NATIONAL SECURITY LAW REPORT
Standing Committee on Law and National Security
AMERICAN BAR ASSOCIATION
VOLUME 32, NUMBER 2
SPRING 2011

inside

A Debate About the Significance of the Ahmed Ghailani Trial Verdict

Tung Yin

President Obama's recent decision to lift his previously imposed freeze on new military trials for Guantanamo Bay detainees will no doubt breathe new life into the debate over the appropriate forum for prosecuting suspected al Qaeda fighters – federal court versus military commission. The President was of two minds himself, declaring at the same time that "we will continue to draw on all aspects of our justice system – including Article III (federal) Courts – to ensure that our security and our values are strengthened."

Proponents of federal court trials have pointed to the successful prosecutions of high profile terrorism defendants such as Omar Abdel-Rahman (the Blind Sheikh responsible in part for the 1993 World Trade Center bombing), Timothy McVeigh, Richard Reid, Zacarias Moussaoui, and Ahmed Ghailani, as proof that military courts are unnecessary. In addition, federal court proponents note that concerns about the need to protect classified information in trials can be addressed through the Classified Information Procedures Act. Finally, as far as severity of punishment goes, federal court proponents note that Ghailani received a life sentence on the single count of conviction; because prosecutors had not sought the death penalty, this was the harshest sentence possible.

Yet, the outcome of Ghailani's trial should give pause to the idea that federal courts will necessarily be up to the task of trying high-level al Qaeda suspects like accused 9/11 mastermind Khalid Sheikh Mohammed. Ghailani, who was prosecuted for his role in the 1998 bombings of U.S. embassies in Kenya and Tanzania, was convicted of one count of conspiracy to destroy U.S. buildings, but he was acquitted of 284 other charges, including over 200 counts of murder. The government's case was no doubt weakened substantially because the district judge correctly excluded a key prosecution witness on the ground that the government learned of his identity as a result of coercive interrogation of Ghailani. This witness, Hussein Abebe, supposedly *would* have testified that he sold Ghailani the explosives used to bomb the embassy in Tanzania – evidence that might well have persuaded the jury to convict on the other charges.

The current rules for military commissions exclude evidence obtained through torture or coercion, but do allow derivative evidence obtained through torture or coercion where "use of such evidence would otherwise be consistent with the interests of justice." A military judge could arguably conclude that since there was no allegation that Abebe – unlike Ghailani – was mistreated, the factfinder would be deprived of relevant, probative evidence, and that "the interests of justice" would call for Abebe's testimony. To be sure, it is far from clear that Abebe would have been allowed to testify in a military commission, only that it would have been *possible*.

Still, Ghailani *was* convicted, even if only on a single count, and he did receive a life sentence. One might argue that,

Continued on **page 2**

Ahmed Ghailani Trial Verdict, from page 1

short of a death sentence, it is difficult to see how a military commission would have led to a "better" result.

The problem with this argument is that it fails to take into account the possible outcome of the appeals process. Because of the Double Jeopardy Clause, the government cannot appeal the counts on which Ghailani was acquitted. Ghailani, however, is entitled to appeal his count of conviction. If Ghailani wins his appeal, he could be retried – unless, of course, the reversal were for insufficiency of the evidence, which operates as an acquittal.

If retried, however, Ghailani may have a potent collateral estoppel argument to wield against the government. In *Ashe v. Swenson*, 397 U.S. 436 (1970), the Supreme Court held that the Double Jeopardy Clause contains a collateral estoppel element that bars the relitigation of any fact that was necessarily decided against the government by a previous acquittal. Thus, in *Ashe*, the defendant had allegedly robbed six men at a poker game. He was acquitted of robbing the first victim and then faced trial for robbing the second victim. Because identity was the only issue, and because the acquittal in the first trial necessarily resolved that fact against the government, collateral estoppel barred relitigation of identity in the second trial – and hence, the defendant could not be convicted.

In Ghailani's case, the acquittal on the 200+ murder counts may mean that Ghailani could invoke collateral estoppel to block relitigation of the facts of the deaths of the bombing victims. *Ashe*-style collateral estoppel can be complicated; a court must

> [E]xamine the record of a prior proceeding, taking into account the pleadings, evidence, charge, and other relevant matter, and conclude whether a rational jury could have grounded its verdict upon an issue other than that which the defendant seeks to foreclose from consideration.

The strange nature of the split verdicts in Ghailani's case – essentially, the jury found that he conspired to bomb the embassy buildings but did not conspire to kill the people inside – make it even more difficult to assess the likelihood of any collateral estoppel effect. And of course, Ghailani may ultimately fail in his appeal, in which case he would remain incarcerated for life (unless pardoned or commuted, which seem unlikely). Thus, the point here is modest: Ghailani may or may not demonstrate that federal courts are up to the task of trying high-level al Qaeda suspects, but to the extent that the frame of reference for that debate lies in the outcome of the case, it is far too early to say anything definitive.

Stephen I. Vladeck

To my mind, the *Ghailani* litigation—and the commentary it has provoked—is proof of nothing other than how far our popular legal discourse has sunk over the past decade. After all, many who seek to defend the ability of Article III courts to handle high-profile terrorism cases look to Ghailani's conviction and life sentence as "proof" that the civilian courts work, as if an individual conviction could ever prove anything more than the absence of a particular petit jury's reasonable doubt. Not to be outdone, those who would relegate all terrorism suspects (however defined) to trial by military commission point to Ghailani's "near-acquittal," aided by the exclusion of a witness whose testimony *might* have been admissible in a military commission, as proof that the civilian courts can't be trusted. Apparently, to both sets of commentators, civilian courts only "work" if there's no reasonable possibility that the defendant might be (perish the thought!) acquitted.

It seems to me that a far more useful conversation about the *Ghailani* case would focus on the precedent-setting substantive law at the heart of the litigation, to wit: the district court's May 2010 decision denying Ghailani's motion to dismiss based on allegations of torture; its July 2010 decision denying Ghailani's motion to dismiss based on his claim that trying him after his years of detention at "black sites" and Guantánamo violated his Sixth Amendment right to a speedy trial; and its October 2010 ruling granting Ghailani's motion to suppress Abebe's testimony. More than the number of counts on which Ghailani *was* convicted, or the length of his prison sentence, it is the *analysis* in these opinions that will have the greatest impact going forward, especially if the government attempts any future civilian prosecutions of individuals previously subject to military detention. Thus, a meaningful conversation about *Ghailani* would be one that asked in which circumstances torture (if proven) *should* warrant dismissal of a criminal case. Or one that questioned

***Continued on* page 3**

Ahmed Ghailani Trial Verdict, from page 2

whether it's really fair to allow the government to detain individuals for years on end prior to trying them, without ever being subjected to the restrictions of the Speedy Trial Clause, so long as the pretrial detention wasn't "in anticipation" of a future trial. Or one that examined why the government would *concede* that Abebe's testimony was a product of coercion and try to get it in anyway, rather than litigating that issue on the merits. To understand the feasibility and desirability of future civilian prosecutions, it is to these issues that we should direct our study.

Instead, we're reduced to platitudes—to hortatory statements that reflect a rather perverse understanding of why the criminal justice system is set up the way that it is, failing to heed Justice Frankfurter's admonition that "the safeguards of liberty have frequently been forged in controversies involving not very nice people." Thus, I completely agree with Professor Yin that it is premature for either side of this silly debate to claim victory until the appellate process has run its course. And I can't quibble with his reading of *Ashe*, or with the difficulties the government would face both directly and indirectly in any potential retrial. But from my perspective, nothing that happens in the Second Circuit will truly affect *Ghaliani's* depressing bottom-line: that we have lost the ability to talk seriously about the capabilities and shortcomings of our criminal justice system in terrorism cases, and look instead only to the final score.

Tung Yin

I don't disagree with Professor Vladeck that much of the discussion of *Ghailani* has focused too much on the outcome, both the verdict as well as the sentence, instead of process- and substance-based issues, including the remedies, if any, for potentially outrageous government misconduct. However, I also would add to something else to the list of *Ghailani*-related issues that really matter: should we really be bothering to prosecute detainees like Ghailani in any forum? In other words, the policy choice isn't just between Article III versus military court prosecution, but also, as Jack Goldsmith and Ben Wittes have argued, between prosecution at all versus indefinite military detention.

Whether to try terrorism suspects like Ghailani has to be asked in the shadow of military detention. As Professor Vladeck implies, a fair criminal process (whether Article III or military) should admit to some possibility, no how small, of acquittal; otherwise, it is just a show trial. Even if Ghailani were acquitted, however, the government apparently would redesignate him for indefinite military detention.

Intellectually, one can understand that a defendant can be acquitted without being exonerated (i.e., he's probably guilty, but it wasn't proven beyond a reasonable doubt), and that military detention would still be justified under the terms of the Authorization for Use of Military Force. As a policy matter, however, especially to non-lawyers, this probably looks to be of questionable legitimacy. It doesn't make the criminal case a show trial, not exactly, but there is something of that "quality" to the entire situation where, at the end of the day, Ghailani remains in *some* U.S. custody.

"More than the number of counts on which Ghailani was convicted, or the length of his prison sentence, it is the analysis in these opinions that will have the greatest impact…"

In short, maybe what the Ghailani case should really stand for is that if there are serious reasons to doubt that the government can bring a successful case (due to torture or coercion, or tainted derivative evidence, or other legal problem), we shouldn't argue about the "best" prosecution forum. Instead, we should recognize and admit that the rewards to be gained from a successful prosecution might not be worth the risks involved given the negative image that would result from an acquittal followed by renewed military detention. The die has already been cast with regard to Ahmed Ghailani, but the lesson might still apply to others, like Khalid Sheikh Mohammed. Foregoing a criminal prosecution of KSM would necessarily evade the important questions that Professor Vladeck raises, but it would also avoid the situation where distortions of constitutional law in terrorism cases "bleed" into ordinary criminal cases. True, deciding which cases qualify as "terrorism" cases involves its own degree of discretionary judgment, but there is a clear line here at least: only those cases where the suspected terrorist falls within the definition of the enemy in the

***Continued on* page 4**

Ahmed Ghailani Trial Verdict, from page 3

AUMF, for those are the only cases where the government can forego prosecution and still claim a lawful basis for continued detention of the suspect.

