Statement before the

House Committee on Foreign Affairs

"CYBER WAR: DEFINITIONS, DETERRENCE AND FOREIGN POLICY"

A Statement by:

James A. Lewis

Director and Senior Fellow Strategic Technologies Program

Center for Strategic and International Studies (CSIS)

September 30, 2015

2172 Rayburn House Office Building

I would like to thanks the Committee for this opportunity to testify. Cybersecurity is a central issue in American foreign policy, on a par with terrorism or proliferation. There can be no cybersecurity without international agreement on state behavior. The internet provides countries with new ways to grow and trade, but it is also a means of coercion, espionage, crime, and attack. The ability conduct remote exploits on computer networks (known colloquially as "hacking") has become another tool for state's to use against each other.

While much of the discussion of cybersecurity has focused on things like information sharing, critical infrastructure protection, or incentives for private action, these concepts are largely defensive, reactive and ineffective. They would harden American networks to some degree, but not enough to improve the situation. Building a better Maginot line is not good strategy. We face determined and well resourced foreign opponents who are responsible for the most damaging malicious cyber actions against the U.S. This makes cybersecurity a foreign policy problem. It is not technical; it is political and requires diplomatic and military responses.

We can assess the cybersecurity problem by looking at the numbers. There have been thousands of incidents of cyber espionage and cybercrime (the most expensive usually victimize financial institutions). In contrast, there have been perhaps a dozen incidents of countries using cyber tools for political coercion, and only three or four incidents that would qualify as the use of force or armed attack. Reaching international agreement on what qualifies as the use of force or an armed attack is a crucial problem for international negotiation and agreement on cybersecurity, and continued ambiguity hampers the application of international law and limits our ability to deter cyber attacks.

Another set of numbers is also telling. Two countries, Russia and China, are responsible for most of the malicious cyber actions taken against the United States, Chinese actors, usually from the People Liberation Army, are responsible for more than half of all economic espionage in the United States, more than all other countries in the world put together. Russian criminal groups, operating with the approval of the Russian government, are responsible for most of the major cybercrimes against U.S. financial institutions. If these two counties behaved responsibly and cooperated in law enforcement, the magnitude of the cyber problem would diminish appreciably.

A unilateral approach to cybersecurity will not work. The U.S. ultimately needs to persuade or compel those nations who take action against us in cyberspace to stop. A purely defensive strategy will not work. Nor can we deter cyber espionage and crime. This means that negotiations, with allies, opponents, and the undecided nations, are indispensable for improving cybersecurity. These negotiations will be difficult and slow, but they are essential and this makes cybersecurity a topic that should be of central concern to this committee.

What does "cyber war" look like?

Cyberwar has been a topic of interest and concern for more than two decades, but the phrase itself is misleading. Cyber operations - the ability to remotely manipulate computer networks - have created a new military capability. The internet and computers provide cyber tools and techniques

that counties use for influence, coercion and, potentially, attack. Militaries will use cyber attacks to disrupt command and control, manipulate software, degrade weapons performance and produce political or psychological effect.

Most cyber "attacks" will not produce destructive effects similar to kinetic weapons, but will instead seek to disrupt data and services, create confusion, damage networks and computers (including software and computers embedded in weapons systems) and perhaps destroy machinery. Cyber attacks could strike military, government and perhaps civilian targets, such as critical infrastructure in the opponent homeland.

Advanced cyber attacks can produce effects equivalent to an attack using a bomb or missile, but this is not the most likely use. Cyber attacks that produce military effect can include the manipulation of software, data, knowledge, and opinion to degrade performance and produce political or psychological effect. Since most modern weapons depend on software for their performance, an ability to damage or degrade weapons system software can provide real military advantage by making the weapons inoperable or by degrading their performance.

We should not interpret cyber war solely from the perspective of physical damage. Command and control networks are an important target and attacks on them need not produce physical damage. The Russian penetration of Central Command's classified networks in 2008 showed that Russia, who is our most skilled opponent, would probably try to disrupt command and control in the event of a crisis. Similarly, China penetrating the networks of U.S. Transportation Command and its contractors to test the ability to disrupt American power projection capabilities by interrupting deployments and supply efforts. The absence of physical damage complicates the application of international law.

No non-state actor has acquired or developed the capabilities for a cyber attack that could cause physical damage or casualties. In fact, only a few nations now possess these capabilities. Non-state actors use cyberspace for recruitment, training, fund-raising and proselytizing, not to exert force. Non-state actors have used cyber attacks for coercive purposes, such as denial of service attacks or leaks of damaging information. These actions do not qualify as the use of force but give non-state actors new tools for coercion. Non-state actors like Hezbollah, Hamas or ISIS have not yet used cyber attacks, but Iran may be supporting Hezbollah and Hamas in developing such capabilities for use against Israel.

