ACD AMERICAN CENTER for DEMOCRACY ECONOMIC WARFARE INSTITUTE

Economic Warfare Subversions: Anticipating the Threats

A Capitol Hill Briefing

Rachel Ehrenfeld, Ph.D.
Kenneth M. Jensen, Ph.D.
Editors

The American Center for Democracy/Economic Warfare Institute is a New York-based nonprofit organization dedicated to tracking and analyzing economic threats directed against the United States and other Western democracies by state and non-state actors. More information about ACD and EWI may be found at http://www.acdemocracy.org and http://www.econwarfare.org

American Center for Democracy/Economic Warfare Institute
330 W. 56 Street, Suite #24E
New York, NY 10019

POST-EVENT REACTIONS FROM PARTICIPANTS

"Challenging thoughts for challenging times."
— **General Michael Hayden**

“The Economic Warfare Institute recognizes that the key to meeting economic threats is knowing who can afford to—and who will gain by—acting on them.”
— **R. James Woolsey**

"This was a high-level discussion of a high-risk subject. EWI is to be commended for drawing together panelists with experience in intelligence, law and commerce to at least begin the process of informing public discussion of the dangerous prospect of economic warfare."
— **Michael Mukasey**

"Thoughtful people must thank the Economic Warfare Institute for gathering authoritative, creative panelists in a wide range of areas who offer the alarming insights and unsettling questions that can renew our vigilance and protect our freedoms."
— **Daniel Heath**

“You presented a remarkably informed panel—with a remarkably troubling message. We will only be safe if we take seriously and prepare for the risks your speakers identified so ably.”
— **Stewart Baker**

"Economic Warfare is the current generation’s Weapon of Mass Destruction . . . and the Western system of finance and trade is the target."
— **David Hamon**

“The Economic Warfare Institute is today's Paul Revere, sounding an urgent alarm, before attacks on key sectors of the American economy bring modern society to its knees. Just as 19 jihadists armed with box cutters murdered about 3,000 of our fellow citizens, equally determined enemies could cripple the U.S. with dirty money, a few computers and a box of matches.
— **William B. Scott**

Special thanks to Senator Jon Kyl (R-AZ) for his sponsorship of ACD/EWI's Capitol Hill briefing on which the following publication is based.

CONTENTS

EXECUTIVE SUMMARY

On July 9, 2012, the Economic Warfare Institute at the American Center for Democracy held a briefing on Capitol Hill that brought together nine preeminent experts from different sectors on defending the United States from economic threats and attack.

The purpose of the event was not simply to get their perspectives on topics such as financial vulnerabilities, espionage (commercial, security, and political), cyber warfare, transnational crime, and the like. ACD/EWI's goal was to generate ideas regarding future threats, the relationships between threats of various sorts, and review whether policies and actions of government and business are adequate to meet these threats.

Accordingly, the July 9 event was the first in what we hope will be a series of briefings, both for the government and the private sector, carrying the generation of ideas forward.

PRINCIPAL INSIGHTS

The following bullet points identify our insights from the July 9 event. In some cases, the insight derives from a single speaker's remarks. In others, we combined related remarks by a number of speakers.

• Does the economy have a "keeper"—an entity to protect it from attacks? Is this a government responsibility or a private sector one? If both are responsible, why aren't they working together?

• State and non-state actors wishing to harm the U.S. economy are likely to strike when the economy is vulnerable. They have the ability to adjust strategies and tactics to attack the specific vulnerabilities. Policy and regulation as the means to protect the economy at such dangerous times becomes more important, less easy, and subject to the law of unintended consequences.

• The greatest threat to the U.S. economy is posed by wealthy state and non-state actors, particularly those who rule or are manipulated by authoritarian governments. They have both the most to gain and the means to make the greatest and most persistent efforts.

• Serious economic threats are most likely to progress from the exploitation of small vulnerabilities at times when confidence in the economy and our ability to protect it are low. As with the crisis of 2008, which was self-inflicted, the cumulative effects of small disruptions of various sorts can create crises in the public's confidence with mass effect on the economy.

• The money trade amounts to some 8.4 percent of the U.S. economy,

surpassing our trade in other goods. This renders the financial sector substantially more vulnerable than ever before. Given exponential increase in the electronic management of the money trade, we face vulnerabilities and potential mass effects that neither government nor the private sector could have imagined just a short time ago. Accordingly, policy, regulation, and practice related to protecting the financial sector are far behind the vulnerability curve.

• It is worthwhile to compare the terrorist attack of 9/11 and the financial crisis of 2008. One was kinetic and created by outside forces; the other was self-inflicted. However, both aimed to undermine the confidence in the U.S. economy. The September 11 attack intended to shake the world's confidence in our economic system. To al-Qaeda's chagrin it created no crisis in confidence because our response showed national resilience. The 2008 crisis, however, created a crisis in confidence from which our economy did not recover. Although that crisis is considered to be self-inflicted, there is no evidence to exclude the possibility that the crisis had been caused by an economic attack from the outside. Confidence has not been restored four years later. Indeed, we have yet to understand exactly what happened in 2008, let alone taken action to prevent its reoccurrence.

• Potential economic threats are diverse. Anticipating them begins with the recognition of vulnerabilities. Vulnerabilities must not be conceived simply as weaknesses in financial systems and physical infrastructures. A good example of a vulnerability we haven't recognized, but al-Qaeda has (proof of the same is in the Osama documents), is the susceptibility of America's West to wild land arson. While the catastrophic effect on life and property may be limited to the targeted areas, the economic cost to the state and sometimes to the whole nation could be enormous.

• Transnational organized crime, terrorism, and insurgency have moved into tight lock step with one another, both in terms of funding and action. This, in its turn, has vastly increased the corruption of foreign government officials and could effectively cause whole countries to fail, as in the case of Lebanon. The linchpin that holds this insidious three-way partnership together is drug trade and trafficking.

• In the cyber-realm, nation-states present the greatest threat to the U.S. economy, with criminals (increasingly in league with terrorists) close behind. Nation-states may consider themselves constrained by their very status internationally. Criminals, for their part, are parasites that do not really want to destroy the economies they're stealing from. Private individuals and groups wishing to disrupt the economy for political or social purposes could be intrinsically the most dangerous. Their capabilities grow as the digital world develops.

• Cyber-espionage threatens not only American businesses and commerce. It can be used to produce information useful in influencing elections and legislation.

• Protecting computers and computer networks against cyber intrusion does not work. *The only defense is cyber offense.* Intruders must themselves be intruded upon. And the beneficiaries of the intrusions, whether foreign businesses or governments, must be sanctioned. Tracing cyber intrusions is difficult, but possible with a large concerted effort. If the U.S. private sector is the principal victim of cyber-espionage, its resources and talents need to be harnessed to go on the offense. However, only government intelligence agencies can legally "hack." There needs to be a partnership between government and the private sector, as government has the authority and the private sector the means.

• Whatever is claimed regarding increased government agency cooperation in dealing with economic threats is hyperbole. There is no ultimate authority that thinks in terms of economic threats and works on the synergies among them, coordinating the host of official agencies accordingly. U.S. offices that deal with threats continue to regard their work as limited and proscribed. And, in the current budget climate, there is less flexibility to adapt to developments and only small capacity to deal with new threats. These facts not only reflect circumstances of bureaucratic history but also the lack of understanding as to the limitations of our means to deal with threats that come from old thinking in the policy, regulatory, and legal areas.

• In dealing with new economic threats and circumstances, the law has a strong tendency to get in the way. This is not to disparage the law but, rather, to recognize that new circumstances beg some jettisoning of old principles and the creation of new ones. For example, the legal lines traditionally drawn between what government and the private sector can and cannot do are put under stress by cyber threats and approaches to meeting them. Another example is afforded by the role of an entity like the inter-governmental Committee on Foreign Investments in the United States. It deals almost exclusively with screening foreign defense contractors and passes on foreign acquisitions in which the government has a bona fide interest. It cannot, and does not, screen investments for the private sector. Greater transparency regarding foreign private sector investors should be pursued, but currently it is not perceived as a government problem.

• Economic warfare is a form of aggression, whether it is pursued by state or non-state actors. However, "aggression" and the "right of self-defense" as concepts enshrined in international law (e.g., in the UN Charter) are of little use when it comes to countering economic threats. The problem is that there is not now, nor has there ever been, any clarity in international law as to what aggression is. We do, however, know it when we see it and react as we reasonably, carefully, cautiously, and prudentially can. Because of this, the law needs to get out of the way for the time being and, thereafter, learn from the actions taken.

INTRODUCTION AND CUTTING-EDGE THREATS

Rachel Ehrenfeld, Ph.D., Director of the American Center for Democracy and the Economic Warfare Institute

Event Introduction

Following the trail of money that fuels terrorism and pays for the corruption of government officials over the past two decades was useful to better understand the assorted threats of economic warfare. My book, *Funding Evil - How Terrorism is Financed and How to Stop It,* caused me to look closer into one form of economic warfare that also assaulted Americans' First Amendment rights. This led to me to initiate a new law, which was unanimously passed by Congress in 2010. As a result, American journalists, authors and publishers are protected by

the SPEECH Act from the enforcement of foreign libel judgment in the United States.

This briefing is the first in, we hope, many briefings on the different aspects of economic warfare and their interaction**.** It is fitting that this briefing provides an initial overview of conceivable economic warfare attacks, and their potential impacts on key elements of the American economy.

EWI is of the strong opinion that threats to the U.S. economy are the next great field of battle. Indeed, we are already at economic war with such state actors as China and Iran and such non-state actors as al-Qaeda and its affiliates. The future battlefield is vast: it not only includes the realms of cyber and space but also of banking and finance, market and currency manipulation, energy, and drug trafficking. The list could go on and on.

EWI believes that this vast potential field of battle, while widely worried and written about, has not been understood as a whole. And we are concerned that, if we continue as we have been, we will not be able to recognize the interrelations between its many parts. Moreover, although we are not privy to what the government does, we feel that insufficient attention has been paid to anticipating potential vulnerabilities and taking preventive action.

Our purpose today is to go out to the cutting edge of the threats we face and to begin a dialogue on how to address them in a sophisticated and methodical fashion.

Cutting-Edge Threats

Opacity and greed combine to threaten the security of the U.S. financial markets, compromising the stability of our economy and national security.

