Prepared Keynote Remarks of Michele Markoff:
An Overview of the Identification of Norms in the GGE
Delivered at the International Security Cyber Issues Workshop Series Workshop on "The Future of Norms to Preserve and Enhance International Cyber Stability"
February 9, 2016
Palais des Nations, Geneva, Switzerland

Introduction

- Good morning. It is a pleasure to be here in the Palais des Nations, at the start of a very a timely workshop on "The Future of Norms to Preserve and Enhances International Cyber Stability."

- Before I begin, I would like to express my sincere thanks to the organizers of this workshop at the United Nations Institute for Disarmament Research, and the Center for Strategic and International Studies for their hard work making this day possible. I would also like to thank our co-sponsors from the Government of Netherlands for their contribution to this day. And then of course, it's important to thank all of you that are here. I would like to especially thank our distinguished speakers, who have traveled here from around the world—your presence here makes this a truly multistakeholder exchange. And finally, of course, I would like to recognize the government participants in this workshop. You all represent some of the best governmental thinkers on appropriate state behavior in cyberspace. I have engaged with many of you on these issues in the past, and I look forward to a spirited discussion over the next two days.

- Before I speak about norms specifically, I think it is important to provide as general context the U.S. view on international security in cyberspace. Overall, the United States' goal is to begin to create a framework of strategic cyber stability. As we all know, the Internet is not a technology that can easily be controlled. Instead, we must forge consensus and promote active international collaboration on a series of mutually reinforcing cooperative strategies that together address the transnational nature of the various threats to networked information systems.

- There are two pillars to our approach: principles of responsible state behavior and practical confidence building measures. While our discussion today and tomorrow will focus on an element of the first pillar, I see all of these ideas as interlocking and mutually reinforcing. It is important to briefly describe both pillars in order to present a complete picture.

Pillar 1: Identifying Principles of Responsible State Behavior

- With regard to the first pillar, our work to identify principles of responsible state behavior in cyberspace has primarily taken place at the UN Group of Government Experts (GGE). And there has been significant progress in recent years—particularly in the last two GGEs.

- In the 2013 GGE, there was consensus among the 15 participating governmental experts that existing international law applies to state conduct in cyberspace. The membership of this group was a very diverse set of governments, yet they reached this consensus because they recognized that acknowledging this basic fact could reduce the risk of conflict and misunderstanding.

- In the 2015 GGE report, an expanded group representing 20 states took a further step forward by highlighting that the UN Charter applies in its entirety, affirming the applicability of the inherent right to self-defense as recognized in Article 51 of the Charter, and noting the applicability of the law of armed conflict's fundamental principles of humanity, necessity, proportionality, and distinction. Importantly, for our conversation today, the experts also recommended a number of voluntary norms designed for peacetime. I'll discuss more on that in a moment.

- While the GGE plays a distinct role in the global conversation on principles of responsible state behavior cyberspace, we certainly want all states to affirm the applicability of international law in cyberspace as well as commit to adhering to certain voluntary peacetime norms. This is why I have been particularly pleased in recent years to see an increasing number of states—both on their own and in multilateral settings—affirming many of the concepts agreed to at the GGE. The most recent example of this can be found in the ICT security language included in the recent G20 leadership statement.

Pillar 2: Confidence Building Measures

- The second pillar is to construct practical measures to build confidence in cyberspace. These measures allow states to cooperate regularly and pragmatically in order to build some transparency and predictability into their behavior in cyberspace.

- While the 2013 GGE report as well as the more recent GGE consensus have affirmed the importance of CBMs, the more practical nature of CBMs means that it is really in the hands of individual countries—whether working bilaterally or multilaterally through regional security organizations, like the OSCE or the ARF—to develop and implement CBMs that address the specific threats and challenges that they face.

- I think of cyber CBMs as coming in three varieties. Transparency measures—like sharing cyber strategies—are aimed at reducing uncertainty about states' intentions in cyberspace, which in turn increases stability. Cooperative measures—like putting in

place points of contact or mediation mechanisms or conducting joint tabletop exercises—are meant to provide states with means to work together to respond to or prevent cyber incidents. Finally, there are stability measures, which are measures of self-restraint.

- I provide this detail, because norms and CBMs—particularly when it comes to stability measures—often dovetail nicely. Agreement to adhere to a norm, like the norm against intentionally damaging critical infrastructure, is itself a measure of self-restraint that can help to build confidence. As a result, we should be aware that our efforts today and tomorrow are doubly important because they can lead to practical steps that states can take to build confidence in cyberspace. With that, let me turn back to the topic of norms within the context of the GGE.

Norms in the GGE

- In a broader sense, all of our work to promote international security in cyberspace, including in the GGE, is normative. It is based on the view that principles of responsible state behavior that have long been held to apply to states in other domains—and that have maintained stability and prevented major conflicts for decades—also apply to states' acts in cyberspace.

- It is true that ICTs are technologies that continue to undergo rapid change and development, which presents both opportunities and challenges. But that should not prevent us from doing what we have always done when other new and potentially disruptive technologies have emerged. It is particularly important that States find a way to maintain stability in cyberspace, because these technologies offer such promise for our economies and societies.

- Our discussion of voluntary, non-binding norms of state behavior in peacetime, or "peacetime norms," emerged from our discussion of international law at the GGE. And here, I have to give due credit to my Chinese and Russian colleagues. They observed during our discussions in the GGE that most state conduct in cyberspace takes place—and is likely to continue take place—during peacetime.

- Now I must point out that there are important and very relevant areas of international law that do apply during peacetime. The law of state responsibility, including the law of countermeasures, and international human rights law are only two examples. But this observation from our Chinese and Russian colleagues did get me thinking: Are there additional voluntary, non-binding norms that would promote greater stability in cyberspace if all responsible states agreed to adhere to them? Others of us asked themselves the same question.

- And so began a series of discussions both within many of our own governments and at the GGE. These discussions culminated in last year's GGE report, which put forward 11 proposed peacetime norms. These included several norms long championed by the United States concerning the protection of critical infrastructure, the protection of computer incident response teams, and cooperation between states in responding to appropriate requests to mitigate malicious cyber activity emanating from their territory. But it also included norms championed by other states. One norm, for example, calls on states to seek to prevent the proliferation of cyber tools that can be used for malicious purposes.

- I believe that this work is an important step forward in our collective efforts because it helps us to draw clearer lines about what types of actions by states are unacceptable in cyberspace. As more norms are accepted by more states, my hope is that this acceptance will lead to stronger coalitions of states who can work together to respond to and prevent irresponsible behavior.

- At the same time, I do not see the norms we identified last year as the end of the conversation. I believe that there may be additional norms that we should identify. Some of them could be further elaborations on the norms that already have been proposed—perhaps providing more specificity on issues like critical infrastructure and the spread of cyber tools that can be used for malicious purposes. Others could be entirely new. I am particularly interested in the idea of technical norms. For example, one could consider norms against disrupting or manipulating certain core functions that the Internet relies on.

- This is why I have particularly been looking forward to our discussions today and tomorrow. I see them as the beginning of the next phase in our continuing dialogue about norms. And I hope that it can serve the dual purpose of both bringing new states into the conversation and providing a sound foundation for the next round of the UN GGE, due to begin later this year.