Testimony
Subcommittee on East Asia, the Pacific, and International Cybersecurity Policy
Senate Foreign Relations Committee
[US International strategy for Cybersecurity]
James A. Lewis, Center for Strategic and International Studies
March 14, 2015

I would like to thank the Committee of this opportunity to testify.

Cybersecurity is a new challenge for foreign policy. The internet and other cyber technologies have reshaped economies and accelerated growth, providing immense benefit, but like any tool it can be used for purposes good or bad. Digital connections provide countries with new ways to grow and trade, but they are also a means of coercion, influence, and attack. Exploiting computer networks has become another tool for state power and competition. Countries use the internet and cyberspace to gain advantage over others. The use of cyber tools and techniques as an instrument of national power is now the norm. Getting international agreement on how states should behave in cyberspace is essential, but it will also be difficult.

The first known examples of what we would now call cyber espionage occurred in the early 1980s, when the KGB hired German hackers to break into U.S. military research computer networks. The first use of cyber attack for military purposes occurred in the mid 1990s, when the US 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 flurry of military activity led Russia in 1998 to introduce in the UN a treaty to limit the development and use of cyber weapons.

The draft treaty drew extensively on Russia's experience with strategic arms control. One precedent may have been the 1960's Outer Space Treaty, which establish principles of state responsibility and banned nuclear and other weapons of mass destruction from space. The analogy between space and outer space is inexact however, despite rhetoric about there being no borders in cyberspace. It is difficult to gain access to space and the technology, particularity in the 1960s, was expensive and limited to only a handful of nations. In contrast, the technologies needed for malicious action in cyberspace are ubiquitous and easily acquired. Clandestine operations are particularly easy in cyberspace. Nor do cyber attacks pose the risk of horrific effect similar to nuclear weapons, which created a shared desire for restraint even among opponents.

The very covertness of cyber action works against international agreements on security, and until 2010, there no progress on international agreement. There was too much distrust among competing nations for a treaty. The technology was also very new, and there was a general unfamiliarity in the international community with cybersecurity as a national security issue. The U.S. only began to consider diplomatic solutions in the last few years.

Some of this slow start reflects a too great reliance on the technical community to manage cybersecurity. The problems we face are not technical; they are political and requires policy and diplomatic skills to make progress. Some of the slow start reflects the millennial beliefs of the

1990s about the internet and the future of international relations. It seems hard to believe, but in the 1990s people believed that with the end of the Cold war, the world would become one big market democracy with shared values and no borders. Governments would play a smaller role in global affairs and could be replaced by a collection of civil society organizations and multinational corporations in some multistakeholder process. Those who believed this dream had a rude awakening in 2001 and while things have not gotten better since then, many in the internet community cling to these shattered beliefs.

Opponents

For the U.S., better cybersecurity requires changing the behavior of four countries. Russia is the principle source of cyber crime and extremely active in political-military espionage, and is the most skilled opponent we face. China leads in economic cyber espionage. Iran has developed significant cyber capabilities and uses them to apply political pressure on the U.S. It has also done the network reconnaissance necessary to launch cyber attacks against critical infrastructures, as have China and Russia. North Korea has invested for decades in building cyber attack capabilities. There are also jihadist groups who have rudimentary cyber capabilities. Hezbollah and the Syrian Electronic Army are connected to Iran and through Iran, perhaps to Russia. ISIS, with its sophisticated internet skill, bears watching carefully as a group that could develop the capability for low-level attack.

Dealing with these countries also requires a broad diplomatic strategy to win support from key allies and from emerging new powers, like Brazil, India and others. These new powers from a middle ground between western democracies and authoritarian regimes, and the policies these countries choose to pursue will determine the future of the internet and cybersecurity. Most of the new powers support fundamental human rights, and in particular freedom of speech and free access to information. This puts them at odds with the authoritarian view of cyberspace, but they also believe that national sovereignty and government must play a larger role in internet matters, and they were troubled by the NSA revelations, factors that work against U.S. influence. To win the global support, the U.S. needs persuasive arguments on privacy, internet governance, and the use of force in cyberspace. We do not now have these persuasive arguments and some of what we say now about the internet is seen as duplicitous. The NSA leaks of the last two years, whose selective release is used intentionally to damage the U.S., have not helped us.

Cybersecurity is a military and intelligence contest with dangerous opponents. There are significant trade issues. The internet has immense political effect that threatens authoritarian regimes and has led them to mount significant challenges to market and democratic ideals and the international institutions created to support them. The focal point of this challenge is to reduce U.S. influence, not just over the internet but also in trade, security, and finance. We face a determined effort to dismantle American leadership in international affairs.

