Harvard National Security Journal
2011

Keynote Address

THE DEVELOPING LEGAL FRAMEWORK FOR DEFENSIVE AND OFFENSIVE CYBER OPERTIONS

(Excerpted)

Steven G. **Bradbury** [FNa1]

I. Introduction

Unlike the participants on your panels, I'm not a noted expert on cybersecurity. But I did have the privilege to serve as head of the Office of Legal Counsel in the Department of Justice for almost five years during the last administration, and in that position I did have occasion to advise on cybersecurity issues. And I've watched developments in the area of cybersecurity since my tenure in government.

What I'd like to do today is to sketch out the basic legal framework that I see developing to govern the cyber operations of the federal government. I want to talk, first, about the legal framework for defensive cybersecurity activities. Then I'll address legal authorities potentially applicable to offensive cyber operations, including cyberwarfare. Lastly, I'll say a word about possible responses to WikiLeaks.

II. Defensive Cyber Security Activities

Last year, in his confirmation hearing to lead the new U.S. Cyber Command, Gen. Keith Alexander, who is also Director of the National Security Agency, testified that the Defense Department's computer systems in the U.S. are bombarded with “hundreds of thousands” of hostile incursions each and every day. And that's just the Defense Department's networks.

All the computer systems of the federal government are vulnerable to infiltration and disruption from hostile foreign governments or other foreign powers, international criminal enterprises, and lone hackers.

And the concerns about network protection don't end at the outer bounds of the dot.mil or even the dot.gov cyber domains. We're also concerned about the serious national security threat to non-federal computer systems, including the networks of defense contractors working on sensitive projects, as well as the computers that control America's critical infrastructure, such as power plants and pipelines, electric grids, dams, water supply systems, air traffic control and rail

transportation systems, banking systems and financial exchanges, and health care networks.

Some folks -- notably, for example, Richard Clarke -- have gone further and have also urged that it's vital to our national security for the federal government to mandate steps to protect the public backbone networks of the Internet, including the major public peering points where backbone traffic is exchanged. I'm not convinced of that; I think that raises difficult issues, as I'll touch on in a bit.

Let's look initially at the federal government's computer systems, and then we can work our way out from there.

Defensive protections. So what is the capability we want to have in place to protect our vital networks?

Certainly, we'll want to be able to scrub the software and data *inside* our computer systems to find and eliminate any hostile viruses, worms, trapdoors, Trojan horses, logic bombs, etc., and to trace them back, if we can, to try to find out how they got in and where they originated.

But I want to focus now on the *perimeter* of the network, on the gateways where it connects to the public Internet or to any external web of networks beyond our control.

We'll want to be able to detect unwanted intrusions -- in real time, if possible, as they stream across the gateway. Ideally, we'd like to be able to block them before they cross the perimeter and enter the critical systems.

To spot the potentially malicious intrusions, we'll look for the known “signatures” of previously identified malware and hostile actors. We can collect our list of malicious “signatures” from all kinds of places -- from private firms that develop anti-virus software, from law enforcement units that investigate cyber crimes, from intrusions we've already detected in our networks, from our own intelligence agencies, and from foreign governments and their intelligence services.

The detection system will need to “learn” from new intrusions, so the list of screening signatures is constantly being refreshed.

To make this work, we'll need sophisticated, high-speed sensors that can search the enormous volume of data traffic without an unacceptable delay in communications.

It won't be enough to search just the “to” and “from” addressing information in each data packet; we'll absolutely need to search down deeper, into the content of messages, since malicious code can hide in any part of a message or its attachments.

We'll need to search outbound traffic as well as inbound, to detect the unauthorized exfiltration of sensitive information, and to identify any moles on the inside working with the infiltrators.

When we do detect a hostile intrusion, it won't be enough just to block it. We'll want law enforcement experts or intelligence analysts to be able to review it and we may want to take follow-up action, as necessary, directed against the source of the intrusion. That could mean action by the FBI, since maliciously disrupting or hacking into government computers is a federal crime, *or* it could mean action by our intelligence agencies or by the military, depending on the

nature of the intrusion.

EINSTEIN. It turns out the Department of Homeland Security is right now rolling out an intrusion-detection system that's designed to implement many of the capabilities I've just described. It's called "EINSTEIN," and it's meant to protect the unclassified civilian computer networks of the federal government.

EINSTEIN will work by making a mirror copy of all the data packets passing through the gateways, and then automatically screening the duplicate data stream for any malicious signature codes.