Stephen I. Vladeck

I don't doubt for a moment that the civilian courts in terrorism cases feel pressure to reach doctrinal accommodations that, in "ordinary" criminal prosecutions, they might not otherwise endorse. Nor do I doubt "the tendency of a principle to expand itself to the limit of its logic," as Cardozo suggested in *The Nature of the Judicial Process,* pursuant to which such exceptions would eventually become the rule. This is why, in my view, the "seepage" concern is the single biggest issue in the civilian courts vs. military commissions debate, even if there is an irony in hearing this critique come from those (not including Professor Yin) who tend not to be the most vocal supporters of protecting criminal defendants' rights. I don't accept, however, that this concern is unique to terrorism cases—even if we could agree on which cases fit within that rather amorphous category. To the contrary, there is plenty of anecdotal evidence suggesting that judges feel the same pressure in lots of other high-profile criminal cases, especially gang- and mob-related prosecutions. Tellingly, no one ever seriously suggests that we need a separate system for *those* cases. Instead, the solution to seepage is foresight—appreciation by responsible jurists that, whatever rule they hand down, it will likely resist efforts to cabin such reasoning to terrorism prosecutions.

"…there is at least some consensus for the proposition that detention power should atrophy over time, especially to the extent that detainees no longer pose a danger to U.S. national security."

The alternative that Professor Yin offers is non-criminal military detention as a middle ground, since it risks neither the potential damage to our ordinary criminal justice system nor the potential illegitimacy of a military conviction obtained at Guantánamo. I've already addressed this argument at some length in a guest post I wrote for the ACSblog shortly after the *Ghailani* verdict (*see* http://www.acslaw.org/node/17734), but let me recap two of the highlights here:

First, it should go without saying that military detention of enemy belligerents and prosecution, even for war crimes, vindicate very different interests. The argument that detention is a substitute for prosecution necessarily presupposes that prosecution in these cases is not *actually* about establishing guilt or imposing punishment, but is merely a pretext for incapacitation. There's value to the former, though, which we lose if we can and do resort automatically to the latter. And in any event, I'm not so sure that the power to detain without charges can properly be understood as a *lesser* form of the power to prosecute; just ask David Hicks and Salim Hamdan, both of whom have long-since finished serving the sentences imposed on them by military commissions.

Second, and more fundamentally, even if one accepts that extracriminal detention "avoids" the problems that both civilian courts and military commissions may present in terrorism prosecutions, it carries its own baggage. The courts are still hashing out the full scope of the government's detention power; and even if that's ever settled, the larger the detention regime grows, the more unsustainable it will necessarily become over the long term. As the Obama Administration's March 2011 Executive Order suggests, there is at least some consensus for the proposition that detention power should atrophy over time, especially to the extent that detainees no longer pose a danger to U.S. national security. If this idea manifests in practice, detention will thereby become at most a temporary solution in most cases, such that we'll be right back here sometime in the future, when prosecutions for offenses already a decade in the past will be that much more logistically and legally difficult.

In short, detention only "solves" the civilian courts vs. military commissions debate by changing its terms. And other than the seepage concern addressed above, there is simply no evidence that the concerns raised by critics of civilian prosecutions have actually manifested themselves. Until and unless they do, if it ain't broke, why fix it? ■

Tung Yin is a Professor of Law at Lewis & Clark Law School.

Stephen I. Vladeck is a Professor of Law at American University Washington College of Law.

"How Can We Make the Internet More Secure?"

March 2011

by Senator Susan Collins

The Internet is vital to almost every facet of Americans' daily lives and is essential to the free flow of ideas and information. It has changed how we communicate with family and friends, how we exchange information, and even how we bank and shop. And recently, as we have seen in the Middle East, the Internet literally has helped change the world.

The Internet and our access to it must be protected to ensure both reliability of the critical services and the availability of the information.

We also must be mindful that the Internet is becoming more vulnerable to exploitation and attack. Those vulnerabilities increase each day, as more and more activity finds its way onto cyber platforms.

In a single month, an estimated 1.8 billion cyber attacks will target the computer systems of Congress and executive branch agencies according to the Senate's Sergeant at Arms. The annual cost of cyber crime worldwide has climbed to more than $1 trillion — $8 billion annually here in the United States.

These dangers pose serious threats. Hackers could attack critical civilian infrastructures, such as electrical grids and transportation systems, harming whole regions. Our military assets are at risk, too. Adversaries have acquired thousands of files from U.S. networks and from the networks of U.S. allies and industry partners, including weapons blueprints and operational plans. In fact, military officials now describe cyberspace as the fifth domain of war – in addition to land, sea, air, and space. They note that cyberspace is unique because it is the only battlefield to be invented by humans.

Clearly the Internet must be made more secure while doing so in a manner that does not in any way infringe on our Constitutional rights to receive information and express our views.

Last year, Senator Lieberman, Senator Carper, and I introduced legislation to strengthen the government's efforts to safeguard America's cyber networks from attack and to prevent Presidential overreach. That bill was unanimously approved by the Senate Homeland Security and Governmental Affairs Committee.

Last month, we introduced a new version of the bill with stronger, more explicit provisions preventing the President from ever shutting down the Internet. It also provides an opportunity for judicial review of designations of our most sensitive systems and assets as "covered critical infrastructure."

President Mubarak's actions in January to shut down Internet communications in Egypt were, and are, totally inappropriate. Freedom of speech is a fundamental right that must be protected, and his ban was clearly designed to limit criticisms of his government.

Our bill would not only prevent such a shut down, but also would make America's critical assets safer.

Our bill would:

- ✧ Establish a cyber security leader within the Department of Homeland Security who has the authority to coordinate policy and to mandate protective measures across all federal civilian agencies. This leader would be in charge of a new National Cybersecurity Center – much like the National Counterterrorism Center – that brings together expertise from across the federal government.

- ✧ Promote information-sharing on cyber vulnerabilities and on protective measures, distributing data among federal, state, local, and tribal governments and private sector stakeholders.

***Continued on* page 6**

How Can We Make the Internet More Secure, from page 5

- ✧ Create incentives for the private sector to implement cybersecurity "best practices", with a special focus on helping small businesses.
- ✧ Provide specific authority to National Cybersecurity Center – based on a risk-based, collaborative model – to identify and mitigate cyber vulnerabilities on the most critical infrastructure.
- ✧ Prevent the President or any official from shutting down the Internet.

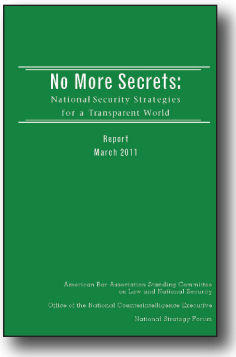
This legislation would set our nation on a course to be better equipped to anticipate, neutralize, and build additional safeguards against cyber attacks. It would help protect the ever-evolving frontier of cyberspace, which now encompasses so much of our modern-day life and will continue to grow in importance.

If we don't build adequate protections into our federal networks and critical infrastructure, then the malicious hackers – including nation states and terrorist groups – will exploit, attack, and destroy them. As a nation, we must be prepared to aggressively and proactively meet this emerging global cyber threat.

We cannot afford to wait for a "cyber 9/11" before our government finally realizes the importance of protecting our digital resources, limiting our vulnerabilities, and mitigating the consequences of penetrations to our networks.

We must be ready. It is vitally important that we build a strong public-private partnership to protect cyberspace. It is a vital engine of our economy, our government, our country, and our future.■

David Kris, retiring Assistant Attorney General for the National Security Division of the U.S. Department of Justice speaks to the Standing Committee on Law and National Security at a lunch on March 8, 2011 hosted in his honor. As head of the National Security Division, Kris was responsible for the authorization of electronic surveillance or physical searches through cases brought before the Foreign Intelligence Surveillance Court and supervised the Department's conduct of dozens of counterterrorism trials.



ABA Standing Committee on Law and National Security releases workshop report on "No More Secrets" The report summarizes workshop discussions led by national security experts identifying national security strategies for addressing this challenge. The group discussed whether the world is rapidly approaching a time when secrets no longer exist and how the government might prepare for and function in such circumstances.

Morris I. Leibman: 100th Birth-date Commemoration

The month of February 2011 marks the 100th year of the birth of our founder, Morris I. Leibman's, birth. This issue of the National Strategy Forum Review commemorates and is dedicated to him. His legacy as advisor to U.S. Presidents and Congress, and founder of the National Strategy Forum, co-founder of the American Bar Association Standing Committee on Law and National Security, and several other national security and world peace organizations, is very much alive.

Morrie Leibman's profession was as an attorney, and, most importantly, as a counselor who possessed the rare abilities to think and act strategically, to identify paramount objectives among conflicting and competing ideas, and to resolve issues for his business clients and for America which he loved passionately.

Many vexing national security issues have occurred since Morrie's death. As we analyze these issues, the starting points are always what would Morrie do, what are the critical objectives, what is the appropriate strategy, and how do we communicate? These principles provide a way forward through the morass of competing voices, ideologies, and imperfectly understood facts. The National Strategy Forum operating standard is derived from Morrie who was a consummate educator for those who had the good sense to know that they were in the presence of a wise elder.