Take the May 6th, 2010, U.S. stock market plunge of about 1000 points (9 percent), recovering most of those losses in minutes. Still, two years later, the joint report by the SEC and the Commodity Futures Trading Committee (CFTC) did not rule out "terrorism" as a possible cause for the May 2010 “flash crash,” and the entire financial industry still has no uniform explanation of why or how this event occurred. There is, however, general agreement that the current market structure based on high-speed trading, dark pools and fragmentation of exchanges—some 13 stock exchanges and 50 “dark pools”—has been the enabler.

The new market system is highly electronic (facilitating high-frequency trading), is opaque, and the security protocols are deficient (they do not register the origin, only the final destination of trades). It is unregulated and misunderstood. This makes the current market structure vulnerable to attacks. The "flash crash" of 2010 is evidence of this vulnerability. Some theorize that activities in the futures

market used by HFT, trying to hedge their trading, crossed over from one asset class to another triggering the “flash crash.” While the industry does not want another "flash crash," it still has not provided a conclusive answer regarding how it happened.

Direct Market Access (DMA)—a term used to describe electronic trading facilities that give investors wishing to trade in financial instruments a way to interact with the order book of an exchange—plays a key role in accessing market threats. Today, DMA is often combined with proprietary algorithmic trading strategies. Aggravating the situation are dark pools. Approved by the SEC in July, the NYSE operates a new dark pool order system. Knight Capital, the biggest trader in U.S. equities on the NYSE and NASDAQ (and one of the largest dark pool operators), was quick to get on board and into trouble using the new dark route. On August 1, Knight reportedly executed over $7 billion in erroneous trades in less than an hour as the result of software glitch. The algorithmic error led to Knight losing almost 85 percent of its market capitalization, ultimately leading to a bailout by institutional investors—including a private equity firm behind the high-frequency-trading behemoth. It took about $400 million to save Knight from bankruptcy.

The Securities and Exchange Commission (SEC) finally issued Rule 613, Consolidated Audit Trail (CAT), an audit system that will apply to mostly secondary market transactions in the NASDAQ National Market. CAT will capture all orders, including those made for customers or for the taxer's own account. It will cover stocks listed on the exchange, but not over-the-counter options, futures, bonds, etc.

CAT audit will take place a day after the trading took place. This decision was made apparently because the cost of auditing the whole market—more than $4 billion—is considered too high. While this is a positive beginning, it’s too limited, too little, and too late.

Adding to the market vulnerability are the large number of the leading high-frequency programmers who reside in countries such as Ukraine, Romania, India, and the Philippines, and are not scrutinized in proper background checks. This opens the door for cyber threats from DMA clients and even by possible “sleepers” residing at member or brokerage firms.

A new rule designed to impact one aspect of dark pools, the "trade at rule," has been kicked around for the last two years. It would require dark pool participants to place real orders into the pool before they trade, providing more transparency to the market. But this attempt to prevent dark pool operators from picking their prey—like a sniper—milliseconds before the trading closes faces the objection of the HFT crowd.

Unfortunately, the greed of the HFT crowd seems to have eroded investors' confidence, hurting capital formation and job creation. This atmosphere of greed

also makes us more vulnerable to a “flash crash” that could devastate the market.

These and other vulnerabilities of our financial markets are known to those aiming to sabotage them. HFT would facilitate swift attacks to erode confidence in the stability of the U.S. economy. The stagnating economy and the uncertainty of the presidential elections could create a perfect opportunity for just such an attack. Accordingly, early identification of financial threats is the focus of the EWI work. We also work with various customers, organizing both Table Top Exercises and the development of decision aids.

[From prepared remarks and later additions.]

FUTURE ECONOMIC THREATS

David Hamon, Distinguished Analyst, Analytic Services (ANSER), former Director for Strategic Research and Dialogues, Defense Threat Reduction Agency (DTRA)

These thoughts are my own and they don't reflect my company or any of our clients.

About seven years ago, while I was director of research for the advanced systems and concepts office, which was set up by John Hamre in 1998 at DTRA to be an in-house think tank, I initiated a research inquiry to look at what the next generation of weapons of mass destruction—weapons of mass effect—would be. It resulted in several spin-off inquiries and was quite an interesting little exercise. The best part of it was I wasn't responsible for implementing any of it, just capturing the thoughts and sending them down the stream.

It's important to note the distinction between WMD and WME. WMD is thought of as traditional nuclear, biological, chemical, radiological and high explosive threats; whereas weapons of mass effect are a little more social science squishy-like, which [is why] we used to keep the definition that they were non-traditional weapons, including weapons inducing mass terror designed to attack some aspect of society.

One study in particular I oversaw (which I enjoyed and really piqued my interest and which I've been trying to follow these last few years when I've had the opportunity) was the question, at what point do terrorist organizations (as we

knew them then, as we know them now—they and their state sponsors, that is) might evolve from creating kinetic kill terrorist actions to attacking the Western economic system. Is it possible that warfare in the future may involve actions either taken by state adversaries or non-state adversaries specifically designed activities to damage the U.S. economy and economic system?

Our thinking back then in my little group (and in those we used to do some of this research for) didn't evolve enough to take into account the generational changes in offensive cyber and other induced systemic attacks. If anything, as we shall see today, from the panel that you are going to hear, this aspect of the problem has gotten much worse. For example, if stealth viruses can be used to attack military systems— defense systems—with the purpose to create physical destruction or to cripple capability—then imagine what could be done if these same viruses were turned onto the economic and financial systems. So since I have but a short time for this presentation, let me list several observations and make some points on the future threat environment.

First, the observations. I'm going to use the acronyms EW and ET in the interests of time to stand for economic warfare and economic terrorism.

So, first observation. The experts we consulted back in 2005, when we had a small get-together on the subject of economic terrorism, were completely unable to come to a consensus on what the possible future nature of the threat was and whether or not the threat was real. However a clear and present danger the threat may have been judged, the experts we assembled were, in fact, divided. The government experts and the terrorist experts—those who do terrorist research (we all know who they are, so let's not go into it)—doubted that terrorist organizations had the ability and sophistication to evolve toward economic terrorism as a weapon of choice, certainly not in one generation.

However, interestingly enough, the private sector folks—and these people were spread across a number of different industries—felt not only that they were vulnerable then, in 2005, but felt strongly enough about the subject to freely discuss their concerns in this "Chatham House Rules environment/conference" site set-up. Unfortunately, we didn't discuss progress/conduct on the research of state-sponsored economic warfare simply because it was a little bit beyond the scope of that meeting. I hope we'll get into that today in more detail.

Next observation. The insurance industry experts, especially the risk-analyst community for the re-insurance industry felt that, in addition to more 911 incidents, mass panic-induced psychological terror would not only strain their resources to the breaking point: it was something they were betting on—predicting would happen—back in 2005. In fact, mass-terror-induced economic attacks were decided by this group of people (people that look at risk for these companies and decide how much insurance they should have on their own) to be the biggest threat they faced in the future. I would define this as attacks designed

to drive human behavior in a massive way, having a cascading effect and ending up doing some kind of harm to the economic system.

Third observation. Agricultural industries were especially believed to be vulnerable, ranging from disease induced into food production to attacks on the supply chain.

Fourth observation. The United States, because it is so big, represents a target-rich environment across the whole front for either ET or EW. Public reaction is the key. Bolt-out-of-the-blue attacks would likely have a cascading effect and be difficult for the government to manage. Predicting these kinds of attacks would be impossible.

It was generally believed that to be successful, a campaign of tactical maneuvers or smaller attacks would be needed because the economy was believed to be too resilient. So the question here would be (again, this is 2005) was would you be able to determine if these events—these pinprick attacks—were anomalies or actual attacks.

On the open source side, that is, the unclassified side of gathering information, economic jihad is possible, even likely. Because it hasn't occurred in the intervening years doesn't mean it's not going to happen. I would say, based on what we can read in the open sources, just give it time. Jihadi literature contains many references to attacking economic systems—and symbols. I think Rachel [Ehrenfeld] has written much about that subject.

And lastly, the big observation that should be a take-away from this get-together is that preparing countermeasures is extremely difficult. More on that below.

Now a few points on the future threat environment: first and foremost, on how to identify targets. The most important part of this, in my estimation, is (unless there is a serious and immediate public-private partnership created to work on this problem) that we have virtually no way of knowing if what we see coming at us is an attack or is criminal activity of some variety: i.e., a hacker or group of hackers that is in it for fun-seeking thrills; an anarchistic event, for the purpose of creating anarchy in a system they are opposed to; or some sort of cascading technological failure.

Essentially—unlike the sort of clear mission space we are all used to working in the Defense Department and from my military background—the big question is, who owns the economy? Who is the keeper of the economy in the first place? If some entity attacks the private international financial systems, for example, is this a national security threat? Or is that their problem? The economy is more than a tax-collecting entity to fund government, or an engine to promote growth, or a source of jobs and wealth. Put another way: if government believes it may be vulnerable to attack, government should take the necessary steps to protect it.

And further on this topic, what's the role of the public? Should they be informed? Should they be educated on the threat? And how does government provide the resiliency "blanket" that we all seem to need? It's the same thing we all talked about back at 9/11 with the kinetic destruction of infrastructure. My thinking here is that the government did a pretty good job of educating the American public in the 1950s about nuclear weapon strikes in the United States and the need to be prepared. Some of that could be useful today.

Second, EW/ET attacks that are kinetic cannot be ruled out, even in a digital age. The research points to four types of future attacks: traditional kinetic, innovative use of cyber or spoofing, traditional WMD, and long campaigns combining multiple attacks at narrow targets to prolong economic damage.

Third, in an age of cyber, about which we are going to hear from others, there are many ways to damage/attack economic/financial systems for kinetic effect: ways to destroy digital systems, to deliberately steal or divert economic assets, to spoof or obfuscate in a manner than creates panic, [erodes] confidence in institutions, governments and security organizations, and masks real intent. The entire domain of cyber used in this manner as a weapon of EW/ET is not well understood as a threat, especially in the economic domain. This also includes disinformation campaigns as well.