Only the messages found to contain malicious codes will be collected and further analyzed by humans; the rest of the copied data will be immediately deleted.

And the messages that are subject to further review will be handled in accordance with established "minimization procedures," which are requirements designed to avoid the unnecessary retention and distribution of non-public information about U.S. persons. For example, minimization would mean that the names of identified U.S. persons or content discussing U.S. persons will be masked when the message is sent on to law enforcement or intelligence agencies to the extent that such information is unnecessary to understanding the law enforcement or intelligence significance of the message.

These minimization procedures have been approved by the Attorney General, as well as by the Article III judges who sit on the Foreign Intelligence Surveillance Court.

DHS will also apply auditing and training procedures and adopt restrictions to ensure that the list of target signatures will focus only on malicious computer code and will not be used improperly to intrude on any legitimate privacy rights of the users of the network.

Legality. The federal government's implementation of a system like this raises a host of legal issues involving the constitutional and statutorily protected privacy rights of Americans. So how do we approach the question of legality?

Well, we have a roadmap in the opinions the Justice Department has issued analyzing the legality of EINSTEIN.

I signed a lengthy opinion on this topic for OLC in January 2009 that memorialized DOJ's analysis up to that point. The Obama administration adopted this opinion and made it public in August 2009, along with some follow-up advice from OLC. [FN1] (So, you see, it's not true that the current administration only publishes opinions of mine when it disagrees with them!)

Fourth Amendment protections. The most fundamental legal restriction at issue is the Fourth Amendment, which protects against an unreasonable search by the government that infringes a person's legitimate expectation of privacy. If the person doesn't have a reasonable expectation of privacy in the communications reviewed, there is no "search" under the Fourth Amendment. And where there is a search, the Fourth Amendment's basic requirement is reasonableness.

The courts have made it clear that for purposes of the Fourth Amendment, people who make a call or send an e-mail message or visit a Web site do not have a reasonable expectation of pri-

vacy in the phone number called or in the addressing and routing information for an Internet communication. [FN2]

Just like an address on the outside of an ordinary envelope, the to/from addressing information or Internet routing protocol for an e-mail or Web visit is information the sender is voluntarily making available to the communications provider in order to complete the connection, and the sender can't claim a reasonable expectation that that routing information is private.

That means there would be no "search" within the meaning of the Fourth Amendment if the government screened just the "to" and "from" lines of e-mails and other IP addressing data of Internet traffic for malicious signatures.

But here, as I said, we need to go beyond that; we *do* need to search the content and the attachments of all Internet messages. And that would definitely implicate the privacy interests that the Fourth Amendment is concerned with.

Statutory protections. Moreover, there are a number of federal statutes that impose separate and independent privacy protections beyond the Fourth Amendment. These include:

(1) the wiretap provisions of title 18, as amended by the Electronic Communications Privacy Act, 18 U.S.C. § 2510 *et seq.*, which protect e-mail messages while in transmission;

(2) the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, which protects electronic communications while stored in a database;

(3) the Foreign Intelligence Surveillance Act, or FISA, 50 U.S.C. § 1801 *et seq.*, which requires special court orders for electronic surveillance of wire communications in the U.S.; and

(4) the pen register and trap and trace provisions of title 18, 18 U.S.C. § 3121 *et seq.*, which provide protection for calling numbers and the to-and-from addressing information for e-mails.

Warrant vs. no warrant. Ordinarily, the Fourth Amendment requires that government officials obtain a warrant supported by probable cause to conduct a search. But a warrant, or any individualized court order, like a traditional FISA order or a pen register/trap and trace approval, is not possible here. We need to screen all the traffic coursing in and out of the gateway and we need to do so 24/7.

Fourth Amendment jurisprudence allows the government to conduct reasonable searches without a warrant in certain circumstances where the government has "special needs" going beyond law enforcement.

The need to protect the integrity of vital government computer networks from attack in the face of a massive number of unauthorized intrusions should constitute such a "special need," and the various conditions, limitations, and minimization efforts that DHS will use with EINSTEIN should be sufficient to assure the reasonableness of the search.

"Rights or property." Certain of the statutory protections at issue also permit the operator of a communications network to intercept and screen traffic on the network where and as necessary to protect the "rights or property" of the network operator.

Those provisions should also enable the government, as the network operator here, to conduct the kind of screening that EINSTEIN would entail, since it's reasonable to believe the

screening is necessary to detect and prevent harmful intrusions that could compromise the integrity of the networks.