Morrie counseled, gathered objective facts, asked questions (and didn't answer them), arrayed options, and constructed an overarching strategy that addressed the contemporary problem and its anticipated future consequence. All of this was done on a scrupulously non-partisan basis, with great respect for competing ideologies. All of these principles were to be presented with respect, civility, and good humor.

In addition to being a counselor and educator, Morrie was a talent scout and a recruiter. Morrie mentored a legion of talented young people who shared his impulse to serve America as national security practitioners. This younger generation has become the present generation of national security strategy policymakers and counselors. In turn, they have used Morrie's principles to recruit and mentor a new generation of America's leaders. Thus, continuity and sustainability is being achieved.

Morrie would have reveled in the daunting array of contemporary U.S. and global issues that the National Strategy Forum is addressing. For example, the U.S. budget deficit; the U.S. military presence in Afghanistan and Iraq; counterterrorism; political instability in the Middle East — Egypt and Tunisia; how to strengthen Pakistan; the multi-relationships among the U.S., PRC, Taiwan, India, and Pakistan; Iranian and North Korean nuclear proliferation; the compatibility of civil liberties and national security; the U.S. adaptation to a multi-polar world; immigration; how to learn fiscal responsibility from Canada; cybersecurity; and how to enhance a good neighbor policy with Mexico and Central and Latin America.

"Not to worry" as Morrie would often say. For us, Morrie is here and always available for good advice. ■

Remarks as Prepared for Delivery by Assistant Attorney General Tony West at the ABA Standing Committee on Law and National Security Breakfast – February 18, 2011

Washington, D.C.

Let me express my thanks to Harvey Rishikof for his gracious invitation to speak today. Thanks also to Holly McMahon for bringing us together this morning.

It's a pleasure to be here with you to talk about the work we're doing in the Civil Division to promote and protect the Nation's national security interests. The work of this Standing Committee furthers the scholarship of national security law and encourages dialogue on these important issues. And your influence is far and wide—a member of my senior team, Mary Smith, works closely with the Standing Committee as its liaison to the ABA Board of Governors.

"…detaining battlefield captures to prevent them from re-engaging in warfare is not in itself particularly controversial-indeed, that concept is as old as war itself."

As many of you know, the Civil Division represents the United States in courts throughout the Nation in a wide variety of matters. Essentially, we're the federal government's law firm, representing the President, the Cabinet, federal agencies and the Congress, and with over 1000 lawyers and more than 400 support staff, we are the Justice Department's largest litigating component. Nearly every aspect of Federal Government operations and this Administration's domestic, foreign and national security policy priorities finds its ways through our doors at one time or another.

And probably nothing we do in the Civil Division is as vital to the safety and security of the American people as is our work on national security matters. Indeed, there's scarcely a week that goes by where I don't deal with a significant, often controversial national security issue.

And the largest amount of my time spent in this area concerns our defense of the wartime detentions of individuals held at Guantanamo Bay.

Currently, there are about 140 active habeas cases involving GTMO detainees who are challenging the legal basis for their detentions. Three years ago in Boumediene, the Supreme Court held that GTMO petitioners have a right to habeas and could challenge the legality of their detention in federal court.

Since then, the Civil Division has defended those cases on behalf of the United States. That effort has required enormous resources, including dozens of Justice Department attorneys, hundreds of thousands of hours of DOJ time and constant coordination with several of our sister federal agencies throughout the Executive Branch.

This enormous effort stems from the fact that these are uniquely challenging cases, where the stakes are high because both national security and liberty interests are at issue, and there is tremendous pressure to get it right. I've spent many late nights with Civil Division lawyers in the Justice Command Center grappling with the difficult and frequently novel legal and evidentiary questions posed by these cases.

And added to that is a history of skepticism surrounding the legal legitimacy of detentions at GTMO. As President Obama has said, following the tragic events of 9/11, our government, "motivated by a sincere desire to protect the American people," made a series of deci-

***Continued on* page 9**

Tony West, from page 8

sions that took us "off course" and undermined the integrity of our efforts to defend the detention of individuals captured on the battlefield.

Now, detaining battlefield captures to prevent them from re-engaging in warfare is not in itself particularly controversial—indeed, that concept is as old as war itself. The challenge, however, is to litigate these GTMO habeas cases within a framework that offers an accepted legal basis for detention that is bounded by the rule of law, as well as procedural safeguards that are robust and fair.

But how do we do that? How has the Obama Administration and this Department of Justice litigated these important cases in a manner that is rooted in the Constitution and consistent with our Nation's unique values? I think, over the last two years, we've done so in two significant ways:

First, this Administration has stated, for the first time, that the legal standard underlying the President's authority to detain individuals at GTMO must be rooted in Congressional legislative action that draws guidance from the common laws of war.

Second, through our district and appellate court litigation, we have developed important procedural safeguards that ensure detainees have a meaningful opportunity to present their habeas cases to neutral federal judges, because the legitimacy of wartime detention is advanced—and national security is enhanced—when the government proves its case in a process that is perceived as fair.

So I'd like to talk about these two developments because together they have allowed us to meet our Number One priority of keeping the American people safe consistent with the rule of law: a legal standard rooted in Congressional authority and informed by the laws of war on the one hand; coupled with procedural safeguards that are just and reasonable on the other. Let's look briefly at each.

First: the substantive legal basis for detention. On this point, there is some common ground: We are a nation at war and the courts in the Guantanamo cases have repeatedly agreed with the government that the President has the authority, consistent with U.S. law and longstanding law-of-war principles, to detain those who are part of enemy forces in this ongoing conflict. This is what the Supreme Court held in the Hamdi case.

But while the fact of the government's wartime detention authority may be fairly settled, the breadth of that authority—that is, to whom it applies and under what circumstances—has been the subject of much debate.

To inform this debate, this Administration in March 2009 established a definition outlining who may be subject to the President's detention authority. That definition indicated that the President may detain those individuals responsible for authorizing or participating in the 9/11 attacks, as well as anyone who harbors them. It also indicated that the President may detain persons who were part of, or substantially supported, Taliban or al Qaida forces or associated forces engaged in hostilities against the U.S. or its coalition partners.

This definition, known as the March 13th Definition, forms the substantive legal regime underlying all of our habeas cases. And, importantly, it is backed by two sources of legal authority: First, it is based on a duly-enacted Congressional statute – the Authorization for Use of Military Force or "AUMF" – which authorizes the use of force against "organizations" and "persons" connected to the 9/11 attacks, as well as those that "harbored" or "assisted" them.

And second, the March 13th definition draws upon the international laws of war to inform our interpretation of the statutory detention authority conferred by Congress in the AUMF.

So for example, while the language of Congress' AUMF speaks directly to al Qaida and Taliban forces, longstanding law-of-war principles support our interpreting that authority to include other armed groups we have confronted in Afghanistan who are fighting with al Qaida and the Taliban.

And when Civil Division lawyers brief these cases in the federal courts, we take great care to articulate how the scope of our authority

Continued on **page 10**

Tony West, from page 9

under Congress' AUMF is supported by these legitimate and established principles. Notably, we have not relied on claims of independent constitutional authority under Article II as the substantive basis for the President's detention authority.

We have presented the March 13th definition in case after case to the federal courts, and it has been repeatedly upheld. And by testing our authority in the independent federal courts, we've underscored the paramount importance of the rule of law, and lent substantial legitimacy to the government's actions in detaining enemy forces.

Of course, applying the relatively straightforward principles of the March 13th definition can prove challenging when applied to an organization like al Qaida, which operates in violation of the laws of war; does not have formal enlistment procedures or uniforms; has a diffuse command structure; and operates in many cases clandestinely around the world.

Take, for example, the principle that those who are "part of" enemy forces may be detained: Courts are grappling with what it means to be "part of" al Qaida or the Taliban – every case poses a unique challenge, involving individuals with a different degree and type of connection to these terrorist organizations.

The D.C. Circuit has, in the course of applying the March 13th definition and developing the law, given us some guideposts that indicate some highly relevant facts to the inquiry – for example, to be "part of," a person has to have a sufficient link to the organization—being a free-lancer is not enough; evidence that the person received or executed orders, or was integrated into the formal command structure of al Qaida is both relevant and sufficient but not necessary in every case; travel patterns consistent with al Qaida are highly relevant, as are associations with al Qaida members, which may show trust and acceptance by the group; and attendance at al Qaida training camps and safehouses that were used to facilitate training and fighting by recruits—that can be key evidence.

Now, in addition to the substantive legal standard I've just talked about, the courts have worked hard, with the help of the Civil Division and the detainee habeas bar, to develop procedural safeguards that are fair but which also acknowledge the unique nature of these cases.

So, two important take-aways here:

First: fairness. Courts must have the procedural tools that enable them to conduct meaningful reviews of the lawfulness of the government's action. Additionally, detainees must have fulsome procedures that allow them to test the legality of their detention. Both of these are necessary for a process that has legitimacy and integrity, particularly when the government's detention determinations are upheld.

And we in the Civil Division have embraced procedures to help ensure a meaningful review and fair process. For example, we've worked hard to create a process that allows habeas counsel to review classified evidence; we have taken on significant discovery obligations to provide access to classified material in the government's files that could be helpful to the detainee in challenging the government's case; detainees have the right to present their own evidence, including the right to testify in court by remote video from GTMO; and the burden of proof rests with the government—not the detainee—and we must demonstrate that detention is lawful by a preponderance of the evidence.

The second take-away is this: these cases are unique and require procedures that take that into account. More often than not, the evidence in these cases comes from a far-away battlefield, obtained under circumstances that don't resemble anything you'd see on CSI; often it's years old and based on hearsay; and much of the time, it comes from interrogations that were conducted for intelligence purposes in circumstances very different from the Mirandized, police interviews we're all used to seeing in domestic criminal cases.

