and Chinese. Perhaps most important, as (then) Taiwan President Chen Shui-bian sought to further a Taiwan independence agenda, President Bush clearly let both sides of

THE NATIONAL STRATEGY FORUM REVIEW

the strait know the U.S. wanted neither to take unilateral actions that would change the status quo. This statement helped maintain stability in cross-Strait and in U.S.-China relations at a critical moment.

But for all the success of the Administration's China policy, there was one misstep: a reining in of military-to-military exchanges. A number of Administration officials came to their positions hyping "the China threat". The tragedy of September 11 caused them quickly to shift their focus. Not only was China a potential ally in the war on terror, but senior national security figures skeptical of China were soon fully occupied in another part of the world. That said, and though China did not get the full brunt of their focus, strong signals discouraging deepened military exchanges with China went out through the DOD system.

The 2001 EP-3 collision and recent incident in the South China Sea between U.S. and Chinese ships are just two examples of why such exchanges are so important. We need the intensified interaction that helps both sides learn how to avoid or (if necessary) deal with crises or near misses. But the roots of this issue go deeper.

Over the course of 25 years, I have observed the striking evolution in the backgrounds and attitudes of my civilian Chinese counterparts. In the early 1980s, it was rare to find a counterpart who had spent extensive time abroad. Though intelligent, these officials were uncomfortable in dealing with foreign counterparts and they suffered from a lack of familiarity with international norms, especially as practiced in the real world. For example, it is one thing to read the rules of the WTO. It is another to have the understanding of them that comes from experience in international business and trade negotiations.

Today, when U.S. officials travel to Beijing they are sitting across from a group of sophisticated, self-confident, and experienced international diplomats. Many differences in perspective and interests remain, but discussions today are substantive in a way that was impossible when Chinese officials had only glimmerings of how the outside world operated.

The contrast with the Chinese military establishment is striking. Of all of the entities in China today, the PLA almost alone remains highly cloistered. Colleagues who interact with the PLA describe meetings that bring me back to the early days of my encounters with civilian officials. And the PLA remains apart not just from foreigners. Within China it operates as a largely independent entity, supervised by the highest member of the Chinese Communist Party, but more or less severed from the rest of the Chinese government at levels below this. To have seen the driver of a military vehicle involved in a traffic accident drive away from the scene despite the entreaties of a traffic cop is to see a concrete expression of this reality. To see the Foreign Ministry taken by surprise and out of the loop following the EP-3 and South China Sea naval incidents is to see a more substantive example.

An isolated, insecure PLA is not in the U.S. interest. For this reason, the Obama Administration has the opportunity to make a significant contribution to the stability of U.S.-China relations by embarking on an activist program of exchanges with the Chinese military. We need to get to the point where, not only do counterparts sit together in classes and tour each others' facilities, but where, when the day is done, they sit down together over beers and get to know each other.

One step in particular might help facilitate the interaction we need. The U.S. Secretaries of State and Defense sit down every year together for security discussions with their counterparts from Japan. There is a similar forum with Australia. Why not use the same mechanism for enhancing security dialogue with China? Maybe add the Chairman of the Joint Chiefs and the PLA's Chief of Staff, so the uniformed military is represented too. This would help bilateral understanding and civilian-military coordination on the Chinese side and pave the way for deepened exchanges at lower levels.

I know that despite the best of intentions on the U.S. side there may be reluctance from the Chinese side to engage. But we should not let ourselves be discouraged by this. At his March 24 press conference, President Obama, in speaking about his approach to the challenges his administration is facing referred to his belief in "persistence". He noted that on tough problems we may not see results immediately, but he would keep at it and over time we would make progress.

I think that is a great perspective to bring to U.S.-China relations overall, and to the important issue of enhancing relationships with the PLA in particular. This should be a high priority item, persistently pursued.

SPECIAL SUPPLEMENT: NON-LETHAL WEAPONRY

On January 29, 2009, the National Strategy Forum hosted **Colonel Kirk Hymes, Director of the Joint Non-Lethal Weapons Directorate, and Mr. Jeff Keuter, President of the George C. Marshall Institute**. The speakers addressed the National Strategy Forum membership on the subject of non-lethal weaponry.

In brief, Colonel Hymes and Mr. Keuter explained that the issue of non-lethal weaponry is increasingly recognized as a necessary component of a balanced future strategy within the Pentagon. What is “Non-Lethal Weaponry”? The definition according to the Department of Defense’s Joint Non-Lethal Weapons Program (JNLWP) is: “Weapons, devices and munitions that are explicitly designed and primarily employed to incapacitate targeted personnel or materiel immediately, while minimizing fatalities, permanent injury to personnel, and undesired damage to property in the target area or environment. Non-lethal weapons are intended to have reversible effects on personnel and materiel.”

