Countering State-Sponsored Cyber Attacks: Who Should Lead?

Mr. Levon (Rick) Anderson
United States Army

> *Our Nation's critical infrastructures consist of the physical and cyber assets of public and private institutions in several sectors: agriculture, food, water, public health, emergency services, government, defense industrial base, information and telecommunications, energy, transportation, banking and finance, chemicals and hazardous materials, and postal and shipping. Cyberspace is the nervous system of these infrastructures--the control system of our country. Cyberspace comprises hundreds of thousands of interconnected computers, servers, routers, switches, and fiber optic cables that make our critical infrastructures work. Thus, the healthy functioning of cyber space is essential to our economy and national security.*[1]
>
> —The National Strategy to Secure Cyberspace, 2003

What is cyberspace? How important is it to the overall United States National Strategy? The opening paragraph (cited above) in the introductory section of *The National Strategy to Secure Cyberspace* sums up the importance of cyberspace to the United States very clearly. An attack needing U.S. federal government response (counterattack) is defined as "a deliberate attempt by a state-sponsored or other organized group to destroy or threaten lives, property, the economy, and/or national security."[2] An organized-group could be any group that may pose a legitimate threat to the United States government and national security (including terrorist or insurgent organizations). An actual state-sponsored or organized group controlled cyber attack could undermine the U.S. information network infrastructure and disrupt the nation's functioning sectors—public, private, and governmental.[3] Once a cyber attack on the U.S. is determined or confirmed to have been conducted by a state-sponsored or other organized group, should the Department of Homeland Security (DHS) or Department of Defense (DoD) lead the cyber counterattack? The purpose of this paper is to attempt to determine which federal government organization should lead the cyber attack/counterattack against state-sponsored or organized group cyber attacks on the United States homeland. It will discuss background information on cyberspace, current cyberspace roles of DHS and DoD, and other key players of cyber defense; provide a comparative analysis of DHS and DoD as lead for cyber attack/counterattack; present the results of analysis; and finish with recommendations and conclusions.

Background of Cyber Defense/Attack

The threat of a state-sponsored or organized-group (e.g., terrorist) cyber attack is a growing concern for many government and private strategists.[4] Many historians and military experts believe that in future wars, seizing and dominating information operations (including cyberspace) will be critical to winning the war. Indeed, the domination of information could be as important as dominating the air, sea and land battles today.[5] Understanding the role of cyberspace is critical to an effective national defense. We are quickly approaching an era when information systems will be being controlled, managed, and protected as weapon systems.[6] If the United States is attacked, it is a foregone conclusion that the United States will retaliate and make every attempt to seize the offense with an active defense.[7]

There is convincing evidence that other countries are already assigning a high priority to cyberspace and information warfare in their national and military strategies. "We are already at war in cyberspace," according to Lani Kass, director of the Air Force's Cyber Task Force. She claims countries and terrorists use cyberspace to wage asymmetric attacks on U.S. interests. "Countries such as China have been trying to extricate information from U.S. networks for more than a decade," Kass said. She added that "Chinese attacks on DoD networks are on the upswing, and China is now the United States' peer competitor in cyberspace."[8] China, like many other countries, including the U.S., is likely to sustain cyber attacks throughout any type of conflict (kinetic or non-kinetic). If not countered effectively, a well-planned and executed cyber attack could significantly cripple the use of a country's critical infrastructure and could possibly provide the deciding blow for the attacker.

It is no secret that the United States has already detected preliminary cyber espionage activities from other state-sponsored or organized groups.[9] If our information systems are blatantly attacked, could we effectively defend and ultimately counterattack in a coordinated manner? This would be a huge coordinating effort. There are many security and control levels for all the Information Technology (IT) systems in the United States. Federal information systems appear to be protected by more stringent security measures than private and public systems. To improve the Nation's cyber security, the federal government may consider imposing stricter collaboration security requirements on public and private systems, as well as on state and local governments, especially those critical infrastructure systems that have national implications. These measures may be required to form a more cohesive team to fight and win the cyber war. The Hurricane Katrina incident proved our need to improve our response to emergencies at all levels.[10] A cyber war could significantly magnify the coordinating effort—nationally. The recommendation in the 2003 National Strategy to Secure Cyberspace that stated "state and local governments are encouraged to establish IT security programs for their departments and agencies, including awareness, audits, and standards"[11] seems too passive. In a major cyber attack, all U.S. citizens could be affected and almost all of them would be involved during the response and recovery/reconstruction phases of a cyber attack:

> *Cyber attacks on U.S. information networks can have serious consequences such as disrupting critical operations, causing loss of revenue and intellectual property, or loss of life. Countering such attacks requires the development of robust capabilities where they do not exist today if we are to reduce vulnerabilities and deter those with the capabilities and intent to harm our critical infrastructure.*[12]

Cyberspace is a critical component of our infrastructure; it is totally interconnected to the network and systems beyond the U.S. control and boundaries. Cyberspace's incredible global reach transcends all perceived country or even continental borders. The U.S. has become helplessly dependent on the Internet.