Deterrence

There is a hope that the U.S. could use military force to deter malicious cyber activity, but this has not been effective. Deterrence was the linchpin of U.S. strategy for decades, but the political and military context for deterrence has changed significantly. Instead of a single, near-peer

opponent, the U.S. faces an array of possible foes, each with differing capabilities and tolerances for risk. Deterrence is of much less utility as a guide for policy in this new environment.

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 that if a threshold or "redline" is crossed, it will lead to unacceptable loss. In the Cold War, the threat of nuclear war deterred the Soviets from invading Western Europe and Japan or launching strategic attacks against the U.S. While it was often a subject of debate, the nuclear "umbrella" set redlines the Soviets could understand and found credible because they were linked to core American interests. The U.S. has thresholds or declaratory policies, but they are surrounded by a mass of caveats. This is sometimes lauded as "strategic ambiguity," but in fact, our adversaries just find it confusing. If opponents do not know what lines they should not cross, or do not believe that we will penalize them for crossing those lines, it will be hard to deter them.

Our most active opponents also seek to circumvent deterrence. They look for tactics that stay below this ill-defined threshold that allow them to damage the U.S. without triggering retaliation. They believe that the U.S. will also build new weapons, including cyber weapons that will allow it to circumvent their own deterrent forces and strike them with impunity. While we can be confident that our nuclear and conventional forces will deter major attacks on the U.S. and it sallies, it will not deter challenges in Crimea or he South China Sea, terrorism, or malicious cyber activities. Even nuclear threats in the Cold War did not stop Soviet espionage or regional adventures and we cannot deter cyber espionage or cyber crime. A different approach is required to bring security and stability to cyberspace. This is important because deterrence, if it works, if unilateral and does not require international agreement. The ineffectiveness of unilateral deterrence increases the need for international agreement.

U.S. Diplomatic Strategy

Getting international agreement is what the 2011 International Strategy for Cyberspace tries to do. This administration is the first to have a published international strategy for cyberspace, which it released in 2011. That strategy now needs significant reconsideration since we are now in a very different political environment, less peaceful, more challenging, and with overt opposition.

The U.S. diplomatic strategy for cybersecurity is based on the building cooperation among countries and reaching agreement on norms and confidence building measures (CBMs). Its starting point is recognition that a cybersecurity treaty is not possible. The core of the strategy is agreement by on norms for responsible state behavior in cyberspace. Unlike a treaty, norms are not legally binding. They reflect instead international expectations about state behavior. The normative builds on the experience of non-proliferation. With the Missile Technology Control regime, for example, a few like-minded nations (NATO, Japan, and Australia) agreed that responsible states do not transfer ballistic missile technology. Eventually the number of adherent nations grew and there was acceptance of a new global norm of behavior, including, after several decades, a measure of formal agreement. A similar process helped to create norms for chemical and biological weapons.

There are already implicit norms governing cyber conflict that are derived from existing international law and practice. Making these norms explicit and expanding, their scope would increase stability. The argument that norms are too weak can be dismissed as there is no serious alternative. Legally binding commitments have serious drawbacks. Our most likely adversaries will just ignore treaties. Treaties face serious implementation problems involving compliance and verification. Non-state actors have limited influence over major states, cannot themselves commit their country to an agreement, s and lack legal standing under international law. The existing 'state of nature" is too Hobbesian to be sustained as the internet and other digital networks become the most essential of global infrastructures. A norms based approach offers the greatest chance for progress.

There is now agreement among most countries that existing internal commitments apply in cyberspace as they did in the physical domain. Gaining this agreement has been a multifaceted effort, with work in the Organization for Security Cooperation in Europe (OSCE), the ASEAN Regional Forum (ARF), and the Organization of American States (OAS), the forum for Asia-Pacific Economic Cooperation (APEC), the "London Process," and the UN to develop confidence building measures and norms. Work to win greater acceptance of the Budapest Convention on cyber crime reinforces the central concept of 'normalizing'' cyberspace by defining state responsibilities towards other stated and their citizens. While there are regional differences (certainly in pace, if not substance), there is an emerging consensus about responsible state behavior in cyberspace that is consistent with existing norms and commitments among states.

