https://www.state.gov/s/l/releases/remarks/264303.htm

REMARKS ON INTERNATIONAL LAW AND STABILITY IN CYBERSPACE

Brian J. Egan
Legal Adviser
Berkeley Law School, California
November 10, 2016

Thank you to Saira for that kind introduction, and thank you to the Miller Institute, the Human Rights Center, and the Berkeley Center for Law and Technology for inviting me to give this talk. I am honored to be back at Boalt Hall. I've had the chance to spend a few days in Berkeley meeting with students and feeling nostalgic. I also spent some time at the beginning of my trip at the Stanford campus, where I was an undergraduate. Please do not hold that against me as you listen to my remarks! From my short time back, it is clear that this city and this law school remain as vibrant and socially engaged today as they were when I was a student here nearly 20 years ago.

This is a fitting place to discuss the topic I am here to speak about today—the importance of international law and stability in cyberspace—just across the Bay from Silicon Valley, home to many of the world's largest and most innovative information technology companies. The remarkable reach of the Internet and the ever-growing number of connections between computers and other networked devices are delivering significant economic, social, and political benefits to individuals and societies around the world. In addition, an increasing number of States and non-State actors are developing the operational capability and capacity to pursue their objectives through cyberspace. Unfortunately, a number of those actors are employing their capabilities to conduct malicious cyber activities that cause effects in other States' territories. Significant cyber incidents—including many that are reportedly State-sponsored—frequently make headline news.

In light of this, it is reasonable to ask: could we someday reach a tipping point where the risks of connectivity outweigh the benefits we reap from cyberspace? And how can we prevent cyberspace from becoming a source of instability that could lead to inter-State conflict?

I don't think we will reach such a tipping point, but how we maintain cyber stability in order to preserve the continued benefits of connectivity remains a critical question. And international law, I would submit, is an essential element of the answer.

Existing principles of international law form a cornerstone of the United States' strategic framework of international cyber stability during peacetime and during armed conflict. The U.S. strategic framework is designed to achieve and maintain a stable cyberspace environment where all States and individuals are able to realize its benefits fully, where there are advantages to cooperating against common threats and avoiding conflict, and where there is little incentive for States to engage in disruptive behavior or to attack one another.

There are three pillars to the U.S. strategic framework, each of which can help to ensure stability in cyberspace by reducing the risks of misperception and escalation. The first is global affirmation of the applicability of existing international law to State activity in cyberspace in both peacetime and during armed conflict. The second is the development of international consensus on certain additional voluntary, non-binding norms of responsible State behavior in cyberspace during peacetime, which is of course the predominant context in

which States interact. And the third is the development and implementation of practical confidence-building measures to facilitate inter-State cooperation on cyber-related matters. I'll address two of these pillars—international law and voluntary, non-binding norms—in greater detail today.

International Law

In September 2012, my predecessor, Harold Koh, delivered remarks on "International Law in Cyberspace" at U.S. Cyber Command's Legal Conference. It says a lot about where we were four years ago that the first two questions Koh addressed in his speech were as fundamental as: "Do established principles of international law apply to cyberspace?" and "Is cyberspace a law-free zone, where anything goes?" (So as not to leave you hanging, the answers to those questions are an emphatic "yes" and "no" respectively!)

We have made significant progress since then. One prominent forum in which these issues are discussed is the United Nations (UN) Group of Governmental Experts (GGE) that deals with cyber issues in the context of international security. The GGE is a body established by the UN Secretary-General with a mandate from the UN General Assembly to study, among other things, how international law applies to States' cyber activities, with a view to promoting common understandings. In 2013, the 15-State GGE recognized the applicability of existing international law to States' cyber activities. Just last year, the subsequent UN GGE on the same topic, expanded to include 20 States, built on the 2013 report and took an additional step by recognizing the applicability in cyberspace of the inherent right of self-defense as recognized in Article 51 of the UN Charter. The 2015 GGE report also recognized the applicability of the law of armed conflict's fundamental principles of humanity, necessity, proportionality, and distinction to the conduct of hostilities in and through cyberspace. With other recent bilateral and multilateral statements, including that of the leaders of the Group of Twenty (G20) States in 2015, we have seen an emerging consensus that existing international law applies to States' cyber activities.