What this means is that our major opponents are likely to only launch damaging cyber attacks (e.g. those with effects equivalent to a kinetic attack) in the event of armed conflict with the United States. Outside of armed conflict, the primary state use of will be cyber espionage and cyber actions intended to coerce (such as in Estonia or with Sony) that fall below the level of the use of force.

True cyber attacks (e.g. those that inflict physical damage) have been rare, but that does not mean we should dismiss their risk. Most major militaries are developing cyber attack capabilities. Cyber attack will be part of any future war. For the U.S., all of our most likely opponents in any armed

conflict – Russia, China, Iran and North Korea – have developed cyber attack capabilities and have engaged in cyber reconnaissance against U.S. military targets and critical infrastructure to prepare for possible attack. We have done the same to them.

Cyber attacks against critical infrastructure could disrupt vital services and possible cause physical destruction, but only a few major powers have this capability and they have been very cautious in using it. How a country uses cyber techniques is determined by its interests, strategies, experience, institutions, and its perceptions of and tolerance for risk. This means that critical infrastructure is a target for cyber attack as it was a target for nuclear missiles, but will only be attacked when an opposing state finds itself in a conflict wish the U.S.

This spread of attack capabilities makes cybersecurity is an increasingly important problem for collective self-defense. In the last few years, the U.S. has worked with its allies to create structures and capabilities for collective cyber defense and has amended collective defense treaties with NATO, Australia and Japan to expand their application to include cyber attacks. NATO's September 2014 summit established that cyber defence is part of the Alliance's core tasks of collective defence, crisis management, and cooperative security. Consistent with its defensive mission, NATO emphasizes "prevention, detection, resilience, recovery." Japan has made significant strides to improve its cybersecurity posture in the last few years, but cybersecurity remains an area of vulnerability for Japan and the bilateral security alliance. The place of cybersecurity in mutual defense is linked to the larger constitutional debate in Japan over the role of the armed forces and redefining the scope of self-defense. Moving forward, alliance relationships will require both greater cooperation and greater effort in cybersecurity.

Since 2007, the U.S. has also developed a framework of policy, doctrine and operational concepts for the use of offensive cyber operations. This framework embeds cyber operations in the existing structure of rules that apply to military and intelligence operations. Cyber actions are approved by the President under Title 50 or Title 10, authorities for intelligence or the use of military force, in consultation with the committees of jurisdiction. In the next year, we should also expect to see greater use of "countermeasures" (such as indictment and sanctions) that do not involve the use of force and which do not require further Congressional assent.

The U.S. has engaged in offensive cyber actions, largely in Afghanistan and Iraq, under the existing Authorization for the Use of Military Force. These have not been attacks in the kinetic sense but the manipulation of opponent command and control networks. A hypothetical example might be the penetration of an insurgent communication network to tell a commander that it is safe to move in a certain direction when in fact he is moving into a U.S. ambush. There are also public allegations, the most salient being Stuxnet, that the U.S. has engaged cyber attacks under intelligence authorities.

Deterrence in Cyberspace

Despite having demonstrated capabilities in cyber defense, the U.S. has obtained little or no deterrent benefit from them. A number of issues complicate and limit the utility of deterrence for

cyber security. Deterrence is the threat to use force in retaliation for an attack. We cannot deter cyber crime or espionage. New opponents have a greater tolerance for risk and have planned their actions to avoid triggering U.S. deterrent responses. International law and norms define when force can be used in self-defense and require that it be proportional to the attack. China knows that espionage has never justified a military response. Iran may wonder how many bank websites it needs to disrupt to trigger retaliation. Equally important, an inability to make credible threats makes cyber deterrence ineffective. Within the limits of its applicability, because deterrence will not shield us from most malicious cyber actions, the best way the U.S. could improve deterrence would be to increase its ability to make credible threats.

International law and State practice do not define espionage or crime as attacks that justify the use of force in response. Deterrence will not work against these activities. Cyber deterrence faced a crisis this year. This crisis grew out of a string of failures for "extended deterrence," including our inability to deter Russia in Crimea, to deter ISIS or the Assad Regime in Syria, and on a lesser scale, a failure to deter the attacks on Sony, the Sands Casino, and Github.