The 2010 and 2013 Reports of the UN Group of Governmental Experts (GGE) has been foundational. Russia first proposed GGEs in the early 2000s. The first GGE failed to reach agreement. The second GGE (2010) produced a short report that called on the international community to further develop norms and CBMs (as well as to build capacity in developing countries). While short, this 2010 report laid out the agenda for international discussion of cybersecurity, identifying the application of international law, the development of norms and CBMS, and measures to promote capacity building, as the core elements of an international approach to stability and security in cyberspace.

The third GGE produced agreement among countries as diverse as the major NATO allies, Russia, India, and China (albeit reluctantly) that the principle of sovereignty applied to cyberspace, that the commitments to the UN Charter, existing international law (including the laws of armed conflict) and commitments to protect universal human rights all applied in cyberspace. While the implications of sovereignty for cyberspace are complex, the physical infrastructure that supports cyber activities is generally located in sovereign territory and is subject to the State's territorial jurisdiction. The agreement on the applicability of sovereignty and international law has fundamentally changed the political landscape for the discussion of cybersecurity, but it is only an initial step in defining how States will act in cyberspace. A fourth GGE is currently underway.

To increase trust, the US has also promoted agreement on a series of confidence building measures (CBMs). CBMs are a normal diplomatic measure to reduce tension and suspicion. CBMs strengthen international peace and security. They can increase transparency, cooperation,

and stability. Building confidence through greater transparency in doctrine, either bilaterally or in multilateral exchanges, could reduce the chance of miscalculation or inadvertent escalation. The lack of transparency makes it more difficult to reach agreement on norms for responsible state behavior or to limit cyber conflict.

The development and agreement on CBMS have had the most success in the OSCE, where Cold War precedents and participant experience with arms control created familiarity with such measures. In other regions of the world, where there is less experience with security negotiations, there has been less progress, but there are significant efforts to develop CBMs underway in the ASEAN Regional Forum and the Organization of American States.

Work by the OSCE has been foundational in defining CBMs. These CBMs focus on transparency and coordination. Voluntarily measures agreed ad ref in the OSCE 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 U.S. has worked in the UN and regional forums to promote agreement on cybersecurity. It also plays a leading role in the London Process, launched by UK Foreign Secretary William Hague, is a series of informal international meetings whose aim is to generate a consensus on responsible behavior in cyberspace. Initially the London process was seen as the vehicle for gathering like-minded nations to agree on norms, but its goals have become more diffuse. There have been four meetings, the last of which (in The Hague), produced a robust Chairman's Report. The next meeting is scheduled for 2017 in Mexico.

The U.S. also worked closely with its allies to make cybersecurity part of its defensive alliances. It has modified it collective defense arrangements with Australia, Korea, and Japan to include cybersecurity. NATO, in its 2014 Summit, agreed on when a cyber incident could trigger the collective defence provision of Article 5 of the North Atlantic Treaty. The key changes have been to create mechanisms for greater cooperation with allies and to agree that damaging cyber attacks fall under collective defense.

The Role of the Private Sector

There is international agreement to involve the private sector in cybersecurity "as appropriate." These last two words - "as appropriate" are the key. The role of the private sector varies by issue. For some issues, such as security negotiations, there is very little the private sector can do. Some countries, particularly China and Russia, do not see private sector actors as equals and believe that companies are tools of U.S. policy, something that says much about how they see their own national companies.

For issues like internet governance, the private sector is vital. There are three broad sets of

actors in internet governance – states, companies, and civil society organizations. In the past, states played a small role by design. This is changing as states assert their traditional roles. Internet governance is in transition, and what we will end up with, if this is well managed, is something like international finance, where private banks, Finance Ministries, and international institutions make decision about governance. This means that the influence of governments over the internet will increase and the influence of civil society organizations will shrink.

It can be hard to parse through the rhetoric that surrounds cybersecurity, but one way to think of this is that the internet is not that different form anything else and people should play the roles the usually play in guiding and securing it. Companies should be responsible for innovation in technology and providing services. Governments cannot do as well. Governments should play their traditional roles, ensuring public safety and law enforcement (including enforcement of contracts, defending citizens, and negotiating with other nations on trade, human rights, and all the other issues. Companies cannot do this, nor should we want them to – their job is to generate return to their shareholder.

The idea of formal cooperation among governments on internet issues is anathema to the old-school internet community. They fear that rules will harm the "free and open internet" to which all kinds of miraculous economic powers are ascribed. It is true that the global network has brought us immense economic benefits and offers still more. However, the free and open internet is long gone. To make cyberspace safe, we need transnational rules, norms, and institutions to manage and reduce risk, using international agreement on a collective approach to reduce risk and increase stability. Some countries will balk at cybersecurity norms, as they balked at norms against nuclear proliferation or money-laundering - but the right blend of incentives and penalties (like indictments in U.S. courts) will help change their minds.