> *Our economy and national security are fully dependent upon information technology and the information infrastructure. At the core of the information infrastructure upon which we depend is the Internet, a system originally designed to share unclassified research among scientists who were assumed to be uninterested in abusing the network. It is that same Internet that today connects millions of other computer networks making most of the nation's essential services and infrastructures work. These computer networks also control physical objects such as electrical transformers, trains, pipeline, pumps, chemical vats, radars, and stock markets, all of which exist beyond cyberspace.*[13]

With the outburst of globalization and the increased need to have more, better and faster service or products, IT is becoming more cumbersome and more complex than ever. This complexity creates coordination problems for any organization or country fighting the cyber war. This paper seeks to determine which U.S. organization is better equipped or positioned to lead the coordinated response to a confirmed cyber attack on U.S. information systems and critical infrastructure. Considering current roles, policies, and the criticality of cyberspace to the United States, DHS and DoD are the most likely government departments to lead the fight against a state-sponsored or organized group cyber attack.

Department of Homeland Security Role in Cyber Attack/Defense

Should DHS serve as the lead organization for cyber counterattacks against state-sponsored or organized group cyber attacks on U.S. cyber assets? The current role of the DHS is to secure the homeland—not a small task. This clearly includes the cyber war which is major part of the U.S. infrastructure. The 2002 *National Strategy for Homeland Security* seems to focus only on terrorist attacks on the homeland. Consider its definition of homeland security: "Homeland security is a concerted national effort to prevent terrorist attacks within the United States, reduce America's vulnerability to terrorism, and minimize the damage and recover from attacks that do occur."[14] This somewhat limited definition was produced in 2002 shortly after the DHS was created as a new cabinet-level department. Not all potential organized cyber attacks on the United States homeland will be conducted by terrorists. All the attention on terrorists, especially during the time the 2002 Homeland Security document was developed, may have been a significant contributing factor for this document's seemingly exclusive focus on terrorism—a very limited view of the cyber enemy or U.S. enemies in general. The U.S. must be prepared to fight the cyber war on U.S. territory against any type of adversary that threatens our national security.

The DHS mission is to protect the U.S. homeland from attack or from natural disasters. However, the cyber world is a different world—it has no rigorous boundaries. What happens when a cyber attack extends outside of the United States? Is countering such an attack still a DHS mission? There could be more than 100 federal, state, public, private, and international organizations that DHS must coordinate with to secure the homeland.[15] The DHS has established its organization as the focal point for managing U.S. domestic cyber incidents, including protecting the national critical information infrastructures. The DHS effort has focused mainly on cyber security measures. The Secretary of Homeland Security certainly has important responsibilities in cyberspace security, including developing a comprehensive national responsive plan for securing the critical infrastructures and resources of the U.S., as well as information technology and telecommunications systems (including satellites) and the physical and technological assets that support these systems.[16]

The Department of Homeland Security has been building and improving a very responsive system for sharing cyber information across the government and throughout the public and private sectors.[17] A robust system of this type must become operational as quickly as possible, no matter which federal agency leads the cyber fight against state-sponsored or organized group cyber attacks. So DHS has already assumed significant training and operational responsibilities to support the nation's cyber defense strategy, and this DHS responsive information sharing system is an integral part in the cyber defense/counterattack process. If DHS's mission area or span of control is limited to U.S. territory, can it legally conduct a cyber attack against a state-sponsored or organized group outside of the U.S.? Or should DoD lead the cyber attack mission?

Because of its on-going national coordination and response effort, DHS will be one of the first government organizations to determine when a cyber attack has been launched.[18] Neither the DHS nor any other agency has the ability to instantly determine if an attack has been launched by an individual or by a state-sponsored organization.[19] There is no certain way to know initially when a system is experiencing normal or routine hacks by inexperience hackers (commonly called script kiddies), seasoned hackers, or organized groups that are staging a cyber-war on the United States. "The speed and anonymity of cyber attacks makes distinguishing among the actions of terrorists, criminals, and nation-states difficult, a task which often occurs only after the fact, if at all. Therefore, the *National Strategy to Secure Cyberspace* works to reduce the U.S. vulnerability to debilitating attacks against our critical information infrastructures or the physical assets that support them."[20]

The strategy warns that "In wartime or crisis, adversaries may seek to intimidate the Nation's political leaders by attacking critical infrastructures and key economic functions or eroding public confidence in information systems."[21]

Department of Defense (DoD) Current Role in Cyber Attack on United States

The Department of Defense has steadily forged ahead of other agencies in planning for war against cyberspace adversaries. The Defense Department has been fighting the defensive cyber war with the Chinese and others and is equipped to conduct cyber attack if needed. The Department, in particular its military organizations, is dealing with the cyber espionage daily. The U.S. military has a robust information assurance program that strongly promotes the concept of "defense in depth," employing critical network systems that use the data/information security classification system effectively to reduce compromise of sensitive information. The examples that follow illustrate some of the DoD organizations that are blistering the trails in cyberspace.