Fourth, it's not very clear, even if an attack is labeled as a bona fide attack, what's to be done about it. What are the motivations and intent of such an attack? Is it an act of war that draws a military response? What exactly is the role of the defense and military forces of this country, for example, in an economic warfare or economic terror campaign? Do we think differently about this if the source of the threat comes from a state or states, either wittingly or unwittingly helping non-state groups, or in a deliberate campaign designed to undermine our economy? Are we certain that the government of the state is behind it or are these bad actors? Does cyber-space behavior that includes attacks on economic systems merit some kind of an arms control approach to manage the cyber common spaces: will that work? And lastly, on that question, are these attacks deterrable? If so, can we reach back into classic deterrence theory and use as a way of designing countermeasures?

Fifth, speaking of countermeasures, work must begin now on a suite of countermeasures that take into account a wide variety of proportional responses and system resiliency. These countermeasures need to be exercised at the interagency level and with our friends from the private sector in order to be effective. This is one of those learn-as-you-go tasks. We need to do it over and over again so that we understand what we are facing.

Sixth, I would not rule out in the future attacks on the agricultural production in some form, although interestingly enough, my analysis has led me to conclude

that the movement to buy organic, buy local, buy from small farms, at least in this country, may have mitigated some of the food-chain vulnerability issues. There are still many threats related to food and animal production, especially from overseas, as well as to distribution.

Finally, my last point. One of the most important aspects of the threat space is the existing environment, the one we all live in now.

If the economy is perceived—either here in this country or across the Atlantic and across the Pacific to our friends in Japan and other big economies of the G20 states—if these economies are perceived as suffering from a number of failures of various kinds (obviously you know what comes to mind here—the European Union) and may be exacerbated by poor leadership of these countries, then this preexisting damage and weakness will be a part of the attackers' calculus.

[Edited from transcript.]

CYBER NIGHTMARE: THE WORST WEAPONS WITH THE WORST ACTORS. HOW MUCH SHOULD WE FEAR 'HACKTIVISTS' ACHIEVING STATE-LIKE CAPABILITIES?

General Michael Hayden, principal, Chertoff Group, and former director, CIA and NSA

Good afternoon, and thanks for the opportunity to come and share a few thoughts. When I looked at the batting order we had here this afternoon, I knew we were going to get very detailed, great expertise on an awful lot of threats. And so I decided I didn't want to compete with that, and that I was going to take the option of stepping back a little bit, and try to project a bit into the future and to

suggest that this could actually get a lot worse if we are not careful. My title [has to do with] the most dangerous tools in the most dangerous hands.

Now you'll hear me echo a few things that have been said already, and I think I'm going to foreshadow some of the things that will follow me: but hear me out.

I come to you as an American GI, 39 years in the Department of Defense, and I think most of you who follow this understand that in our Department of Defense, we look upon the cyber thing as a domain. We do land, sea, air, space, cyber. It's a place where you want us to go to defend you. It's a place we will go to conduct operations. But like those other domains—land, sea, air, space—[cyber] has its own peculiar characteristics: inherently strategic, inherently global, characterized by great speed, characterized by great maneuverability, and, because of its inherent characteristics, for me, as a military man, practically every advantage goes to the attacker, just by the nature of the domain in which we are operating. And yet, you and I, and I include myself in that, attracted by the convenience, speed, ubiquity, of this thing have decided to put stuff that you and I formerly kept in a safe or in a wallet, out there into this domain, which I've already told you is very, very hard to defend. The line I jotted down was "such a combination of insecurity and indispensability we have probably not seen before. "

Now when I talk about things going on in this domain I usually divide them into sins and sinners. So let me run through my catalog of sins. These will be touched on later by some of the other speakers.

The first is just stealing your stuff. What we would technically call computer network exploitation. Espionage, okay? It's [been] an international activity for centuries, just made far more enabled by the nature of the cyber domain.

And then there's computer network attack for cyber effect. Estonia 2007: patriotic Russian hackers collapsing the Estonian Internet system. Apparently, those same patriots did the same thing to Georgia in August of 2008, collapsing the Georgian Internet system. Cyber for cyber effect. Not just stealing your stuff, but causing damage.

Then finally, one classic example out there now is Stuxnet, which, whoever conducted the attack, did something that's never done before—using a weapon comprised of ones and zeroes to actually create physical destruction in one of those other domains. So I feel like a line in that old cop show—Hill Street Blues—"Gotta be careful out there." Well, there are a lot of dangers out there, from stealing your stuff, to affecting your network, and now to creating physical destruction.

Those are the sins. Who are the sinners? And here's where I really want to emphasize the point I'm trying to bring. Let me do this from most to least capable.

I think the most capable by far are nation states. They know what they are doing. By and large the nation states are out there for the intelligence value, nation states are out there doing what we call CNE—computer network exploitation—the cyber-espionage thing. It's not that nation states don't think about doing some other stuff. Recall the press accounts before the NATO military action in Libya? Where there appears to have been speculation about whether we wanted to physically destroy the Libyan air defense system or simply to use a cyber attack to disable it? All right?

So, state actors are out there. Now look: I know state actors can be very destructive, and I'm creative enough to doodle on the back of an envelope [and] think of a state actor or two—Iran, North Korea—that could act incredibly irresponsibly almost without limit in the cyber domain if they perceive themselves to be provoked in a certain way.

But frankly, even though deterrence doesn't work as well in the cyber place as it does in the others, I think absent total war there are rough limits on state activity in the cyber domain. Bad, capable. But there are consequences, and that might limit what they could do. Remember: dangerous tools in most dangerous hands.

The second category is criminals. They do it for profit. They are stealing not your data, but your money. They are stealing your wealth. Frankly, they've got a symbiotic relationship with their victims. It's rare in nature where a parasite decides to destroy its host. And so, although criminals are bad, and we are suffering greatly from them, I don't think criminals go out there to destroy the American banking system. They are living off of it. They are profiting from its continued existence.

Which now brings me to, I think, the most dangerous hands. And that's that third group that David Hamon already suggested. It's really hard to label them. They could be terrorists, they could be hackers, they could be activists, they could be anarchists. But they are all living off of the peculiar empowerment that this new cyber thing is giving to individuals. And currently—frankly—they are the least capable in this taxonomy. I don't mean to offend them—I really don't, because want to be able to use my computer tonight. An awful lot of what they do, and get the headlines for in the physical domain, we'd call cyber graffiti, or a cyber picket line.

But as all of these actors act, as the world becomes more sophisticated with these tools, the water level for all three of these groups gets higher in the harbor. All boats begin to rise. And so my nightmare scenario is that this third group, currently least capable but also least responsible, least limited, least influenced by consequences—over a period of time, not measured in months but not measured in decades, either—begin to acquire the skills and the tools we currently associate with nation states.

I leave it to your imagination as to what would trigger this third group so empowered to do things without limits, to do things catastrophic, to begin to [cause] the walls to start tumbling down. It all suggests to me that there is much, much work to be done to make the cyber domain, so indispensable and so insecure, perhaps a bit more secure, before these two trend lines meet. Again, the most dangerous tools merging with the most dangerous hands.

[Edited from transcript.]

THE IMPACT OF OIL ON ECONOMIC WARFARE

R. James Woolsey, Chairman, Foundation for the Defense of Democracies, former director, CIA, and member, ACD/EWI Board of Directors.

Some forty years ago there was a burglary in Washington, over at the Watergate, and it gave rise, among many other things, to the best advice I know of, ever, with respect to understanding wrongdoing; and that is Deep Throat's famous line, "Follow the money." In order to understand why the bad guys have the money, to run their dark pools and their naked short selling, and their economic jihad and all the rest, we need to understand why it is they are so rich. And the reason they are rich is oil, almost entirely oil. Oil dominates—monopolizes—world

transportation. Only about 5 percent of world transportation is not on some oil fuel. A few trolleys, Olympic rowing crews, fox hunts, and that's about it, don't run on oil. Everything else essentially does. And over three quarters of the world's oil, 78 percent to be exact, of the conventional reserves, reserves of conventional oil, are in the hands of OPEC: a cartel, a conspiracy in restraint of trade, of twelve countries, eight in the Middle East, two in sub-Saharan Africa, two in South America.

Regarding that cartel, should anyone need any proof that it is a cartel, that it is a conspiracy in restraint of free trade, a couple of quick facts:

In 1972, the time of Watergate, forty years ago, on the eve of the Yom Kippur War, OPEC was pumping about 31 million barrels of oil a day. The world has gone through a lot of halting but nonetheless real economic growth over the course of the last forty years and today's world wide GDP is around double, some would say close to three times, but let's be conservative, around double, what it was forty years ago. OPEC is still pumping 31 million barrels of oil a day. They pumped less in many of the intervening years, because being a cartel, they drop production when they want to get the price up, but 31 million barrels is what they want to pump, and that's what they are pumping. Now, if you have an organization that controls three-quarters, or more than three-quarters, of a vital substance, and it sells on the market every day a little less than one-third of that vital substance and if it's pumping 31 million barrels a day, same as it was when the world's economies and GDP and oil demand were about half what they are now, there's really no other conclusion you can draw that it is a conspiracy in restraint of trade.

Now this is not new. That phrase comes from the antitrust laws, which were, of course, Teddy Roosevelt's response to an earlier conspirator in restraint of trade named John D. Rockefeller, a most admirable man in some ways; but, there is no doubt, Standard Oil was a cartel, a massive one. Roosevelt broke it in his own way by moving the world oil market and the American oil market in particular toward competition. Oil today, for all practical purposes—either its monopoly of transportation or OPEC's dominance of the trade—does not have competition.

We need to understand what that means. Among the things it means is that almost all of the oil states are dictatorships or autocratic kingdoms. Why is that so? Twenty-two countries in the world have 60 percent or more of their national incomes come from oil and gas. All twenty-two are in Freedom House's category of not free. They are all dictatorships or autocratic kingdoms. There are exactly nine of the ten largest exporting countries of oil that are dictatorships or autocratic kingdoms. Only nice Norway is out of place in there, in the top ten. Canada is eleventh. So nine of ten, or nine of eleven, are dictatorships or autocratic kingdoms.

What is going on? Paul Collier, professor at St. Anthony's College, Oxford, head

of the African Economics Institute, is the originator, I believe, of the phrase, “the oil curse.” As Collier points out, it is not just oil where this occurs, it’s with any commodity which is absolutely essential to some key operation in the world and which a country comes into a massive amount of, by discovering it, by war, one way or another. It has happened with salt frequently in human history.