Log-on banners and user agreements. But the federal government, with the advice of Justice Department lawyers, has settled on a simpler and broader solution as the principal legal foundation for EINSTEIN.

Each federal agency that participates in EINSTEIN will enter into a Memorandum of Agreement with DHS, and that MOA will obligate the agency to put in place detailed log-on banners, user agreements, and computer training programs for each employee, contractor, or agent who is authorized to use the agency's computer system.

The log-on banner and user agreements will declare that the computer system is for authorized government use only, and they'll clearly state that by using the system, the employee understands and consents that he or she has no reasonable expectation of privacy in communications passing through or stored on the system; that the government may monitor, intercept, or search any data transiting or stored on the system; and that any communication or data on the system may be disclosed or used for any authorized government purpose. To access the system, the user will have to sign a consent form or click a button acknowledging and agreeing to these terms. (The Justice Department has actually used a log-on banner like this for some years now.)

All agencies whose network traffic is screened by EINSTEIN must ensure that they consistently adopt, implement, and enforce these consent and notification procedures in their computer training and usage practices.

Fourth Amendment analysis. DOJ concluded that the consistent application of these log-on banners and agreements will be effective in establishing as a legal matter that the users of the agency's computer network will not have a reasonable expectation of privacy in any communications they send or receive over the network.

That will go for personal communications sent over the network, too, including employees' use of the network to access their own personal Gmail or Yahoo accounts or Facebook pages.

Without a reasonable expectation of privacy, there will be no “search” within the meaning of the Fourth Amendment.

The same conclusion will apply to a private individual outside the government who communicates with the agency or with an employee of the agency, including where the individual is communicating with the employee's personal e-mail account and doesn't know that the person on the other end is accessing the account from a government network.

The Supreme Court has held that “a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties,” [FN3] and that “when a person communicates to a third party even on the understanding that the communication is confidential, he cannot object ***599** if the third party conveys that information or records thereof to law enforcement authorities.” [FN4]

Statutory analysis. The log-on banners and user agreements described above will also ensure that the screening system will comply with all statutory privacy restrictions.

Each of the relevant statutes I mentioned -- the Electronic Communications Privacy Act, the Stored Communications Act, FISA, and the pen register/trap and trace laws -- permits the interception and disclosure of otherwise private communications if done with the "consent" of a party to the communication. Here, that means the consent of the individual employee or other user of the agency's computers.

Thus, the wiretap provisions of title 18, as amended by ECPA, provide that "[i]t shall not be unlawful ... for a person acting under color of law to intercept [or divulge] a[n] ... electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception [or divulging]." [FN5]

Similarly, the Stored Communications Act states that the provider of an electronic communications service "may divulge the contents of a communication ... with the lawful consent of the originator or an addressee or intended recipient of such communication." [FN6]

And the government does not engage in "electronic surveillance" within the meaning of FISA where it intercepts the contents of a wire communication with "the consent of any party" to the communication or in circumstances where a party to the communication lacks a reasonable expectation of privacy. [FN7]

Finally, the pen register and trap and trace provisions of title 18 do not apply to the use of such devices by the provider of an electronic communications service "where the consent of the user of th[e] service has been obtained." [FN8] In the case of EINSTEIN, the provider of the service would be the federal government.

So that's the analysis for federal government networks.

Expansion to certain non-federal networks. Now, can a system like EINSTEIN be expanded to cover private or state-operated networks that contain especially sensitive information or that control the nation's most critical infrastructure? Can we apply a similar legal analysis?

It should be pretty straightforward to do so, provided the network is owned or operated by a single entity or group of entities and is set up like an intranet with a limited set of authorized users, and provided the operator can agree by contract or can be required by regulation to use log-on banners and user agreements like those employed by the federal agencies participating in EINSTEIN.

Take, for example, a defense contractor working on a classified or sensitive weapons system. The government, as a condition of the contract, could require the contractor to ensure that all sensitive information about the project is confined to a discrete network and that all persons using the network understand and agree that their communications over the network, including personal communications, will be subject to monitoring and disclosure, including disclosure to the government. The contractor would be the provider of the electronic communications service and, with the consent of the users of the network, would be authorized under the various statutory provisions discussed above to conduct the monitoring of all communications on the network and make the disclosures of any communications containing malicious code. In undertaking the screening, the private party could contract with the federal government to participate in the EIN-

STEIN system.

