FSC-PC.DEL/30/10
9 June 2010

Original: ENGLISH

United States Mission to the OSCE

Cyber Security Keynote Address by Dr. Deborah Schneider, U.S. Department of State

As delivered to the Joint FSC/PC, Vienna
June 2, 2010

Thank you very much for that very kind introduction. Good morning ladies and gentlemen and thank you for having me here. It's my pleasure this morning to discuss the U.S. proposal on expanding discussion of responsible State behavior in cyberspace. Considerable work has been done in the past 10 years in various fora to come to understandings amongst States of how States can work together to enhance cyber security. This morning I will review some of that work, propose that the next step is to discuss State-on-State behavior, explain why we believe the OSCE is a particularly appropriate forum for expanding the discussion, and finally I will preview for you U.S. thinking on how existing international legal principles apply in cyberspace and identify a few challenges for the discussion. This discussion follows on the U.S. Food for Thought paper which was introduced several months ago.

Beginning in the year 2000 we saw a number of resolutions in the UN General Assembly on combating the criminal misuse of information technology. For example in 2000 a resolution underscored the need to have modern, effective, national laws to adequately prosecute cyber crimes and to facilitate timely transnational investigative cooperation. That resolution in 2000 noted the value of a variety of measures, including:

- That States should ensure that their laws and practice eliminate safe havens for those who criminally misuse cyberspace;
- Encouraging law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse;
- That information should be exchanged between States regarding the problems that they face in combating the criminal misuse of information technologies;
- That States should make the general public aware of the need to prevent and combat criminal misuse;
- That to the extent practicable, information and communication technologies should be designed to help prevent and detect criminal misuse, to trace criminals and to collect evidence;
- That the fight against the criminal misuse of cyberspace requires the development of solutions taking into account both the protection of individual freedoms and the preservation of the capacity of States to fight criminal misuse.

In 2001 an UNGA Resolution on combating high technology crimes specifically noted the work of international and regional organizations. I will return shortly to this point of the valuable role of regional organizations in discussing behavior in cyberspace.

This resolution included reference to the work of the Council of Europe in elaborating the Convention on Cybercrime, as well as the work of those organizations in promoting dialogue between government and the private sector on safety and confidence in cyberspace.

Following these discussions, in 2003 States affirmed the need for the creation of a widespread culture of cyber security, and recognizes the responsibility of States to lead all elements of society to understand their roles and responsibilities with regard to cyber security. A resolution in 2003 highlighted nine complementary elements that all participants should address. These included:

- Augmenting awareness of the need for security;
- What steps States could take to enhance cyber security;
- Responsibility for the security of information and communication technologies;
- Responsiveness, to act in a timely manner to prevent, detect and respond to security incidents;
- Ethics, in recognizing that our actions or inactions in cyberspace may harm others;
- Democracy, in the sense that security should be implemented in a fashion consistent with democratic societies;
- And a variety of measures on Risk Assessments;
- Security design and implementation;
- Security management; and
- Reassessment, to mean that periodically we should reevaluate current approaches to security policies, based on changing threats and vulnerabilities of this quick changing medium of communication.

In 2004 we took up the issue of critical infrastructure protection in an UNGA resolution which focused in particular on those behaviors and actions that Member States should consider in their efforts to create a culture of cyber security and to protect critical information infrastructures. These too can be considered a set of common understandings to which governments should ascribe, and they provide an essential basis in order to facilitate international understanding and international collaboration on risk management. Among many items this resolution took up:

- The necessity for emergency warning networks for cyber-vulnerabilities;
- Raising awareness to facilitate stakeholders' understanding of the nature and extent of critical information infrastructures;
- Examining the infrastructures and identify interdependence among them;
- Promoting partnerships, both public and private, to share and analyze critical information infrastructure vulnerabilities, and to respond to damage or attacks;
- Creating and maintaining crisis communication networks;

- Ensuring that data availability policies take into account the need to protect critical information infrastructures;
- And a variety of engagements in international cooperation to secure these infrastructures, including facilitating tracing attacks, conduct training and exercises, having adequate substantive and procedural laws and trained personnel to enable States to investigate and prosecute attacks, and promoting national and international research and development, encouraging the applicability of security technologies that meet international standards.

Other common international understandings affect how States pursue our cyber security goals. The right to the free flow of information for example is well-established internationally. It's embodied in the UN Declaration of Human Rights and the International Covenant on Civil and Political Rights. A number of these principles have been affirmed in numerous international fora, to include the UN General Assembly, the International Telecommunication Union, and the World Summit on the Information Society, among others.