Colonel Hymes stated that the U.S. government is developing an array of non-lethal weaponry and technology which will provide the warfighter options when lethal force is not the best response. As insurgency violence continues to escalate despite intelligence and force efforts, non-lethal weapons will become an increasingly integral tool within the U.S. national security arsenal.

The following article was submitted by the U.S. Department of Defense’s Joint Non-Lethal Weapons Directorate: “Non-Lethal Weapons: The Right Tools for the Job.” For more information about the Joint Non-Lethal Weapons Program, visit <https://www.jnlwp.com>.

Non-Lethal Weapons: The Right Tools for the Job

By David J. Trachtenberg and William E. Malone

Published with permission from *Jane’s Defence Weekly*

William E. Malone is Vice President and Division Manager of CACI International’s Strategic and Analytic Solutions Division.

David J. Trachtenberg is President and CEO of Shortwaver Consulting, LLC, and a member of Jane’s Strategic Advisory Services’ expert network. He was Principal Deputy Assistant Secretary of Defense for International Security Policy from 2001 to 2003.

Non-lethal weapons, described by some as “smart power,” can help bridge the gap between hard and soft power. Non-lethal weapons can play a critical role in irregular warfare, where distinguishing between adversaries and innocent civilians is sometimes nearly impossible.

In a recent *Foreign Affairs* article, U.S. Secretary of Defense Robert Gates argued that the United States must be prepared to fight “irregular” wars such as counter-insurgencies and to win the peace during post-conflict stability operations.

“The U.S. needs a military whose ability to kick down the door is matched by its ability to clean up the mess and even rebuild the house afterward,” Gates stated.

One set of tools uniquely applicable to such irregular types of operations - non-lethal weapons - has not been fully integrated into the warfighter’s toolkit.

Non-lethal weapons are intended to incapacitate personnel or materiel while minimizing casualties and collateral property damage. Their use could help bridge the gap between hard power and soft power in a way some have described as “smart power.”

Efforts to expand the use of non-lethal capabilities by the armed forces have met with resistance, even among the uniformed services whose missions might be better achieved with alternatives to the use of lethal force.

THE NATIONAL STRATEGY FORUM REVIEW

Much like an Allen wrench that sits in a toolbox unused because the owner does not understand when to use it, non-lethal weapons are viewed as specialized capabilities poorly suited to volatile environments where deadly violence is commonplace.

Given the culture and training of the military, reluctance to use weapons that are designed not to kill is understandable. However, Gates correctly warns that “over the long term, the U.S. cannot kill or capture its way to victory.”

Future conflicts will require U.S. forces to maintain security and stability. U.S. Department of Defense (DoD) guidance now explicitly calls stability operations “a core U.S. military mission” with “priority comparable to combat operations.”

There is a growing recognition that non-lethal weapons provide useful capabilities for dealing with unconventional contingencies.

The DoD’s 2005 Strategy for Homeland Defense and Civil Support recommended greater investment in non-lethal weapons capabilities. The 2006 Quadrennial Defense Review noted their potential role in the “war on terror” and counter-proliferation, while the Pentagon’s 2008 Guidance for the Development of the Force acknowledged their utility for irregular warfare, for combating weapons of mass destruction and for homeland defense.

So what accounts for the reluctance to integrate non-lethal weapons more broadly into the military?

Some believe that non-lethal technologies, especially advanced directed-energy technologies like the Active Denial System, are insufficiently mature or may have dangerous long-term human effects. Others believe there are legal or treaty issues that increase the risks associated with their use.

Most importantly, the military is unaccustomed to training with and using non-lethal weapons and does not fully appreciate their potential benefits, especially in urban environments and complex coalition operations with international partners.

All of these issues can be overcome by educating senior DoD leadership, military commanders and operators on the utility of non-lethal weapons, their unique applicability to future contingencies and the processes and procedures that are in place to ensure their use is safe, effective and legal- and treaty-compliant.

A new Army Field Manual acknowledges that non-lethal weapons “will often be the primary weapons” in future irregular warfare contingencies and notes that effective training includes “employing both lethal and non-lethal means.” Broadening this awareness across all Services will help ensure these capabilities are fully integrated into the joint warfighter’s toolkit.

Non-lethal capabilities also lend themselves to the unique domestic homeland security environment. For example, they could help enforce a domestic quarantine in the event of pandemic influenza and secure the country’s borders more effectively. However, the military has not proactively embraced this type of capability despite Pentagon guidance acknowledging its utility for both the warfighter abroad and in support of domestic civil authorities.

Ensuring that the U.S. military uses the right tools to fight and win the coming battles will require the active involvement of Gates.