I think DHS could negotiate similar cooperative arrangements with state entities and could impose similar conditions on computer networks, including private networks that are used to control the infrastructure most vital to national security. This should fall within DHS's regulatory authority over the security of "critical infrastructure."

If the non-federal network in question happens to be located in a state that requires the consent of both parties before a communication can lawfully be monitored, a valid federal requirement should preempt the state law, though in some circumstances, for example involving only contractual conditions, preemption may require an act of Congress.

Public Internet. What about trying to expand our intrusion-detection system out to the public Internet itself, to scour the vast streams of data that flow through the public peering points and across the gateways of the major backbone networks? Some have argued that that's the only way to achieve sufficient protection for vital U.S. computer networks.

But this is where I think I would draw the line. I don't see an easy way to dispel the legitimate privacy interests of the millions of users of the public Internet. We can't insist that they all consent to having their communications monitored, and I don't think the public would support such a policy.

Even if Congress in theory could enact some kind of sweeping legislation to impose such a regime -- for example, by requiring that all ISPs be licensed and making EINSTEIN-like user agreements a condition of licensing -- that's not realistic. The Internet culture would rise up in revolt, and Congress won't want to suppress the freedom and vibrancy of the Internet and risk squelching the golden goose of e-commerce.

So, one man's opinion, but I think we should focus on achieving cybersecurity for contained networks that have a discrete set of authorized users and readily controlled gateways to the Internet. But if we can do just that much, that will go a long way toward improving our national security.

III. Offensive Cyber Operations

Okay, that's enough about cyber security and privacy. Now let's do a 180 and talk about the legal authorities available to the U.S. government for offensive cyber operations.

By offensive cyber operations, I'm referring to a range of potential activities that could be aimed at foreign computer systems: from straight intelligence collection (the extraction or copying of data for intelligence purposes), to counterintelligence operations (meant to deter or disrupt espionage by others against us), to covert actions conducted abroad (traditionally managed by the CIA), to cyberwarfare (executed by DoD's Cyber Command, either in support of conventional, kinetic war fighting or on a stand-alone basis).

These various kinds of operations can be authorized under different authorities using different procedures.

I should step back here and note something important: If the computer system in question is located in the United States or if it's owned and controlled by a U.S. company or individual, it's likely the FBI would take the lead, and the operation may be conducted as a law enforcement matter.

Executive Order 12333. Executive Order 12333 provides a useful launching pad for reviewing these authorities and procedures. It mirrors several provisions of the National Security Act, found in chapter 15 of title 50 of the U.S. Code.

Intelligence and counterintelligence authorities flow from the President through the Director of National Intelligence, and they're usually vetted through an inter-agency process overseen by the National Security Council.

If they're sufficiently sensitive, they'll be reviewed by the principals committee of the NSC, which is typically chaired by the National Security Adviser and includes the Vice President, the Secretary of State, the Secretary of Defense, the DNI, the Attorney General, the Chairman of the Joint Chiefs, and often the Director of the CIA. Depending on the issues involved, the principals can include the Secretary of Homeland Security and the Secretary of the Treasury. The Chief of Staff and the Counsel to the President also usually attend principals meetings.

Covert action. Now, what about covert action?

As defined in Executive Order 12333 and the National Security Act, "covert action," as distinct from clandestine intelligence collection, means an operation undertaken by the U.S. government primarily designed "to influence political, economic, or military conditions abroad, where it is intended that the role of the United States Government will not be apparent or acknowledged publicly." [FN9]

What would be an example of covert action? Well, obviously, I can't talk about any real covert action of which I'm aware. But let's imagine a wild, fantastical, counterfactual, and purely hypothetical scenario that bears no relation to reality: Suppose the democracy protests in the Middle East were actually organized and fomented by the United States. If that were true, the United States would not want its role to be apparent, because that would doom the effort -- the local population would likely turn against the protests if they knew the United States was behind them.

Now, importantly, the definition of covert action does *not* include, among other things, "traditional counterintelligence activities" and "traditional military activities." (It also excludes diplomacy, law enforcement, and pure intelligence collection, but I'm going to focus mostly on the military exception, and I'll come back a little later to the counterintelligence exception.)

Covert action operations are traditionally conducted by the CIA with assistance as needed from the military and other intelligence agencies. Under Executive Order 12333, the National Security Council must consider each proposed covert action and present a policy recommendation to the President, along with any dissenting views.

