CSIS | CENTER FOR STRATEGIC & INTERNATIONAL STUDIES

Statement Before the

Senate Judiciary Committee

Subcommittee on Crime and Terrorism

"Cyber Threats to Our Nation's Critical Infrastructure"

A Testimony by:

James A. Lewis

Senior Vice President
Center for Strategic and International Studies

Distinguished Visiting Professor
Center for Cyber Security Studies
U.S. Naval Academy

August 21, 2018

226 Dirksen Senate Office Building

Mr. Chairman and Mr. Ranking Member, I thank you and the Committee for the opportunity to testify. I would like to discuss both domestic efforts to improve critical infrastructure cybersecurity and actions to dissuade other countries from attacking us in cyberspace. Both are essential.

The first federal policy on critical infrastructure and cybersecurity appeared in 1998. In hindsight, it focused on the wrong threat. It assumed that terrorists or non-state actors would launch crippling cyber-attacks against critical infrastructure. In twenty years, this has never happened, and it is unlikely to happen in the foreseeable future. Instead, our most dangerous and active opponents are hostile states.

Four countries - Russia, China, Iran, and North Korea - are in conflict with the United States in cyberspace. They use cyber operations for espionage and coercion, and they are prepared to use cyber operations to threaten or attack critical infrastructure when it serves their interest to do so. Russia and North Korea can be considered state-sponsors of cybercrime. All four have probed American critical infrastructure, with varying degrees of sophistication and success. Russia and Iran pose the greatest threat, since they have used infrastructure attacks against opponents and are actively hostile to the United States (it appears that China does not want to exacerbate trade tensions, and North Korea will be on its best behavior while its negotiations with the United States seem promising, making them less likely to attack critical infrastructure than Russia and Iran). Russia has peer or near peer cyber-attack capabilities and Iran's capabilities have improved rapidly. Both have prepared cyber-attacks against U.S. critical infrastructure, particularly energy infrastructure.

The most important critical infrastructures are energy, finance, telecommunications, and government services. None of these are secure if Russia, Iran, or other states chose to attack them. Changing this requires two elements: hardening the target through better cybersecurity at companies and agencies, and changing a potential attacker's calculations of risk and benefit. Neither of these are impossible tasks, but, while there has been progress in strengthening our cybersecurity, it has been too slow.

To rank our four most important critical infrastructures, the financial sector is in the most secure (although it also faces the greatest criminal threat), at least for big companies. One constant in cybersecurity is that if a network is difficult to hack, attackers move to an easier target. This can be small and medium companies, subcontractors, law firms, or even home computers of company employees. Small and medium firms and their contractors in all sectors face greater risk, as they do not have the resources for a high level of defense. This is also true for telecom and electrical power, where big providers have more resources and may be better defended than smaller regional companies.

Government agencies face a different set of problems. The federal government is a huge, sprawling enterprise where the problems have been in management and resources. Agencies do not control their own funding for cybersecurity or IT modernization. This administration has announced plans to improve cybersecurity at government agencies by modernizing IT, an essential first step, but there remain issues with workforce and senior management attention. State and local governments, which regulate and sometimes operate critical infrastructure, face similar problems with even less resources.

Looking specifically at the electrical power grid, which may be the most important national infrastructure, a general conclusion is that it is not adequately defended. This varies from company to company: some do a good job, while others do not. If you talk to cybersecurity experts with a deep knowledge of the industry and its control systems, they say we are vulnerable. Experts who investigated the Russian attacks against Ukrainian electrical facilities in 2015 and 2017 say the United States is absolutely vulnerable to similar Russian attacks on the power grid.

Cyber Defense and Opponent Risk Calculus

Changing this “absolute vulnerability” requires two sets of actions. The first is improving cyber defenses at critical infrastructure companies. Given the complexity of the technology and its interconnections, this is no easy task, but there are a number of steps that could be taken, including setting a mandatory baseline for security, increasing research into more secure control technologies, getting a full accounting of incidents and vulnerabilities at companies, and creating a national “red team” program that would carry out unannounced penetration tests against utilities. As a general rule, if a company is unwilling to report a breach or to have its defenses tested, there is probably something wrong. Investor confidence might be affected in the short term if companies were more transparent about their cybersecurity status, but research shows that this effect is temporary and no reason to avoid transparency.