What happens? If there is a huge amount of economic rent in that commodity—that is income well over and above what would be a reasonable return on capital and labor—when that rent comes into an autocratic, totalitarian structure, it goes to the elites. They get richer, they get more powerful.

What happens if oil, if a lot of oil, is discovered by Canada or Norway? Not much. Nice democracies with free economies, they just get richer, like Alaska. But they don’t become dictatorships. But the ones that already are, the autocracy is added

to.

So we have a situation in which we are indirectly, by our oil thirst, promoting dictatorship and autocracy and its embedding around the world, and we are doing one or two other things as well. We borrow approximately one billion dollars a day; the United States does, to import oil. That means that we are paying a tax of something in the neighborhood of four thousand dollars per year per American family, and that tax does not go to Washington to pay the Marine Corps, or to Annapolis to pay for roads in Maryland. That tax goes in the pockets of Venezuela, Iran, Saudi Arabia, etc.

Does it matter that we are getting away from buying oil from some of these places and [that] we buy most of our oil from Canada? A little bit. Helps Canada's balance of payments, that's a good thing for a nice country. But there's one worldwide oil market, so basically if we buy more from Canada and less from Saudi Arabia, somebody is going to buy more from Saudi Arabia and less from Canada. So we are not solving the problem by buying just more oil from some different place. Oil over the long run is fungible. There are some differences, in trade patterns and refinery types and sulfur content and such; but generally speaking, we are not doing anything that useful. And with respect to [shifting] buying from one country to another to buying from American producers—"drill, baby, drill"—that's good from the point of view of our balance of payments. It would be great if we only had to borrow 900 million dollars a day instead of a billion dollars a day.

But that's all we are accomplishing by drilling domestically in oil, as long as oil dominates world transportation and as long as OPEC is the conspiracy in restraint of trade that controls the oil market. And as long as oil has a huge amount of economic rent attached to it, we, under our current knuckling-under to it, our lack of willingness to have other ways to drive compete with it, the rigidity that [characterizes] our cars (we're not addicted to oil, but our cars are, they can't drive on anything except petroleum products)—as long as we let that happen, we will continue to boost the content of the coffers of the Saudi Arabias, the Irans, and others, who are the source of the dark pools and the naked short selling and all the rest. We will not solve our economic warfare problems, cyber or otherwise, until we destroy—not modify—destroy oil's monopoly over transportation and OPEC's control of the oil market.

[Edited from transcript.]

FINANCIAL WARFARE: POLICY, PRACTICE AND VULNERABILITIES IN U.S. FINANCE

Daniel Heath, Managing Director for North America, Maxwell Stamp PLC, and former U.S. Executive Director Alternate, IMF

Opportunities for financial warfare in the United States are growing.

Serious threats are likely to result from the exploitation of small vulnerabilities at times when confidence in the economy and our ability to protect it are low. As with the financial crisis of 2008, which was self-inflicted, the effects of small disruptions of various sorts cascade and coalesce and can produce crises in confidence with mass effect. Potential threats are diverse. Anticipating them

begins with the recognition and acknowledgement of vulnerabilities.

Financial attack is very different from conventional economic warfare activities, ranging from overt actions like trade embargos to covert techniques like counterfeiting the enemy's currency. Finance, especially current sophisticated financial systems in high-income countries, is inherently susceptible to cyber attack. The public no longer is shocked by a flash crash, or the $75 billion recently that disappeared from bank accounts. Just as many low-income countries avoided direct harm from the 2008 financial markets turmoil because they were bypassed by global finance, so conversely has the pursuit of global financial efficiencies engendered this category of specialized vulnerability. Given exponential increases in the electronic management of a vastly larger financial industry, we face vulnerabilities and potential impacts that neither government nor the private sector imagined just a short time ago. Accordingly, policy, regulation, and practice related to protecting the financial sector and mitigating future threats are far behind the cyber vulnerability curve. Cyber security and counter-terrorism is a vital national priority.

A less dramatic but no less serious perspective on financial warfare involves commonplace materials, the vulnerabilities that arise from familiar products, conditions, and routine events. These are the threats hiding in plain sight, the "weaponizing" or leveraging of the ordinary under the right circumstances.

Consider a speculation to engage our economic imaginations on financial system security:

In mid-2014 Chinese creditors announce the exchange of $2 trillion in U.S. Treasury and agency debt for exclusive food production rights in California and mineral rights in Alaska for 100 years. As the implications settle in, a significant capital outflow trend from the U.S. takes hold. Later that year, in the holiday week between Christmas and New Year's Day, a massive storm hits the East Coast. Electricity is gone, as recently in Washington. Minor but incapacitating sabotage occurs on subway systems and on other limping transport infrastructure. Most government and commercial activity ceases. Then, odd killings occur, appearing to be random, like the 2001 sniper attack in Washington's suburbs. But some are clearly assassinations of high-value targets, including the heads of two large Wall Street firms, prominent traders, and officials of the New York Fed. While security forces scramble in a state of emergency, minor biochemical attacks on East coast water supplies occur. Like the 2001 anthrax attack in Washington, direct physical damage is minimal but trust in city services is shattered. Emergency ad hoc work arrangements are found to deliver incomplete information for markets, and the financial system "browns out" then freezes. Panic spreads beyond the East coast as employers across the United States ration cash.

Such a fantasy scenario is realistic and not unthinkable. In fact, the elements are all familiar, to the point of cliché. We can adjust or substitute elements since

there are plenty to use. The scenario does not involve cyber attack. It waits for the U.S. finance target to appear in its sights, rather than attack at an ineffective time. Most importantly, such low-level attacks using the ordinary cause panic and a cumulative loss of confidence in the future, which can be devastating for the functioning of current sophisticated financial systems in complex economies.

Consider another scenario involving finance alone. A Pentagon-funded report released last year speculated that unidentified parties manipulated the price of oil to rise from 2007 as the U.S. housing market collapsed, followed by a series of systemic bear raids prominently on Bear Stearns and then Lehman using CDS and dark pool shorting, leading to the massive U.S. debt spiral, which depletes Federal borrowing capacity before the real financial attack occurs—in a few months. Ultimately the renminbi ends up as the world's reserve currency, a process supported by currency reforms underway and IMF discussions.

Again, many consider such a scenario to be within the realm of possibility. And again, the target is U.S. finance.

The U.S. financial sector has become an obvious prize and target for attack. It has a larger place in the U.S. economy than ever before---at 8.5 percent of GDP in 2010, up from 2.8 percent in 1950.

Finance is now a direct and major source of GDP rather than just a facilitator of growth, which is its traditional function, by efficient allocation of resources. U.S. money trade has surpassed real trade in goods and merchandise. But while the sector is large, deep and innovative, it also is concentrated, its practices obscure and cyber-dependent. Moreover, the United States has enabled dependency of the real economy, the manufacturing economy, on finance. In 2008 Fed Chair Bernanke with Treasury Secretary Paulson warned Congress "we may not have an economy on Monday," because corporate finance markets froze when counterparty risks became opaque and trust vanished. The two finance officials traditionally tasked with stabilizing markets expressed the panic of the world's premier financial system apparently on the verge of collapse. The ascendant financial sector, with its inherent and created vulnerabilities, is inevitably a prize for terrorists.

The finance sector target is central to the two disaster events associated with Wall Street—September 11 and the 2008 financial meltdown with which we are still contending. It is instructive for financial warfare analysis to compare the two.

September 11 was a traditional guerrilla attack by an external enemy that had a single non-discretionary target in the sense that there is little way to reduce the attractiveness of the World Trade Center except to prohibit tall buildings. The event was intelligible to the public: it was made possible because fairly simple procedures failed. The Wall Street target was attractive for its symbolic value worldwide and its kinetic purpose, both widely acknowledged. But the attempt at

real impact on the U.S. economy failed. There was little damage to U.S. confidence: in fact, national resilience surged after 9/11.

The 2008 meltdown, by contrast, originated in an internally generated, or self-inflicted, event, systemic practices and conditions. Flawed procedures and regulatory failure enabled it, along with complex products, risks not understood even by professionals. The financial crisis remains mysterious to most Americans, with obscure origins and confusing results—the U.S. Financial Crisis Inquiry Commission generated competing accounts—but the bulk of the blame rests on the domestic finance sector. In fact, it was an aggregation of discretionary problems, little issues, little reasons, little regulations. The target was central to the U.S. economy and had a huge impact on the real economy, in no small part through great damage to business confidence. Economists are developing new appreciation for the role of confidence about the future in determining the success of economic policies, whether austerity or deficit spending. If trust in institutions is weak, as it could be after an orchestrated attack, the economy will be at risk. The 2008 meltdown was more significant to the economy, and led to wider, longer damage.

In short, while both Wall Street disasters involved familiar things that were used to hurt the United States, and might have been prevented, 9/11 was clearly a terrorist act, but the consequential financial meltdown carries greater discretion over its circumstances. That implies more responsibility and scope for preparedness, starting with more exacting knowledge of what happened in 2008 so we can take the proper action to prevent its recurrence.

What if terrorists aim to engineer a renewed financial meltdown? Is it possible? How would the financial system handle a massive attack on New York City? Is enough being done to buttress financial resilience—to limit the contagion of cascading failures throughout the economy? In what ways could different kinds of

terrorist attacks succeed in destabilizing our financial sector and impair the real economy?

One helpful approach to evaluating this prospect is informed by our comparison of the two Wall Street events. There is a natural taxonomy, that of financial *vulnerabilities* grouped by their degree of discretion. These range from the *macro-financial policy* (e.g., U.S. public external debt; sector size and concentration; capital flows) through *finance industry products and practices* (e.g., naked short selling, CDS, dark pools, derivatives, and the like) to *guerrilla action* against finance sector targets (e.g., arson, cyber). In macro-financial policy much can be done to reduce opportunities for people intent on harming the U.S. financial system. Guerrilla-targeting shows more need for traditional security interventions than fields for discretionary action, but here too much more can be done than at present. Our intransigence reflects in part society's inattention to the offensive security dimension of financial systems.