Section 503 of the National Security Act, 50 U.S.C. § 413b, requires the President, in authorizing a covert action, to make written findings that the operation is necessary to promote

identifiable foreign policy objectives and is important to the national security of the United States, and it prohibits the President from authorizing any covert action that would violate the Constitution or any statute of the United States.

Covert actions also can't take place in the United States and can't be used to influence U.S. policies or public opinion. (So it would be illegal if the CIA were involved in organizing the union protests in Wisconsin.)

Congressional reporting. The National Security Act also requires the President and DNI to ensure that the Intelligence Committees of the House and Senate are fully and currently informed of all intelligence and counterintelligence activities, to the extent consistent with the protection of sensitive sources and methods or other exceptionally sensitive matters. [FN10]

With respect to covert actions, the Act requires the President to report presidential findings supporting covert actions to the Intelligence Committees, but where the President determines that it's essential because of "extraordinary circumstances affecting vital interests of the United States," the President may limit access to the so-called "Gang of Eight" -- the chairs and ranking members of the two Intelligence Committees, the Speaker and minority leader of the House, and the majority and minority leaders of the Senate, along with whatever other congressional leaders the President chooses to include. [FN11]

The committee chairs hate when briefings are limited to the Gang of Eight, because they catch hell from the members of their committees who are outside the circle. So when former-Senator Obama first became President, there was hope among some in Congress that he would eliminate the Gang of Eight briefings. But when Congress proposed an Intelligence Authorization bill that would do just that, President Obama threatened to veto it. Once he became head of the Executive Branch, he clearly understood the importance of being able to limit the scope of briefings for the most sensitive matters. So the statute still allows for Gang of Eight briefings.

In contrast to these title 50 intelligence activities, military operations conducted under title 10 authorities are subject to oversight by the Armed Services Committees of Congress. (Title 10 of the U.S. Code governs DoD's military authorities and the military command structure; title 50 governs the Intelligence Community and intelligence activities.)

And make no mistake, in the world of Washington, it really does matter whether an activity is characterized as covert action or a traditional military action because different Executive Branch departments or agencies will have ownership of the operation and different committees of Congress will have oversight jurisdiction, and they all jealously guard their respective domains.

Traditional military activities. So what *is* meant by "traditional military activities" and how do we apply it in classifying offensive cyber operations?

Note that it's not the case that an operation must be treated as covert action just because the role of the United States is intended to be secret. That's true of lots of military and counterintelligence missions as well. Think of special ops, military deception operations, or clandestine operations to prepare the environment for potential future military action.

And another thing: “traditional” can't refer to the technology being used. The military is always at the cutting edge in developing new war fighting technologies, and information systems and computer network operations are integral parts of war in the 21st century.

One possibility is to define “traditional military activities” by reference to the laws and customs of war.

The laws of war impose a number of very important limitations on when and how military force is to be used.

These include, for example, the basic principles of non-aggression and self-defense enshrined in the United Nations Charter; the humanitarian protections and restrictions on warfare embodied in the War Crimes Act, the Geneva Conventions, and related treaties and principles of customary international law; and the laws and treaty provisions prohibiting the use of certain types of weapons, such as chemical and biological weapons.

Some of the fundamental rules of war include the principle of military necessity (that an appropriate target is one that will confer a definite military advantage), the requirement to distinguish military forces from civilian populations, the prohibition on targeting civilians and civilian objects, the principle of proportionality of response, the imperative to minimize collateral damage, the ban on perfidy, and the principle of neutrality.

One thing that distinguishes the United States from lots of other nations is the care we take to honor our international commitments. In carrying out military missions, for example, DoD is scrupulous about always trying to comply with the laws and customs of war. You may be surprised to learn that it's quite often the norm these days for combatant commanders to make significant targeting decisions on the battlefield with the real-time input of JAG lawyers.

Military operations occur within the title 10 chain of command, which means that they're conducted pursuant to “execute orders” from the President through the SecDef down to the combatant commanders. Execute orders usually define the general scope and purpose of the operation, and the details are filled in with operational plans and specific rules of engagement. It's fair to assume that by the time the President signs an execute order for a particular military operation, DoD has satisfied itself that the operation can be conducted in accordance with the laws of war.

So, in my view, a good, practical way to think about “traditional military activities,” for purposes of distinguishing them from covert action, is that they can include any operation the President chooses to order the military to carry out under title 10 authorities, provided it's consistent with the accepted norms of war.

