

Press Release

As part of its ongoing efforts to deliver timely analysis to its clients, [DiploNews](#) recently reviewed the state of the United States' trajectory towards recognizing cyberwar as a space for the Defense Department to operate in both in policy and law.

Paris, France, February 6, 2012 — As a country that is used to being dominant in the more traditional sense, the U.S. has been working to come to grips with a new sense of supremacy as a result of cyber threats, says a report released today by DiploNews. Even with a team of people responding to a threat, all it takes is one skilled person to continue to execute a cyber attack unaffected and even unnoticed. Thus, the possibilities for supremacy do not favor those with the most money, staff, or equipment. Instead, supremacy belongs to the one with the most knowledge and who can hide himself and his work the best.

According to the DiploNews report, the U.S. has taken steps towards allowing cyberwarfare. The most recent step includes a bill President Barack Obama signed into law in early January, the National Defense Authorization Act for Fiscal Year 2012. This bill includes an amendment in which Congress affirms that the Defense Department may wage cyberwar in the manner it deems fit while respecting existing laws and policies.

However, challenges remain in defining how United States Cyber Command (CYBERCOM) will use these policy and legal definitions in practice. Among these include: defining when a cyberattack has crossed the line from a civil offense to one that warrants a military response, identifying and locating the aggressor, responding with an underdeveloped international legal regime for defining and punishing cyber crimes, and defining precisely how responding to an attack or potential attack will manifest in practice. In remaining opaque in where it intends to draw the line in the sand, DiploNews finds that the U.S. is remaining flexible, fighting asymmetric threats by being asymmetric itself.

About DiploNews:

DiploNews's global team of information and intelligence professionals provides an audience of decision-makers and news consumers around the world with a unique monitoring and insight into geopolitical and diplomatic developments. The company uses a wide array of human and electronic sources directly treated by our analytical center.

Contact:

Charles Rault, Editor and Founder

DiploNews

contact@diplonews.com

www.diplonews.com

Report

Cyber security is a complicated domain. Perpetrators may be foreign nations, criminal groups, hackers, hacktivists, disgruntled insiders, or terrorists. The attacker may have multiple motivations, including the theft or exploitation of data, interruption of communication services, or even the destruction of networks or connected systems that civilians and militaries rely on to function. Vulnerable targets can be overcome without warning, and an effective response can take days or weeks to cobble together. Even with a team of people responding to a threat, all it takes is one skilled person to continue to execute an attack unaffected and even unnoticed. Thus, the possibilities for supremacy do not favor those with the most money, staff, or equipment. Instead, supremacy belongs to the one with the most knowledge and who can hide himself and his work the best. In cyberspace, the attacker functions like a sniper, except his physical location can be anywhere in the world. As a country that is used to being dominant in the more traditional sense, this concept of supremacy is one that the U.S. has been working to come to grips with.

The U.S. recognizes that cyberspace is unique in that civilians and militaries alike build and rely on massive interconnected networks and systems to function. As a result, it put the Pentagon and CYBERCOM in control of the military aspects of deterring and responding to a cyber attack while the Department of Homeland Security is in control of the civilian aspects. This is simplistically described as DHS taking care of the .gov and .com domains, and CYBERCOM taking care of the .mil domain. The [2011 U.S. cyberspace policy review](#) focuses on the civilian aspect of cybersecurity, and many of the goals revolved around establishing communication and management strategies for preparing for and warding off cyber attacks, including increasing interagency cooperation and public awareness. The 2012 U.S. defense [review](#) mentions the cyber threat in several places: deterring and defeating aggression in all spaces, including cyberspace; projecting power despite anti-access measures by implementing the Joint Operational Access Concept, a cross-domain capability sharing instrument; and by operating effectively in cyberspace by investing in advanced network defense and operation capabilities. Despite the threat of cyber attacks, the U.S. hopes to preserve internet freedom by dissuading and deterring potential aggressors by removing the benefit of waging an attack. Both actors play a role in achieving this, and ultimately, DHS and CYBERCOM will both play a large role in [defining](#) if an attack warrants a civilian response or a military response.