The conflict in this lies between those countries like Russia and China that would like to see governments play a dominant role in cyberspace, in order to control information and minimize the political risk to undemocratic regimes, and those few governments that continue to insists that the informal arrangements for security and governance developed in the 1990s are still adequate. Neither approach is desirable but we have not yet identified an adequate replacement that does not diminish the private sectors role in those areas where their leadership is crucial.

There are several areas for partnership between companies and the government in international cybersecurity. At a company level, cybersecurity is a business decision about how much risk a company is willing to accept and how much they are willing to spend to mitigate this risk. Such decisions are best left to individual companies. In the foreign relations context, this largely involves company decisions about the risk of cyber espionage. Where the government can play an essential role is in helping companies adequately assess risk by providing relevant information and by developing penalties and sanctions for cyber economic espionage.

Similarly, American companies and the government must cooperate in rebuilding trust in American products and services. American information technology companies are often caught in the middle of an awkward debate, as foreign government fear to trust U.S. products while at the same time asking U.S. companies to cooperate with them in providing information. Rebuilding international trust requires a longer discussion that involves new ideas on data

protection, encryption, localization, and related issues. These issues fall outside the scope of cybersecurity when it is narrowly defined, but no major decision about cybersecurity can be made without reference to them, but the touchstone should be that our national interest is best served by foreign policies that keep American companies strong, competitive and secure in cyberspace.

The most difficult question for the role of companies in cybersecurity involves hacking back or active defense. Companies can do what they want on their own networks. Companies can do what their national laws allow on national networks. However, they cannot take action on networks in another country. This is illegal and poses serious political risk, even if a U.S. company uses a third party in countries like Israel.

Remember that Russia and China believe that U.S. companies are a tool of the government. They will interpret hacking back as an attack by the U.S. This poses real risk of retaliation and escalation into armed conflict. Our opponents include the Russian FSB and the Iranian Revolutionary Guard. They are unscrupulous, have a taste for violence, and will not hesitate to use force against an attacker. Cyber attacks can have unpredictable effects. The U.S. has led the way in seeking to have countries observe the rule of law in cyberspace. Hacking back not only undercuts this effort, but could put an American company in an awkward position. What if China, for example, was to ask the FBI to cooperate in an investigation of a hack-back or took out Interpol warrants for U.S. executives? If we say no, it ends any effort to get China to cooperate when we request investigations (as we did with the Sony incident). If we say yes, American executive will go to jail. I understand the frustration with the slow pace of reducing cyber crime, and U.S. efforts could usefully be accelerated, but we do not want amateur mistakes to lead to war or retaliation.

Cybersecurity at the State Department

The U.S. strategy has helped shape the diplomatic strategies of other western democracies. The global challenge to western institutions and to US-centric internet governance from authoritarian states and the effect of the NSA leaks – mean that we must reconsider this strategy and strengthen the organization framework that supports it.

The fundamental point for reconsideration is one that has been discussed for years. Should the U.S. try to win global agreement on cybersecurity norms for responsible state behavior, or should it begin with agreement among like-minded national and then seek to broaden this. Of course, it is possible to pursue both strategies simultaneously, but we now need to recognize that Russia and China are unlikely to agree with us on political issues in any meaningful way. The announcement of a cybersecurity agreement between Russia and China is an example of new and more oppositional policies (as are the recent maneuvers by their tiny flotilla of ships in the Mediterranean). The bilateral cyber agreement itself is largely for show, to annoy the Americans and the west, so we do not want to overstate it, but we also should not expect them to defer to American policy the way they did in the 1990s.

The counter argument against a like-minded approach is that we will lose the ‘fence sitters,” the new powers who are in neither in the western or the authoritarian camp. This fear results in

paralysis. The counterexample used against a like-minded approach is the Budapest Convention on cybercrime, which was negotiated among western countries and now faces opposition from new powers like India who say that since they were not involved in the negotiation, they cannot accept the agreement. It is also very likely that some of the new powers would refuse to participate if Russia and China are not involved. However, if progress in cybersecurity is held hostage to winning the agreement of authoritarian states, we will not get anywhere anytime soon.