The second is changing the risk calculus of potential attackers. This is not deterrence, at least in the Cold War sense of using nuclear threats to deter attack or create “strategic stability”. It is actively engaging with opponents using a variety of direct measures to affect their thinking. These measures include private and public communications, indictments, sanctions, building coalitions, and making credible threats of retaliatory action. Potential attackers need to know the full range of responses the United States could undertake in response to a cyber-attack, and this requires coherent policy. They need to believe that the United States will actually undertake these actions, and after the overly-cautious Obama Administration, we have an immense credibility deficit; our opponents know we have great capabilities, but they believe we will never actually use them.

Public discussion has tended to confuse the consequences of a major cyber-attack on critical infrastructure, which would be very damaging, with the likelihood of such as attack, which remains low. Our most dangerous opponents are states. They want to avoid a military confrontation with the United States without renouncing coercive acts. While all have plans to attack U.S. critical infrastructure, have done the reconnaissance for such an attack, and in some cases, have implanted malware for future use, all would be cautious in launching an actual attack since it could provoke a damaging U.S. response. They watch U.S. actions closely. When the United States backed down from its Syria chemical weapons redline, hostile cyber actions increased. Some categories of cyber-attack – espionage and political operations – are ideal for this kind of coercive action as they fall below the threshold that would justify an American military response. We need to both make critical infrastructure more secure and develop a range of responses – both military and legal – that discourage our opponents from attack.

Both sets of actions require a national strategy, leadership, and resources. Since 1998, cybersecurity has become front page news, with greater awareness among the public and sustained attention from businesses and policymakers. This is progress, but it would be overly optimistic to say that we are secure. Skilled, well-resourced, and determined criminal groups and state agencies continue to infiltrate American networks to extract money and information, and, in some cases, to plan for damaging attacks.

We can roughly assess progress by using two basic measurements: whether hackers can get into a network and whether they can take data out. For critical infrastructure, we could also ask whether essential services can continue to operate even after networks have been penetrated. Using these three measurements suggests that we are at best slowing the degradation of the cyber environment. While the script-kiddies, hacktivists and amateurs of the past have largely been eliminated as threats due to better law enforcement, they have been replaced by highly skilled, well-resourced, professional cybercriminals and intelligence agencies who are persistent in their efforts to defeat even advanced defenses. Not that hacking usually requires advanced skills. Most successful hacks still require only the most basic techniques.

Other metrics also do not suggest progress. By any measure, losses from cybercrime continue to increase at a dramatic rate. The best cybercriminals in the world live in Russia, where the government provides them a sanctuary from which they are safe from Western law enforcement as long as they do not go out of the country (and the Russian government warns its citizens not to go abroad where they face arrest). There are, as you know, very close ties between Russian cyber criminals, Russian organized crime, and the Kremlin, and these criminal groups reinforce the already powerful cyber capabilities of Russia's intelligence and military services.

Media reports that Chinese government hackers were able to steal classified data related to undersea warfare — which are likely to be accurate – are very disquieting since they come after more than a decade of effort by the Department of Defense to harden its networks. This report fit a long pattern of Chinese activity against U.S. military targets, and China has had spectacular intelligence success against the United States, beginning with the theft of nuclear weapons data in the early 2000s.

Commercial espionage appears to have decreased after a 2015 agreement with China, which was always the most aggressive collector of business information, but the agreement did not ban spying against military or defense industry targets, and according to U.S. government sources, the overall level of espionage activity against the United States by China, Russia, and others has increased to levels not seen since the Cold War. The most worrisome aspect of this is the brazen intrusions by Russian intelligence services into American politics, something that began well before the 2016 elections.

Russia, the Power Grid and Election Interference

Recent media accounts of Russian success in penetrating American power companies is part of the larger narrative of Russian political interference. Judging from the experience of Russian penetration of Ukrainian power facilities, Russian intent is more to signal and warn than to cripple. As the United States begins to discuss how to respond to Russian cyber activities, including the possibility of retaliatory cyber actions, the Russians are signaling that any American retaliation faces a Russian response that could disrupt critical infrastructure. The Russians were able to penetrate the networks of dozens of American power companies and, in some cases, implant malware in order to warn the United States and deter it from cyber retaliation.