This approach preserves critical flexibility for the President in deciding when and how to employ the military might of the United States to meet a national security threat that justifies our use of force.

It should be recognized that in the context of our armed conflict with the Taliban and international terrorist organizations like al Qaeda, there will be a range of missions, including in the realm of cyber operations, where the President can decide to use either the military option or the ***607** covert action option, or both. They are two instruments of national policy available to the

President, and they need not be mutually exclusive.

The fact that the administration is standing up a unified Cyber Command and putting such focus and resources into it suggests that the President has largely decided to conduct offensive cyber operations through the military option.

Evolving customary law. This approach also accommodates the reality that how the U.S. chooses to use its armed forces will significantly influence the development of customary international law.

As the label implies, customary law can evolve depending on the accepted conduct of major nations like the United States. The real-world practice of the United States in adapting the use of its military to the new challenges raised by computer warfare will (and should) help clarify the accepted customs of war in areas where the limits are not clearly established today.

And if you just review the literature on cyber war, you quickly see that that's where we are: precisely how the laws and customs of war should apply to offensive cyber operations is not yet crystallized in key respects.

For example, there aren't always bright lines to tell us when a cyber attack on computer systems constitutes an "armed attack" or a "use of force" that justifies a nation in launching a responsive military strike under Article 51 of the U.N. Charter.

Some questions are easy: Hacking into a sensitive government computer system to steal information is an act of espionage, not an armed attack. It's clearly not prohibited by the laws and customs of war.

On the other hand, if the cyber intrusion inflicts significant physical destruction or loss of life by causing the failure of critical infrastructure, like a dam or water supply system, then it obviously would constitute an armed attack under the law of war and would justify a full military response if it could be attributed to a foreign power. Where committed as an offensive act of aggression, such an attack may violate international law.

If significant enough, the effect of the attack will determine its treatment, not necessarily whether the attack is delivered through computer lines as opposed to conventional weapons systems. In these cases, the laws and customs of war provide a clear rule to apply.

But there will be gray areas in the middle. Thus, it's far less clear that a computer assault that's limited to deleting or corrupting data or temporarily disabling or disrupting a computer network or some specific equipment associated with the network in a way that's not life threatening or widely destructive should be considered a use of force justifying military retaliation, even if the network belongs to the military or another government agency.

This was the case with the "distributed denial of service" attacks experienced by Estonia in 2007, which severely disrupted the country's banking and communications systems. Suspecting that Russia was behind it, Estonia suggested that NATO declare that Estonia's sovereignty had been attacked, which would have triggered the collective self-defense article of the NATO Treaty, but that suggestion was rebuffed on the ground that a cyber attack is not a clear military action. [FN12]

There's an echo of that reasoning in Article 41 of the U.N. Charter, which says that a "complete or partial interruption of economic relations and of rail, sea, air, postal, telegraphic, radio, and other means of communications" is not a "measure ... involving armed force."

And what about Stuxnet? As I understand it from public reports, Stuxnet was a computer worm that found its way into the systems controlling Iran's nuclear program and gave faulty commands causing the destruction of the centrifuges used for enriching uranium. Suppose President Ahmadinejad claimed that Israel was behind the Stuxnet worm and claimed that Stuxnet constituted an armed attack on Iran that justified a military response against Israel. I suspect the United States would disagree.

At the same time, when it comes to a cyber attack directed against U.S. computer systems, I certainly want the President to have leeway in determining whether or not to treat the attack as a use of force that supports military retaliation. Making such judgments is a traditional power exercised by the President, and I think he retains that leeway.

Similarly, I submit, it's not clearly established that a cyber attack aimed at disrupting a server or Web site located in a neutral country or in a country outside a theater of open hostilities would be a violation of that country's neutrality.

The server might be a valid military target because it's being used for the communications or command and control of the enemy fighters in the area of hostilities (after all, al Qaeda regularly uses the Internet in planning and ordering operations). The server might have no connection to the host country's military, government, or critical infrastructure, and it might be readily targeted for a computer attack without inflicting widespread damage on unrelated systems used for civilian purposes.

Such a focused cyber operation -- with little physical impact beyond the destruction of data or the crippling of a server -- is very different from the kind of physical violation of territory -- such as a conventional troop incursion or a kinetic bombing raid -- that we ordinarily think of as constituting an affront to neutrality. [FN13]

Although every server has a physical location, the Internet is not segmented along national borders, and the enemy may gain greater tactical advantage from a server hosted half way around the world than from one located right in the middle of hostilities.