A recent article, "Air Force to Create Cyber Command," described U.S. Air Force plans to create a Cyber Command to bring full-scale military operations to cyberspace, although no one knows whether the tactics and policies that the DoD currently uses to wage war will be effective on the cyber battlefield.[22] The Air Force is just one of DoD's examples of the military services' dedication to combating cyber problems.

The Joint Task Force-Global Network Operations (JTF-GNO) of the United States Strategic Command is the DoD organization chiefly responsible for operating and defending the DoD information infrastructure.[23] The JTF-GNO serves as the joint authority that coordinates and synchronizes all the military services and other DoD organizations' cyber actions. Much of the information about Computer Network Operations, which includes defense against cyber attacks and security breaches, as well as the related area of offensive computer network attack, are classified.[24]

One of the key DoD agencies for using and controlling cyberspace spectrum is the National Security Agency (NSA). NSA has a highly technical and efficient staff that supports DoD and other agencies in cyber actions. Details on the type of support to these organizations are sensitive and in some cases classified. NSA serves as a leader in computer network operations.[25] Although technically aligned with the DoD, NSA could offer some real advantages in leading the cyber war and could serve as the catalyst for merging the security-defense mission challenges between DHS, DoD, and others.

Other Key Players/Actors in Cyber War

Since information has become even more important to fighting and winning wars, it has become a viable critical vulnerability. Information dominance and superiority are now crucial to winning the war (kinetic or non-kinetic). Fighting and winning a cyber war has become a national effort. It is everyone's war.

> *Protecting the widely distributed assets of cyberspace requires the efforts of many Americans. The Federal government alone cannot sufficiently defend America's cyberspace. Our traditions of federalism and limited government require that*

> *organizations outside the federal government take the lead in many of these efforts. Every American who can contribute to securing part of cyberspace is encouraged to do so. The federal government invites the creation of, participation in public – private partnerships to raise cyber security awareness, train personnel, stimulate market forces, improve technology, identify and remediate vulnerabilities, exchange information, and plan recovery operations.*[26]

Private industry is a critical player in cyber war and plays a very important role in securing, defending, and protecting the U.S. infrastructure from cyber incidents. Industry, along with government research, will enable the U.S. to sustain its technological advantage by producing the best and most secure products. Industry will also play a key role in developing and implementing the best processes and advanced tools to combat cyber attacks. U.S. businesses must also be sensitive to national policies for preserving the technological advantage and honor the trade laws and policy on such matters as patents. The DHS has begun working with the private and public sectors on general awareness, as well as on specific issues impacting particular sectors.[27] The private sector owns and operates most of the U.S. cyberspace infrastructure.[28] Businesses are long-time partners in the effort to secure cyberspace, and many key players in the industrial sectors have developed plans to support *The National Strategy to Secure Cyberspace* by strengthening the security of their critical infrastructures.[29]

Although the private sector is an integral part of the overall cyber defense effort, more of the management burden and responsibility on active defense[30] must be assumed by the national government. Genuine defense requires the exercise of sovereign power, and implementation of active measures will have national impact.[31] The effects of cyber war on businesses could also jeopardize economic stability and disrupt the services of the personal computers of the general public.[32] Although the private sector may have better technology and excellent experienced personnel, the response to cyber attacks affecting national resources or assets must be provided to the government for monitoring, and command and control purposes in support of a national or international coordinated effort. The private sector should continue to clean or stabilize internal systems but must follow the government's lead and advice if forensic or other evidence is solicited.

> *In general, the private sector is best equipped and structured to respond to an evolving cyber threat. There are specific instances, however, where federal government responses are most appropriate and justified. Looking inward, providing continuity if government requires ensuring the safety of its own cyber infrastructure and those assets required for supporting its essential missions and services. Externally, a government role in cyber security is warranted in cases where high transaction costs or legal barriers lead to significant coordination problems, cases in which governments operate in the absence of private sectors forces.*[33]

The general public of the United States is also a key player in protecting the nation's cyberspace. Given customer awareness training and education on the impact of a cyber attack to the U.S. infrastructure, the American public will be more inclined to do their part in this all-inclusive effort to win the cyber war. Although home computers are not considered part of the critical infrastructure, the expanse of the internet has made all systems connected to the internet possible "spoofing" targets. Spoofing occurs when hackers at all levels (including state-sponsored or organized group) actually use another person's home or office computer to hack into another computer (personal , industry, or government) or to carry a malicious code (e.g., virus, worm, etc…) payload to any other unprotected computer.[34] The malicious code could also penetrate a protected computer if the receiver thinks actions are originating from legitimate source—therefore trusted.