The U.S. congress began discussing the [potential](#) for a cyber attack to lead to war in the early 2000's. The discussions became more [sophisticated](#) in the [years](#) and after 9/11. The realization of cyberspace as an operational domain of concern for U.S. military was formalized in 2009 when Defense Secretary Robert Gates ordered loosely affiliated joint task forces consolidate into what is now known as U.S. Cyber Command, which began [operation](#) in May of 2010. With this move, the U.S. worked to anticipate and reduce problems that would arise from having too loose a network tracking and fighting cyber attacks from what would probably need to be a tight-knit network to be able to launch a successful attack. In the last month, U.S. Congress approved and President Barack Obama signed the National Defense [Authorization](#) Act for Fiscal Year 2012 with a curious [addition](#). At section 954, the U.S. Congress affirmed that the Department of Defense may wage cyberwar to defend the U.S. and its allies and interests. It acknowledged that the evolving nature of cyberspace means there is no precedent for how to define the military aspects of cyber attacks, so it provided the Department of Defense the flexibility to act so long as its actions, both offensive and defensive, respect both its [current](#) policy and legal regimes and the War Powers [Resolution](#).

While the U.S. has taken steps towards allowing cyberwarfare, challenges remain in defining how it will use these policy and legal definitions in practice. First and foremost, militaries generally have identifiable enemies whose attacks come with a traceable return address. With the rise of terrorism and other asymmetric threats, the military has already needed to become more flexible in how it tracks and responds to threats, yet cyber attacks are another new breed of threat. Identifying who the attacker actually is can take weeks or months to determine, and even then the true identity of the source of an attack may still be in question.

Even if the U.S. is able to identify the true source of an attack, knowing how to respond in a measured and legal way will be a challenge. For instance, under whose jurisdiction does an attack fall under and which laws apply to an offender if an attack is waged from a different country or multiple countries, with data traveling through even more countries to reach its destination? Internationally, codified law regarding cyberwar and the rules of engagement is in a state of [underdevelopment](#). There is no one body with the responsibility to coordinate global cyber security policy. Paradoxically, even though NATO members are expected to share cyber information, transparency and information sharing between countries concerning their capabilities, vulnerabilities, policies, and goals is still a challenge despite the speed at which these technologies allow communication to take place. In locations where no laws or outdated laws exist and someone

is caught committing a cybercrime, the pre-existing criminal laws will provide the basis from which to punish the civilian offender. On a grander scale, however, there is no agreement internationally on the definitions of and punishment for engaging in cybercrime and cyberwar. In these instances, like before, the already agreed on rules of war will likely need to be relied on to provide the basis for a response to cyber threats. The fact that the U.S. may legally use its laws of war to engage in cyberwarfare does not resolve the international legal aspects of preempting or intercepting an attack.

While U.S. forces have the right and ability to, when it **deems** necessary, use a military to respond to specific threats, cyberspace is unique in that civilians and militaries alike build and rely on massive interconnected networks and systems to function. The murky line between a civilian infringement and a military infringement will be a source of a grand debate when a dramatic international crisis as a result of hackers eventually occurs. The U.S. Congress did discuss examples of a military response, including releasing worms, bringing down power grids, and disabling websites. However, the Defense Department has chosen to be rather vague in publicly defining what an attack warranting a military response will look like and the precise rules of engagement for cyberwar. Reports suggest that development for the next strategy is already in progress. The field is complex, and perhaps there is a fear that a scenario no one has planned a contingency for will occur. For the U.S., then, a publicly declared strategy will likely limit the number of politically viable responses it could wage against a cyber attacker. In remaining opaque in where it intends to draw the line in the sand, the U.S. is remaining flexible, fighting asymmetric threats by being asymmetric itself.

