Written Statement of

Bruce W. McConnell
Global Vice President
EastWest Institute

March 22, 2017
"A Borderless Battle: Defending Against Cyber Threats"
Committee on Homeland Security
U.S. House of Representatives

I am Bruce W. McConnell, Global Vice President of the EastWest Institute, a 36-year-old, independent, non-partisan, non-profit organization dedicated to preventing and reducing security conflicts among nations on the ground and in cyberspace. EWI works closely with senior government and private sector officials in all the major powers around the world to establish and support trustworthy dialogue about some of the most difficult security issues facing the planet.

Before joining EWI I served for four years at the US Department of Homeland Security (DHS), departing in 2013 as the Acting Deputy Under Secretary for Cybersecurity. I also served at the US Office of Management and Budget under Presidents Ronald Reagan, George H. W. Bush, and William Clinton, with responsibility for information technology policy and security.

This statement covers two topics: an assessment of the current state of conflict in cyberspace, and my views on how the US government should address those conflicts.

1. How Unstable is Cyberspace Today?

Nearly four years ago US national security advisor Susan Rice observed that the world's "most vexing security challenges are transnational security threats that transcend borders: climate change, piracy, infectious disease, transnational crime, cyber theft, and the modern-day slavery of human trafficking." Today, one would add migration, violent extremism, and the safety of fissile nuclear materials to that list.

These issues share at least two characteristics: First they are accentuated in their severity by modern technology. The bad guys, both state and non-state actors, are well equipped with the latest computers, communications equipment, and weaponry, and their ability to use these tools is enhanced by their access to global networks.

Second, no international regimes or institutions have these transborder issues well in hand. Rather, global bodies like the World Health Organization or the International Telecommunication Union are generally struggling to remain relevant. The post-war structures that have kept peace for 70 years face a crisis of legitimacy as rising powers that were not present at Bretton Woods scorn the old order and create their own institutions and power centers.

Today we are focusing on security and cyberspace. Cyber-enabled attacks in the lead-up to the U.S. Presidential election roiled relationships in Washington and globally. The term cyber-enabled emphasizes a new characteristic of cyberspace -- it's no longer its own thing. It's part of everything. There is very little actual "cyber crime." Instead, we see a plethora of ordinary crimes and attacks: theft, fraud, trespassing and destruction of property that use cyber means.

From a geopolitical standpoint, this cyber-enablement has produced a runaway cyber arms race, led by the United States, Russia, China, Iran, Israel, and some European countries, with many others, including the Democratic People's Republic of Korea **(**DPRK), following close behind. Over thirty countries have formed cyber offense units. Non-state actors such as organized criminal gangs and the Islamic State are also players.

The U.S. Democratic National Committee hacks and related incidents consist of burglary and publication of the fruits on Wikileaks. From a legal standpoint, while it is against U.S. law to enter a computer without authorization, these incidents may fall more into the shadow zone of espionage. As for the publication, the U.S. Supreme Court has generally protected media publication of accurate, stolen materials of public interest obtained by a third party.

What's new for Americans is the possibility that there is an "information war" between East and West. Indeed, some states do not use the term cybersecurity, preferring the broader term "information security." The events around the U.S. election evoked a spirited conversation last month at the Munich Security Conference around fake news, political trolling, social media bots, and the weaponization of intelligence.[1]

On the other hand, earlier this month, we also saw additional evidence regarding Western actions against North Korean missile systems and the CIA's capabilities. Even assuming the most benign motivations by all parties, these continuing, ungoverned state-on-state skirmishes in cyberspace increasingly undermine terrestrial security and stability.

In contrast to cyberspace, other international domains are governed by norms of behavior and international law. In the airspace it is illegal to shoot down a commercial aircraft. But in cyberspace, the way in which international law applies is still being debated.

[1] US Homeland Security Secretary John Kelly was on hand in Munich to remind European participants that DHS had reaffirmed the previous administration's designation of election systems as critical infrastructure and that the Department continued its work with state election officials to help them secure their systems on a voluntary basis.

In commercial aviation we have organizations like the private sector International Air Transport Association and the governmental International Commercial Aviation Organization that partner to maintain safety and security on a global basis. There are no comparable institutions for cyberspace.

Everyone in this room is painfully familiar with the provisions that keep that network secure: identity proofing of everyone who gets close to a passenger plane, licensing of pilots, filing of flight plans, certification of aircraft, etc. We have none of these things in cyberspace. Yet the financial value of the commercial transactions conducted over the Internet (and here I'm not even counting SWIFT and other special purpose networks) is actually 100 times greater on an annual basis than the value of goods transported in the air cargo system.

Progress is modest. A group of governmental cyber experts has worked at the United Nations for over 10 years to come up with an initial set of non-binding norms of behavior in cyberspace.