The Kremlin may be playing a game of "chicken" with the United States to see who backs down first. They assume that it will be the Americans. They probe U.S. infrastructure; in response, the United States goes public on the Russian actions to warn them that they are not invisible and that we are not (completely) defenseless. Russia may have a sense of invulnerability in these efforts, and from his statements, it appears that Russian president Vladimir Putin despises the West. This is a new kind of conflict created by cyber capabilities, which gives countries the ability to manipulate, coerce, and perhaps attack. In this new style of conflict, the issue is not whether Russia attacks, but how we ensure that they do not.

Russian behavior is shaped by its assumptions about benefits and consequences. The Russians have been able to get away with unprecedented hostile and illegal actions in the United States and allied countries. Russia has little respect for the West and may have a sense of impunity. The Russian intelligence services are keen students of American society and have watched it closely and with hostile intent for decades. Their observations are colored by Leninism, which sees the United States as a corrupt hegemon, and by their cynical views of the hypocrisy of American democracy – the Russians, like the Chinese, believe that "House of Cards" is a documentary.

The Russians have penetrated the electrical grid for coercive purposes, to deter the United States from retaliating for their interference and possibly to disrupt service during the election, but so far, Russia's coercive actions have stayed below the use-of-force threshold (roughly defined in international law) and have avoided the violence that could trigger a crisis.

The United States and its allies have been slow to respond to this Russian effort and to find ways to counter what the Russians call "New Generation Warfare. New Generation Warfare uses disinformation, propaganda, coercive cyber-attacks, to disrupt Western politics to shape the thinking and politics of opponents. The Russians will continue to use New Generation Warfare against the United States. They have had tremendous success. There is no reason for them to stop.

The likelihood of further Russian coercive action is high if the United States does not do more in response. We need a different kind of strategy if we are to change Russian behavior, and this means the United States will need to be more aggressive in what theorists are calling the "grey zone" of conflict. At a minimum, it would be useful to publicly release an outline of a hierarchy of potential responses, ranging from limited military action, covert action, diplomatic efforts (including further expulsions), and the whole range of actions defined as retorsion and countermeasures under international law – these include sanctions, indictments, travel bans, and freezing assets.

For now, responding to Russia means using legal and financial actions. Any retaliation must have political effect, and in Russia, that means going after Putin's relationships with the oligarchs and their money. The United States could use Cyber Command against Russia, perhaps in a way similar to what Joint Task Force Ares was able to do against ISIS, but any action would need to be carefully considered to ensure proportionality and to manage the risk of escalation. Passage of the draft legislation entitled "Defending American Security from Kremlin Aggression" would greatly strengthen the American arsenal of responses.

Russia is eager to reclaim its status as a great power and push back against what they see as American predominance. Russia believes it has an opportunity to achieve long-standing goals: to damage NATO and the transatlantic alliance, undercut democratic values, re-establish its dominance in what it regards as its rightful sphere of influence, and, above all, to harm the United States. We have not pushed back hard enough against Russian interference. The absence of a coherent Russia policy in this administration compounds the failure of the Obama Administration to act against Russia. Individual actions, like indictments and sanctions are helpful, and there is good evidence now that sanctions are inflicting pain on the Russian economy. Additional sanctions would be helpful in dissuading Russia from attacking the United States, whether it is electoral machinery or the electrical grid, but such measures will be most effective if they are part a comprehensive approach that lays out the full range of U.S. responses. U.S. efforts in the next few months should focus on preventing the Russians from overestimating their impunity and miscalculating how much they can get away with in their actions.

Administration Cybersecurity Efforts

This strategy must be complemented by a robust domestic effort to improve cybersecurity. Each administration since 1998 had made efforts to improve cybersecurity through the development of policies and organizational changes. The latest is the May 2017 Executive Order on "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." This EO proposes a number of valuable initiatives. Its three main subjects are improving the cybersecurity of federal networks, strengthening cybersecurity in critical infrastructure, and developing international and deterrence strategies for the United States. It has been seventeen months since the EO was issued, and we can ask how much progress there has been in fulfilling its mandate.