The DHS is working with the Department of Education and state and local governments to work with the general public (home users, students, children, and small businesses) on basic cyberspace safety and security.[35] Many believe vendors should play a more proactive role in ensuring home computers are secure. Even so, the general public must take their role seriously. But does recruiting the general public as cyber defense team members present legal concerns for the government entities involved in or leading the a cyber war?

The international community, which includes all the non-U.S. countries that are conceivably connected to the global network via the internet, is another very important player. Their roles could influence who leads the cyber fight. The only way to possibly fight and win the cyber war is to ensure at a minimum that our current allies support our effort to fight a global cyber war. The United States has recognized the importance of international involvement and commitment in cyber affairs and has engaged in several initiatives to help pave the way to fight the cyber war.[36] This issue has been made more noticeable with constant attacks by individual hackers from other countries.[37] These individual hackers could actually be fronting for a state-sponsored or organized group attack. To engage in effective dialogue with the international community on cyber war issues, the United States should first try to establish working relationships through current treaties and agreements.

It may be impossible to solve cyber incidents if the international community does not agree to share cyberspace to pursue or track cyber crime or attacks. Cooperation from the international community is critical; it will allow Internet service providers in different nations to create alliances to counter cyber crime or cyber attacks.

> *America's cyberspace joins the United States to the rest of the world. A network of networks spans the solar system and allows malicious actors on one continent to act on systems thousands of miles away. Cyber attacks cross borders at light speed, and discerning the source of malicious activity is difficult. America must be capable of safeguarding, and defending its critical systems and networks. Enabling our ability to do so requires a system of international cooperation to facilitate information sharing, reduce vulnerabilities, and deter malicious actors.*[38]

The legal policies of these cooperating states should not conflict with each other. The technical problems of pursuit and detection become more difficult if one or more of the nations involved has a legal policy that conflicts with that of the United States.[39]

Some observers claim that international cooperation such as that of the Council of Europe is very important for defending against cyber attacks and improving global cyber security. But others point out that the treaty also contains a questionable protocol that violates the First Amendment of the U.S. Constitution.[40] Also, other laws that are being developed to address computer espionage and computer network attacks have clearly different legal characteristics. Computer network espionage, like any form of pure espionage, is not prohibited by international law,[41] but it is usually not lawful under domestic law of the targeted state. Computer network espionage usually involves very little, if any, force; it involves only as much intrusion as necessary to collect the required information from the adversary's systems.[42] Computer network attack, on the other hand, involves some kind of destruction with consequences in the physical world. Computer network attacks should be analyzed like any other use of force. Depending on the scope, duration, and intensity of the force employed, it may rise to the level of armed attack.[43]

Several U.S. interagency players are also critical for fighting and winning the cyber war and will have significant roles throughout cyber conflict. This analysis focuses primarily on what many believe are the obvious agencies (DHS and DoD) to lead the United States cyber effort against an organized cyber attack. These other key players offer some special capabilities and strategic viewpoints that must be considered when developing and assigning critical roles and responsibilities for fighting the cyber war, including the recovery/reconstruction phase. This analysis considers some of the major organizations with significant supporting roles in the cyber war, such as the Department of State (DoS) and Department of Justice (DoJ).

A case could be made for the DoS to play a lead role in reconstruction if the cyber war is fought on several international fronts. The DoS has very limited resources, some intra-departmental experience with modern cyber war technology, and possibly limited legal authority to engage in a war on U.S. territory in terms of United States Code (USC), Title 10 responsibilities which include attacking the enemy. However, cyber war pre- and post-hostilities' requirements and diplomatic functions in the international world should warrant strong consideration for DoS to assume lead role in post-hostilities cyber war, specifically the reconstruction involving international players. DoS would possibly also have the critical and dubious role (mentioned earlier) in establishing international agreements and treaties to legally take the cyber fight across the globe. The DoS chairs the interagency International Critical Infrastructure Protection Working Group. This group serves as an interagency coordination mechanism on international cyber security matters of a bilateral, multilateral, or international nature."[44] Although the DOS will play a key role in resolving international cyber conflict and possibly a lead role in reconstruction effort, it must maintain its diplomatic advantage to remain effective as the major U.S. international political peacemaker and honest broker.