At least 16 UN Security Council resolutions have called on States to combat terrorism. For example, UNSCR 1373 (2001) called on all States to work together to prevent terrorist acts, obligated States to suppress terrorist financing, recruitment, planning, and facilitation within their territories, and called on all States to share information to prevent and suppress terrorist activities . The International Convention for the Suppressing of Financing of Terrorism, to which 169 States are parties, criminalized the collection or provision of funds to support terrorist acts. Some resolutions, such as UNSCR 1822 (2008), call for information sharing and cooperation and are concerned with terrorists' criminal misuse of the Internet in particular.

We believe the time is right to expand conversations between States to include views regarding State on State behavior in cyberspace. Both global and regional organizations have a role in these discussions.

Our goal here today is to stimulate discussion in the OSCE on these measures and these common understandings. We believe that European security is intrinsically linked to cyber security in many ways and that a particularly productive discussion could be held in this forum. The geographic scope of the membership of the OSCE, 56 States with extremely high levels of Internet penetration and even more importantly very high levels of government dependence on cyber infrastructure and high dependence on SCADA systems (that is, energy, water and other critical infrastructures that are linked to the information and communications technologies we are discussing today) means in our understanding that the OSCE might have a particularly strong interest in discussing measures to increase stability along these lines. This forum provides a comprehensive concept of security and a mature forum for discussion in which to raise these issues, we believe.

The U.S. Food for Thought paper introduced in March provides the U.S. thinking on questions such as:

- How we can extend to the cyber sphere the common understanding between States that help ensure international peace and stability;
- How existing principles of international law apply in cyberspace;
- How we can increase the predictably of State behavior in cyberspace.

These questions have to do with the continuum of activities States undertake nationally to be able to coordinate internationally and to maintain and contribute to international stability.

Our goal in providing our Food for Thought paper and following up with my presentation this morning is to catalyze discussions among participating States on this topic.

The focus of discussion, we believe, should be to explore whether there are common views among States that would increase predictability and stability, and to identify and discuss any major differences in views among States. Simply the process of having these discussions, we believe, will provide a useful increase in confidence among States that one can predict and understand another State's behavior in cyberspace.

Delegations in the UN Group of Governmental Experts studied the notion of enhancing predictability and regularizing notions of State behavior. That group, including the United States, this year came to the conclusion that the principles of *jus ad bellum* and *jus in bello* apply in cyberspace. Cyberspace is in no way exempt. We believe the basic principles apply and provide a firm basis for discussions on expectations about States' behavior in cyberspace.

Specifically, it is the U.S. understanding with regard to *jus ad bellum* that some cyber incidents can rise to the level of a use of force.

With regard to *jus in bello* we believe the Law of Armed Conflict applies generally in cyberspace.

The U.S. continues, however, to study the unique attributes of information and communications technology that provide challenges in how to apply these principles. We believe this is a useful and fruitful avenue of exploration for OSCE dialogue.

In light of the unique attributes of information and communications technology, it may be difficult to reach a definitive legal conclusion as to whether a particular disruptive activity in cyberspace constitutes an armed attack triggering the right to self-defense. For example, where the responsible actor and the motive for the disruptive activity are unknown and damaging effects result that do not directly result in substantial death or physical destruction, it may be possible to reach differing conclusions about whether an armed attack has occurred. However, such ambiguities and room for disagreement do not in our view suggest the need for a new legal framework specific to cyberspace. They simply are a reflection of the challenges in applying the UN Charter framework that already exists in many contexts. Nevertheless, under some circumstances, a disruptive activity could constitute an armed attack. In that context, the established principle of the right to self-defense against an

imminent or actual armed attack would apply whether the attacker is a State actor or a non-State actor.

Further, the use of force in self-defense must be limited to what is necessary to address an imminent or actual armed attack and must be proportionate to the threat that is faced.

Indeed, in the NATO Center of Excellence report, recently published, it was noted that a large scale attack on NATO command and control or energy grids could warrant consultations under article 4 and could lead to collective defense measures under article 5.

Under this framework States are required to take all necessary measures to ensure that their territories are not used by other States or by non-State actors for purposes of armed activities – including planning, threatening, perpetrating, or providing material support for armed attacks – against other States and their interests.