These include:

- Not allowing the use of information and communications technology, or ICT, to intentionally damage another country's critical infrastructure.
- Not allowing international cyber attacks to emanate from their territory.
- Responding to requests for assistance from another country that has been attacked by computers in the first country.
- Preventing the proliferation of malicious tools and techniques and the use of harmful hidden functions.
- Encouraging responsible reporting of ICT vulnerabilities and sharing associated information.
- Not harming the information systems of the authorized cybersecurity incident response teams.

In February 2017, the government of the Netherlands, with the support of Microsoft, the Internet Society, the EastWest Institute, and the Hague Centre for Strategic Studies, launched the Global Commission on the Stability of Cyberspace. The GCSC is chaired by Marina Kaljurand, former Estonian foreign minister, and co-chaired by Michael Chertoff, former US Secretary of Homeland Security and Latha Reddy, India's former deputy national security adviser. This multistakeholder commission will build on and extend existing efforts to develop and advocate for norms and polices to enhance international security and stability and guide responsible state and non-state behavior in cyberspace.

On the private sector side, global ICT companies are beginning to step up to the responsibility that comes with their great power in cyberspace. For example, Microsoft recently issued a set of norms of industry behavior that global ICT companies should follow in their business practices. Examples of the kinds of norms that companies are considering include:

- Creating more secure products and services.
- Not enabling states to weaken the security of commercial, mass-market ICT products and services.
- Practicing responsible vulnerability disclosure.
- Collaborating to defend their customers against and recover from serious cyber attacks.
- Issuing updates to protect their customers no matter where the customer is located.

Clearly, the industry is at an immature stage. Its rapid growth in importance has outstripped systems of governance, including the first line of defense – the market. As a general matter, until very recently customers demanded two things from the firms that supply ICTs – price and features. The market has responded, giving us all manner of convenience and efficiency, in business and in our private lives. Finally, however, buyers are starting to recognize the criticality of ICT to their daily activities, and thus they demand, and may be willing to pay for, security.

Yet there is a gap between what they need and what they are able to command. To address this gap, we recently published a "Buyers Guide for Secure ICT."[2] This guide recommends questions that buyers can ask ICT suppliers to help them evaluate the security of the products and services that these suppliers deliver.

Despite best efforts, the reality of today's dynamic technological environment -- with product cycles of 18 months or less – continues to challenge policy development. Two developments are dramatically altering the security picture.

First, we are moving to the cloud. We store our information there on virtual machines operated by major providers like Amazon Web Services. While AWS and Microsoft's Azure provide much stronger cybersecurity and resilience than any single enterprise can field, they also create systemic risk, with large potential consequences from technology failures or attacks.

A second emerging source of risk is the Internet of Everything (IoE). In a few years there will be ten times as many devices -- Fitbits, heart monitors, automobiles, thermostats, machine tools and floodgates -- connected to the Internet than today's smartphones and computers. These devices, when combined with 3-D printing, promise to disruptively transform manufacturing and transportation. They will also create a ubiquitous, global sensor network that will be communicating what is going on everywhere. And these sensors are shockingly insecure -- built with easy to guess passwords, transmitting their data unencrypted, and being essentially un-patchable.

[2] "Purchasing Secure ICT Products and Services: A Buyers Guide," EastWest Institute, September 2016, https://www.eastwest.ngo/sites/default/files/EWI_BuyersGuide.pdf.

The conventional wisdom is that the IoE represents a massive increase in the attack surface. But at EWI, we are exploring two questions. First, why do we assume the bad guys will own the sensor network? Why not have the good guys own it and use the knowledge of what is happening on the Internet to increase security -- for example, by isolating problems and fixing them before they can spread? Second, we ask, how will the IoE shift the balance between endpoint and network security, and what are the societal implications of that shift?

One that is gaining currency in the US is the Cybersecurity Framework created by the National Institute of Standards and Technology, or NIST, which is part of the US Department of Commerce. The framework lays out the basics of a cybersecurity program that all firms should manage to. It also lays the foundation for future cyber insurance underwriting standards.

For at least a decade, there has been a lot of hype that we will all be left freezing in the dark, as was the case before the turn of the 21st century with the so-called millennium or Y2K bug. These scenarios have not materialized, and in fact it is actually quite difficult to create broad systemic damage today. But the capability to attempt catastrophic attacks is increasing, and the generally deteriorating international security situation does not help.

In sum, it is a dynamic risk environment, augmented by our electronic connectedness and interdependence. We must continually adapt risk management to rapidly changing technology. Agility rules.

2. How Should the US Government Move Forward to Meet these Challenges?

Over the past eight years, the previous Administration working closely with this Committee and the rest of Congress, tested, revised, and eventually established a clear set of roles and responsibilities for cybersecurity among the relevant federal agencies. One can trace the progress of these efforts that took place on a bipartisan basis across administrations and Congresses, including:

- Homeland Security Presidential Directive 23/National Security Presidential Directive 54, "Cybersecurity Policy," January 8, 2008.[3]
- The Comprehensive National Cybersecurity Initiative, May 2009.[4]
- The March 2013 "Bubble Chart" (See Attachment A).
- Six statutes enacted in 2014 and 2015 –
    - National Cybersecurity Protection Act of 2014 (S. 2519), which codifies DHS's cybersecurity center.

