





**Position of the United States of America for the purpose of the conference held by Forum for 21<sup>st</sup> Century on 29 November 2011 reflected in the first draft of the negotiation paper, regarding the global Cybersecurity issues.**

The United States highly appreciate the initiation of the discussion and organizing the conference on global cybersecurity issues, today's diplomatic priority for the United States. We would like to thank the Forum for 21<sup>st</sup> Century for the invitation to the Conference. At the same time the United States express full support towards solving the challenges occurring in the new global scenario and towards building a future for cyberspace that will be profitable for everyone.

After an in-depth analysis of the first draft proposed by the Forum for 21<sup>st</sup> Century let us submit the position of the United States including our suggestions about selected topics as well.

Today, we are faced with a crucial decision. We can either work together to reveal the full potential of networks all around us which will provide greater prosperity and security for all, or we can succumb to narrow interests and undue fears that limit progress. The choice of the United States is unequivocal. We invite all nations to join us in the process of creating a future for cyberspace that is open, interoperable, secure and reliable. The United States see the most important issues in assecuration of collective security in the 21<sup>st</sup> century.

In the section *Notes*:

-  America's growing dependence on information technology has given rise to the need for greater protection of digital networks and infrastructures. The United States agree with the Forum for 21<sup>st</sup> Century that the protection of communication systems is essential in order to ensure prosperity, security and openness in a networked world so that innovation could continue to flourish, drive markets and improve lives. At the same time we believe that without proper cybersecurity strategy the other security strategies might lose their purpose. Therefore, cybersecurity should be perceived as an obligation that our governments and societies must take on willingly. There are more than four billion digital wireless devices in the world today. Scarcely a half-century ago, that number was zero. We live in a rare historical moment with an opportunity to build on cyberspace's successes and help secure its future for U.S. citizens and the global community.
-  The United States strongly believe that the Forum for 21<sup>st</sup> Century has identified properly the cyberattacks to be one of the major threats today. The growing number of attacks on our cyber networks has become one of the most serious economic and national security threats our nation faces. While the United States have faced a host of potential threats in cyberspace from freelance hackers to militants and potentially rival states, safety, protection of international cyberspace, and international cooperation in risk management of cyberattacks should certainly become a



# The Model Conference Global Security Issues

Faculty of International Relations, University of Economics in Bratislava



## Modelová konferencia Bezpečnostná sekcia

Fakulta medzinárodných vzťahov, Ekonomická univerzita v Bratislave

priority for international community, as the Forum for 21<sup>st</sup> Century stated. In particular, we seek to ensure that we provide adequate protections to our classified information to prevent breaches such as the 2010 WikiLeaks episode, while at the same time sharing the information with all who reasonably need it to do their jobs, and respecting the American people's privacy, civil rights and civil liberties.

- ❖ The United States consider new security challenges and the changing nature of wars and criminal acts with more harmful impacts mentioned by the Forum for 21<sup>st</sup> Century to be the most significant ones. While offline challenges of crime have made their way to the digital world, we will confront them consistent with the principles we hold dear – free speech and association, free flow of information and privacy. The world must collectively recognize the challenges posed by malevolent actors' entry into cyberspace, and update and strengthen our national and international policies accordingly.
- ❖ As the digital world is no longer a lawless frontier, nor the province of small elite, the United States agree with the Forum for 21<sup>st</sup> Century that cyberspace needs certain legal basis. We will foster and participate fully in discussions, advancing a principled approach to Internet policy-making. While cyberspace is a dynamic environment, international behavior in it must be grounded in the principles of responsible domestic governance, peaceful interstate conduct, and reliable network management. The United States will work with like-minded states to establish norms of behavior that ground foreign and defense policies and guide international partnerships. Adherence to such norms brings predictability to state conduct, helping prevent the misunderstandings that could lead to conflict.
- ❖ The United States agree with the Forum for 21<sup>st</sup> Century that the risk of unprecedented cyberattacks cannot be decreased without requiring necessary limits in anonymity of Internet users, which would be in compliance with basic ethical standards. Our international cyberspace policy will reflect our core commitments to fundamental freedoms, privacy and the free flow of information. At the same time, the United States believe that criminal behavior in cyberspace should be met with effective law enforcement, not policies that restrict legitimate access to or content on the Internet.
- ❖ We, the United States, will engage the international community in frank and urgent dialogue, to build consensus around principles of responsible behavior in cyberspace and the actions necessary, both domestically and as an international community, to build a system of cyberspace stability, and to ensure peaceful environment for next generations. In our international relations, the United States will work to establish an environment of international expectations that anchor foreign and defense policies and strengthen our international relationships.