From the outside, it appears that one administration goal is to shift authority for cybersecurity from the National Security Council (NSC) and back to the agencies, part of a larger effort to streamline the NSC and other White House offices. Every President becomes frustrated with slow pace and occasional unresponsiveness of agency work, and one solution has been to draw implementation and oversight into a White House staff that is more responsive to the President. This reached new heights under the Obama Administration, with an NSC swollen to almost four hundred employees, accompanied by a plethora of new "Chief Officers." This was twice as many as the Bush Administration and perhaps five times as many as the Reagan Administration. Trimming the NSC and returning responsibilities to the agencies is a good idea – if the agencies actually perform.

Eliminating the cybersecurity coordinator was one cut to NSC staff that deserves a closer look. It may be an underestimation of the need for coordination among the agencies. It is appropriate for a new National Security Advisor to pick his own staff, but some suspect this cut indicates that cybersecurity is a lower priority in this administration. No one would ever say cybersecurity is less important, but we should review administration actions to strengthen defenses and dissuade opponents from cyberattack.

The May 2017 EO set a variety of deadlines – 45 days, 90 days, 180 days, and 240 days. From the outside, these deadlines appear to have been met. This may not be the case in all instances and the administration could help by providing a public scorecard on progress on these taskings. A report on the readiness of the United States to manage an attack on the electrical sector was due a year ago, for example. If there is a classified report, it would be useful to provide an unclassified version to guide public discussions and highlight where legislative action may be needed.

Agency Activities

Most of the steps taken by the administration have been organizational, and they are too recent to judge their effectiveness. DHS recently held its first National Cybersecurity Summit to help develop a coordinated approach to protecting critical infrastructure. At the Summit, DHS announced the creation of the National Risk Management Center, which will evaluate U.S. critical infrastructure in the energy, finance, and telecommunications sectors. This is a good first step, although it is not clear if the Center has any new funding or authorities, but it is not a substitute for the reorganization DHS needs for its cyber function.

The U.S. was at the cutting edge of cybersecurity policy in 2009, but it is no longer there. In 2009, it set the precedent of drafting comprehensive national, international, and military strategies and created a cyber coordinator at the White House. Many countries followed the U.S. example, but many have moved to a next generation cyber policy. This usually means creating an independent cyber agency with some regulatory authority that works with and guides critical infrastructure companies to improve their own security and the national defense. The UK's National Cyber Security Center is a leading example of the new approach and one the United States could learn from.

The United States has consistently preferred to locate critical infrastructure protection functions at DHS, but DHS's cyber function needs to be restructured. The important parts of any reorganization are for DHS to clearly articulate a cyber mission that falls within the scope of its authorities, improve its cybersecurity capabilities, and make the National Protection and Programs Directorate (NPPD) an operational component of DHS, similar to TSA, CBP, or FEMA, rather than be an element of the Office of the Secretary of DHS, including a new name for NPPD that emphasizes it cyber mission. These changes could require legislative approval if reorganization is to be meaningful.

Some argue that since DHS lacks the capabilities for cybersecurity DOD or NSA should assume a greater role in protecting infrastructure. This move would be unpopular with companies and poses constitutional challenges. The best answer for domestic cybersecurity is to make DHS more effective and develop (as has been done in the UK and elsewhere) a robust operational partnership with the intelligence agencies, as part of a larger coherent national approach.

The Department of Energy released a cybersecurity strategy for the energy sector in June and created a new Office of Cybersecurity, Energy Security, and Emergency Response in February to strengthen DOE's efforts in cybersecurity and energy security. This administration has announced that strengthening the cybersecurity of the electrical sector is a priority, and DOE has statutory authorities under the FAST Act. These are welcome steps and the new office is very promising – it may have inspired DHS to create its own Center—, but it is too early to gauge effectiveness, with a new Assistant Secretary still waiting to be confirmed.