The DoJ also plays a key role in cyber security and could offer some advantages as the lead federal government agency to combat cyber crimes (individual or home-grown terrorists). Its law enforcement role, which deals with legal domestic issues related to federal statutes, provides great experience in cyber war and will be very helpful in verifying and confirming state sponsored or organized-group cyber activity. The DoJ should also play a key role in addressing all the legal problems that could be encountered in a cyber attack/counterattack. The current technological and processing experience the DoJ organizations have with national cyber defense issues also provides an excellent advantage in fighting the cyber war. However, the DoJ is not resourced or legally empowered to manage the cyber war on a large-scale national or international level for a long period of time.

This list of cyber interested agencies does not intend to be all inclusive. It primarily illustrates the magnitude and complexity of the coordination effort involved in potential cyber war. There are other key inter-agencies (i.e., Department of Commerce, Department of Treasury, Department of Transportation, and others) that are critical to the cyber war process.

Comparative Analysis: Department of Homeland Security and Department of Defense

Let's review in detail the two primary candidates this paper assumes have the best chance to lead the cyber attack/counterattack—DHS and DoD. They appear to be the two departments that should be considered to lead the cyber counterattack against a state-sponsored or organized group attack on the homeland. This paper assumes the United

States will not initiate a cyber war unless provoked, but will initiate an operational counter attack as part of a conflict or physical war declared by the President. However, this scenario includes the launching of a counterattack from a strategic defensive posture of guarding the U.S. homeland. This analysis compares two major organizations, DHS and DoD, for the lead role in the cyber counterattack against state-sponsored or organized group cyber attacks. The comparison is based primarily on four categories: resources, experience, legal status, and technology.

The DHS's mission is to secure the United States and DoD's mission is to defend the United States. There is some overlap in these organizations' responsibilities (secure vs. defend) that could create some legal and unity-of-command issues. The DHS has a disadvantage in resources (personnel and funding) compared to DoD. The DHS cyber experience of preparing some of the major players for the potential cyber war has grown considerably over the past two years according to senior DHS analysts. It has included many of the major players in recent exercises with very good results.[45] Although DoD participates in these exercises, it has not led a coordinated effort of this magnitude, which involves personnel and organizations from private industry and the public sector. Besides, DoD may have USC, Title 10 or/and USC Title 18 (Posse Comitatus) legal concerns with such a coordination effort (overseeing and law enforcement of private industry and American public computer responses). "Cyber defense on the domestic front is primarily a civilian law enforcement function which seriously limits DoD's role on cyber attack on the United States Homeland."[46]

The role of protecting the United States homeland cyber space seems to fall squarely into the realm of the DHS. Or does it? This would be a viable solution if the United States' security was only passive in nature. However, once the United States has determined it is under attack from a state sponsored or an organized group (e.g., terrorists); it will retaliate with an appropriate response.[47] The response or retaliation could be more than a return cyber attack. It could conceivably escalate into an all-out armed conflict, justified as self-defense or proportionate to loss of property or life.[48] In the cyber international legal world, there would have to be grave evidence without reasonable doubt warranting such "drastic" measures.[49] In such a case should DHS relinquish control of cyber war to DoD, which has more resources and experience for waging war, even a cyber war?

We have noted that the DHS has a major legal role in cyber defense of the homeland from a domestic perspective. However, what is its role in responding to a state-sponsored or organized group attack? The DHS has limited resources and will depend heavily on DoD resources to fight the cyber war. The DoD's budget is about 10 times the size of DHS. The DHS would also be heavily dependent on DoD for technological support as well as relying on DoD's extensive cyber space experience. However, individual state Governors could activate and control National Guard resources through the State Adjutant General, who could coordinate cyber actions with DHS. This could alleviate DHS resource issues. This, however, will not help with legal issues where the cyber war expands across international borders via the Internet.

So to recap the analysis, DoD has a clear advantage over DHS in the matter of resources (i.e., Guard, Reserve and Active forces and budget), technical operational experience (daily attacks/defense), and technological capabilities. Although not involved extensively with external coordination efforts, DoD has a very effective internal cyber response system that does do some coordination with external sources. It brings experience and process maturity in teamwork, collaboration, and command and control to the cyber war. The DoD will also have the most advanced technological equipment used for combating cyber attacks. However, as illustrated earlier, DoD may have some legal hurdles to deal with when active-duty forces fight a cyber war on the homeland, especially if most of the resources reside with the active-duty force whose domestic activities may be restricted by Title 10 (Insurrection) or/and Title 18 (Posse Comitatus).[50] How will DoD or DHS legally control or give orders to their U.S. private business and citizen partners during cyber war? Should a cyber war on the U.S. be fought in compliance with the same principles, policies, and laws as an armed war on U.S. soil? Consider the following scenario regarding DoD's legal issues if armed and cyber wars were treated the same:

> *If circumstances warrant, the President or the Secretary of Defense may direct military forces and assets to intercept and defeat threats on U.S. territory. When conducting land defense missions on U.S. territory, DoD does so as a core, warfighting mission, fulfilling the Commander in Chief's Constitutional obligation to defend the nation. To fulfill this responsibility, DoD will ensure the availability of appropriately sized, trained, equipped, and ready forces. Currently, this capability is provided by quick reaction forces (QRFs) and rapid reaction forces (RRFs).*[51]

This scenario concludes that if all wars (kinetic and non-kinetic) were waged the same DoD could legally lead the cyber attack against state-sponsored or organized groups on the U.S homeland. However, as currently understood DHS has slight advantage in the legal aspects of leading the cyber fight on the homeland. DoD has a clear advantage on all other criteria—resources, experience, and technology for leading the war. Consider also the matter of command and control: DHS would probably have an easier time communicating with the private and public sectors since this is part of their current operations. On the other hand, DoD, although with more experience in command and control function, faces operational and legal issues in its efforts to coordinate with or manage public or private sector assets.

Results of Analysis between DHS and DoD for Organized or State-Sponsored Attack

Based on the analysis above, DoD is better resourced and positioned to lead the cyber war during an attack from state-sponsored or organized group adversaries using cyber capability. However, other major players must be involved and provide support as they would in any armed conflict.[52] Based on the foregoing criteria, DoD seems to be the logical choice to lead the effort against an attack. However, one key issue is DoD's legal status in leading a war effort that conceivably includes private industry and the general U.S. public. There are also issues regarding use of international cyberspace which we do not own.

Once the organized cyber attack has been contained or rebuffed, DoD seems to be the most logical department to lead the cyber counterattack based on the most experience, more advanced technology, and the most resources (money and people). The clean-up and on-going defensive posture must be maintained even after the United States goes on the attack. Resource issues and warfighting experience are the most limiting factors for using DHS as the lead in a cyber counterattack against state sponsored or organized group attacks. However, as noted earlier, the legal issues and coordination with private and public sectors favor the DHS.

The DoD should take full advantage of DHS's role to secure the homeland and control the other players (private and public) and interagency partners. The robust response system DHS currently has in place and continues to update will be critical in helping to control and monitor the cyber challenges affecting the government, businesses and the general public.[53] This DHS role may be the most important part of the cyber warfare process. However, designating the DoD as the overall lead element during actual attack will better facilitate overall command and control and unity of effort. Total commitment by all responsible agencies is needed and expected to win the cyber war.

Recommendations

The DoD should lead the effort during a cyber attack or the hostility phase of the cyber war. Although time is of the essence, careful consideration and actual validation of enemy cyber attack must be confirmed before performing a counterattack. Once the enemy cyber attack has been confirmed the U.S. must take immediate and appropriate action.[54] The DoD, the DHS, and the DoS should serve as main agencies (with dedicated support from others; some listed in key players' paragraph above) to develop a comprehensive plan for three stages of the cyber war: pre-hostility, hostility, and post-hostility. Current interagency and external exercises conducted by DHS need to be expanded to include all players (including international community when feasible) through all stages of cyber war. Roles and responsibilities among the three major players (and others as well) must be carefully defined in specific detail as soon as practical. Also, the seamless transition among each as lead organization (DoD, DHS, and DoS) through the different phases of the cyber war must be planned and exercised/rehearsed extensively. All three agencies will be intricately involved throughout each of the major stages; they must work as a team in support or lead roles. This collaborative effort will be met with legal challenges during a cyber war—nationally as well as internationally.[55] Legal experts in DoD, DHS, and DoS in coordination with DoJ should anticipate and address these legal concerns now. This critical planning effort must begin, before a "Pearl Harbor" type cyber attack is launched. International collaboration efforts must continue and cyberspace agreements or/and treaties developed soonest. Because of the complexities of cyberspace, this effort could be even more involved than "fly over" international requirements for military or commercial air space.

Conclusion/Summary

Cyber war should no longer be regarded as a fictitious event. It is a real potential wartime dilemma that must be taken seriously by all Americans and the international community in general. The effects of a cyber war, although not as deadly as a nuclear war or other weapons of mass destruction, could create similar catastrophic results. The fact that an all-out cyber war could potentially affect every home and every work place in America; seriously impact our economy; cripple our infrastructure (lights, power, energy, etc.); disrupt our military forces; and trigger many other devastating effects, makes it a critical concern for America.[56] The *National Strategy to Secure Cyber Space* states "securing cyberspace is a difficult strategic challenge that requires a coordinated and focused effort from our entire society—the Federal, state and local governments, the private sector and the American people."[57] Several U.S. agencies are currently working the very important cyber issues. However, to most effectively counter a cyber attack, the United States must focus its efforts by assuring command and control and unity of effort in cyber warfighting.