There is also a second taxonomy, that of *mitigations*. These range from *pre-emption* (e.g., reducing foreign indebtedness, restricting vulnerable industry products) through *defense* (e.g., counter-insurgency) to *restoration* (e.g., plans for emergency money supplies). Plotted together, the dual taxonomies form a matrix of data points for analysis and action. The matrix highlights the vulnerabilities most discretionary, that is, about which we can most successfully take action, preferably of the pre-emptive order. It also juxtaposes the vulnerabilities for which pre-emptive action is known and effective, but Plan B defensive action or Plan C restoration action are not developed, with vulnerabilities presenting an opposite action plan menu. There clearly are gaps that warrant further analysis and creative thinking.

Attending to the security dimension of financial policy and systems incidentally can yield secondary benefits that may prove as important as the direct advantages of needed reform. A prime example is "too big to fail." The direct risks to U.S. finance created by a large, concentrated sector dominated by a few huge firms, whatever the alleged productivity gains are well documented by various proposals for decentralization. "Too big to fail" is inconsistent with a competitive sector, one with regular market entrants and departures, births and deaths of firms, without domination by oligopolistic firms requiring occasional public support. Significant segments of the public understanding of "too big to fail" is flawed policy, and their low "systemic" confidence in oligopolistic banks predisposes them to withdraw from the finance system with minimal provocation by a terrorist act. In this way the direct risks of a concentrated financial sector are joined or amplified by an indirectly generated vulnerability through lost confidence in finance and disposition to withdraw from the system. Section 342 of the Dodd-Frank legislation offers one approach to a more inclusive and decentralized finance sector.

The “too big to fail” example illustrates the final and most important category in the taxonomy and matrix, that is, the *synergistic* effect of ordinary or minor vulnerabilities. Public disenchantment over excessive concentration in finance damages creates a “platform” of distrust, so that a minor attack triggers panic and withdrawal from the sector. Synergistic vulnerabilities grow from the accumulative impact of small familiar events, leveraging relatively minor familiar conditions into something significant. It is like the automobile, not invented *de novo,* where several separate individuals integrated technologies that were known for other uses. When they were put together in a novel way, the result was important, transformative and enduring. So too the way in which familiar, unnoticed financial vulnerabilities are combined and sequenced can produce a cumulative impact that damages the U.S. economy.

The matrix’s final category, the synergistic impacts, considers two roles of the sector: first, the financial industry by itself, and second, the use of finance by the real economy. The vulnerabilities attached to these two elicit mitigations of every kind—pre-emptive, defensive, and restorative. They aim to grow a resilient sector, and they reinforce one another. Pre-emption may depend on restorative plans being made known to terrorists—for maximum deterrence—rather than kept secret. The restorative actions, a stress test for financial vulnerability to terrorist attack or emergency liquidity plans for backup sources of money in time of dire cyber attack will give assurance to participants in the finance sector.

The big synergistic impact is on confidence. It is widely known that the financial sector is built on trust. In economics the role of confidence and trust has been underappreciated, though work is increasing in this area. So it is prudent to ask what are the tipping points at which loss of confidence harms the financial system? What are the marginal losses of confidence associated with various vulnerabilities? How large do these attacks on confidence have to be for real impact? And under what kind of economic conditions, political conditions, public debt levels, or biochemical attacks will the financial system seize up worse than it did in the 2008 attack on confidence? What are the “elasticities” for panic—of any origin—to harm U.S. finance?

More study and inventory is needed. Specifying and measuring the risks, and the design of interventions, should be expanded. The lessons for deepening financial markets in emerging market countries, and for industrial policy in developing countries, should be explored in order to make the global economy more resilient. Domestic financial vulnerability is a prism through which to view financial policy and structure and industry practices, and attention to this topic should be expanded.

[Prepared remarks and subsequent author edits.]

STATE-SPONSORED CYBER-ESPIONAGE

Stewart Baker, partner, Steptoe & Johnson LLP, former assistant secretary for policy, Department of Homeland Security, and author of *Skating on Stilts: Why Aren't We Stopping Tomorrow's Terrorism*

I'm going to talk about cyber-espionage. I'm going to talk about three or four topics.

First, how bad it is.
Second, why I think it's going to get much worse.

And third, what we need to do if we are going to stop it or control it—a response that is more serious than we have made to date, without significantly changing current law.

First, how bad is it now? I suspect that everybody here knows how bad it is: there's nothing classified about it. The Dalai Lama network attack is still what's happening to all of us. People get into your network by sending you an email that you want to open, you open the email, your security system has no objection to it, but, in fact, it compromises your network and the attackers upload their software into your network, into your computer. The software turns on your camera, it watches you at your desk, it turns on your mike and listens to you at your desk, it records your every keystroke, so it knows what you're thinking as you formulate the thoughts. It is the full 1984 package. Except you had to buy the equipment. That's bad.

Second, why do I think it's going to get worse? Mainly because the people who are doing this, mostly large nation-states, have used it for just a couple of purposes. They're doing espionage against the U.S. government—obviously we would sort of expect that—and they're doing espionage against a number of companies that have state-sponsored competitors. And mostly what they look for is the low-hanging fruit for intelligence gathering. For example, their principal may say, "If I'm going to be in a negotiation with these guys, can you find out what their negotiating position is, and what their bottom line is?" And that information is routinely extracted from the networks of companies and their corporate advisors such as law firms like mine. The other thing they look for is big secrets—really cool technology that they can steal to give to state-sponsored companies who are building competitive products.

Those are obvious and effective and very dangerous espionage campaigns that are happening right now, but it will get worse. I've spent time in the intelligence community. The more time you spend with a particular intelligence capability, the more the customer comes to understand what that capability is, and the more they can fine-tune what they want the intelligence collectors to get for them.

So they aren't just going to be getting negotiating positions and big technology secrets. In the long run, they will want to know whom your salesmen are calling on next week, and what they think those sales prospects want, and what prices they are going to be offering. That allows the company getting the intelligence to go to each customer, beforehand or after, with a slightly better offer. So that they will systematically hollow out every tactical advantage their competitor has in the market place. That's what's going to happen as state-sponsored enterprises learn to task the state intelligence collectors effectively.

That's bad, but it's going to be worse than that. Rachel [Ehrenfeld] is a perfect sponsor for this concern. Rachel, you [know] that totalitarianism is mostly dead outside of North Korea; instead, we have a whole bunch of authoritarian

governments that have had to work within a kind of quasi-open electoral system in which they don't have total control of the information citizens get. But these governments do have an enormous amount of information about their users—who's on-line, who's doing what—and they've learned to more or less achieve their goals in a context of something that resembles a democratic, open exchange of information.

The tools they've used to work within a veneer of democracy are exactly the tools they will eventually use against real democracies—to change the debates we that have, to punish people who say things they don't like. Today, we actually heard General Hayden say, "You know, I'd like to make sure my computer works tonight. Maybe I shouldn't say this." Now that was mostly a joke, but imagine if we knew for sure that people were listening, and that when we went home tonight we would pay a price for what we said, that our refrigerator had been turned off remotely or our online connection had been broken or our bank account broken into. Dealing out such fine-tuned punishments is increasingly going to be part of the strategy by which other countries seek to control the democracies they are contending with.

And not just that. You know, the last presidential campaign was the first in which it was acknowledged that both campaigns had been compromised by foreign espionage services. As far as we know, all the foreign nations did was watch. But most countries know who they favor in the next election. So what's going to stop [them] from deciding that the candidate it doesn't like simply won't be allowed to have secrets?

I remember Debategate—when it was thought that Jimmy Carter's debate preparation materials had gone to Ronald Regan. It was seen as a disaster for Carter's campaign. Everybody was very upset about it. Imagine that happening on a regular basis because another country wants the other candidate to win that election.

So this will get worse, as foreign countries get better at using cyber-espionage to influence [other] governments. If you're like me, that makes you deeply unhappy—and eager to do something about it.

So what can we do? We know one thing that isn't going to work. Defending our networks is not going to solve our problems. We can defend out networks 'til the cows come home, but as General Hayden said, all the advantages are with the offense. The offense will get in; and if we are counting just on defense, we're toast.

So what do can we do?

I'd like to take a quick detour to talk about psychobiology. Scientists working with MRIs have found a reward center in the human brain that fires when [the] subject punishes others, often at great cost, for violating the subject's sense of justice. The study involves putting the subject in an MRI and giving the subject, say, $200. The researchers then say "We're going to take $100 of your money, match it three for one, and give $400 to another person in the next room. Then we'll ask him to send back to you as much as seems fair to him." Sometimes the guy next door sends back nothing, human nature being what it is. That doesn't fire anyone's reward center. But then the researchers offer another three-for-one deal. For every dollar the subject gives them, they'll take four from the fellow who just stiffed him. As the subject hands over his last one hundred dollars, the grim satisfaction of dealing justice (at great cost to himself) sets the reward center alight. Of course you don't need an MRI to understand this phenomenon, which is often called altruistic punishment. You just need to drive in Washington for two days.

But altruistic punishment is a challenge to people who believe that Darwin was right. How can we have a biological mechanism that encourages us to hurt ourselves just to hurt somebody else, even someone who violated our sense of justice? That does not make evolutionary sense, unless you believe that the human evolutionary advantage, the thing that made us successful was our ability to form groups and enforce the rules of that group, so that we could engage in large-scale social organization. That is, in fact, the best explanation for altruistic punishment. Enforcing social rules is crucial to our evolutionary success—so crucial that it's been built into our brains.

If we turn the Internet into a realm where breaking the rules is not punished, then we're messing with the keys to our evolutionary success. So we have got to find

ways to punish people who violate the rules that we think should be part of our society. But right now, when we try to do that online, the answer we get from the intelligence and law enforcement community is “Whoa, we can’t find them, we don’t know who they are, we can’t attribute this attack.”

What is the solution? I’ve got three.

First, we should stop thinking that attribution is impossible. We know a lot about these guys. We have watched them in our networks. We have learned a lot about them. We’ve found some of the intermediate servers where they are downloading stuff. We know whether they learned their hacking on Linux or Windows, we know whether they are left-handed or right-handed, we know what their tactics are, we know what hours they work (turns out it’s nine to five Beijing time). We know a lot about these guys.

What we haven’t been able to do is actually track them back to their networks, because we don’t actually know enough about the environment in which they are operating. We find clues to who they are but we can’t find them out in the real world.

And so my second suggestion is this. If a country is conducting massive, indiscriminate cyber-espionage against everybody in the United States, it’s time to say, okay, that’s what we are going to do to you, too: your whole country. We want to map your social graph for you, and then we are going to use what we know to find the people who are attacking us. I think this is doable. But we’re not doing it. So that’s one thing we could do—find the collectors.