The targeting of a server in a third country may well raise significant diplomatic difficulties (and I wouldn't minimize those), but I don't think the law-of-war principle of neutrality categorically precludes the President from authorizing such an operation by an execute order to Cyber Command.

Conclusion. So here's my thesis: To my view, the lack of clarity on certain of these issues under international law means that with respect to those issues, the President is free to decide, as a policy matter, where and how the lines should be drawn on the limits of traditional military power in the sphere of cyberspace. For example, that means that within certain parameters, the President could decide when and to what extent military cyber operations may target computers located outside areas of hot fighting that the enemy is using for military advantage. And when a

cyber attack is directed at us, the President can decide, as a matter of national policy, whether and when to treat it as an act of war.

The corollary to all this is that in situations where the customs of war, in fact, are not crystallized, the lawyers at the State Department and the Justice Department shouldn't make up new red lines -- out of some aspirational sense of what they think international law ought to be -- that end up putting dangerous limitations on the options available to the United States. Certainly, the advice of lawyers is always important, especially so where the legal lines are established or firmly suggested. No one would contend that the laws of war have no application to cyber operations or that cyberspace is a law-free zone. But it's not the role of the lawyers to make up new lines that don't yet exist in a way that preempts the development of policy. [FN14]

In the face of this lack of clarity on key questions, some advocate for the negotiation of a new international convention on cyberwarfare -- perhaps a kind of arms control agreement for cyber weapons. I believe there is no foreseeable prospect that that will happen. Instead, the outlines of accepted norms and limitations in this area will develop through the practice of leading nations. And the policy decisions made by the United States in response to particular events will have great influence in shaping those international norms. I think that's the way we should want it to work.

One final admonition I'll offer on the topic of offensive cyber operations: In cases where the President shapes new policy by choosing military action over covert action for a cyber operation, or vice versa, I would strongly urge that the President fully brief both sets of committees in Congress -- the Intelligence Committees and the Armed Services Committees -- and explain the basis for the choice. It's inevitable the committees will find out anyway when a jurisdictional marker is crossed, and it will help smooth the development of consistent policies and standards for the committee members and staff to understand and appreciate the choices made on both sides of the question.

IV. WikiLeaks

Now, as a last word, let me say something about WikiLeaks.

There's been a lot of focus on whether to bring criminal charges against Julian Assange for the purposeful exploitation and release of classified U.S. information, including military and diplomatic communications. A criminal investigation is evidently ongoing, and I think there are strong arguments supporting that course.

But there's also been a suggestion that we consider using offensive cyber capabilities to block or disrupt the servers overseas where WikiLeaks is holding the sensitive U.S. information.

If such an action were to be entertained, I don't think it would be characterized as a traditional military operation (we're not engaged in an armed conflict with WikiLeaks), and it wouldn't have to be done as covert action. Rather, I think it could be characterized as “traditional counterintelligence activities,” which you'll recall is another category that's distinguished from covert

action.

Executive Order 12333 defines "counterintelligence" to include, among other things, "activities conducted to ... disrupt or protect against espionage ... [or] sabotage" directed against the United States by "foreign powers, organizations, or persons." I think it can be argued quite easily that the WikiLeaks crusade to exfiltrate sensitive U.S. information and selectively disclose it in order to undermine and weaken American foreign policy does constitute espionage or sabotage.

But that doesn't mean that such an operation would or should be approved. It would undoubtedly be considered an exceptionally sensitive proposal and would be thoroughly debated by the principals of the National Security Council, as contemplated by Executive Order 12333. (And I wouldn't be surprised to learn that the principals committee actually has discussed just this possibility.)

The idea would certainly raise serious difficulties. If the servers were located in a friendly western country like Sweden, the notion of launching a cyber operation would cause major diplomatic heartburn, and the State Department would almost certainly insist that it be closely coordinated with the host country. There's also the strong chance that any such operation would be futile. I understand from news reports that Assange has stored copies of the stolen data set on scores of servers around the world, many of which are not connected to the Internet, as well as on lots of thumb drives that he and his compatriots carry around in their backpacks.

In the end, therefore, I think the President and his advisers would probably determine that it wasn't prudent and it wasn't practical to rely on a cyber response to WikiLeaks. And I suspect that's the conclusion they reached.

* * *

So with that anti-climax, let me end there.