A good way to think about this is to ask what would happen if the U.S. were to agree to condition any action by NATO on winning agreement from Russia or China, or from powerful non-aligned nations. This would be the end of collective security; we would hobble ourselves. While we need to engage with Russia and China, and perhaps some initial arms-control style agreements on cyber warfare are possible, and while we need to engage with and be respectful of the view of new powers like India, Brazil, and others, we should not refrain from action until we have their consent.

The NSA leaks had little effect on Russia and China, who either suspected or knew of NSA activities, but they have skillfully exploited them to try and divide the U.S. and key western allies. Crimea has caused far more damage to international negotiations on cybersecurity. The Russians have suspended the bilateral cybersecurity discussions that drove diplomatic progress, and their evaluation of the usefulness of an agreement limiting cyber attack may have changed as they move into a more militant posture vis-à-vis NATO. Crimea has sharpened interstate conflict, albeit in a hybrid rather than conventional venue, and has greatly reduced the chances for international agreement. Russian strategy has successfully made that country the focal point for agreement on cybersecurity.

A new strategy will need to be complex in that it would require differing 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 the use of financial sanctions and technological restraints to encourage better behavior and strengthen the rule of law in cyberspace. Precedents from the financial sector are particularly useful, where governments and leading banks work together to develop and follow principles and practices to increase stability and fight crime, suggest a new direction for cyber diplomacy.

A new strategy also requires an institutional underpinning. Cybersecurity is still an appendage within the Department. It is not incorporated into the structure of Bureaus and Undersecretaries State uses for most issues. In an ideal world, cybersecurity would be part of the politico-military Bureau and part of the portfolio of the Undersecretary for International Security Affairs. Arguments could be made that this issue should be place within the Economics or Global Affairs portfolios, but having sat in many negotiation session on cybersecurity, I can affirm that this is a politic-military issue and the negotiators who have done best in negotiations re from an arms control or international law enforcement background.

The U.S. pioneered the creation of cyber coordinators at the White house and at the State Department, an organizational approach many other countries have also copied, and while State has expanded the office of the cyber coordinator, it needs to further embed cybersecurity into the

fabric of our diplomacy. Any speech by a senior official on security or trade must mention cybersecurity, and while these officials may not be comfortable with the issue or fluent in its details, they cannot afford to avoid it. The best example of a missed opportunity is the negotiations on Russian entry to the WTO, completed in 2006, when the U.S. secured agreement on tariffs but signally failed to even mention cyber crime. This was a lost opportunity. We know from public examples that the President cares about this issue and has engaged foreign leaders, but there should be some thing between the President and Chris Painter. The Chinese, for example, watch this very closely and if a Cabinet Secretary appears in Beijing and does not mention cybersecurity, they judge it to mean that America is not serious.

You sometimes hear that the issue is too technical or too arcane for senior leaders to discuss. This is not true. Cybersecurity is now a central element of the larger international security agenda, the same way that nonproliferation was a new element twenty-five years ago, and it is important to embed cybersecurity into American foreign policy the same way that non-proliferation moved from being a technical issue to something of central importance. The internet is not going to get any less important for economies and security. This is not peripheral issue, particularly as the internet grows more and more important for our economic life and for international trade and security.

Next Steps

This is a much more difficult negotiating environment, but the biggest obstacle to progress is not recalcitrant authoritarians or skeptical new powers, but what some have called an era of "strategic timidity" in the West. If we are afraid of offending Russia, China or the new powers, we should just accept that while cybersecurity can be improved though better technology and greater attention by companies, it will not be secure against our most effective opponents.

There is always a temptation in American foreign policy to explain the international environment by saying that we are in a "new cold war" or to invoke elderly strategies like deterrence or containment to deal with the new challenges we face. We are not in a new Cold War. What we face is a more insidious challenge with countries who are our political and military opponents at the same time that they are our economic partners. In an interconnected world, they cannot be contained nor will they be deterred from challenging us. We can no longer blithely assume that we have the moral high ground – China, Russia and others will challenge our leadership. This is a new kind of contest and we must craft new foreign policies to advance our national interest, the interests of our allies, and of the world. Cybersecurity is among the most salient of these new challenges for American foreign policy and while there has been good progress in the last few years, we need a new a new approach to international agreement on cybersecurity.

In the last decade, cybersecurity has moved from being a peripheral issue or an issue confined to the classified world to one that is central for the internal security and diplomatic agenda. Given its importance for national security, public safety, trade, and development, cybersecurity is the right for the Committee to turn its attention to cybersecurity as it thinks about the foreign policy agenda for this Congress.

Thank you for the opportunity to testify and I would be happy to take any questions.