In this context, it is difficult to make credible threats. Our opponents plan their operations in ways that circumvent deterrence. They look for tactics to manage and reduce risk and stay below the implicit thresholds of use of force or armed attack that allow them to damage the U.S. without triggering retaliation. While we can be confident that our nuclear and conventional superiority will deter major attacks on the U.S. and its allies, it will not deter malicious cyber activities. The ineffectiveness of deterrence increases the need for international agreement on norms and the application of international law

The Administration's response to the Sony incident had the effect of improving cyber deterrence. The public attention given to improved U.S. ability to attribute an attack may have made the DPRK (and others, such as Iran and China) more cautious in considering cyber attacks against U.S. targets, and the creation of new cyber sanctions (and an apparent willingness to use them) has helped to change opponent risk calculus.

That said, we cannot rely on deterrence and need to rethink its place in cybersecurity and our larger national strategies. We have not deterred cyber espionage or cyber crime. Our opponents do not want to start a war with the U.S., but they do not fear starting a war over spying or cyber crime. Deterrence requires opponents to compare the benefits of an action against the potential cost and assess the likelihood that such costs will actually be imposed. There must be credible threats or actual retaliation if deterrence is to work.

The experience of sanctions and indictments show that there are alternatives to the threat to use military force to deter malicious cyber activities, including espionage and crime. These actions change the opponent calculus and fall in the general category of "countermeasures," retaliatory actions not involving the use of force that are considered legitimate under international law. Countermeasures are important because so far, our opponents have faced no cost and little risk in carrying out malicious cyber actions.

For example, eighteen months ago the U.S. indicted five PLA officers for cyber espionage. At the time, many commentators saw indictment as a waste of time as the five would never go to trial. But the Chinese hated the indictments, and the experience of indictments reinforced the threat of potential U.S. sanctions in ways that helped the U.S. and China reach agreement on cybersecurity. The Chinese did not want to re-experience the pain of indictments as a result of any sanctions. While that agreement has yet to be tested, and while sanctions for China IP theft through cyber espionage are still possible, countermeasures not involving the use of force may be more effect in deterring cyber espionage and crime.

What is the role of diplomacy in containing cyber conflict?

The first use of cyber attack for military purposes occurred in the mid 1990s, when the U.S. used primitive cyber attack tools against Serbia. In the late 1990s, Chinese military writings discussed cyber attack as a means to gain asymmetric advantage over the United States. Perhaps this led Russia to propose in the UN in 1998 a treaty to limit the development and use of cyber weapons. The draft treaty drew on Russia's experience with Strategic Arms control, but it was unworkable, largely designed to hobble the U.S., and did not receive much support. However, the Russian proposal began a process of international negotiation that has now produced results.

With the failure of its treaty proposal, Russia called for the UN to create a Group of Government Experts – GGE) to study the problem of cybersecurity and make recommendations on measures to reduce risk and increase stability. A first GGE in 2003 failed to reach agreement. The second GGE (2010) produced a short report that called on the international community to develop norms and confidence building measures (CBMs) and to build cybersecurity capacity in developing countries. This short report created the agenda for international discussion for cybersecurity. A more extensive GGE Report in 2013 changed the Internet's political landscape by agreeing that the national sovereignty, the UN Charter and international law applied in cyberspace to the same degree they apply in the physical world. This agreement got rid of 1990s ideas that hampered negotiations, such as the idea that cyberspace was a borderless global commons, and the application of sovereignty and international law embeds cyberspace and cybersecurity in the existing framework of international relations that government conducts among states.

The U.S. plays a leading role in the work of the GGE. Its diplomatic strategy for cybersecurity is based on the developing cooperative measures, norms or responsible state behavior in cyberspace and confidence building measures (CBMs). Norms reflect the international community's expectations about behavior. Unlike a treaty, norms are not legally binding, but experience shows they are useful. A norms-based approach offers the greatest chance for progress. There are already implicit norms governing cyber conflict that are derived from existing international law and practice. The argument that norms are too weak can be dismissed as there is no serious alternative.

CBMs focus on transparency and coordination. Voluntarily measures agreed ad ref in the Organization for Security Cooperation in Europe (OSCE), which has played a leading role in the development of CBMs, include the provision of national views on cyber doctrine, strategy, and threats. OSCE members will also share information on national organizations, programs, or strategies relevant to cybersecurity, identify a contact point to facilitate communications and dialogue on ICT-security matters, and establish links between national CERTS. OSCE members

discussed how existing OSCE mechanisms, such as the OSCE Communications Network, could be used to facilitate communications on cybersecurity incidents and develop additional measures to reduce the risk of misunderstanding.