The Law of Armed Conflict sets forth the rules, known as *jus in bello,* that apply to the conduct of armed conflict, including the use of information technology tools in the context of an armed conflict. In particular, key principles of the Law of Armed Conflict would play an important role, we believe, in judging the legality of cyber attacks during an armed conflict:

- The principle of *distinction* requires that attacks to be limited to legitimate military objectives and that civilian objects shall not be the object of an attack.
- The *prohibition on indiscriminate attacks* includes a prohibition on attacks which employ a means or method of warfare that cannot be reasonably directed at a specific military objective.
- The principle of *proportionality* prohibits attacks which may be expected to cause incidental loss to civilian life, injury to civilians, or damage to civilian objects which would be excessive in relation to the concrete and direct military advantage anticipated.

These principles prohibit State attacks on purely civilian infrastructure. They prohibit the disruption or destruction of which would produce no meaningful military advantage. In addition, the potential for collateral damage would have to be assessed before attacking a military target. In other words, in an armed conflict, military targeting analysis would have to be conducted for information technology attacks just as it traditionally has been conducted for attacks using conventional and strategic weapons.

I reiterate that there are unique aspects of information and communications technology that provide challenges in this framework. One such challenge presented by the development of cyberspace is the principle of distinction. The principle clearly continues to apply to any use of cyberspace in the context of an armed conflict, but the unique attributes of cyber technology present new questions concerning *how* that principle should be applied.

For example, much cyber infrastructure upon which State militaries rely is shared with, and in many cases owned by, private civilian entities and user communities.

Moreover, because of the interconnected, interoperable nature of cyberspace, attacks affecting networked information infrastructures in one country can have effects on civilians not only in that country, but in many States around the world connected to them via the technology. Facts such as these will require States to develop ways of ensuring that their implementation of the principles of proportionality and distinction take into account these new realities.

Of increasing concern are individuals or groups or organizations who engage in malicious online activities on behalf of others, whether State or non-State actors, whether for financial compensation or for other reasons. Reports abound of "bot-masters" who offer an array of malicious activities for financial compensation, their services available to the highest bidder. Private citizens as well may be motivated by spur of the moment nationalist impulses, or could be motivated by government tolerance or even government encouragement. Unique attributes of information technology would offer a high degree of anonymity to such actors and effectively obscure any relationship to a sponsor, thus offering the sponsor increased plausible deniability.

The challenges States face in addressing the risk created by this threat is formidable. The attributes of cyber technology mean that the actions of each one of these threat actors are likely visible only in their effects in cyberspace or in the physical. Capabilities are difficult to see, and for the most part, highly confident attribution of identity to perpetrators cannot be achieved in a quick manner, if ever, and our success in attribution often depends on a high degree of transnational cooperation. The role of proxies in cyberspace further complicates the process of attribution, as an affected party must identify not only the actual, technical perpetrator, but also the sponsor, promising to make this challenge even more troublesome.

These layered impediments to effectively constraining capabilities or attributing the hostile or unlawful use of such capabilities to a perpetrator require that States organize and lead domestic efforts to develop and deploy a resilient, layered cyber defense, regardless of the source of the threat. At the same time, the complex transnational nature of these threats, and the interdependency of our globally-interconnected cyber system, requires collaboration on mutually reinforcing strategies to effectively manage risks and increased predictability on a global basis.

As I've outlined today, participating States face the daunting challenge of managing a highly varied and complex threat environment in cyberspace. Over the past decade, States have recognized the need for performing domestic due diligence in a variety of areas related to cybercrime and creating a culture of cyber security. They have endorsed State obligations to combat terrorist facilitation and planning, whether or not they take place in cyberspace. They have also affirmed the need for transnational cooperation in the areas of cybercrime, sharing best practices, and managing and responding to incidents.

Other areas of transnational concern have yet to receive similar attention. These include risks of misperception resulting from a lack of shared understanding among States regarding

international norms, or common understandings, pertaining to State behavior in cyberspace, which could affect crisis management or response in the event of major cyber events.

We believe the time is ripe to extend our discussion to the State-on-State behavior in cyberspace.

This argues for the elaboration of mutually reinforcing and overlapping measures designed to enhance cooperation and build confidence where possible. Such measures could be designed to build confidence, reduce risk, or enhance transparency and stability.

We believe the OSCE, as an established regular forum for discussing strategic security concepts, is the right forum. We think that perhaps an exchange of national views on international legal norms in this forum could expand UN discussions and lead the way pertaining to increased understanding of the behavior of States in cyberspace.

Ladies and gentlemen, that concludes my presentation today. Thank you for your time this morning and I look forward to hearing your remarks and to continuing this discussion in the future.