Recognizing the applicability of existing international law as a general matter, however, is the easy part, at least for most like-minded nations. Identifying how that law applies to specific cyber activities is more challenging, and States rarely articulate their views on this subject publicly. The United States already has made some efforts in this area, including by setting forth views on the application of international law to cyber activities in Koh's 2012 speech and also in the U.S. submission to the 2014–15 UN GGE, both of which are publicly available in the Digest of U.S. Practice in International Law. The U.S. Department of Defense also has presented its views on aspects of this topic in its publicly available Law of War Manual. But more work remains to be done.

Increased transparency is important for a number of reasons. Customary international law, of course, develops from a general and consistent practice of States followed by them out of a sense of legal obligation, or opinio juris. Faced with a relative vacuum of public State practice and opinio juris concerning cyber activities, others have sought to fill the void with their views on how international law applies in this area. The most prominent and comprehensive of these efforts is the Tallinn Manual project. Although this is an initiative of the NATO Cooperative Cyber Defence Centre of Excellence, it is neither State-led nor an official NATO project. Instead, the project is a non-governmental effort by international lawyers who first set out to identify the international legal rules applicable to cyber warfare, which led to the publication of "Tallinn Manual 1.0" in 2013. The group is now examining the international legal framework that applies to cyber activities below the threshold of the use of force and outside of the context of armed conflict, which will result in the publication of a "Tallinn Manual 2.0" by the end of this year.

I commend the Tallinn Manual project team on what has clearly been a tremendous and thoughtful effort. The United States has unequivocally been in accord with the underlying premise of this project, which is that existing international law applies to State behavior in cyberspace. In this respect, the Tallinn Manuals will

make a valuable contribution to underscoring and demonstrating this point across a number of bodies of international law, even if we do not necessarily agree with every aspect of the Manuals.

States must also address these challenging issues. Interpretations or applications of international law proposed by non-governmental groups may not reflect the practice or legal views of many or most States. States' relative silence could lead to unpredictability in the cyber realm, where States may be left guessing about each other's views on the applicable legal framework. In the context of a specific cyber incident, this uncertainty could give rise to misperceptions and miscalculations by States, potentially leading to escalation and, in the worst case, conflict.

To mitigate these risks, States should publicly state their views on how existing international law applies to State conduct in cyberspace to the greatest extent possible in international and domestic forums. Specific cyber incidents provide States with opportunities to do this, but it is equally important—and often easier—for States to articulate public views outside of the context of specific cyber operations or incidents. Stating such views publicly will help give rise to more settled expectations of State behavior and thereby contribute to greater predictability and stability in cyberspace. This is true for the question of what legal rules apply to cyber activity that may constitute a use of force, or that may take place in a situation of armed conflict. It is equally true regarding the question of what legal rules apply to cyber activities that fall below the threshold of the use of force and take place outside of the context of armed conflict.

Although many States, including the United States, generally believe that the existing international legal framework is sufficient to regulate State behavior in cyberspace, States likely have divergent views on specific issues. Further discussion, clarification, and cooperation on these issues remains necessary. The present task is for States to begin to make public their views on how existing international law applies.

In this spirit, and building on Harold Koh's remarks in 2012 and the United States' 2014 and 2016 submissions to the UN GGE, I would like to offer some additional U.S. views on how certain rules of international law apply to States' behavior in cyberspace, beginning first with cyber operations during armed conflict, and then turning to the identification of voluntary, non-binding norms applicable to State behavior during peacetime.

Cyber Operations in the Context of Armed Conflict

Turning to cyber operations in armed conflict, I would like to start with the U.S. military's cyber operations in the context of the ongoing armed conflict with the Islamic State of Iraq and the Levant (ISIL). As U.S. Defense Secretary Ashton Carter informed Congress in April 2016, U.S. Cyber Command has been asked "to take on the war against ISIL as essentially [its] first major combat operation […] The objectives there are to interrupt ISIL command-and-control, interrupt its ability to move money around, interrupt its ability to tyrannize and control population[s], [and] interrupt its ability to recruit externally."