The cyber war's primary players, namely DHS, DoD, and DoS (if international cyber space reconstruction is warranted) must promote unity of command/effort; they must seamlessly transfer the lead role among one another as required for conducting defensive, offensive, and international cyber actions. The DHS should lead the U.S. national reconstruction effort for the homeland. The U.S. cannot afford to wait for a state-sponsored or organized group cyber attack to happen to work out the very complex coordination functions and all legal implications of cyber security. The lead agencies for the various phases of cyber security should be designated quickly.

National strategic leaders should focus on the very aggressive response plan and exercises implemented by the DHS. This plan includes all the players—government, businesses, the American people, and even some international countries. Many of the businesses and government agencies have local, national, and international experience. All involved parties must continually maintain the defense, with DHS as the major coordinator for the homeland assets. All of the players need to work closely together and fix legal (domestic and international), communications, and coordination issues. The DoD should have the overall lead for the counterattack effort; the DHS should provide strong homeland cyber defensive support while maintaining the control of the complex national coordination process; and the DoS should assume lead of the reconstruction effort if international players involved. In the event of a cyber war, the roles of the supported and/or supporting commands among the major players must be transparent and confidently executed. Time is of the essence. Our international, national, state, and local policies must continue to emphasize protection of this very critical information attribute called cyberspace.

Endnotes

1. George W. Bush, *The National Strategy to Secure Cyberspace*, February 2003, 1.
2. Department of Homeland Security, "Cyber Incident Annex," National Response Plan, (Washington, D.C., Homeland Security Office, August 2004), 2.
3. Stephen J. Lukasik, Seymour E. Goodman and David W. Longhurst, *Protecting Critical Infrastructures Against Cyber-Attack*, (Oxford University Press for The International Institute for Strategic Studies, 2003), 7-10.
4. Justin Blum, "Hackers Target U.S. Power Grid; government Quietly Warns Utilities to Beef Up Their Computer Security [Final Edition]," *The Washington Post*, Mar 11, 2005: sec E.01, www.proquest.com (accessed February 6, 2007).
5. Josh Rogin, "Air Force to Create Cyber Command," FCW.com, Nov 13, 2006, 2, http://www.fcw.com/article96791 (accessed December 4, 2006).

6. Ibid.

7. Lukasik, Goodman and Longhurst, 23-24.

8. Rogin, 3.

9. Chris Gonsalves, “DOD Attacks Renew Fears; Speculation Swirls about Cyber-terrorism,” *eWeek*, Vol 22, Issue 35, September 5, 2005 (New York), 37, www.proquest.com (accessed February 6, 2007).

10. White House, *The Federal Response to Hurricane Katrina: Lessons Learned* (Appendix A.1) (Washington, D.C.: The White House, 23 February 2006), 87, http://www.whitehouse.gov/reports/katrina-lessons-learned.pdf (accessed February 27, 2007).

11. Bush, 48.

12. Ibid., 6.

13. Ibid., viii.

14. Ibid., 2.

15. “Department of Homeland Security Releases Cyber Storm Public Exercise Report,” U.S. Federal News Service, Including U.S. State News (Washington, D.C., September 13, 2006) www.proquest.com (accessed February 6, 2007).

16. Bush, 6.

17. “DHS Conducts First Full-Scale Cyber Security Exercise,” Defense Daily, (Potomac: Feb 15, 2006, Vol 229, Issue 30): 1, www.proquest.com (accessed February 6, 2007.

18. Ibid., 2.

19. Michael Vatis, “International Cyber-Security Cooperation,” in *Cyber Security: Turning National Solutions into International Corporation*, ed. James Lewis, Volume 25, Number 4, (Center for Strategic and International Studies Press, 2003): 14.

20. Bush, viii.

21. Ibid.

22. Rogin, 1-2.

23. Army War College, *Information Operations Primer*, AY07 Edition (November 2006): 83.

24. Clay Wilson, “Information Operations and Cyberwar; Capabilities and Related Policy Issues,” in Congressional Research Service, Library of Congress, 2006): 7-8.

25. Army War College, *Information Operations Primer*, 87-90.

26. Bush, xiii.

27. "DHS Conducts First Full-Scale Cyber Security Exercise," Defense Daily, (Potomac: 15 Feb 2006, Vol 229, Issue 30) www.proquest.com (assessed February 6, 2007): 1.