In recent engagements, the U.S. came close to using large-scale cyberwar techniques, yet for different reasons chose not to use them. In Iraq, plans were reportedly drafted to restrict access to funds by Saddam that were never used. In part, according to sources, because by the time they were authorized it was too late for them to have any bearing on the outcome of the war. The delay apparently was the result of a concern that due to the interconnected nature of banks that the efforts would bring down some banking operations in Europe. During the engagement with Libya, there was speculation in the press that the U.S. was considering using cyberwarfare to tamper with Libyan electronic warning systems. It is said that critics shot the idea down because of, among other reasons, the fear that such an action might set a precedent for other nations to follow suit. However, considering that the U.S. is leading the way in the use of drone attacks in military engagements, it is unlikely that these hesitations are the result of a sense of moral responsibility. Even the rich U.S. is unable to keep up with the **bleeding** edge of technology; many times, by the time funds are approved and distributed the equipment and training the money was earmarked to

purchase is outdated. Governments are notoriously slow to keep up with technology as the manufacturing of bleeding edge computer technologies is largely a civilian operation now, where as manufacturing tanks and guns is a bit harder to do without a government to fund the manufacturing process. As a result, the U.S. has to rely on its strong relationship with private sector contractors to remain equipped with the newest machines. It has been suggested that success in future conflicts of all kinds will depend more on the popular perception of the engagements rather than the will of the governments involved. Perhaps, instead of morality, the U.S. is not yet ready politically, intellectually, legally, and structurally for an onslaught of retaliation from its global enemies. The recent signing into law of the Defense Authorization Act brings the U.S. one step closer to resolving the political and legal weaknesses, though the others remain.

These problems are not isolated to the U.S., of course. Chapter 5 of The North Atlantic Treaty [states](#) that all other member states will consider an armed attack against another member as an attack against them all. In allowing the Defense Department to engage in cyberwar to protect its allies, the U.S. Congress implicitly addressed this question in the National Defense Authorization Act. However, this potential to use Chapter 5 in a cyberwar suffers from the same problem as defining the difference between a civil attack and one that requires a military response. Estonia experienced a country-crippling attack back in 2007 which the Estonian Defense Minister Jaak Aaviksoo called a cyberwar. While the self-defense clause was not invoked, following the attack the member states started working towards being ready and able to support each other in the event of a cyber attack. Officials carefully support this change under Chapter 4, in which the members agree to consult each other for opinions on territorial integrity and security, making cyber security a national responsibility.

While it helps that the U.S. and its partners conduct [tabletop](#) exercises, it will be difficult to know when or if NATO forces are able to genuinely project unquestioned superiority and a monopoly on force and violence in the cyber space in a way that will successfully deter potential aggressors by removing the benefit from waging an attack. Military strength has easily verifiable metrics that one may use to measure with: number of weapons, amount of money spent, age and service cycle of equipment, military population. Again, while the number of people sitting behind a computer increases the likelihood that an attack can be found and blocked before any serious damage can occur, it only takes one clever hacker at one computer to evade the blockade and prolong the crisis. The response team is only as strong as its weakest link. While the U.S. is certainly not the weakest link, U.S. policies and efforts cannot secure cyberspace on their own. Unilateral and even bilateral efforts in this realm are inferior to a global, holistic approach to defining norms and establishing a legal regime that is able to keep up with dynamic technology development.

Eventually, either a new international body will need to emerge to address these issues or an existing body will need to adapt. However, consensus on what mechanism to use will be hard to come by. Russia and China prefer the UN model and the non-interventionist protections the charter provides. In contrast, the U.S. and its close allies claim that the UN is too slow to appropriately address cyber issues and [prefer](#) to look to the 2001 [Budapest](#) Convention on Cyber-Crime instead.

DiploNews®



DiploNews (www.diplonews.com) is the authoritative one-stop source and world-leading provider for diplomatic and foreign policy information. Our proprietary system works 24/7 to gather, sort, and centralize information directly from official state and international organizations. As a result, **DiploNews** members easily find the information they need and increase their understanding of world developments. Additionally, any reader may subscribe for free to [DiploWeek](#), a summary of the week's diplomatic events in about 20-minutes of reading which is delivered via email each Friday. Today, the archives represent approximately 2 million A4 pages, and 33% of its readership is based in the U.S.