The U.S. military must comply with the United States' obligations under the law of armed conflict and other applicable international law when conducting cyber operations against ISIL, just as it does when conducting other types of military operations during armed conflict. To the extent that such cyber operations constitute "attacks" under the law of armed conflict, the rules on conducting attacks must be applied to those cyber operations. For example, such operations must only be directed against military objectives, such as computers, other networked devices, or possibly specific data that, by their nature, location, purpose, or use, make an effective contribution to military action and whose total or partial destruction, capture, or neutralization, in the circumstances ruling at the time, offers a definite military advantage. Such operations also must comport with the requirements of the principles of distinction and proportionality. Feasible precautions must be taken to reduce the risk of incidental harm to civilian infrastructure and users. In the

cyber context, this requires parties to a conflict to assess the potential effects of cyber activities on both military and civilian infrastructure and users.

Not all cyber operations, however, rise to the level of an "attack" as a legal matter under the law of armed conflict. When determining whether a cyber activity constitutes an "attack" for purposes of the law of armed conflict, States should consider, among other things, whether a cyber activity results in kinetic or non-kinetic effects, and the nature and scope of those effects, as well as the nature of the connection, if any, between the cyber activity and the particular armed conflict in question.

Even if they do not rise to the level of an "attack" under the law of armed conflict, cyber operations during armed conflict must nonetheless be consistent with the principle of military necessity. For example, a cyber operation that would not constitute an "attack," but would nonetheless seize or destroy enemy property, would have to be imperatively demanded by the necessities of war. Additionally, even if a cyber operation does not rise to the level of an "attack" or does not cause injury or damage that would need to be considered under the principle of proportionality in conducting attacks, that cyber operation still should comport with the general principles of the law of war.

Other international legal principles beyond the rules and principles of the law of armed conflict that I just discussed are also relevant to U.S. cyber operations undertaken during armed conflict. As then-Assistant to the President for Homeland Security and Counterterrorism John Brennan said in his September 2011 remarks at Harvard Law School, "[i]nternational legal principles, including respect for a State's sovereignty […], impose important constraints on our ability to act unilaterally […] in foreign territories." It is to this topic—the role played by State sovereignty in the legal analysis of cyber operations—that I'd like to turn now.

Sovereignty and Cyberspace

In his remarks in 2012, Harold Koh stated that "States conducting activities in cyberspace must take into account the sovereignty of other States, including outside the context of armed conflict." I would like to build on that statement and offer a few thoughts about the relevance of sovereignty principles to States' cyber activities.

As an initial matter, remote cyber operations involving computers or other networked devices located on another State's territory do not constitute a per se violation of international law. In other words, there is no absolute prohibition on such operations as a matter of international law. This is perhaps most clear where such activities in another State's territory have no effects or de minimis effects.

Most States, including the United States, engage in intelligence collection abroad. As President Obama said, the collection of intelligence overseas is "not unique to America." As the President has also affirmed, the United States, like other nations, has gathered intelligence throughout its history to ensure that national security and foreign policy decisionmakers have access to timely, accurate, and insightful information. Indeed, the President issued a directive in 2014 to clarify the principles that would be followed by the United States in undertaking the collection of signals intelligence abroad.

Such widespread and perhaps nearly universal practice by States of intelligence collection abroad indicates that there is no per se prohibition on such activities under customary international law. I would caution, however, that because "intelligence collection" is not a defined term, the absence of a per se prohibition on these activities does not settle the question of whether a specific intelligence collection activity might nonetheless violate a provision of international law.

Although certain activities—including cyber operations—may violate another State's domestic law, that is a separate question from whether such activities violate international law. The United States is deeply respectful of other States' sovereign authority to prescribe laws governing activities in their territory. Disrespecting another State's domestic laws can have serious legal and foreign policy consequences. As a legal matter, such an action could result in the criminal prosecution and punishment of a State's agents in the United States or abroad, for example, for offenses such as espionage or for violations of foreign analogs to provisions such as the U.S. Computer Fraud and Abuse Act. From a foreign policy perspective, one can look to the consequences that flow from disclosures related to such programs. But such domestic law and foreign policy issues do not resolve the independent question of whether the activity violates international law.