Having argued that the U.S. military needs “a better balance in the portfolio of capabilities it has” to meet future challenges, it would be reasonable to expect his support for the development, acquisition and use of non-lethal weapons to help achieve mission success.

The DoD should plan, program and budget for these capabilities accordingly. In addition, the Obama administration should recognize their utility as it crafts its new defense and homeland security strategies and develops its own Quadrennial Defense Review.

There is no need to use a screwdriver when an Allen wrench is the right tool for the job.

ECONOMIC AND INDUSTRIAL ESPIONAGE: A QUESTION OF COUNTERINTELLIGENCE OR LAW ENFORCEMENT?

Article Footnotes

[*] See the Department of Justice web site at http://www.usdoj.gov/usao/can/press/2006/2006_12_14_meng.indictment.press.htm.

[1] See Remarks of Joel F. Brenner, ABA Standing Committee on Law and National Security, March 29, 2007, at <http://www.ncix.gov/publications/speeches/ABASpeech.pdf>.

[2] See, William J. Broad, A Spy's Path: Iowa to A-Bomb to Kremlin Honor, New York Times, November 12, 2007 A1.

[3] See Chris Carr, Jack Morton, and Jerry Furniss, "The Economic Espionage Act: Bear Trap or Mousetrap?", Vol. 8.2 Texas Intellectual Property Law Journal (2000) p. 159, 163-170.

[4] Wanja Eric Naef, Economic and Industrial Espionage: A Threat to Corporate America?; Infocon Magazine Issue One, October 2003 at <http://www.iwar.org.uk/infocon/print/espionage-cid.htm>.

[5] Hal R. Varian. June 28, 2007. "An iPod Has Global Value. Ask The (Many) Countries That Make It," <http://www.nytimes.com/2007/06/28/business/worldbusiness/28scene.html>

[6] See "Welcoming Comments by National Counterintelligence Executive Dr. Joel F. Brenner DNI –Private Sector Workshop on Emerging Technologies," Carnegie Endowment for International Peace, Washington, DC, 7 December 2006 <http://www.ncix.gov/publications/speeches/CarnegieSpeech20061207.pdf>

[7] Ibid.

[8] Chris Carr, Jack Morton, and Jerry Furniss, "The Economic Espionage Act: Bear Trap or Mousetrap?", Vol. 8.2 Texas Intellectual Property Law Journal (2000) p. 159, 161.

[9] See p. 3 Report 2003 at http://www.ncix.gov/publications/reports/fecie_all/fecie_2003/fecie_2003.pdf.

[10] ASIS. Trends In Proprietary Information Loss; Survey Report, 3. August 2007. <http://www.asisonline.org/newsroom/surveys/spi2.pdf>. The 2001 FECIE report stated that an estimated \$100-250 billion was lost in sales at the end of calendar year 2000.

[11] See Statement by FBI Director Louis J. Freeh, Hearing on Economic Espionage before the House Judiciary Subcommittee on Crime, May 9, 1996, at http://www.fas.org/irp/congress/1996_hr/h960509f.htm.

[12] 2005 FECIE Report, 1.

[13] The categories for 1997/1997 were: Advanced material coatings; Advanced transportation and engine technology; Aeronautics systems; Armaments and energetic materials; Biotechnology; Chemical and biological systems; Directed and kinetic energy systems; Electronics; Ground systems; Guidance, navigation, and vehicle control; Information systems; Information warfare; Manufacturing and fabrication; Marine systems; Materials; Nuclear systems; Power systems; Semiconductors; Sensors and lasers; Signature control; Space systems; Weapons effects and countermeasures.

[14] The allegations, facts, and plea agreement for this section are drawn directly from the Department of Justice's web sites

at http://www.usdoj.gov/usao/can/press/2006/2006_12_14_meng.indictment.press.html

[15] The Indictment charged Meng under a number of statutes with the following maximum penalties: Conspiracy, in violation of 18 U.S.C. § 371, (five years in prison, a fine of \$250,000 or twice the value of the property involved in the transaction, whichever is greater, a three year term of supervised release); Economic Espionage and Attempted Economic Espionage, in violation of 18 U.S.C. §§ 1831(a)(3), 1831(a)(4), (fifteen years in prison, a fine of \$500,000 or twice the value of the property involved in the transaction, whichever is greater; a three year term of supervised release); Arm Export Control Act, in violation of 22 U.S.C. § 2778, (ten years in prison, a fine of \$1,000,000 or twice the value of the property involved in the transaction, whichever is greater; a three year term of supervised release); Misappropriation of Trade Secrets and Attempted Misappropriation of Trade Secret, in violation of 18 U.S.C. §§ 1832(a)(1), 1832(a)(4), (ten years in prison, a fine of \$250,000 or twice the value of the property involved in the transaction, whichever is greater, a three year term of supervised release); Interstate and Foreign Transportation of Stolen Property count, in violation of 18 U.S.C. §§ 2314, (ten years in prison, a fine of \$250,000 or twice the value of the property involved in the transaction, whichever is greater, a three year term of supervised release); False Statement to Government Agency, in violation of 18 U.S.C. § 1001, (five years in prison, a fine of \$250,000 or twice the value of the property involved in the transaction, whichever is greater, a three year term of supervised release). However, the court could impose any sentence following conviction after consideration of the U.S. Sentencing Guidelines and the federal statute governing the imposition of a sentence, 18 U.S.C. § 3553.