Given these unique circumstances, the courts have taken a pragmatic and balanced approach to the evidence in these cases, such as viewing the evidence as whole, as opposed

Continued on **page 11**

Tony West, from page 10

to evaluating each fragment in a piecemeal fashion; or accepting that hearsay is admissible, but recognizing that it is only valuable if the judge has a way to test its reliability.

And while the evidence we rely on in these cases is often unconventional, we've been unequivocal about one type of evidence we will not rely on: information that the government concludes was procured through the use of torture.

On this point, the President and the Attorney General are crystal clear: Torture is abhorrent to the rule of law and our fundamental values, and our lawyers who litigate these cases take allegations of mistreatment very seriously. They have been diligent and painstaking in investigating such claims. Frequently, this has involved tracking down years later the actual interrogators involved in an alleged incident.

And to the extent there are plausible allegations of detainee abuse, we carefully examine the surrounding circumstances to reassure ourselves that any statements we seek to use from that detainee are sufficiently attenuated from any alleged mistreatment.

So, to sum up: We defend these cases because we believe the GTMO detentions have a solid legal basis to justify them; that basis is grounded in Congressional statute and informed by the laws of war. Further, we believe the procedural safeguards that we have developed ensure fairness for the detainees and a framework for meaningful review by the courts. And the evidence we present, while unconventional, is reliable and untainted by torture.

Of course, courts don't always agree with our view of the facts and evidence. When we have lost and courts have issued orders directing us to release detainees and take diplomatic steps to effectuate their resettlement, we have complied or appealed, if there is a valid basis.

So I believe we have struck the right balance, litigating these cases in a manner that has kept the American people safe, makes the best reasoned arguments, and is consistent with the Constitution and our values.

We've been able to do that primarily through the excellent work of the career Civil Division lawyers, paralegals and staff responsible for litigating these habeas cases. These folks exemplify something I learned over 15 years ago, when I was a young DOJ lawyer. Back then, I had the good fortune to do much of my work for then-Attorney General Janet Reno.

"...we defend these cases because we believe the GTMO detentions have a solid legal basis to justify them; that basis is grounded in Congressional statute and informed by the laws of war."

Just before I left Main Justice to return to my home state of California to serve as an Assistant U.S. Attorney, Attorney General Reno asked to see me, one-on-one.

And during that meeting, she showed me the inscription on the wall just outside her private office, which reads, and I'm paraphrasing: "The Government wins its case when justice is done."

And she told me then that my job as a prosecutor wasn't to win as many cases as I could, but to do justice in every case I handled. I've seen that same spirit in the Civil Division team that deals with these habeas cases day in, day out.

And while, in doing our best, we may not always get it right, I can promise you we'll always try to do what's right. And that, I believe, makes all the difference.

I'm thankful for that opportunity, and I appreciate being with you this morning. ■

Integrating Students into National Security Law

Jeff Mustin, Feb 2011

The ABA Standing Committee on Law and National Security (SCOLANS) is taking active steps to integrate more closely with law schools, faculty, and students. This integration involves two steps: 1) establishing a network of national security-related journals, centers, and student organizations at the law schools, and 2) taking measures to provide more support to those organizations.

In order to establish a network of national security-minded students, professors, and law schools, the SCOLANS is distributing surveys to all ABA-accredited law schools to compile a database of schools with national and homeland security-related journals, centers, student organizations, and classes. The SCOLANS would like every school with any current national security class or organization to be on our roster! Do not wait for the survey; please make sure your school is represented by emailing your point of contact, the ABA SCOLANS student liaison, at jeffmustin (at) gmail (dot) com. By ensuring your school is part of our database, you also ensure you are eligible for SCOLANS support.

The SCOLANS is poised to provide support to any existing national security organizations, or to help your law school establish one. Methods of support include providing speakers for symposia, furnishing first-rate authors for law review articles on prescient issues, or delivering syllabi for establishing new coursework in national security. There could also be some funding available! Being a member of the SCOLANS network also ensures your institution receives information about the annual writing competition and its cash prize. There are a multitude of resources, guides, and Internet links available on the SCOLANS website, and the SCOLANS annual "Lawyer Jurga" provides a forum for leading national security scholars to share their best practices for teaching national security law. Finally, the SCOLANS provides a touchstone for any questions your law school might have about teaching national security law. We suggest you might want to watch our website for the announcement of the next Lawyer Jurga – to be held in September in Washington DC.

In summary, the SCOLANS support to your law school could be immense. In order to qualify for this support, please take the time to fill out your law school survey or email your ABA SCOLANS student liaison, Jeff Mustin, at jeffmustin (at) gmail (dot) com. When emailing, please describe the nature of your program and how SCOLANS can help you in the future.

We look forward to supporting you!

Jeff Mustin is the ABA student liaison to the Standing Committee on Law and National Security. He is a 1998 graduate of the United States Air Force Academy and former F-16 pilot with over 2,000 hours of flight time. Currently a 3L at Texas Tech University, he is studying for his JD, MBA, and MA in International Affairs, and serves as the Editor-in-Chief for Texas Tech's Journal for Biosafety, Biosecurity, & Biodefense Law. ■

American Bar Association Standing Committee on Law and National Security 2011 National Security Law Student Writing Competition

"The Constitution and National Security – First Amendment Issues"

Cash Prize and Trip to the Law and National Security Conference in Washington on December 1 & 2, 2011

Overview: The Standing Committee on Law and National Security, founded in 1962 by then-ABA President and later Supreme Court Justice Lewis J. Powell, conducts studies, sponsors programs and conferences, and administers working groups on law and national security-related issues. The Committee's activities assist policymakers, educate lawyers, the media and the public, and enable the Committee to make recommendations and provide advice on such subjects as the legal responses to terrorism, the restructuring of the intelligence community and its role in law enforcement, and operational international law in the conduct of the military. In furtherance of this mission the Standing Committee is proud to announce the 4th annual writing competition for law students.

Topic: This year's writing competition encourages a scholarly debate regarding current issues affecting US national security, the Constitution and the First Amendment. Protection of the nation from its enemies, foreign and domestic, is a primary obligation of the government. Pursuit of this goal by government officials may involve rights protected by the Constitution — the guarantees of free speech, privacy, and the freedom of the press. Recently the release of classified documents, as in the current Wikileaks controversy, has generated a robust debate about open access to information and the right to prosecute those who may have committed espionage. Many believe precautions must be taken when our national security is threatened but these precautions must be respectful of our constitutional rights. Airport scans, electronic surveillance and 24/7 public videoing has created a new world of transparency. In our time, responsibility for drawing the line between individual rights, press freedoms and society's obligation to protect itself has become a critical legal challenge.

Consider some of the cases in which the necessity to draw these lines has arisen. How should those lines be drawn and in what circumstances? You may look to other countries and take a comparative perspective. You may consider, but need not limit yourself, to the constitutional implications and national security concerns in cases ranging from the Pentagon Papers to Wikileaks to Holder vs. Humanitarian Law Project.

Prize: The winning essay will receive a cash prize of $500 and free registration to the 21st Annual Review of the Field of National Security Law Conference to be held in Washington, DC on December 1 & 2, 2011. In addition to registration for the conference, the prize will include reimbursement for coach travel and one night's lodging. Additionally, the essay will be published in the National Security Law Report. Winner must be present at the conference to receive the award.

Eligibility: The competition is open to all students who are in attendance at an ABA accredited law school between September 1, 2010 and September 15, 2011. Only original and previously unpublished papers are eligible. Papers prepared for law school credit are eligible provided they are original work. Jointly authored papers are not eligible. Entrants can have a faculty member or practicing lawyer review and critique their work, but the submission must be the student's own work product. The name of the reviewing professor or lawyer must be noted

Continued on **page 14**

2011 Writing Competition, from page 13

on the entry. Committee members, staff, and selection committee members shall not participate in the contest or review process. Only one essay may be submitted per entrant.

Format: Essays may not exceed 5,000 words, including title, and citations. Essays over 5,000 words will be rejected. The text of the essay must be double-spaced, with twelve-point font and one-inch margins. Entries should reflect the style of ABA Standing Committee on Law and National Security's National Security Law Report articles rather than law review style. Entrants are encouraged to review past copies of the News available at http://www.abanet.org/natsecurity/ - prior to drafting their submissions. Citations must be embedded in text, NOT footnotes, and must conform to The Bluepages of The Bluebook: A Uniform System of Citation.

Entry Procedure: Each submission must include a SEPARATE COVER PAGE (not included in the 5,000 word count) with the entrant's name, law school, year of study, mailing and email address, and phone number. The contestant's name and other identifying markings, such as school name, MAY NOT appear on any copy of the submitted essay.

Deadlines: Submission must be postmarked no later than September 15, 2011 and mailed to: American Bar Association, Standing Committee on Law and National Security, 740 15th Street NW, Washington, DC 20005; or sent via email to Holly.McMahon@americanbar.org. . The winner will be notified by October 15, 2011. By submitting an entry in this contest, the entrant grants the ABA and the ABA Standing Committee on Law and National Security permission to edit and publish the entry in the Committee's National Security Law Report. Please direct any questions about the contest to the Committee Staff Director at Holly.McMahon@americanbar.org.

Judging: The winning entry will contain a clearly written original analysis of a national security law issue that is substantively accurate and persuasive, and supported by citations. The entries will be judged anonymously by a subcommittee made up of members of the ABA Standing Committee on Law and National Security. ■

Protecting Against Economic Espionage Winner of the 2010 National Security Law Student Writing Competition

By Mark Frazzetto, JD, Loyola Chicago School of Law, admitted to Illinois Bar, April 2011.