The most recent GGE, which concluded in June of this year, was tasked by the UN to identify the application of international law, the development of norms and CBMS, and to further progress on measures to promote capacity building, as the core elements of an international approach to stability and security in cyberspace. In the negotiations, the most difficult of these topics turned out to be the application of international law, as countries were unable to agree on what qualifies as the use of force in cyberspace. Despite this, the 2015 GGE was able to agree on an expanded set of norms and CBMs (modeled loosely on the work of the OSCE) and on the application of international law.

A review of the applicability of existing law of armed conflict suggests that if we approach cyber warfare as a new military technology, existing international law can be largely applied to cyber conflict, but the central obstacle to this is the lack of agreement as to what should be considered the use of force or armed attack in cyberspace. Common understandings on the use of force and armed attack are fundamental both for applying the laws of armed conflict and for modernizing the mutual defense alliances the U.S. has with its allies.

The crux of the disagreement is over UN Charter Article 2/3, which call upon members to renounce the use of force to settle conflict, and Article 51, with reiterates member states inherent right of self defense against armed attack. These ambiguities, however, are not unique to cyber conflict, date from the signing of the Charter, and reflect conflicting desires to renounce the use of force while preserving the right to use force in self-defense.

There is no agreement on what qualifies as the use of force (2/4) and armed attack (51), but there appear to be implicit understanding on these concepts, albeit imprecise. These implicit understandings probably reflect nations understandings of risk; attacks that cause physical damage or casualties are more likely to qualify as the use of force and justify retaliation. Cyber attacks equivalent in effect to kinetic attacks. The area of greatest ambiguity involves cyber attacks that do not produce physical damage or casualties but do involve damage. Examples would include the hacking of Sony by North Korea or on Aramco by Iran. These concepts, use of force and armed attack have major implications for cyber war and for U.S. alliance commitments on mutual defense (which, for the US, are predicated on language that reflects Articles 2/4 and 51).

Continued ambiguity over the application of these UN Charter articles serves the interests of Russia and China by not creating grounds for legitimizing retaliation for cyber actions. This includes a general rejection of Western efforts to define “use of force” and “armed attack” using the concepts of equivalence and effect. The Russian and Chinese goal, similar to other arms control negotiations by these countries, is to constrain the U.S. and its allies.

While the GGE is the most important negotiating venue for multilateral negotiations, there are also important efforts in the Organization for Security Cooperation in Europe, the Organization of

American States, the ASEAN Regional Forum, and in the "London Process," a multilateral effort whose April 2015 meeting in the Netherlands produced valuable results for cooperation, confidence building, and the development of norms. There is also continued effort to increase support for the Budapest Convention, a formal treaty on cyber crime that "normalizes'' cyberspace by defining state responsibilities for enforcement and cooperation, but the Convention has made slow progress in the face of opposition from Russia and other countries, reinforcing the point that there is too much distrust among competing nations for formal global agreement.

Next Steps for Congress and the Administration

Congressional oversight and guidance for cybersecurity is spread among a number of committees, including intelligence, armed services, homeland security and others. The foreign affairs committees, in contrast, have played a lesser role. Given the importance of cybersecurity and the internet for security, commerce and international stability, this should change. The areas for specific attention include:

- Oversight of diplomatic actions and negotiations, including implementation and compliance of alliance commitment and bilateral agreements, such as the recent agreement with China;
- Legislative action to strengthen law enforcement and countermeasures for cyber crime and cyber espionage;
- Greater clarity on the legislative basis for authorizing the use of force in cyberspace;
- The development and review of international strategies for cyber security.

This administration was the first to put in place an international strategy. The 2011 international strategy for cybersecurity aims to build cooperation among countries and reaching agreement on cybersecurity norms and confidence building measures (CBMs). The central goal of the strategy is agreement on norms for responsible state behavior in cyberspace.

Given the very different international environment we now face, the U.S. need to reconsider and revise this strategy. The fundamental point for reconsideration is whether to pursue global agreement on cybersecurity norms for responsible state behavior, or begin by building consensus among like-minded nations. While both approaches can be pursued simultaneously, a new strategy will need to examine different kinds of engagements with other countries and a broader range of tools to win progress. It would continue to pursuit of global agreement but seek immediate agreement among like-minded nations on responsible behavior in cyberspace. These understandings should be reinforced by countermeasures and credible threats to encourage responsible behavior and strengthen the rule of law in cyberspace.

Cybersecurity is the product of larger security and trade issues that shape the international agenda. It poses difficult challenges for foreign policy and international security. In this, it is essential that Congress update its understanding of the problem to giver the international and diplomatic aspects of cybersecurity their appropriate weight. I thank the Committee for the opportunity to testify and will be happy to answer any questions.