[16] Case description quoted from the Testimony of Larry M. Wortzel, Before the Subcommittee on Crime, Terrorism, and Homeland Security of the House Committee on the Judiciary Hearing on “Enforcement of Federal Espionage Laws” January 29, 2008, http://www.fas.org/irp/congress/2008_hr/012908wortzel.pdf

[17] The allegations, facts, and plea agreement for this section are drawn from the Department of Justice’s web sites at http://www.usdoj.gov/criminal/cybercrime/Okamoto_SerizawaIndict.htm and <http://www.usdoj.gov/criminal/cybercrime/serizawaPlea.htm>.

[18] See Alzheimer’s at http://www.piribo.com/publications/diseases_conditions/alzheimers/pipeline_commercial_insight_alzheimers_disease.html

[19] The Indictment is still pending against Okamoto, which charges him with Conspiracy, Economic Espionage Act offenses, and the Transporting of Stolen Property in Interstate and Foreign Commerce.

[20] Thus far Hiroaki Serizawa has pleaded guilty to making false statements to the government. In the plea Serizawa admits he: falsely understated the number of vials of research material which Okamoto had taken from Serizawa’s laboratory (hundreds of vials); initially denied any recent personal contact with Okamoto when in fact Serizawa had been in recent telephone, electronic mail and personal contact with Okamoto; and initially denied any knowledge of Okamoto having accepted a research position with RIKEN when in fact Serizawa knew that Okamoto had accepted a research position at RIKEN. The false statements offense carries a maximum penalty of five years incarceration and a \$250,000 fine. Under the law, conspiracy carries a maximum penalty of five years incarceration and a \$250,000 fine, while economic espionage carries a maximum penalty of 15 years incarceration and a \$500,000 fine, while interstate transportation of stolen property carries a maximum penalty of 10 years incarceration and a \$250,000 fine.

[21] The allegations, facts, and plea agreement for this section are drawn directly from the Department of Justice’s web sites at <http://www.usdoj.gov/criminal/cybercrime/yeIndict.htm> and http://www.usdoj.gov/usao/can/press/2006/2006_12_14_ye.zhong.plea.press.html

[22] Ye and Zhong were charged with a total of ten counts, including: one count of conspiracy, in violation of 18 U.S.C. §§ 371, 1831(a)(5) and 1832(a)(5); two counts of economic espionage, in violation of 18 U.S.C. § 1831(a)(3); five counts of possession of stolen trade secrets, in violation of 18 U.S.C. § 1832(a)(3); and two counts of foreign transportation of stolen property, in violation of 18 U.S.C. § 2314.

[23] In particular I would like to thank the editors, Jennifer Sims and Burton Gerber, for their assistance in framing the article and many helpful suggestions.

[24] Remarks by Joel F. Brenner, National Counterintelligence Executive, "Strategic Counterintelligence: Protecting America in the 21st Century," The Nro/National Military Intelligence Association Counterintelligence Symposium, Washington DC, 24 October 2007 at <http://www.ncix.gov/publications/speeches/NRO-NMIA-CI-Symposium-24-Oct-07.pdf>.

[25]

[26] See, Two Bay Area Men Indicted On Charges Of Economic Espionage <http://www.intellectualpropertylawfirms.com/national-content.cfm/Article/107306/Two-Bay-Area-Men-Indicted-On-Charges.html>.

[27] See, Kelly Uphoff, Tilting the Playing Field: Economic Espionage Hasn't Gone Away Since 9/11 Costs to the U.S. Economy Could Be in the Hundreds of Billions of Dollars, at <http://www.jinsa.org/articles/view.html?documentid=2835>.

[28] Though in 2000 a small controversy erupted when James Woolsey, former DCI, program maintained that the US did not collect or even sort out secret intelligence for the benefit of specific American companies in response to European reports concerning alleged US/British spying on Europe under the Echelon program for industrial espionage purposes. See Woolsey, R. James. "Why We Spy on Our Allies." Wall Street Journal, 17 Mar. 2000.