Introduction

On February 11, 2008 Dongfan "Greg" Chung was arrested for stealing trade secrets concerning military and space vehicles, including the Space Shuttle. Rachanee Srisavasdi and Andrew Galvin, Ex-Boeing Engineer Arrested on Spy Charges, The Orange County Register, February, 11 2008. A year and a half later Najibullah Zazi was indicted for plotting to launch a terrorist attack on U.S. soil. Carrie Johnson and Spencer S. Hsu, Terrorism Suspect Planned Peroxide Bombs, Officials Say, The Washington Post, September 25, 2009. Chung committed acts of espionage. He acquired critical U.S. technological secrets for China. Srisavasdi and Galvin, supra. Zazi is an alleged terrorist; the plot described in his indictment could have cost the lives of many U.S. citizens. Johnson and Hsu, supra.

The indictment against Zazi alleged he traveled to Pakistan in 2008 to receive explosives training from operatives with ties to Al-Qaeda. Id. He is also alleged to have been in "urgent" contact with Al-Qaeda operatives in Pakistan and to have tested a "volatile brew" of chemicals obtained from beauty supply stores before traveling to Queens, New York around the anniversary of the September 11, 2001 attacks. Id. From 1973 to 1996 Chung worked for Rockwell International. Srisavasdi and Galvin, supra. In 1996 Boeing bought Rockwell's defense and space unit, the unit that employed Chung. Id. Chung retired from Boeing in 2002. He returned to Boeing as an independent contractor in 2003 and left Boeing again in 2006. Id. The indictment against Chung alleges that Gu Weihao of China's Ministry of Aviation wrote Chung a letter dated May 2, 1987, asking Chung for "assistance on technical issues" for various aviation programs. Jonathan Eric Lewis, The Economic Espionage Act And the Threat Of Chinese Espionage in the United States, 8 J. Intell. Prop. 189, 216 2008-2009. Chung had a security clearance that allowed him entrée to Boeing's trade secrets. Srisavasdi and Galvin, supra. In addition to the Space Shuttle program, Chung took secrets relating to the C-17 military transport aircraft and the Delta IV rocket. Id.

As the United States enters the 21st century these two cases represent disparate threats to the nation's security. At first glance it seems the threat posed by Zazi and other terrorist cases poses the greater peril. Certainly Zazi posed the more imminent threat. If Zazi had succeeded the deaths of hundreds of Americans would have been the result. But even if Zazi had succeeded the United States as a nation would have continued. While some have posited that a terrorist WMD event involving nuclear or biological weapons could cause paradigmatic changes in the political system of the United States, this is still not an existential outcome. The United States would continue to exist in some form.

Chung's activities did not present an imminent threat of loss of life. However Chung was working for the People's Republic of China ("PRC"). The PRC is the latest government of a civilization that has existed for thousands of years. For all the economic and military might of the United States, its 70-some years as a superpower is the proverbial mote in God's eye to the Chinese. China thinks strategically not in years or decades but generations. It is this paper's position that the Chung type case poses the greater danger. Economic espionage, in both its human and cyber variants, is costing the United States monetarily and also its military and technological advantages. Economic espionage, in other words, is threatening this Nation's very position in the world. What makes this trend even more worrisome is that one of the worst offenders is China.

Continued on **page 16**

Protecting Against Economic Espionage, from page 15

There are many aspects to the danger posed by economic espionage: diplomatic, economic, and military. This paper focuses on the legal aspect. This paper argues that in the area of economic espionage, both the existing and proposed statutes addressed to this peril are woefully inadequate.

The paper begins by examining the nature of the threat posed by economic espionage and China in particular, including both the traditional economic espionage conducted by human actors as well as the increasing use of cyber attacks. The paper examines the statutory tools currently provided to law enforcement, and also examines proposed legislation. This paper focuses on the economic espionage statutes whose purpose is to defend trade secrets. Export controls, as such, are beyond the scope of this paper. Given the nature of the threat, these economic espionage statutory tools are found wanting. The paper then argues that standards for cyber and traditional trade secret security be promulgated by Congress or Congress' designee (as opposed to only cyber security standards under proposed legislation). This paper further argues that companies, management, and employees who violate these standards are criminally reckless. Finally, under federal criminal law as interpreted by the United States Supreme Court these violators are culpable and should be held criminally liable.

Nature of the Threat

In his classic treatise on military strategy "The Art of War" the Chinese general Sun-Tzu wrote "to fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting." Sun Tzu, The Art of War (Project Guttenburg ebook, Lionel Giles trans., http://www.gutenberg.org, 1994, ebook #132). In his 1997 book, "War by Other Means", author John J. Fialka writes "War to the Chinese is a matter of guile, feints, endless patience, and above all spies, whose intelligence reveals the enemy's weak point, that when struck, makes the battle short lived and unnecessary." John J. Fialka, War by Other Means, 19 (1997). This strategy of feint, deception, and patience seems especially well suited to take advantage of American corporate management's fealty to its stockholders, and consequently the daily fluctuation of stock prices. An American CEO was once quoted as saying: "We're in the business of making money for our stockholders. If we have to put jobs and technology in other countries, than we go ahead and do it." Id. at 32. In addition to the loss of jobs, if the intellectual property this displaced technology represents is not adequately protected (it isn't, infra) the loss of these trade secrets severely damages the United States' geopolitical position and more importantly creates profound vulnerabilities the Nation has not faced before.

In the 1990s American aerospace companies, including the company led by the aforementioned CEO, contracted with Chinese factories to make fuselages and nose cones for commercial airliners. Id. at 32. As the Chinese learned to make these components "emerging versions of Chinese fighter planes were suddenly improving; their fuselages were better made and their aluminum skins were better." Id. Further, as American aerospace and other companies invested money and manufacturing capacity in China, China in turn would direct its economic espionage efforts in the United States at these same companies. Id. at 22. In effect, these companies were funding the economic espionage efforts being directed against them. Id.

Little has changed since the last decade of the 20th century. Generally, "The threat to the United States from foreign economic intelligence collection and industrial espionage has continued unabated." National Counterintelligence Executive, Annual Report to Congress on Foreign Economic Collection and Industrial Espionage FY 2008 1 (2009). The FBI has stated that a third of all economic espionage cases can be linked to China. Lewis, supra, at 192. "For many years China has used its military intelligence capabilities for economic purposes." Id. at 205. One author has stated that the "workforce available to the Chinese government and its corporations [for] gathering information in the United States is nearly limitless." Larry M. Wortzel, Sources and Methods of Foreign Nation-

Continued on **page 17**

Protecting Against Economic Espionage, from page 16

als Engaged in Economic and Military Espionage, Heritage Lectures, September 15, 2005 at 1. Accordingly, the FBI has increased the number of agents assigned to economic espionage from 150 agents in 2001 to more than 350 agents as of the summer of 2007. Lewis, supra, at 192.

Additionally, China in 1986 launched the "863" program. This program's mission is to "acquire and develop technology, acquire and develop biotechnology, space technology, information technology, laser technology, automation technology, energy technology, and advanced materials." Wortzel, supra at 2. The 863 program is run by China's central government and linked to the Chinese military. The FBI believes the 863 program is implicated in many economic espionage cases. Id.

In addition to the threat posed by human actors, economic espionage is increasingly becoming the objective of cyber attacks. "Cyber threats are increasingly pervasive and are rapidly becoming a priority means of obtaining economic and technical information. Reports of new cyber attacks against US Government and business entities proliferated in FY 2008." National Counterintelligence Executive, supra, at 13. A proposed federal statute finds that "industrial espionage that exploits weak cybersecurity dilutes our investment in innovation while subsidizing the research and development efforts of foreign competitors." Cybersecurity Act of 2009, S. 773, 111th Cong. § 2(2) (2009). The Obama Administration's cybersecurity review states that "a growing array of state and non-state actors are compromising, stealing, changing, or destroying information and could cause critical disruptions to U.S. systems." Executive Office of the President, Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure 17 (2009), available at http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

Foreign adversaries have been able to "penetrate poorly protected U.S. computer networks and collect immense quantities of valuable information." Ctr. for Strategic and Int'l Studies, Securing Cyberspace for the 44th Presidency 11 (2008), available at http://csis.org/files/media/csis/pubs/081208_securingcyberspace_44.pdf. Consequently,

Porous information systems have allowed our cyberspace opponents to remotely access and download critical military technologies and valuable intellectual property – designs, blue prints, and business processes - that cost billions of dollars to create. The immediate benefits gained by our opponents are less damaging, however, than is the long term loss of U.S. economic competiveness. We are not arming our competitors in cyberspace; we are providing them with the ideas and designs to arm themselves and achieve parity. America's power, status, and security in the world depend in good measure upon its economic strength; our lack of cybersecurity is steadily eroding this advantage. Id. at 13.

China has a finger in this pie. The Chinese military designs viruses to attack its adversaries' computer systems. Lewis, supra, at 229. This has resulted in a new and dangerous military capability which allows China to infiltrate worldwide computer networks. Id. at 227 – 228.

Against this backdrop China has experienced thirty years of economic growth, growth which has seen China's economy double nearly three times over. This surge has no equal in modern times. Ted C. Fishman, China Inc., 12 (2005). Manufacturing increasingly shifts to China from the United States and the rest of the world. Id. at 15. This includes consumer goods and big ticket items as well: cars, trucks, planes, ships, networks, factories, submarines, satellites, and rockets. Id. Additionally, China's plunder of intellectual property creates a "massive global subsidy worth hundreds of billions of dollars to its businesses and people." Id. at 252. The economic result is a sort of neo-colonialism, where China's vast "counterfeiting schemes act on the rest of the world as colonial armies once did, invading deep into the economies of their victims, expropriating their most valued assets, and in doing so, undermining their victims' ability to counter." Id.