[FNa1]. Partner, Dechert, LLP. This speech was delivered as the Keynote Address at the *Harvard National Security Journal* Symposium, Cybersecurity: Law, Privacy, and Warfare in a Digital World (Mar 4. 2011).

[FN1]. *See* Legal Issues Relating to the Testing, Use, and Deployment of an Intrusion-Detection Sys. (EINSTEIN 2.0) to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. (2009); Legality of Intrusion-Detection System to Protect Unclassified Computer Networks in the Exec. Branch, 33 Op. O.L.C. (2009).

[FN2]. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743-44 (1979); Quon v. Arch Wireless Operating Co., 529 F.3d 892, 904-05 (9th Cir. 2008).

[FN3]. *Smith*, 442 U.S. at 743-44 (1979).

[FN4]. SEC v. Jerry T. O'Brien, Inc., 467 U.S. 735, 743 (1984). Even if it were correctly decided, the Sixth Circuit's recent decision in *United States v. Warshak* holding that a person retains a reasonable expectation of privacy in personal e-mails stored with his ISP does not contradict this reasoning. *See* United States v. Warshak, 631 F.3d 266, 282-88 (6th Cir. 2010). While a person may reasonably expect to maintain personal control over the dissemination of e-mails he has stored on his own Web account or with his ISP, a person can no longer expect to retain control over a message he dispatches to its intended recipient. The difference is well illustrated by analogy to the world of paper files: If I send you a letter, I relinquish control over that letter to you; you're free to share it with whomever you will, regardless of any commitment I may have gotten from you. On the other hand, if I keep a copy of the letter stored in my own filing cabinet, I retain control over dissemination of the copy and I continue to have an expectation that the copy will remain private. That expectation does not necessarily change if my filing cabinet is located in a rented storage garage, even though the proprietor of the storage garage retains a master key for necessary access to the garage. In that analogy, the proprietor of the storage garage is like the ISP in *Warshak*.

[FN5]. 18 U.S.C. §§ 2511(2)(c), 2511(3)(b)(ii).

[FN6]. *Id.* § 2702(b)(3).

[FN7]. 50 U.S.C. §§ 1801(f)(2), 1801(f)(4).

[FN8]. 18 U.S.C. § 3121(b)(3).

[FN9]. 50 U.S.C. § 413b(e).

[FN10]. 50 U.S.C. §§ 413-413a.

[FN11]. *Id.* § 413b.

[FN12]. *See* Maj. Arie J. Schaap, *Cyber Warfare Operations: Development and Use Under International Law*, 64 AIR FORCE L. REV. 121, 144-45 (2009).

[FN13]. A 1974 Resolution of the U.N. General Assembly, for example, defines “aggression” to mean “the use of armed force” by a state against “the sovereignty, territorial integrity or political independence” of another state. G.A. Res. 3314 (XXIX), U.N. GAOR, 29th Sess., Supp. No. 31, U.N. Doc A/9361 (Dec. 14, 1974). The focused cyber operation I've described hardly seems to satisfy that definition.

[FN14]. The “Martens Clause,” found in the Hague Conventions and in Additional Protocol I to the Geneva Conventions, does not undercut this thesis. The version of the Martens Clause codified in Protocol I declares that on law-of-war matters not expressly addressed by treaty, “civilians and combatants remain under the protection and authority of the principles of international law derived from established custom, from the principles of humanity and from the dictates of public conscience.” Protocol Additional to the Geneva Conventions of 12 August 1949, and Relating to the Protection of Victims of International Armed Conflicts (Protocol I) art. 1.2, June 8, 1977, 1125 U.N.T.S. 3. There is no accepted or definitive interpretation of this clause, see Rupert Ticehurst, *The Martens Clause and the Laws of Armed Conflict*, 37 INT'L REV. RED CROSS 125 (1997), but I believe the most it can stand for is the proposition that if there are gaps in the provisions of a treaty addressing the laws of war, those gaps may be filled in by customary international law -- i.e., the customs of war -- as established by the consistent practice of major states (and perhaps by the universal humanitarian dictates of conscience). When there is, however, no such established and consistent practice of states (or universal dictates of conscience) as to a particular question, there is not a firm rule to fill in the gaps. That's fully consistent with the notion that the United States has flexibility as a policy matter to develop the appropriate standards it will recognize as applicable to offensive cyber operations with respect to those key questions about which there is no clear international norm.

2 Harv. Nat'l Sec. J. 591