In certain circumstances, one State's non-consensual cyber operation in another State's territory could violate international law, even if it falls below the threshold of a use of force. This is a challenging area of the law that raises difficult questions. The very design of the Internet may lead to some encroachment on other sovereign jurisdictions. Precisely when a non-consensual cyber operation violates the sovereignty of another State is a question lawyers within the U.S. government continue to study carefully, and it is one that ultimately will be resolved through the practice and opinio juris of States.

Relatedly, consider the challenges we face in clarifying the international law prohibition on unlawful intervention. As articulated by the International Court of Justice (ICJ) in its judgment on the merits in the Nicaragua Case, this rule of customary international law forbids States from engaging in coercive action that bears on a matter that each State is entitled, by the principle of State sovereignty, to decide freely, such as the choice of a political, economic, social, and cultural system. This is generally viewed as a relatively narrow rule of customary international law, but States' cyber activities could run afoul of this prohibition. For example, a cyber operation by a State that interferes with another country's ability to hold an election or that manipulates another country's election results would be a clear violation of the rule of non-intervention. For increased transparency, States need to do more work to clarify how the international law on non-intervention applies to States' activities in cyberspace.

Some may ask why it matters where the international community draws these legal lines. Put starkly, why does it matter whether an activity violates international law? It matters, of course, because the community of nations has committed to abide by international law, including with respect to activities in cyberspace. International law enables States to work together to meet common goals, including the pursuit of stability in cyberspace. And international law sets binding standards of State behavior that not only induce compliance by States but also provide compliant States with a stronger basis for criticizing—and rallying others to respond to—States that violate those standards. As Harold Koh stated in 2012, "[i]f we succeed in promoting a culture of compliance, we will reap the benefits. And if we earn a reputation for compliance, the actions we do take will earn enhanced legitimacy worldwide for their adherence to the rule of law." Working to clarify how international law applies to States' activities in cyberspace serves those ends, as it does in so many other critical areas of State activity.

Before leaving the topic of sovereignty, I'd like to address one additional related issue involving a State's control over cyber infrastructure and activities within, rather than outside, its territory. In his 2012 speech, Koh observed that "[t]he physical infrastructure that supports the Internet and cyber activities is generally located in sovereign territory and is subject to the jurisdiction of the territorial State." However, he went on to emphasize that "[t]he exercise of jurisdiction by the territorial State, however, is not unlimited; it must be consistent with applicable international law, including international human rights obligations."

I want to underscore this important point. Some States invoke the concept of State sovereignty as a justification for excessive regulation of online content, including censorship and access restrictions, often

undertaken in the name of counterterrorism or "countering violent extremism." And sometimes, States also deploy the concept of State sovereignty in an attempt to shield themselves from outside criticism.

So let me repeat what Koh made clear: Any regulation by a State of matters within its territory, including use of and access to the Internet, must comply with that State's applicable obligations under international human rights law.

There is no doubt that terrorist groups have become dangerously adept at using the Internet and other communications technologies to propagate their hateful messages, recruit adherents, and urge followers to commit violent acts. This is why all governments must work together to target online criminal activities—such as illicit money transfers, terrorist attack planning and coordination, criminal solicitation, and the provision of material support to terrorist groups. U.S. efforts to prevent the Internet from being used for terrorist purposes also focus on criminal activities that facilitate terrorism, such as financing and recruitment, not on restricting expressive content, even if that content is repugnant or inimical to our core values.

Such efforts must not be conflated with broader calls to restrict public access to or censor the Internet, or even—as some have suggested—to effectively shut down entire portions of the Web. Such measures would not advance our security, and they would be inconsistent with our values. The Internet must remain open to the free flow of information and ideas. Restricting the flow of ideas also inhibits spreading the values of understanding and mutual respect that offer one of the most powerful antidotes to the hateful and violent narratives propagated by terrorist groups.