The United States' military advantage, as

Continued on **page 18**

Protecting Against Economic Espionage, from page 17

well as the global military balance, is impacted as well. China has increased its GDP from 1.95 trillion in 2000 to a projected 4.19 trillion (USD) in 2008. United States Department of Defense, Military Power of the People's Republic of China, Annual Report to Congress VII (2009). This enabled China to devote increased resources to its military capacity without hindering its economy. Id. "As a result, China continues a two-decade trend of double digit percentage annual increases in its military budget." Id. at 31. One of the sources for Chinese military growth is foreign military technology acquisition; and besides actual purchases China acquires military technology by "spin-offs from foreign direct investment and joint ventures in the civilian sector, technical knowledge and expertise of students returned from abroad, and state-sponsored industrial espionage to increase the level of technologies available to support military research, development, and acquisition." Id.

As the preceding shows, the nature of the threat is quite serious. Chinese military thinking looks at war holistically. Sun-Tzu's admonition that a truly victorious general never fights a battle is echoed in modern Chinese strategic planning. The People's Liberation Army's military science text observes that ""war is not only a military struggle, but also a comprehensive contest on fronts of politics, economy, diplomacy, and law." Id. at 14. Economic espionage is incorporated into this strategy. While there are a variety of responses and programs the United States has or will make in response to this threat, the focus of this paper now shifts to how intellectual property is protected from foreign human actors and cyber attack domestically. In particular, the emphasis will be placed on how federal criminal law is applied to this new kind of warfare.

Federal Criminal Statutes and Economic Espionage

Congress enacted the Economic Espionage Act ("EEA") in 1996; its purpose is to federally criminalize acts of economic espionage. See 18 U.S.C. §§ 1831 - 1839 (1996). The act criminalizes both the theft of trade secrets and propri-

Continued on **page 19**

The ABA National Security Law Report
http://www.abanet.org/natsecurity/

Editorial Board
Harvey Rishikof Suzanne E. Spaulding Stewart Baker Richard E. Friedman
Elizabeth Rindskopf Parker Holly Stewart McMahon
Gregory S. McNeal, Editor (gregory.mcneal@pepperdine.edu)
The National Security Law Report (N.S.L.R.) contains articles concerning the law relating to the security of our Nation and associated topics. The N.S.L.R. is sponsored by the ABA Standing Committee on Law and National Security. The views expressed in this publication are not necessarily those of the Standing Committee, the ABA, or any governmental agency or private enterprise. To receive the N.S.L.R., contact Holly Stewart McMahon at 740 15th St., NW, Washington, DC 20005-1009; (202) 662-1035; or Holly.McMahon@americanbar.org.

Protecting Against Economic Espionage, from page 18

etary information by both private individuals and corporations and by foreign governments. Lewis, supra, at 190. The act defines foreign economic espionage, this paper's concern, when a human actor "intending or knowing that the offense will benefit any foreign government, foreign instrumentality, or foreign agent, knowingly…" 18 U.S.C. § 1831(a) (1996). The EEA is a criminal statute and so gives "the federal government authority to prosecute those who engage in trade secret theft against private American corporations." Lewis, supra, at 202. Importantly, no liability is extended to companies and their agents who fail to provide sufficient safeguards for proprietary information and/or fail to report the theft of proprietary information when such theft occurs. Nor does the EEA provide any standards for companies who wish to provide sufficient safeguards for proprietary information.

The primary statute that federally criminalizes hacking is 18 U.S.C. § 1030, which concerns fraud and related activity in connection with computers. In particular, the act makes it a federal crime for anyone who illegally accesses proprietary information for the benefit of a foreign government. See 18 U.S.C. § 1030(a). Again, however, this statute provides no guidance as to computer security standards. Thus the statute can't extend any liability to companies or their agents who violate such standards, or who fail to report theft of valuable intellectual property.

One piece of proposed legislature is interesting in that the statute does call for the formation of standards and even a compliance mechanism. The bill, introduced in the Senate, is called the "Cybersecurity Act of 2009" (S. 773, 111th Cong. (2009)) and currently sits in the Senate Committee on Commerce, Science, and Transportation. The bill's provisions call for among other things, the establishment of standards and a compliance requirement. The bill mandates that, within one year of the statute's enactment, "the National Institute of Standards and Technology shall establish measurable and auditable cybersecurity standards for all Federal Government, government contractor, or grantee critical infrastructure information systems and networks". Id. at §6(a). As to compliance, the bill, if enacted, would require

> "compliance with the standards developed by the Institute under this section by software manufacturers, distributors, and vendors; and shall require each Federal agency, and each operator of an information system or network designated by the President as a critical infrastructure information system or network, periodically to demonstrate compliance with the standards established under this section." Id. at §7(d)(2).

However, the standards relate to software primarily and there is no indication what failure to comply results in for entities or individuals who don't meet the bill's standards. There are no prescriptions for the preservation of trade secrets nor is there an extension of liability to those organizations or their agents who violate the standards.

Finally, there is the "Cybersecurity Enhancement Act of 2010". H. R. 4601, 111th Cong. (2010). This proposed statute has passed the House and currently sits in the Senate Committee on Commerce, Science, and Transportation. The bill would develop a cybersecurity workforce, coordinate and prioritize federal research and development, and promote cybersecurity education and awareness for the general public. Id. The bill does nothing to address the issues of standards and liability.

It is this paper's position that all these statutes fail because they do nothing to assign responsibility to the United States' primary source of vulnerability to economic espionage: corporations, especially those corporations that do business with inimical foreign nations who, like China, seek to compete with the United States itself. Further, this lack of responsibility on the part of corporate America is most damaging when a nation like China regards economic competition as a form of warfare.

American corporations are on the front line of this struggle. "Individual firms decide

Continued on **page 20**

Protecting Against Economic Espionage, from page 19

whether and how to protect trade secrets." Aaron J. Burstein, Trade Secrecy As An Instrument Of National Security? Rethinking The Foundations Of Economic Espionage, 41 Ariz. St. L.J. 933, 962 (2009). Moreover, "[t]he private sector . . . designs, builds, owns, and operates most of the network infrastructures that support government and private users alike." Executive Office of the President, supra, at 17. At the same time, "The damage a clever spy can wreak in a supposedly peaceful economic setting is 'often invisible and decisive.' And the victim – especially if he must answer to angry stockholders - is not often inclined to want a history." Fialka, supra, at XIII.

As noted above, the statutes enacted or proposed by Congress do not really address these issues. The EEA was not "not formulated with the aim of encouraging trade secret holders to invest in additional information security measures; proponents of the statute argued that the government should pay the costs of reducing economic espionage through law enforcement." Burstein, supra, at 949. The other statutes mentioned, with the possible exception of the Cybersecurity Act of 2009, suffer from the same malady. Given the nature of the threat described above, they are inadequate because they don't apply sufficient pressure on the private sector to protect themselves – and, by extension, the United States.

Further, there is nothing in the current economic espionage statutory regime that addresses the fact that companies often keep thefts of their proprietary information secret. "The only thing a company will protect more than its information is the fact that they've lost it." Fialka, supra, at 15. Evidence about Internet based attacks are difficult to obtain; even if it is obtained the perpetrators are often in another country. Burstein, supra, at 972 - 973. Even with private sector cooperation traditional economic espionage cases are difficult to assemble. Id. The failure of American companies to report trade secret theft only exacerbates the situation.

American CEOs seem more concerned with the bottom line than with the threats to national security posed by economic espionage. Recall the statement made by that American CEO : "We're in the business of making money for our stockholders. If we have to put jobs and technology in other countries, than we go ahead and do it." Meanwhile, Chinese engineers were "crawling all over" manufacturing facilities the CEO's company had moved to China. Fialka, supra, at 31 – 34. American companies simply do not seem to consider the larger question -

Continued on **page 21**

Protecting Against Economic Espionage, from page 20

"[I]f you're losing American jobs and American technology while simultaneously building an industrial base in China that will compete with you, there is in fact great damage going on." Id. at 39.

A Proposal: Standards for Trade Secret Protection and Criminal Liability for Failing to Meet Them

Whether we like it or not we have been engaged by China in a struggle that could cost the United States its position in the world. The United States, "the last superpower," would see itself displaced by a totalitarian regime that shows no sign of moving any closer to democracy. See David Shambaugh, The Year China Showed its Claws, Brookings Institution 1 (2010), available at http://www.brookings.edu/opinions/2010/0216_china_shambaugh.aspx. What happens after such a geopolitical shift of that magnitude occurs simply can't be good for the long term future of the United States.

Given these stakes, it is nothing short of reckless for American companies to allow their trade secrets to be stolen by foreign governments, especially when there is a solid probability that the foreign government is the PRC. However, the current statutory regime looks at these companies as "victims" who have no responsibility to protect their proprietary intellectual information beyond the minimum statutory requirements required to classify such property as "trade secrets."

As a first step, Congress needs to promulgate stringent standards that require American businesses to protect trade secrets above and beyond what it is currently required. Because trade secrets can be stolen both by human actors and by cyber attack, the standards need to incorporate provisions for both eventualities. Also, since successful cyber attacks can be accomplished by individuals thousands of miles away from their targets, the standards must apply to all U.S. businesses that have a presence in cyberspace. The standards can be calibrated to the size of the business and the economic and security impact the loss of a particular trade secret may cost the nation as a whole – looser standards for a hardware store as opposed to more stringent standards for a multinational corporation. These details can be worked out and are beyond the scope of this paper.

The greater question is how to enforce a set of standards promulgated by Congress to protect trade secrets. This paper has described the nature of the threat foreign economic espionage poses to the United States. Foreign economic espionage is not simply "a cost of doing business"; rather, it poses a long term strategic threat to the United States' position in the world. As such, the harm done by foreign economic espionage is not just to the companies involved but to the well being of the nation as a whole. Accordingly, it is well within Congress' purview to establish sanctions for those who fail to protect trade secrets according to Congress' specifications. Further, such sanctions should be criminal in nature.