A third suggestion is to unleash some of the private sector resources that I see in my practice. I advise companies that have been hacked—and three-quarters of the time or more they find out not because they find the hackers in their networks, but because somebody from the U.S. government shows up and says we just found a terabyte of your data halfway across the Pacific. When my clients start looking, they usually find that they’ve been penetrated. Then they spend hundreds of thousands of dollars a month trying to figure out where the attackers are. Finally, they come in one weekend and, in big spasm of activity, they try to stop up every rat hole and throw the attackers off the network, a solution that lasts until some idiot in the organization opens another spearfishing email.

So they face an endless and unproductive effort to defend their way out of this problem. They would be delighted to start tracking back these collectors, to start hacking back into the hackers’ own networks. They would cheerfully spend their money to figure out who’s been stealing their stuff.

Now, the only problem with that approach is that most lawyers think it’s illegal for a private party to break into someone else’s computer, even in pursuit of his own property. It’s not illegal for the U.S. government to do that, at least when they

have probable cause and a warrant. The government does it all the time. But the U.S. government doesn't have the resources to pursue every single act of cyber-espionage against a major U.S. company.

It seems to me that there's a wonderful "peanut butter/chocolate" moment here. The U.S. government has the authority but not the resources; the private sector that's under attack has the resources but not the authority. Why not bring the two together and allow investigations to go forward under U.S. government supervision, but using resources provided by the private sector? That's the third thing we could be doing about cyber-espionage.

Two more and then I'll stop.

We should change our target. We are focused on pursuing the collectors, the guys who are breaking into our systems and taking our stuff. And you know, that's pretty aggravating. But I learned when I was in the intelligence community that stealing secrets is no great shakes unless you have a customer who really wants what you're stealing and will use it effectively.

So who are the consumers at the other end of the massive and indiscriminate attacks we're suffering? In many cases, the customers are going to be state-sponsored competitors of the victims. Nobody else really wants or can use detailed intelligence from a commercial enterprise. So instead of trying to deter the thieves, maybe we should go after the buyers of stolen goods. The intelligence customers may turn out to be easier targets than the intelligence collectors, especially if we can find ways to impose sanctions on the customers.

Now what kind of sanctions can we impose? That's my last point. We've got lots of existing authorities—from trade sanctions to criminal prosecution—to go after commercial enterprises that benefit from corporate espionage. The most likely beneficiaries of cyber-espionage are state-sponsored companies in the same line of business as the victims. Those companies are likely to be easier targets for sophisticated computer investigations than the spies who actually steal the data. And they're easier to punish, too. The state-sponsored enterprises that are using stolen information often have to use it outside of their home country. They can't compete unless they compete globally, which means that they will be subject to the legal regimes of other countries. For the cyberspies, a foreign criminal indictment may just limit where they can vacation. For their corporate customers, it's a potential death sentence.

So there are several very real—and very aggressive—things we could do tomorrow to punish those who use cyber-espionage against the United States.

All we need is the determination to attack the problem in new and aggressive ways.

[Edited from transcript with author additions.]

FIRE WARS

William B. Scott, former editor, *Aviation Week*, former official, National Security Agency, and author of *Space Wars*

Perhaps the most simple form of Economic Warfare is wild land arson—setting fires in U.S. forests and grasslands. For terrorists determined to inflict significant damage with very little investment or risk, fire is an extremely high-leverage weapon of mass effect.

When Navy SEALS killed Osama bin Laden, they captured a treasure trove of material that provided unprecedented insight into al Qaeda plans. One was a detailed campaign for starting fires throughout the West. U.S. officials have determined that some fires in California last year were ignited by al Qaeda

operatives. On May 2nd, ABC News ran a story entitled "Al Qaeda Magazine Calls for Firebomb Campaign in U.S." Issues of *Inspire* magazine surfaced on al-Qaeda websites, calling for jihadists to start huge fires with timed explosives planted in U.S. forests. The articles included detailed instructions for constructing remote-controlled "ember bombs."

The concept of "Fire Wars" is not merely a futuristic possibility confined to think-tank musings. As of last Saturday, there were 52 large wildfires burning across the United States. Thirty-eight of them were uncontained. Since July 1st, crews have been battling fires in Colorado, Missouri, Idaho, South and North Dakota, Montana, Utah, Wyoming, New Mexico, Nevada, Tennessee, Kentucky, Alaska, Florida, California, Minnesota, North Carolina, Arizona, Nebraska, Alabama, Arkansas and Georgia. And those were just fires on Federal land. They don't include local and state fires, such as six that were started in wheat-stubble fields of north-central Kansas two weeks ago. Four were started in one night.

Those of us who live in Colorado are already engaged in fire-combat. Recently, 25 fires were started within a few miles of each other in El Paso and Teller Counties. Every one of them was attributed to arson, but fire crews extinguished all 25 before they caused much damage. However, the arsonist is still at large.

In early July, there were 12 major fires burning in Colorado. Six of those consumed almost 167,000 acres, an area that is 4.27 times the size of Washington, D.C. One, the High Point Fire in northern Colorado, burned 87,504 acres and destroyed 259 homes.

But the most destructive fire in Colorado history started 3 miles from my hometown of Colorado Springs on June 23rd. The Waldo Canyon Fire exploded on June 26th, fueled by 100-degree temperatures, relative humidity as low as 2 percent, and 55-65 mile-per-hour winds. In the span of minutes, not hours, wind-driven flames jumped two firebreaks and raced downhill into the Mountain Shadows neighborhood. Exceptionally dedicated, brave firefighters battled "a firestorm from Hell" that, ultimately, destroyed 346 homes and killed two people in a few hours.

The Waldo Canyon Fire burned 18,247 acres, forced 32,000 people to evacuate, and cost about $15 million in direct costs to bring under control. Investigators have not determined the cause, but we know it was not sparked by a lightning strike. The top-level questions are: Was the Waldo Canyon Fire started by terrorists? Did the same person or group that ignited those other 25 fires finally score with the 26th? And was this part of an organized economic-warfare campaign of fires across the U.S.?

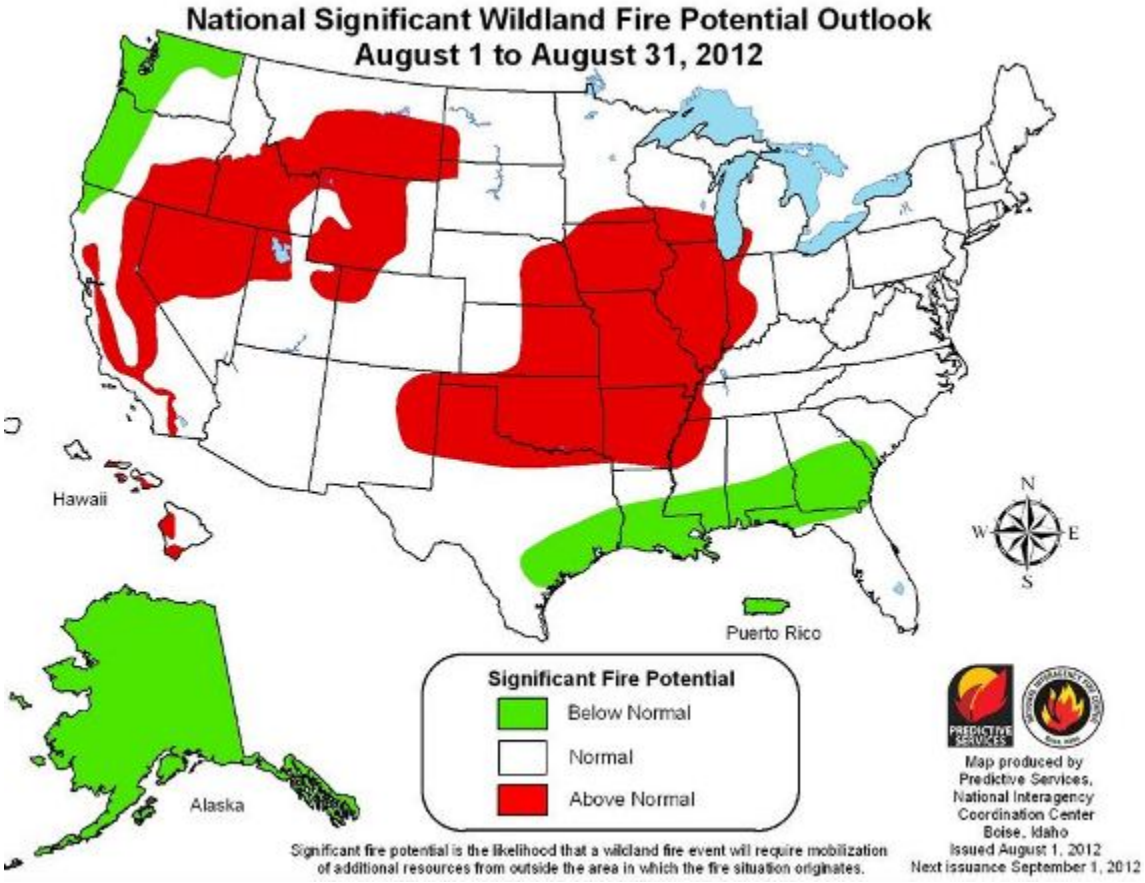
If it was an economic-warfare attack, then the Waldo Canyon Fire was a huge success. Home losses alone will exceed $100 million dollars. Businesses that were evacuated lost another few million. The Broadmoor, a five-star luxury hotel

that wasn't in immediate danger, lost more than 4,000 nights through cancellations. Thousands of tourists were either driven from the mountains by evacuations, or simply didn't come to Colorado Springs, because they were spooked by the massive fire. One community suffered 74 job losses, due to layoffs, and business revenues are down 45-65 percent. Insurance rates will probably rise, as a result of this and hundreds of other fires across the country.

Professional firefighters are warning that this rash of wild land fires may be only the beginning of a terrible fire season that could burn millions of acres across the West before the snow flies this winter.