28. Lukasik, Goodman and Longhurst, 51-52.

29. Bush, 41.

30. Lukasik, Goodman and Longhurst, 35.

31. Ibid.

32. Lukasik, Goodman and Longhurst, 59-60.

33. Ibid., ix.

34. Gonsalves, 37.

35. Bush, 39.

36. Lukasik, Goodman and Longhurst, 83-84.

37. Roger W. Barnett, "A Different Kettle of Fish: Computer Network Attack," in *Computer Network Attack and International Law*, ed. Michael N. Schmitt & Brian T. O'Donnell, 25-26 (Naval War College, Newport RI, 2002).

38. Bush, xii.

39. Wilson, 10.

40. Ibid., 11.

41. Department of Defense, Office of General Counsel, "Implications of Espionage Law" (Appendix VIII to *An Assessment of Legal Issues in Information Operations*) in *Computer Network Attack and International Law*, ed. Michael N. Schmitt and Brian T. O'Donnell (Naval War College, Newport RI, 2002), 516-519.

42. Thomas C. Wingfield and James B. Michael, The Naval Postgraduate School, An Introduction to Legal Aspects of Operations in Cyberspace, (Naval War College, Newport RI, 2004); 13.

43. Ibid.

44. Department of Homeland Security, "Cyber Incident Annex," *National Response Plan*, (Washington DC: Homeland Security Office, August 2004), 7.

45. "Department of Homeland Security Releases Cyber Storm Public Exercise Report," U.S. Federal News Service, Including U.S. State News, (Washington, D.C.: Sep 13, 2006) www.proquest.com (accessed February 6, 2007).

46. Bush, xii.

47. T*he Law of International Conflict: National Security Law in Cyber Space*, 2000, Aegis Research Corporation, 41-46.

48. Wingfield and Michael, 13.

49. Daniel B. Silver, "The Prospect that Law will be Clarified," in *Computer Network Attack and International Law*, ed. Michael N. Schmitt & Brian T. O'Donnell (Naval War College, Newport RI, 2002), 77-79.

50. Douglass C. Lovelace, "Key Strategic Issues List," Strategic Studies Institute, Army War College, July 2006, 41 & 50.

51. Donald Rumsfeld, *Strategy for Homeland Defense and Civil Support*, Department of Defense, June 2005, 26-27.

52. Horace B. Robertson, Jr., "Self-Defense Against Computer Network Attack," in *Computer Network Attack and International Law*, ed. Michael N. Schmitt & Brian T. O'Donnell (Naval War College, Newport RI, 2002), 132-133. "Computer network attacks as 'armed attacks.'" It is important that what is under discussion here is not what may be lawful in an ongoing armed conflict (jus in bello) but rather actions by hostile individual, group, or State against another State while the target state and the State of origin of the actions are not yet engaged in armed conflict (jus ad bellum). In an ongoing armed conflict (war), it is unquestionably legitimate for a State to attack its enemy's military telecommunications infrastructure, including military computer networks. Attacks on other telecommunications and network facilities which serve both military and civilian clientele legitimate military objectives, provided that the international humanitarian law of armed conflict is observed with respect to proportionality, including limiting collateral damage. It is a matter of indifference whether the mode of attack is kinetic or electronic, although the former may be more objectionable since it is more destructive and may cause more long-lasting effects. In examining whether a computer network attack "attack" may constitute an "armed attack," Article 51 cannot be construed in isolation but rather must be read in the context of other articles of the Charter, particularly Articles 2(4), 39, 41 and 42.

53. "DHS Conducts First Full-Scale Cyber Security Exercise," *Defense Daily*, (Potomac: 15 Feb 2006, Vol 229, Issue 30) www.proquest.com (accessed 6 February 2007):1.

54. Silver, 86. Sharp has proposed a rule that appears both sweeping and simple: Any computer network attack that intentionally causes any destructive effect within the sovereign territory of another state is an unlawful use of force within the meaning of Article 2(4) that may produce effects of an armed attack prompting the right of self defense.

55. David Tubbs, Perry G. Luzwick, and Walter Sharp, "Technology and Law: The Evolution of Digital Warfare International Law Studies," in *Computer Network Attack and International Law*, ed. Michael N. Schmitt & Brian T. O'Donnell (Naval War College, Newport RI, 2002), 6. "Despite the difficulties in application, I am persuaded that we will be well served by applying the core principles of international law to information age warfare. We cannot in our zest for tactical mission success, lose sight of our goals as a nation—to protect life and liberty, in our country and throughout the world."

56. “Department of Homeland Security Releases Cyber Storm Public Exercise Report,” U.S. Federal News Service, Including U.S. State News (Sep 13, 2006 Washington, D.C.) www.proquest.com (accessed February 6, 2007).

57. Bush, vii.