But how can corporations and their agents be held criminally culpable? Are they not simply businesses doing business? The most important pillar in the foundation of criminal law is the concept of moral blameworthiness. That is, no one will convicted of (or punished for) a crime unless the act or omission was morally blameworthy. Stephen F. Smith, Proportionality And Federalization, 91 Va. L. Rev. 879, 882 (2005). The United States Supreme Court will demand that the "that the government prove moral culpability when statutory language might reach conduct that is 'not inevitably nefarious'; that is, conduct that is not inevitably blameworthy." John Shepard Wiley Jr., Not Guilty By Reason Of Blamelessness: Culpability In Federal Criminal Interpretation, 85 Va. L. Rev. 1021, 1035 (1999) quoting Ratzlaf v. United States, 510 U.S. 135, 144 (1994). Are companies who don't adhere to standards to protect trade secrets promulgated by Congress morally blameless? (The issue of fair notice is also germane to the question of culpability. Fair notice is largely a question of statutory drafting and beyond the scope of this paper).

In deeming whether conduct is criminally culpable, the Court has increasingly "construed

Continued on **page 22**

Protecting Against Economic Espionage, from page 21

federal statutes to impose broader mens rea requirements in cases in which the federal interest in regulating the subject matter at issue is comparatively high." Note, Mens Rea In Federal Criminal Law, 111 Harv. L. Rev. 2402, 2402 (1998). In the case of companies who fail to adequately protect their trade secrets, and thereby allow foreign nations who are competing with the United States to gain economic advantage, the federal interest is high indeed.

The specific level of moral culpability that fits into what the Supreme Court calls "broader mens rea requirements" is criminal recklessness. The Model Penal Code defines recklessness as the "material element of an offense when [the actor] consciously disregards a substantial and unjustifiable risk that the material element exists or will result from his conduct." Model Penal Code § 2.02(2)(c). Under the Model Penal Code recklessness is part of a descending order of culpability: purpose, knowledge, recklessness, and negligence. Id. at § 2.02(2). Federal criminal law, which is not based on the Model Penal Code, generally recognizes two levels of culpability: purpose and knowledge. Wiley, supra, at 1030. However, in its 1994 decision Posters 'N' Things v. United States the Supreme Court defined "knowledge" type culpability to mean:

Further, we do not think that the knowledge standard in this context requires knowledge on the defendant's part that a particular customer actually will use an item of drug paraphernalia with illegal drugs. It is sufficient that the defendant be aware that customers in general are likely to use the merchandise with drugs. Therefore, the Government must establish that the defendant knew that the items at issue are likely to be used with illegal drugs. Posters 'N' Things v. United States, 511 U.S. 513, 524 (1994).

Under this standard, therefore, a company that does not subscribe to standards promulgated by Congress to protect trade secrets would have to know only that its trade secrets are likely to be stolen by foreign interests – given the current global environment not a huge leap. In subsequent decisions, the Court has adhered to the rule of Posters 'N' Things. See Dixon v. United States, 548 U.S. 1, 5 (2006) quoting Bryan v. United States, 524 U.S. 184, 193 (1998) ("the term 'knowingly' merely requires proof of knowledge of the facts that constitute the offense."); see also Babbit v. Sweet Home, 515 U.S. 687, 701 (1995) ("Secretary's conclusion that activities not intended to harm an endangered species, such as habitat modification, may constitute unlawful takings under the ESA").

After being put on fair notice by Congress' promulgation of trade secrets protection standards, a company, under federal criminal culpability standards as interpreted by the Supreme Court, is guilty of criminal negligence if it does not meet those standards whether it intended for its trade secrets to be stolen or not.

Conclusion

China does not defeat its rivals, it absorbs or rejects them. The Mongol horde of Genghis Khan conquered China; by the time of his grandson Kublai's reign the Mongols were speaking Chinese. The same happened to the Manchus. The 19th century European imperial powers receded. Even the Japanese armies of World War II were slowly being swallowed by the Chinese.

Terrorists are capable of truly horrific acts and deserve the attention they receive from the U.S. national security apparatus. However, the United States continues to ship manufacturing capacity to China. The Chinese intelligence services continue to prod and pilfer U.S. technological and other trade secrets both here and in China. The absorption of the United States has begun.

We need tougher sanctions against those who would put profit before country. The long range costs to this country and its position in the world have far greater import than a particular company's stock price. ■

"Cyber Security: Responding to the Threat of Cyber Crime and Terrorism"

Statement of Stewart A. Baker

Partner, Steptoe & Johnson LLP Former Assistant Secretary for Policy, Department of Homeland Security

Before the Committee on the Judiciary Subcommittee on Crime and Terrorism United States Senate

April 12,2011

Good afternoon, Chairman Whitehouse, Ranking Member Kyl, and members of the subcommittee. My name is Stewart Baker. I have been involved in cybersecurity issues since the early 1990s, when I was General Counsel of the National Security Agency, and most recently as Assistant Secretary for Policy at the Department of Homeland Security during from 2005 to 2009. I appreciate the opportunity to address this vitally important issue.

Everyone knows that cybercrime is a problem. But everyone also seems to believe that the problem can be solved with modest additional effort.

In fact, cybercrime — and the vulnerabilities on which it feeds — will soon pose a profound challenge to our way of life, and perhaps even to America's role in the world.

Those who think the problem of cybercrime can be easily solved have embraced little myths that help them avoid taking harder steps.

I'd like to begin by identifying those myths and debunking them, because we won't begin to address the problem until we recognize that the easy solutions will not work. (I discussed several of these myths in my book, *Skating on Stilts*, and I've drawn on that material for today's testimony.)

Law Enforcement in Cyberspace Not Even a Myth

Before I do, though, I'd like to address one solution that isn't taken seriously enough to even qualify as a myth: the notion that law enforcement can solve the cybercrime problem. It is true that federal authorities occasionally catch and prosecute a successful hacker. But those successes are dwarfed by the massive number of uncaught, unprosecuted, and even unreported hacks that occur every day. Very few victims even bother to go to the authorities any more. It would be like complaining that someone stole a wallet from your unlocked car in a bad neighborhood. You know, and so do the authorities, that the chances of solving the crime are so remote that even going through the motions of a report and investigation isn't worth the trouble.

Most problems of social disorder are contained by the threat of punishment. Human society depends so profoundly on social punishment as a survival mechanism that it is built into our genes. We have reward centers in our brains that fire when we punish rule-breakers – even if we can expect no individual benefit from a change in the rule-breaker's future behavior. Many of us will even incur costs just to punish rule-breakers we will never see again. (I probably don't have to tell you that if you've ever driven in Washington traffic.)

Yet the ease with which attackers can hide in cyberspace makes it almost impossible to punish criminal conduct online. We simply cannot identify the criminals. And so we find ourselves trying to build an online society where there is no real punishment for lawless behavior.

"It is true that federal authorities occasionally catch and prosecute a successful hacker. But those successes are dwarfed by the massive number of uncaught, unprosecuted, and even unreported hacks that occur every day."

***Continued on* page 24**

Responding from the Threat, from page 23

Whether this is even possible is open to question. Those who think it is possible are counting on computer security – a bombproof defense – to make up for our inability to punish wrongdoers.

Counting on a bombproof defense would be a dubious proposal in the best of circumstances. It is particularly dubious when one realizes just how much of our defense is built on myths rather than reality.

The Myths That Keep Us from Dealing Squarely with the Cybersecurity Crisis

Myth 1: It's a Microsoft Problem.

I know plenty of people who still believe that Microsoft's products are uniquely insecure, and that we could solve the problem if we could just get Microsoft to clean up its act. For some, the security of Linux was an article of faith; its source code is open to inspection by anyone, so it is protected from exploit by all those watching eyes. And Apple, which didn't even offer an antivirus program for decades, was protected by Steve Jobs's sheer coolness.

The last few years have been hard on those illusions. As Apple gained market share, malware authors began writing for its operating system, and they didn't have any trouble finding holes. And all those eyes on Linux's code? In August of 2009, two Google researchers discovered a bug in the central core of Linux; it would allow an attacker to acquire complete administrative control of any machine to which he had physical access. You might call that a success for open source, except that the bug had been hiding in plain sight for at least eight years.

Why, then, is there so much more malware running on Windows than on Linux? Almost certainly for the same reason that there are more applications of every sort running on Windows than on Linux. Like other application developers, malware authors want to reach the largest number of users with one piece of code. And the way to do that is to write your application for Windows.

Myth 2: It's a Password Problem.

It's an article of faith among the security-conscious that passwords are a big security hole. People can't remember the hard ones, and hackers have assembled dictionaries of all the memorable ones. Plus, it's easy for hackers with access to a machine to capture the user's keystrokes as he types his password in.

So for real security, companies and government rely on tokens. RSA makes a common token. Every thirty seconds it displays a different security code, known only to the user and his network server. Even if a hacker could compromise my machine and record all my keystrokes, he couldn't know what the token was going to say thirty seconds from now. But hackers have demonstrated in two ways that tokens of this kind are no long-term solution. First, RSA recently announced that hackers had broken into RSA's network and compromised the security of the system. RSA is not providing a lot of details to the public, but it seems quite possible that, at least for some tokens, the hackers can now predict exactly what the token will say every thirty seconds, for years to come. And even those who cannot predict the token's future code have found a way to beat these token systems. Now, when the owner of a compromised machine starts typing in his temporary code, the malware immediately sends a real-time message to its sponsoring hacker. As the owner types, each digit is sent to the hacker, who simply logs in right along with the owner.