Ironically, the Blue Ribbon Panel report we submitted 10 years ago warned of exactly this situation: Extremely dry conditions, exacerbated by forests choked with downed timber and standing beetle-killed trees, that create ideal targets for

terrorists waging economic warfare. There's reason to believe America is under attack, and that the bad guys are waging Fire Wars *right now.* But we, as a people, aren't fighting back. Thanks to an ingrained, out-of-date mindset, we still treat fire as a "land-management" issue. We should be viewing it as a grave national security issue.



When we finally acknowledge that we are engaged in a brutal Economic War-by-Fire, we can adopt strategies to defeat terrorists who are starting those fires. We can use NASA and Defense Department satellites to spot new fires. We can fly infrared-equipped NASA, Forest Service and military aircraft over fire-prone forests, operating Fire Combat Air Patrols around the clock. Let's say an Air National Guard F-16 fighter equipped with a Lantirn or Sniper electro-optic pod spots a new fire start. The pilot can immediately give firefighters its coordinates and vector initial-attack crews to the blaze. He also can track any vehicles near the fire-ignition point, and guide law-enforcement officers to intercept them.

Finally, we must develop and field a robust large air tanker fleet of firefighting aircraft. The Forest Service has made a good start, but it still suffers from a culture and attitude of what some firefighters call "cheapism"—the idea that we have to deal with wild land fire on the cheap. That's no longer acceptable.

America is under attack by terrorists waging Economic Warfare-by-Fire. Unless we admit that, and properly focus our considerable national resources on this enemy, U.S. citizens will suffer intolerable—and completely unnecessary—loss of property and life.

Addendum

Perhaps the most important issue that was revealed/highlighted [during the ACD/EWI event], in my opinion, was the fact that no government agency has primary responsibility for conceiving of, monitoring, or mitigating EW threats. Yes, DHS theoretically has that responsibility, but what unit within DHS is paying any attention or doing anything to thwart EW attacks? None, I suspect.

What needs to be done: 1) Educate American citizens, lawmakers and a number of federal, state and local bureaucracies/agencies; 2) Conduct comprehensive wargames that illustrate how interrelated and synergistic EW attacks can be, their potential impacts, and ways to prevent, mitigate and recover from EW strikes.

New policies for consideration: Honestly, I think a completely new model for combatting EW is in order. Simply adding an Economic Warfare section to DHS will do nothing more than create a layer of bureaucracy that will consume scarce funds, but have very little positive impact.

Instead, an outside entity, contracted to the U.S. government, could do a far better job of selecting sectors of the economy that are particularly vulnerable to EW attack (building on those identified and discussed during the July 9th briefing); identifying potential attackers and their methods/vehicles, then working directly with local, state and federal agencies to alert and recommend preemptive actions to thwart an EW attack. This entity also could work with DHS and its military counterpart, U.S. Northern Command, to develop post-EW attack strategies for mitigating the effects, and for recovering quickly.

[Edited from prepared remarks and author's additions.]

TRANSNATIONAL CRIME: UNHOLY ALLIES IN DISORDER, TERROR AND PROLIFERATION

David Aufhauser, partner, Williams & Connolly LLP, and former general counsel and chief legal officer, U.S. Department of the Treasury

I've been asked to speak a little about transnational organized crime, which tries to capture, I think, General Hayden's comments about some people being sinners, and maybe tries to morph a little bit of Jim Woolsey's statement that our enemies are the rich. But in this case, these are people enriched not from oil necessarily, but principally from drugs and, of course, things like human trafficking.

The point of my talk really is less about organized crime, which presents common public issues of safety, and more about the convergence of organized crime with terrorism and acts of insurgency.

[No] lesser light than Director [James] Clapper recently testified that transnational crime, particularly in the Islamic Maghreb, is the abiding threat to national security in the United States. And in fact when you go back and you take a look at the National Intelligence Council's open source global trend documents, they are really quite consistent, and repeated, in the warning or prediction that what we are facing in the world to come, between now and 2025, is the growing emergence of non-state actors, a multi-polar world without the benefits, if you will, of multilateralism, and a discord of demographics, all of which is a toxic mixture for exploitation by organized crime, and particularly cross-border exploitation by organized crime.

Now what is the threat that transnational organized crime poses to national security? The first I've already mentioned and is pretty much straightforward. It's our common public safety, whether it's drug trafficking, human trafficking, kidnapping, intimidation and extortion, murder (murder now on a scale that we haven't witnessed except in theaters of conflict—when you think about what's happening south of the Mexican border today). Counterfeiting and the kind of cyber-fraud capability of stealing your identify or emptying your bank accounts—all of these threaten our common good, all of these are rather unrevealing, obvious challenges of organized crime.

But there is a second, growing theater of threat that's more far-reaching and presents a kind of uncommon injury, if you will, to our national security. And that is what I referred to before, the convergence of the unholy alliance of crime, terror and insurgency. It affects us in our national security in a number of different ways. The first is the corruption of developing states. The second is capture of failing states. The third is alliances of transnational criminal organizations with state sponsors of terrorism. The fourth is this convergence that I have referred to you, of terrorism, crime and insurgency, which reflects in some cases, not so much a shared ideology (although I'll give you an example where there is a shared ideology in a second) and more so marriages of mere of convenience, where crime, violence and extortion can make both parties rich, or further the political ends of terrorists.

By the way, when I was at Treasury, it was immediately after 9/11, and we had to stand up to what was a nascent terrorist financing organization, trying to trace the source of monies. We believed at the time, and I think we were right, that the principal source of monies for terrorism were through a rather centralized al-Qaeda organization, were the diversion of charitable funds, and/or direct contributions, or knowing contributions, from people in the Middle East.

We got very good at chasing that money, extremely good at chasing that money, and, if you will, terrorists responded by seeking out other sources of money. And the other sources of money they turned to increasingly in a balkanized, atomized world, was plain old pedestrian crime. So when you looked at what happened in Madrid several years ago, close inspection proved that Madrid was not financed by international money. Madrid was a locally financed drug operation (and also smuggling of people across the straits there, from Morocco, financed by crime, and financed by the organized criminal elements of Spain) that killed scores and scores of people.

So increasingly terrorist financing concerns have focused upon the growing alliance between the funding of the terrorist activities by crime—and indeed the marquee-attraction, of maximizing, of leveraging, by reaching out and shaking hands with transnational organized crime.

None of this is really imagined, and you have to appreciate the scope to appreciate that this is real. This is a real current, abiding, corrosive, constant threat. It may not have the immediacy, it may not have the marquee-value of talking about cyber warfare or about even fires, set out in California and Arizona, but it is a constant eroding drip, which actually has the capability of bringing weapons of mass destruction to our borders.

There is a very interesting piece of testimony people ought to read by Douglas Farah, about two or three months ago here in the Senate, on the incredible, incredibly tight alliance of Iran and Quds forces, and the Iranian Guard, and FARC and the government of Chavez, and what they are standing up there, including military universities and including, quite frankly, the building or the ambition to build a nuclear plant, which is the same blueprint as the nuclear plant in Iran, that's been bedeviling us now for more than seven years.

But back to the scope. You know these numbers are imperfect, and the reason these numbers are imperfect is by definition—this is clandestine activity, this is hidden market, and this is black, dark-pool money. And ironically the anonymity of the money has additional protections—monitoring the system now for the transfer of wealth across borders today. I don't know if it's Michael [Hayden] or Jim [Woolsey] who referred to it, but we now transfer money less in bulk and more in "X"es and "O"s. "X"es and "O"s are sometimes easy to follow if you have penetrated a system, like we once upon a time did, now publicly known, called Swift; but otherwise, very difficult to figure out who is sending what to whom, when it's a digital transfer of huge amounts of money across borders, frequently hidden as false transactions and trade activity.

[The size of transactions, even] with all those caveats, [by] the White House's numbers in their announcements of the July 2011 strategy on transnational crime, is one to three trillion dollars—trillion dollars in accounts, a billion dollars in public official bribery, 750 to a trillion dollars in drug money. Illicit weaponry sales, 170-

320 billion, counterfeited and pirated goods, 500 million. Those numbers add up, if my arithmetic is right, to 6.2 billion dollars, at the high side the equivalent of 10 percent of GDP in the United States. Now World Bank estimates put it lower, but whether it's 4 percent or 10 percent, it's still a staggering amount of money, and that money is used to corrupt states, and [push further] failing states, to buy safe haven, and to help both illicit activity and terrorist activity. Disorder favors the bad guys, the sinners that Michael [Hayden] was referring to.

Who are these guys? Well, in Russia and Eurasia, they now go by a newly-dubbed name, the "Brother's Circle." In India there's a guy named Dawood Ibrahim, whom I'll speak more about, and the "D Company." In Latin America there are many large cartels that you are familiar with, but the most savage and gory one is Los Zetos. In Italy, it's the Camorra. In Japan it's one of the Yakuza crime families, the most prominent of which was recently designated by Treasury—I'm going to butcher the name—but Yamaguchi-gumi is what the name of the family is. The trade is commonplace: counterfeiting, human chattel, illicit arms trade, fraud, and, above all, drugs. They use shell companies, compromise accountants, lawyers and bankers, and investment bankers; but most importantly, they corrupt public officials as they ply their trade. Perhaps more importantly, they spirit the money that they earn locally across the globe to expand their criminal enterprise.

Now these organizations—the five I named by way of example, which have been named by the Treasury Department—these aren't, you know, Marlon Brando hierarchy old-world cartels. These are very complex, networked, loosely knit together criminal syndicate families and clans and tribes. They are allied because of the convenience of it, and they are allied unfortunately because of—this is the dark side of the Internet, of course—by the ease with which you can communicate, engage in social intercourse, and engage in criminal intercourse, and transfer funds and logistics necessary to become a global criminal enterprise.

Let me give you some examples. I'm giving you these examples to impress upon you that there is no one model for the crime family, and there is no one model for the nexus that I'm concerned about, [and so is] the current administration which has been really on top of this. The nexus between terrorism and transnational organized crime: there is no single model. Some are marriages of convenience, some are revolutionary fronts that have morphed to commercial criminal enterprises, and some are criminal enterprises that have morphed to revolutionary fronts.

Afghanistan is the most obvious up front for all of us, the alliance with criminal networks, like the Haqqani network, which is basically responsible for many of the IED deaths that we've encountered in Afghanistan, and for the corruption of officials and thereby undermining the legitimacy of the capacity of the government that we are trying to stand up there.