The State Department's cyber function was hampered by ill-conceived efforts at reorganization. The turmoil this created still reverberates in the Department and, combined with the absence of an NSC Cyber Coordinator, has slowed the efforts to rewrite the 2011 International Cybersecurity Strategy, which is badly out of date. While there are very effective people in the Department's Cyber office, the disorganization and bureaucratic infighting damage our ability to work with allies and opponents to construct a comprehensive defense for protecting critical infrastructure from cyber-attack.

The Justice Department created a Cyber-Digital Task Force in February. The Task Force released its report and recommendations in July. These recommendations focused on election interference, cybercrime, and the law enforcement response to cyber incidents. Again, this is a good first step, and the creation of a DOJ Task Force is in itself a good organizational step, but it has been only seven weeks, and it is too early to assess how well these recommendations are being implemented.

The Justice Task Force Report first chapter discusses the DOJ and FBI responsibilities to counter foreign influence operations. Much of the responsibility falls on the states, raising problems of federalism in designing a response, but it is now clear that interfering in the 2016 election was a major Russian espionage operation, falling within the mandate of the DOJ/FBI responsibilities for counterintelligence.

Efforts to defend elections involve identifying hostile state activity (entirely Russian) on social media and developing ideas to protect the electoral infrastructure. The social media efforts, while complicated by free speech concerns and a lack of regulatory authority, have had some success. The efforts to weed out malign foreign activity from social media may be the most important for electoral defense, given the attention Russian doctrine gives to manipulating opinion, sowing mistrust, and causing confusion.

When it comes to hardening electoral infrastructure, we do not know if the Russians will attack the electoral infrastructure in 2018 – they did not in 2016 – so strengthening it could be immaterial. Russia may save their best tricks for 2020. A focus on improving cybersecurity in electoral or electrical infrastructure is inadequate to blunt the Russian threat. This will require an all-of-government strategy, aggressive counterintelligence operations by FBI and its intelligence community partners, accompanied by actions (such as sanctions) to deter the Russians from further interference and punish them if they do not.

The Department of Defense has spearheaded the effort to rewrite PPD-20, the directive on government cyber operations, to give Cyber Command more flexibility in taking action. The effect will not be to "unleash" Cyber Command, but to give the same authorities to manage operations as any other combatant commander. Presidential approval is still required, but once the use of military force has been authorized, Cyber Command could develop and undertake operations under the guidance of the Department of Defense and the White House, but without continual consultation with the interagency process, something that greatly hampered and delayed U.S. actions in the past.

Clearer authorities and better capabilities (provided by the cyber mission teams) will be most useful for national defense when it is embedded in a comprehensive and coherent cyber strategy under White House guidance and messaging. An important first step would be to issue a simple, clear declaratory policy about the consequences of cyber-attacks against the United States.

Resilience is a Last Resort.

Resilience is a last resort. It means opponents have decided to attack and our defenses have failed. The best outcome is to discourage countries from attacking the United States in the first place. If we cannot, most research suggests that our cyber defenses are inadequate. This is something that can be improved, but this will take years, and the United States would benefit from planning how to build resilience into critical infrastructure.

The United States has some experience with this from blizzards and hurricanes, but there are unresolved issues on acquiring and maintaining redundant capacity; coordination among companies, federal, state, and local governments; and in funding. Most companies do not want redundant capacity – it means using capital for an activity that does not generate returns. Concrete planning for how to quickly restore critical infrastructure services in the aftermath of an attack, including actual exercises, and how to continue to operate in a degraded cyber environment, is necessary for the hostile and conflictive environment we find ourselves in today. This could begin with a focus on critical infrastructure of greatest risk.

Better, But Still Not Secure

To summarize, after eighteen months, the administration has recently taken a number of positive steps on cybersecurity, but they are so recent that we cannot assess implementation, nor has there been time for these new policies and organizations to improve our cyber defenses. As it moves forward, the administration needs to avoid the mistake previous administrations have made of confusing drafting a report or policy with taking action. We can make critical infrastructure more resilient and better protected, over time, but this will take years. The immediately useful step is to change the calculation of our opponents, particularly Russia and Iran, about the risk of cyber-attacks against the United States. With the right policies, this can be done quickly and with effect.

I thank the Committee for the opportunity to testify and welcome any questions.