In the section *Proposals*:

- ❖ The United States welcome the proposal for the creation of legal basis for cyberspace. The development of norms for state conduct in cyberspace does not require a reinvention of customary international law. Long-standing international norms also apply in cyberspace. Nonetheless, unique attributes of networked technology require additional work to clarify how these norms apply and what additional understandings might be necessary to supplement them. Rules that promote order and peace, advance basic human dignity and promote freedom in economic competition are essential to any international environment. These principles provide a basic roadmap for how states can meet their traditional international obligations in cyberspace and reflect duties of states as well. The existing principles that should support cyberspace norms include: Upholding Fundamental Freedoms; Respect for Property (intellectual property rights); Valuing Privacy (individuals protected from arbitrary or unlawful state interference with their privacy when using the Internet); Protection from Crime (cooperation with international criminal investigations in a timely manner); Right of Self-Defense (consistent with the United Nations Charter). Many of responsibilities more specific to cyberspace are rooted in the technical realities of the Internet. Because the Internet's core functionality relies on systems of trust, states need to recognize the international implications of their technical decisions, and act with respect for one another's networks and the broader Internet. Emerging norms, also essential to this space, include: Global Interoperability; Network Stability; Reliable Access (not to arbitrarily deprive or disrupt individual's access to the Internet or other networked technologies); Multi-stakeholder Governance (governance efforts must not be limited to governments, but should include all appropriate stakeholders); Cybersecurity Due Diligence. To enhance confidence in cyberspace and pursue those who would exploit online systems, we will: participate fully in international cybercrime policy development; harmonize cybercrime laws internationally by expanding accession to the Budapest Convention; focus cybercrime laws on combating illegal activities, not restricting access to the Internet; deny terrorists and other criminals the ability to exploit the Internet for operational planning, financing or attacks.
- ❖ The United States approve the suggestion that every attack on national defense system and government body should be considered as an act of aggression. We will defend our networks, whether the threat comes from terrorists, cybercriminals or states and their proxies. In all our defense endeavor, we will protect civil liberties and privacy in accordance with our laws and principles. Because strong cybersecurity is critical to national and economic security, we will reduce intrusions into and disruptions of U.S. networks; and ensure robust incident management, resiliency and recovery capabilities for information infrastructure. In order to develop best practices for protecting the integrity of information systems, we will greatly enhance the security of the globalized supply chains (in consultation with industry) on which free and open trade depends. Since our commitment to defend our citizens, allies and interests in new security



environment, we will recognize and adapt to the military's increasing need for reliable and secure networks; build and enhance existing military alliances to confront potential threats in cyberspace; expand cyberspace cooperation with allies and partners to increase collective security. In the case of criminals and other non-states actors who would threaten our national and economic security, domestic deterrence requires all states have processes that permit them to investigate, apprehend and prosecute those who intrude or disrupt networks at home or abroad. When warranted, the United States will respond to hostile acts in cyberspace as we would to any other threat to our country. We reserve the right to use all necessary means – diplomatic, informational, military and economic – consistent with applicable international law, in order to defend our Nation, our allies, our partners and our interests. In so doing, we will exhaust all options before military force whenever we can. The online crimes should be approached by focusing on preventing crime and catching and punishing offenders, rather than by broadly limiting access to the Internet, as a broad limitation of access would affect innocent Internet users as well.

- 🇺🇸 The United States agree that the further cooperation of engaged parties in the creation of a joint database could lead to a peaceful and credible cooperation between the parties concerned. As we continue to build and enhance our own response capabilities, we will work with other countries to expand the international networks that support greater global situational awareness and incident response – including between government and industry. The U.S. Government actively participates in watch, warning and incident response through exchanging information with trusted networks of international partners. We will expand these capabilities through international collaboration to enhance overall resilience. The United States will also work to engage international participation in cybersecurity exercises, to elevate and strengthen established operating procedures with our partners.
- 🇺🇸 We propose to create the Internet governance structures that would effectively serve the needs of all Internet users. In so doing, the United States will prioritize openness and innovation on the Internet. Although governments around the globe recognize the value of the Internet, many of them place arbitrary restrictions on the free flow of information or use it to suppress dissent or opposition activities. We should not allow the Internet's governance or technical architecture to be reengineered to accommodate decisions that violate fundamental freedoms or stifle innovation. The United States are convinced that when the international community meets to discuss the range of Internet governance issues, these conversations must take place in a multi-stakeholder manner, which embodies the open nature of the Internet itself by allowing nongovernment stakeholders to contribute to the discussion on equal footing with governments.
- 🇺🇸 The United States propose to focus internationally on building stronger public and private partnerships around cybersecurity; on pushing new security research and development; and on launching an international campaign to spread cybersecurity awareness. The benefits of an interconnected world should not be limited by national borders. To promote the benefits of





# The Model Conference Global Security Issues

Faculty of International Relations, University of Economics in Bratislava



## Modelová konferencia Bezpečnostná sekcia

Fakulta medzinárodných vzťahov, Ekonomická univerzita v Bratislave

networked technology globally, the developed countries should provide the necessary knowledge, training and other resources to the countries seeking to build technical and cybersecurity capacity.



FORUM FOR  
21<sup>ST</sup> CENTURY