The Afghanistan [operation], however, pales in terms of sagacity, in terms of its footprint, [compared] to Hezbollah. Hezbollah has been around for years and years and years. It is now confirmed, through indictments, through designations and through intelligence, that it's a major drug trafficking and money-laundering organization, as well as a terrorist organization. And it's reach goes from the tri-border area down in Latin America, in alliances with the FARC up in the north of Latin America, to West Africa, and [to] captured or near-captured nations, like Mali or Guinea-Bissau, and money flowing through Lebanese banks, all of which became disclosed, and all of which was seriously shut-down or frustrated by the efforts of the U.S. government, in the closing of what was known as the Lebanese Canadian bank.

Hezbollah's activities. There's such a long history of Hezbollah's activities in Latin America alone, that it's frightening to think about, and it's all allied with the drug trade in terms of underwriting and goes back to 1994 and the bombing of the AMIA Buenos Aires Jewish Center, which directly implicated Hezbollah and Iran. [In] December 2001, a Lebanese drug king-pin and Hezbollah financier was charged with smuggling tons of U.S.-bound cocaine in concert with the Los Zetas Mexican organized crime cartel.

And then you hear, at least from open-source material, and I mention this almost because it sounds like Keystone Cops, is the quixotic open-source story that the Quds [Force and] Iranian Revolutionary Guard allied themselves with hit men of Los Zetas to go after the ambassador from Saudi Arabia here in America. Gentlemen at this table may know sources I don't have available to me. It's both stunning in its stupidity, stunning in its ambition, frightening if it does represent a willingness to kill in America through an alliance of organized crime and terrorist political activity.

There's less tilting at windmills if you turn east and we turn to what I mentioned about a different organization, the D Company, which is in India and Pakistan.

This is a criminal group that has actually transformed itself from twenty years of being the most powerful criminal network in India and Pakistan, to becoming the champion—the champion—of terrorist activity in the area, with direct ties to and responsibility for the Mumbai bombings. Congressional reports have called this a fusion company; that is crime and terror that numbers 5,000 people in Pakistan and the UAE. It was designated originally as a global terrorist organization in 2003, but then graduated, if you will, to being designated in 2006 also as a drug-king-pin operation. Its core products are extortion, smuggling, narcotics and contract killing. It was overseen by Mr. Ibrahim throughout the 1990s and became and morphed into a politically purposeful designed criminal organization after the destruction of the Babri Mosque in Pradesh in the 1990s. That's a criminal organization that morphed into a terrorist organization whose money sponsors terrorist activity.

FARC is a different story. FARC was always a terrorist organization, which over time (after it was awarded 42,000 hectares of territory in an attempt by the Colombian government to assuage them, and to buy some level of peace) propagated, then started promoting, a drug trade which finances them today, and finances the havoc they continue to wreak down in the Latin American area.

The old cartels that we used to read about, like the Cali cartels, seem to have been crushed. The one cartel that hasn't been crushed is FARC, and FARC continues today with close alliances with to Iran. [O]n that point, instead of either plagiarizing or taking more time, I really recommend that you read Doug Farah's testimony of about three months ago on Iran's presence in Latin America, and the direct national security threat it poses in its alliance with the drug trade in Latin America.

Let me give you a couple of conclusions, or observations. The scope, as I said, of this threat, is incredibly large. It's almost unimaginable. There are more resources devoted to violence than any other non-state source. It's growing. It's growing exponentially. It undermines our international development aid. There are lots of numbers out there, but they are substantial. I've read numbers that suggest that 30 to 40 percent of development aid gets in the wrong pockets, gets diverted. It goes to corrupt public officials, who then harbor the activity of organized crime and terrorist activity.

As I said it threatens to bring disorder to the failing states, and there is a growing literature that they are getting smart about what they do with their investments. And the smartness is to leverage their power by with becoming significant forces

in strategic materials and natural resources, thereby giving them leverage in those markets and thereby distorting those markets much to our economic disadvantage.

I'm going to leave you with one large irony about this convergence. In a world of asymmetrical warfare—and that's what this is—leverage risk from the non-state actors depends in part upon their ability to ally themselves as networks. What we have found, and what my friends and colleagues from my days at Treasury have found, ironically, is that one of the most powerful weapons against these networks is to shame them, to pick out a node in the network, to name them, to out them. You know, it's one thing to say you're going to freeze their assets—and most of these networks don't have material assets in the U.S. to freeze—and it's another thing to prohibit trade with them—most U.S. legitimate businesses wouldn't be trading with them anyway—but it's another thing simply to name them and brand them and put the scarlet letter on them.

The success that flows from that has two reasons. One is legitimate businesses will certainly shun [their] company. The second is their former allies in the illegitimate businesses are frightened of enhanced scrutiny and so they may shy away from the alliances that they formerly had with these networks. And so the U.S. government strategy right now is to try to take down the networks by outing each individual node that's identifiable in the network. And it's actually quite a smart way to go about it. It is not a top-down but a bottom-up erosion of their powers.

If you don't break that circuitry, what's promised over the next twenty years is an enormous amount of civil disorder around the world, and the prospect of an acceleration of proliferation of weapons of mass destruction at your doors.

[Edited from transcript.]

LEGAL PERSPECTIVES

Michael Mukasey, partner, Debevoise & Plimpton, ACD/EWI board member, former attorney general of the United States

I want to thank Rachel [Ehrenfeld], and even in his absence, Senator Kyl, for organizing this wonderful afternoon, which I hope will have a more substantial purpose than simply a bunch of people getting together and scaring the living hell out of one another and out of the non-participants as well.

We've been talking about all manner of possible assaults, cyber and non-cyber, state and non-state actors, that could affect the economic health of this country.

Because the means of conducting these assaults are so varied, and, to the extent that they rely on technology, are constantly evolving, I think it's fair to say that the law, as we conventionally think of it, is an increasingly feeble tool with which to combat these kinds of assaults.

In fact, one of the principal lessons I'm going to draw today is [that the] one thing we can do is make sure that the law stays out of the way of developments in private industry, and in private industry and government cooperation, because, if you think about it, possibly the most lawyered war that we've ever had is the current war on terror. And our experience, I think, has been that the law has been better at getting in the way of combating it than it has in combating it.

In order to understand how feckless a venture it is to try to create a set of rules, particularly international rules, that will control the kinds of forces that we've been talking about, I want to take you back over a century, to the year 1906, when Russia, which was disadvantaged by a then new technology: hot air balloons, backed an effort to outlaw aerial bombardment. And, in fact, at the first Hague Peace Conference in that year, the Russians proposed a ban on what was, what they called, "the discharge of any kind of projectile or explosive from balloons or similar means" for a term of five years. It was adopted. The following year, when the advantages of aerial bombardment began to be perceived, the ban was reinstituted, but it applied only to undefended towns and villages, which is to say, when it came to aerial bombardment in support of conventional warfare, all the bars were down.

This example seems quaint, but it illustrates two approaches that are sometimes attempted to try to explain feared military potential of advancing technology. The first is to prohibit certain kinds of activity outright, and the second is to try to limit it. There are some relatively primitive practices [under], which an outright ban has been moderately successful. The use of poison gas in warfare is an example of that, but even here there are, of course, some regimes that have used it, both against their own people and in international struggles. Think back on the Iraq-Iran War and you know. You can think about the limits of international conventions of that kind.

The limitation approach with respect to nuclear weapons—I think we are watching that unravel, right before our eyes.

I think it should be no surprise, as to the matter we've been talking about, [that] it seems unlikely that a set of rules, however widely concurred in by public and private agencies, are going to resort—are going to limit—resort to economic warfare in the various channels that are open to both state and non-state actors. Reliance on any government is at least problematic. For example, in the cyber sphere, the Defense Department is authorized to act with respect with threats to the ".mil" and ".gov" networks. It may, under some circumstances, be able to warn of a cyber attack on a ".com" network. But as General Keith Alexander, Director of the Defense Intelligence Agency, has said, in many cases the only thing his agency is authorized to do is to watch the screen and say "Ooh, that's going to be a bad one."

As to the criminal law, it punishes unlawful intrusions, unlawful damage of the sort that we've been describing; but it acts after the fact. And obviously we want to create ideally a system in which people cannot act before the fact.

I think private actors within the ".com" domain, as Stewart [Baker] suggested, can certainly set up their own detection networks, and, if we keep the legal channels sufficiently open, can cooperate with the government in strategies that will not only protect but in some cases punish the hijacking of information and the destruction of systems. It's difficult to get private companies to go along with these cooperative activities. The first reaction tends to be "what about our secrets, won't they become known to other companies?" Firewalls and clean teams can get around that, and I think these [entities] have shown themselves in recent years to be more and more receptive to that kind of activity.

I think government can contribute, does contribute, in a plodding sort of way. I hadn't heard mention of today something called the CFIUS process—that's one of those splendid government acronyms that stands for the Committee on Foreign Investment in the United States. It's an interagency group that passes on the acquisition by foreign persons and entities of interest of U.S. companies that, for example, have defense contracts with the government. It's comprised of representatives from the departments of Defense, Justice, Treasury, State and Commerce at a minimum, and it passes on those foreign acquisitions. Of course, the downside is there has to be a government hook in order to do that. And the government hook is generally a government defense contract. Obviously the government cannot be passing on all foreign acquisitions.

We live in a free society, a society that has a bias in favor of the free movement of capital and the free movement of people. But we can, it seems to me, monitor and disclose. Requiring disclosure from listed companies, requiring disclosure of foreign holdings from companies that are regulated through the exchanges and

otherwise, is one approach that will at least allow people like Rachel [Ehrenfeld] to figure out who owns what and how much.

There is a bit of good news in all of this that I found plodding through particularly dense verbiage of a book on international law. I came upon the following passage. It says, “No international convention to include the charter of the United Nations defines threats or use of force-on-force or armed attack, and despite decades of earnest work, the international community has failed to define aggression with any clarity in any other document.” And here’s the bold type: “Existing international law that governs the use of force must therefore be derived from the heuristic analysis of how the Charter use of the force paradigm has been interpreted through state practice.” Now believe it or not, that’s actually good news, because you know what it means? What it means in plain English is “what they say is what they say, what they do is what counts,” which is to say, “It’s not what they say, but what we do that counts.” And as long as we can focus on these problems and act freely, in the international arena, we may be able to overcome some of the problems you’ve heard about this afternoon.

[Edited from transcript.]