That is why the United States holds the view that use of the Internet, including social media, in furtherance of terrorism and other criminal activity must be addressed through lawful means that respect each State's international obligations and commitments regarding human rights, including the freedom of expression, and that serve the objectives of the free flow of information and a free and open Internet. To be sure, the incitement of imminent terrorist violence may be restricted. However, certain censorship and content control, including blocking websites simply because they contain content that criticizes a leader, a government policy, or an ideology, or because the content espouses particular religious beliefs, violates international human rights law and must not be engaged in by States.

State Responsibility and the "Problem of Attribution" in Cyberspace

I have been talking thus far about States' activities and operations in cyberspace. But as many of you know, it is often difficult to detect who or what is responsible for a given cyber incident. This leads me to the frequently raised and much debated "problem of attribution" in cyberspace.

States and commentators often express concerns about the challenge of attribution in a technical sense—that is, the challenge of obtaining facts, whether through technical indicators or all-source intelligence, that would inform a State's determinations about a particular cyber incident. Others have raised issues related to political decisions about attribution—that is, considerations that might be relevant to a State's decision to go public and identify another State as the actor responsible for a particular cyber incident and to condemn that act as unacceptable. These technical and policy discussions about attribution, however, should be distinguished from the legal questions about attribution. In my present remarks, I will focus on the issue of attribution in the legal sense.

From a legal perspective, the customary international law of state responsibility supplies the standards for attributing acts, including cyber acts, to States. For example, cyber operations conducted by organs of a State or by persons or entities empowered by domestic law to exercise governmental authority are attributable to that State, if such organs, persons, or entities are acting in that capacity.

Additionally, cyber operations conducted by non-State actors are attributable to a State under the law of state responsibility when such actors engage in operations pursuant to the State's instructions or under the State's direction or control, or when the State later acknowledges and adopts the operations as its own.

Thus, as a legal matter, States cannot escape responsibility for internationally wrongful cyber acts by perpetrating them through proxies. When there is information—whether obtained through technical means or all-source intelligence—that permits a cyber act engaged in by a non-State actor to be attributed legally to a State under one of the standards set forth in the law of state responsibility, the victim State has all of the rights and remedies against the responsible State allowed under international law.

The law of state responsibility does not set forth explicit burdens or standards of proof for making a determination about legal attribution. In this context, a State acts as its own judge of the facts and may make a unilateral determination with respect to attribution of a cyber operation to another State. Absolute certainty is not—and cannot be—required. Instead, international law generally requires that States act reasonably under the circumstances when they gather information and draw conclusions based on that information.

I also want to note that, despite the suggestion by some States to the contrary, there is no international legal obligation to reveal evidence on which attribution is based prior to taking appropriate action. There may, of course, be political pressure to do so, and States may choose to reveal such evidence to convince other States to join them in condemnation, for example. But that is a policy choice—it is not compelled by international law.

Countermeasures and Other "Defensive" Measures

I want to turn now to the question of what options a victim State might have to respond to malicious cyber activity that falls below the threshold of an armed attack. As an initial matter, a State can always undertake unfriendly acts that are not inconsistent with any of its international obligations in order to influence the behavior of other States. Such acts—which are known as acts of retorsion—may include, for example, the imposition of sanctions or the declaration that a diplomat is persona non grata.

In certain circumstances, a State may take action that would otherwise violate international law in response to malicious cyber activity. One example is the use of force in self-defense in response to an actual or imminent armed attack. Another example is that, in exceptional circumstances, a State may be able to avail itself of the plea of necessity, which, subject to certain conditions, might preclude the wrongfulness of an act if the act is the only way for the State to safeguard an essential interest against a grave and imminent peril.

In the time that remains, however, I would like to talk about a type of State response that has received a lot of attention in discussions about cyberspace: countermeasures. The customary international law doctrine of countermeasures permits a State that is the victim of an internationally wrongful act of another State to take otherwise unlawful measures against the responsible State in order to cause that State to comply with its international obligations, for example, the obligation to cease its internationally wrongful act. Therefore, as a threshold matter, the availability of countermeasures to address malicious cyber activity requires a prior internationally wrongful act that is attributable to another State. As with all countermeasures, this puts the responding State in the position of potentially being held responsible for violating international law if it turns out that there wasn't actually an internationally wrongful act that triggered the right to take countermeasures, or if the responding State made an inaccurate attribution determination. That is one reason why countermeasures should not be engaged in lightly.