Myth 3: Really Important Transactions Can Be Confirmed Offline.

More sophisticated users know that their home machines simply cannot be trusted. To protect their financial accounts, they've locked them up; they may bank on line, but no serious money can leave their account unless the bank calls to verify the transaction.

In fact, even those who haven't locked everything down may get a verifying call. Like the credit card companies, mutual funds and financial institutions have stopped trusting their customers' computers. For risky transactions, they insist on offline, or out-of-band, confirmation.

Out-of-band communication is today's most common fail-safe solution for computer compromises. But using another line of communication won't solve the problem for long. Finding a truly

Continued on **page 25**

Responding from the Threat, from page 24

offline method of communication is going to get harder. Businesses and consumers are switching in large numbers to "voice over IP," or VoIP, telephony. They cannot resist the allure of bringing to voice communications the cheap, flexible features of Internet communications. But the switch means that they are also bringing to voice communications all the insecurity that plagues other Internet communications. In fact, telephone insecurity could be worse, as users download apps from unknown providers to no-name phones made cheap in the People's Republic of China, where hacking remains widespread. If an attacker who has compromised your computer's online bank account is also able to divert calls to your Internet telephone, then it will be easy for the attacker to confirm that you really do want to transfer your life savings to Moldova or Nigeria.

Myth 4: If Worse Comes to Worst, We'll Disconnect Our Critical Systems from the Internet.

The government used to have its own special illusion about security. Maybe our unclassified networks are compromised, Defense Department officials would say, but the classified networks are still bombproof. They can't be compromised because they aren't connected to the Internet. There's an "air gap" between the two. That assumes, of course, that network security decrees are perfectly enforced—and that the most important secrets are only discussed on classified networks—notions that contradict everything we know about human nature. But never mind, because the air gap illusion, too, has fallen prey to the exponential empowerment of hackers that we've seen in recent years.

The French navy's Rafale Marine jets train out of Villacoublay air base, in the southwest suburbs of Paris. These fighters are state of the art, packed with stealth and electronic warfare capabilities and capable of landing on carriers. But to do that, they first have to take off. And for two days in January 2009, the jets couldn't take off.

They'd been grounded by a hacker.

The "Conficker" computer worm had been exploiting vulnerabilities in Windows servers for months. It was the most ambitious computer infection in years. At the time it had infiltrated as many as 15 million machines around the world. One of the ways it spreads is by infecting the USB thumb drives that carry data from one machine to the next. Even classified or isolated networks could be captured if a bad thumb drive was used to transfer data to a machine on a secured network.

That's what grounded the French fighters. Before the navy even knew it was under attack, the worm was coursing through its internal network. Rushing to contain the damage, the navy told its staff not to turn on their machines, and its systems administrators began quarantining parts of the network.

Too late for Villacoublay. Its systems were already hosed.

The Rafale fighter downloads its flight plans, a far more efficient process than paper-based systems. But once the contagion had spread to Villacoublay no flight plans could be downloaded. Until an alternative method of delivering the flight plans could be cobbled together, the Rafales were no more useful than scrap iron. The French press reported the embarrassment in detail.

Perhaps as consolation, the papers were careful to note that things could have been worse—and were, in Great Britain. There, the French press said, twenty-four Royal Air Force bases and three-quarters of the Royal Navy Fleet had succumbed to Conficker. The British and French navies may have been unintended victims of a worm designed for criminal ends. But after Conficker, no one can believe that an air gap is a security fail-safe.

Indeed, the Deputy Secretary of Defense has acknowledged that hackers successfully jumped the air gap to compromise DOD's classified networks. And it is hard to believe that the Iranian government did not keep its Natanz enrichment plan far from the Internet – a tactic that evidently did not prevent the Stuxnet malware from making the jump via thumb drive.

Myth 5: They're Not Looking for Me.

The last of our illusions is that we're just not that interesting. Other people have more money. Other people have more valuable secrets. Who's going to come looking for me?

That's the last hope of every herd animal. The predators can't eat everyone. If you lie low and

Continued on **page 26**

Responding from the Threat, from page 25

blend in, they won't pick you.

Wrong on two counts, I'm afraid. First, take this test. Add up your savings, car value, house equity, and investments. Is the total over $65,000? If so, you've got a lot of company on the globe. Probably 10 percent of the world's 6.8 billion people have assets exceeding that amount—say 700 million in all. Being one in 700 million sounds like pretty good herd-animal odds until you realize that, for every person with more than $65,000, there are nine people with less. As computers become exponentially cheaper, most of those nine people will be able to get online. Then there will be nine people to see you as a rich outsider who deserves to be relieved of his assets. And another nine for your spouse, nine for your neighbor, and nine for each of your business partners. Maybe nine each for every person you know.

The world is already full of scam artists willing to work for less than minimum wage. Most of them know English and have access to the Internet. The relentless march of empowerment will soon give those scam artists new tools for finding and fleecing you.

They can send out ten million emails telling people that they've won the Spanish lottery. If one in ten thousand responds, even with great caution, that person has selected himself for fleecing, and the pitch can then be tailored precisely to his failings.

"In short, cybercrime is bad now, but it will be far worse in the future."

So what if that part of the scam is a bit labor intensive? There are as many as nine people with nothing better to do than sit around trying to get into the mark's head.

In fact, it's worse than that. Because Moore's Law is working for the outlaws too. The increasing speed of new computers means that outlaws can use the victim's own computer to decide whether he's interesting enough to rob.

Remember that real-time password-stealing program? Well, the thieves don't have to go looking for rich people to infect. Instead, they infect everyone, and let the malware find the rich ones. The password-stealing program consumes an infinitesimal part of a modern chip's processing power to run quietly in the background, watching and waiting until its victim logs on to one of about fifteen hundred predetermined financial sites. Anyone logging in to one of those sites, the authors figure, probably has enough money to be worth cleaning out.

So when an infected computer sets itself apart from the crowd by logging on to a financial site, the malware alerts its author, who can now focus on taking money from that computer's owner. Moore's Law has taken a lot of the work out of the hunt. And, thanks to the empowerment of information technology, it will keep making the job exponentially easier, year in and year out.

What Can We Do About Cybercrime?

In short, cybercrime is bad now, but it will be far worse in the future. The success of cybercriminals has already inspired more than a dozen governments to flirt with cyberweapons. And Stuxnet shows that some have moved beyond flirtation.

Stuxnet seems to have been highly targeted on the industrial control system for centrifuges in a single facility in Iran. But the tools it deployed could just as easily be used to bring down the power grid for a city or a region – and probably also to destroy the generating equipment on which the region depends, forcing city dwellers to live without power for weeks or months, if they can.

That kind of attack would change the nation. The leaders who failed to prevent the attack would be swept away, and massive changes would be made in our information networks to thwart future attacks.

Or perhaps we'll escape an international conflict. Even if we are that lucky, cybercrime will keep growing, for all the reasons I've already given. It is dead easy, and it pays remarkably well. We shouldn't wait for disaster if we can head it off.

The problem is that any change big enough to seriously address the problem is big enough to offend one or more well-represented lobby. With that in mind, and with some diffidence, let me sketch the kinds of changes that might change the direction in which we are traveling.

First, when you can't trust the devices on your network, which is increasingly true of all organizations, one successful defense seems to be back-office pattern recognition. The most obvious use of

Continued on **page 27**

Responding from the Threat, from page 26

this technique is the system that credit card companies use to stop suspicious transactions; anyone who has used a credit card in an unusual context is familiar with the "just checking" calls that come from the card issuer. We need to create incentives for companies to deploy such systems more widely. Two examples: US home computers are badly infected and widely used for bot attacks and other crime. The ISPs that carry traffic from these infected machines can often identify the machines from their pattern of behavior. But the ISPs have no incentive, and much disincentive, to notify the owners, or to quarantine or restrict the machine's access to the internet. Similarly, small businesses that have been compromised with key loggers cannot protect their Electronic Funds Transfer accounts from hackers on their own. The banks that receive unusual EFT requests are in a much better position to spot a fraud in the making, but today liability for that fraud rests on the business owner, not the bank. Again, finding a way to encourage banks to use their central position in the payment stream to identify EFT fraud would likely make fraud less attractive.

Another way to reduce cybercrime is to reduce anonymity in cyberspace. Better attribution of machines and users on networks will make it easier to punish lawbreakers, and without punishment of those who break the law, all the defenses in the world are not likely to succeed.

"Another way to reduce cybercrime is to reduce anonymity in cyberspace. Better attribution of machines and users on networks will make it easier to punish lawbreakers, and without punishment of those who break the law, all the defenses in the world are not likely to succeed."

There are no doubt other steps that could be taken, but at this point, the federal government doesn't even have authority to call on industry to take obviously needed security measures. The Defense Department lacks insight into the origins of critical supply-chain components. The federal government lacks authority to set high security standards for the industries on which our civilization depends. Congress has been considering bills to address these security gaps for many months; it's past time to enact one.

Finally, deep as this security hole is, we should at least stop digging. We should slow or stop initiatives that will increase our risk. The "smart grid" movement, for example, won't look so smart if it results in a whole new set of vulnerabilities for the populace as a whole; we need confidence in the entire security architecture before we deploy smart grid technology. By the same token, filling our telecommunications networks with unvetted equipment from vendors beholden to the Chinese government makes little sense, yet the administration apparently felt compelled to approve foreign vendors as the beneficiaries of federal broadband stimulus funds.

I offer these ideas not because they will all work or they are all the best possible solution but to show the kinds of changes that we must be willing to consider if we want to bend our extraordinarily risky trajectory. But if you kept track of the industries, the foreign governments, and the civil liberties groups likely to be offended just by that short list of possible measures, you understand why we are still sliding down a slope that leads to serious trouble.

Thank you for your attention. ■