[3] *See*, https://fas.org/irp/offdocs/nspd/nspd-54.pdf.
[4] Currently archived after partial declassification in 2011 at: https://obamawhitehouse.archives.gov/node/233086.

    - Cybersecurity Enhancement Act of 2014 (S. 1353), which codifies the National Institute of Standards and Technology's (NIST's) role in cybersecurity.
    - Cybersecurity Workforce Assessment Act (H.R. 2952), which requires the DHS to develop a cyber-workforce strategy.
    - Border Patrol Agent Pay Reform Act of 2014 (S. 1691), which gives DHS new authorities for cybersecurity hiring.
    - Federal Information Security Modernization Act of 2014 (S. 2521), which reforms federal IT security management.
    - Cybersecurity Act of 2015 (within H.R. 2029), December 15, 2015, which enhances protections for information sharing and further strengthen's DHS viila coordination role.
- Presidential Policy Directive 41, "US Cyber Incident Coordination."[5]

These documents firmly cement the primary role of the Department of Homeland Security in securing the Nation's critical cyber infrastructure. In doing so, these documents are broadly consistent with each other and reflect two important assumptions:

- First, cyberspace is fundamentally a civilian space. As former Deputy Secretary of Homeland Security Jane Holl Lute and I wrote in Wired in 2011, cyberspace is "a neighborhood, a library, a marketplace, a school yard, a workshop – and a new, exciting age in human experience, exploration and development. Portions of it are part of America's defense infrastructure, and these are properly protected by soldiers."[6]

This is an important assumption for two reasons. First and foremost, it is fundamentally consistent with American values. As a nation, we have long recognized the importance of the military in providing the common defense, within limitations in tradition and law that respect the historical lessons learned when the Crown quartered soldiers in civilian homes without consent, after the actions taken to suppress the Whiskey Rebellion of 1794 with the authorization of Justice James Wilson, and, post-Reconstruction in the Posse Comitatus Act of 1878. This tradition is reflected in Department of Defense Directive 3025.18, "Defense Support of Civilian Authorities."

The appropriate role of the military in cyberspace is also important from a practical standpoint. The military must protect its own assets and its ability to project force globally. It relies on a safe and secure cyberspace to do both of those things. But simply as a practical matter, the Defense Department cannot secure all of cyberspace. Indeed, as we have seen over the past ten years, it is challenged to protect its own electronic assets and those of critical defense contractors from

[5] *See*, "Presidential Policy Directive -- United States Cyber Incident Coordination," July 26, 2016, https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident.
[6] *See*, "A Civil Perspective on Cybersecurity," https://www.wired.com/2011/02/dhs-op-ed/. (Also provided as Attachment B.)

internal and external attacks. These jobs are too important to our national security to permit DoD to be distracted by other tasks that are in the end not part of its core mission.

- The second assumption reflected in current law and policy is that securing cyberspace is a team effort. No single agency, and no single company or group of companies, can handle this challenge by itself. There must be cooperation and coordination. Agencies must work with each other and with the private sector, applying their capabilities and authorities in a seamless manner.

Seamlessness is not easy. In fact, in order to achieve it and avoid key problems falling through the cracks, there needs to be some overlap in responsibilities. While overlap can generate confusion, it is essential for full coverage.

These policy documents are explicit about the overlap, laying out joint responsibilities for tasks where appropriate. Such joint activities have become the norm in today's US government. Every morning, the Departments of Homeland Security, Justice, and Defense coordinate on a "First Look" video conference, sharing the latest developments and coordinating action plans. Conflicts can arise, for example, between the DHS mission to mitigate problems in critical infrastructure and the FBI's mission to preserve evidence for prosecution. These operational problems get worked out on the ground when these agencies work together with the victim of a cyber attack. And, when chronic or policy differences arise, a well-organized National Security Council will do its job and resolve those differences satisfactorily among the agencies for the good of the Nation.

3. Conclusion

Cyberspace is a dynamic and dangerous environment. It is also the global endoskeleton of commerce, trade, and all manner of human interaction. Securing it, an essential task, is a global, multistakeholder effort that must bring all capabilities to bear in a cooperative manner. Agility rules. The US is a world leader in having clearly established roles and responsibilities within government so that it can play its critical role. The new administration and the Congress should focus on getting the implementation right.[7] Time is too short to do otherwise.

[7] As co-panelist Frank Cilluffo stated, "PPD-41 is a good initiative, but the real test will lie in the manner and nature of its implementation." *See*, "Overview and Analysis of PPD-41: US Cyber Incident Coordination," July 27, 2016, https://www.lawfareblog.com/overview-and-analysis-ppd-41-us-cyber-incident-coordination.