Additionally, under the law of countermeasures, measures undertaken in response to an internationally wrongful act performed in or through cyberspace that is attributable to a State must be directed only at the State responsible for the wrongful act and must meet the principles of necessity and proportionality, including the requirements that a countermeasure must be designed to cause the State to comply with its international obligations—for example, the obligation to cease its internationally wrongful act—and must cease as soon as the offending State begins complying with the obligations in question.

The doctrine of countermeasures also generally requires the injured State to call upon the responsible State to comply with its international obligations before a countermeasure may be taken—in other words, the doctrine generally requires what I will call a "prior demand." The sufficiency of a prior demand should be evaluated on a case-by-case basis in light of the particular circumstances of the situation at hand and the purpose of the requirement, which is to give the responsible State notice of the injured State's claim and an opportunity to respond.

I also should note that countermeasures taken in response to internationally wrongful cyber activities attributable to a State generally may take the form of cyber-based countermeasures or non-cyber-based countermeasures. That is a decision typically within the discretion of the responding State and will depend on the circumstances.

Voluntary, Non-Binding Norms of Responsible State Behavior in Peacetime

In the remainder of my remarks, I'd like to discuss very briefly another element of the United States' strategic framework for international cyber stability: the development of international consensus on certain additional voluntary, non-binding norms of responsible State behavior in cyberspace that apply during peacetime.

Internationally, the United States has identified and promoted four such norms:

- First, a State should not conduct or knowingly support cyber-enabled theft of intellectual property, trade secrets, or other confidential business information with the intent of providing competitive advantages to its companies or commercial sectors.

- Second, a State should not conduct or knowingly support online activity that intentionally damages critical infrastructure or otherwise impairs the use of critical infrastructure to provide service to the public.

- Third, a State should not conduct or knowingly support activity intended to prevent national computer security incident response teams (CSIRTs) from responding to cyber incidents. A State also should not use CSIRTs to enable online activity that is intended to do harm.

- Fourth, a State should cooperate, in a manner consistent with its domestic and international obligations, with requests for assistance from other States in investigating cyber crimes, collecting electronic evidence, and mitigating malicious cyber activity emanating from its territory.

These four U.S.-promoted norms seek to address specific areas of risk that are of national and/or economic security concern to all States. Although voluntary and non-binding in nature, these norms can serve to define an international standard of behavior to be observed by responsible, like-minded States with the goal of preventing bad actors from engaging in malicious cyber activity. If observed, these measures—which can include measures of self-restraint—can contribute substantially to conflict prevention and stability. Over time, these norms can potentially provide common standards for responsible States to use to identify and respond to behavior that deviates from these norms. As more States commit to observing these norms, they will be

increasingly willing to condemn the malicious activities of bad actors and to join together to ensure that there are consequences for those activities.

It is important, however, to distinguish clearly between international law, on the one hand, and voluntary, non-binding norms on the other. These four norms identified by the United States, or the other peacetime cyber norms recommended in the 2015 UN GGE report, fall squarely in the voluntary, non-binding category. These voluntary, non-binding norms set out standards of expected State behavior that may, in certain circumstances, overlap with standards of behavior that are required as a matter of international law. Such norms are intended to supplement existing international law. They are designed to address certain cyber activities by States that occur outside of the context of armed conflict that are potentially destabilizing. That said, it is possible that if States begin to accept the standards set out in such non-binding norms as legally required and act in conformity with them, such norms could, over time, crystallize into binding customary international law. As a result, States should approach the process of identifying and committing to such non-binding norms with care.

In closing, I wanted to highlight a few points. First, cyberspace may be a relatively new frontier, but State behavior in cyberspace, as in other areas, remains embedded in an existing framework of law, including international law. Second, States have the primary responsibility for identifying how existing legal frameworks apply in cyberspace. Third, States have a responsibility to publicly articulate applicable standards. This is critical to enable an accurate understanding of international law, in the area of cyberspace and beyond. I hope that these remarks have furthered this goal of transparency, and highlighted the important role of international law, and international lawyers, in this important and dynamic area.

Thank you for bearing with me, and I would be happy to field a few questions.