



Position of the United States of America for the purpose of the conference held by The Forum for 21st Century on 29 November 2011 reflected in the second draft of the negotiation paper, regarding the global Cybersecurity issues.

After an in-depth analysis of the second draft proposed by *The Forum for 21st Century* let us submit the position of the United States including our suggestions about selected topics.

The growth of the Internet has been one of the greatest forces for innovation and progress in history. Today, cyberspace touches practically everything and everyone. It provides a platform for innovation and prosperity and the means to improve general welfare around the globe. But with the broad reach of a loose and lightly regulated digital infrastructure, great risks threaten nations, private enterprises, and individual rights. Cybersecurity issues have therefore become a diplomatic priority for the United States.


Our digital infrastructure has already suffered intrusions that have allowed criminals to steal hundreds of millions of dollars and nation-states and other entities to steal intellectual property and sensitive military information. Other intrusions threaten to damage portions of our critical infrastructure. These and other risks have the potential to undermine the Nation's confidence in the information systems that underlie our economic and national security interests.

There are two possible outcomes in cybersecurity for the United States. We can continue to pursue outdated strategies and spend our time describing the problem until there is some crisis. Then it is likely that the United States will act, in haste, possibly with unfortunate consequences. Alternatively, we can take action on measurably effective policies. Our opponents still have the advantage, but we can change this.

The United States seek to conduct a multinational dialogue on cybersecurity to develop more international awareness of the threat and risks.

Consequently, we invite all nations to join us in the process of creating a future for cyberspace that is open, interoperable, secure and reliable while at the same time respecting people's privacy and civil rights as well as free speech and association, and free flow of information.

In the section *Proposes*:

-  The United States welcome the proposal for the creation of legal basis and terms with respect to usage and control of the Internet and local intranets. In so doing, the **Budapest Convention on Cybercrime** of Council of Europe should be taken into account. We propose to revise the Budapest Convention instead of creating brand-new International Cyberlaw, which is considered to be a long-term action plan.



The Convention on Cybercrime is the first international treaty on crimes committed via the Internet and other computer networks, dealing particularly with infringements of copyright, computer-related fraud, child pornography, xenophobia, racism, and violations of network security. Its main objective is to pursue a common criminal policy aimed at the protection of society against cybercrime, especially by adopting appropriate legislation and fostering international co-operation.

The United States, as well as all member states of the EU and Turkey (among others) have signed and supported the Budapest Convention, which requires countries to make cyber attacks a substantive criminal offense and to adopt procedural and mutual assistance measures to better combat cybercrime across international borders.

The Convention includes a list of crimes that each signatory state must transpose into their own law. It requires the criminalization of such activities as hacking (including the production, sale, or distribution of hacking tools) and offenses relating to child pornography, and expands criminal liability for intellectual property violations. It also requires each signatory state to implement certain procedural mechanisms within their laws. For example, law enforcement authorities must be granted the power to compel an Internet Service Provider to monitor a person's activities online in real time. Finally, the Convention requires signatory states to provide international cooperation to the widest extent possible for investigations and proceedings concerning criminal offenses related to computer systems and data, or for the collection of evidence in electronic form of a criminal offense. Law enforcement agencies will have to assist police from other participating countries to cooperate with their mutual assistance requests.

Therefore, we will continue to encourage other countries to accede to the Council of Europe Convention on Cybercrime, and will help current non-parties use the Convention as a basis for their own laws, easing bilateral cooperation in the short term, and preparing them for the possibility of accession in the long term.

- 🇺🇸 The United States approve the creation of **Basic Cyberspace Principles** repeatedly emphasizing the general principles that should support cyberspace norms, which are: upholding fundamental freedoms; respect for property; valuing privacy; protection from crime; right of self-defense (consistent with the United Nations Charter); global interoperability; network stability; reliable access; multi-stakeholder governance; cybersecurity due diligence.

In respect to the supervision of companies which profit from personal data collecting, the United States suggest supervising these companies by state representatives and representatives of NGO's (multi-stakeholder model) rather than strictly regulating and controlling them.



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

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 (which provides countries with a model for drafting and updating their current laws, and it has proven to be an effective mechanism for enhancing international cooperation in cybercrime cases);
- Focus cybercrime laws on combating illegal activities, not restricting access to the Internet (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);
- Deny terrorists and other criminals the ability to exploit the Internet for operational planning, financing or attacks (preventing terrorists from enhancing capabilities through „hackers for hire“ and organized crime tools is an important priority for the international community, and demands effective cybercrime laws). The United States is committed to tracking and disrupting terrorist and cybercrime finance networks through technical tools and international cooperation frameworks such as Financial Action Task Force;

🇺🇸 The United States agree with *The Forum for 21st Century* that malevolent misuse of personal data should be approached seriously. However, we suggest further specification of proposed „hard sanctions“ as well as “economic reasons” because the use of personal data represent the cornerstone for e.g. Facebook Ads or Google Ads that are used (for marketing and economic reasons) worldwide on a daily basis. Moreover, in certain cases it is inevitable for countries to use e.g. wiretapping (stated by *The Forum for 21st Century*) explicitly for national intelligence purposes.

🇺🇸 We, the United States, propose more accurate and broader definition of **Cyberspace**:

“The interdependent network of information technology infrastructures, and includes the Internet, telecommunications networks, computer systems, and embedded processors and controllers in critical industries. Common usage of the term also refers to the virtual environment of information and interactions between people.”

The Budapest Convention offers more specific definitions of computer system; computer data; service provider; and traffic data.



🇺🇸 The United States welcome the proposal for differentiation sanctions in accordance with the type of criminal or illegal activity conducted.

Cybercrime is a global problem that affects governments, corporations, and individuals. It can take a variety of forms, from online fraud, to cyberstalking, espionage, hacking, identity and data theft, to terrorism. A 2010 study found that nearly two-thirds of people worldwide have been the victim of cybercrime, and another 2009 study shows cybercrime may have cost global businesses as much as \$1 trillion globally.

We suggest further specification of “small crimes”. Furthermore, in determining sanctions or retaliatory measures as well, different level of innovation, technology capabilities and various approaches to national security among nations should be taken into account.

We categorize deliberate cyber threats as follows:

- **National Governments** – national cyber warfare programs (threats range from propaganda and low-level nuisance web page defacements to espionage and serious disruption with loss of life and extensive infrastructure disruption).
- **Terrorists** – they are likely to pose only a limited cyber threat (terrorists are likely to stay focused on traditional attack methods in the near term).
- **Industrial Spies and Organized Crime Groups** – they pose a medium-level threat to the US through their ability to conduct industrial espionage and large-scale monetary theft as well as their ability to hire or develop hacker talent (with profit-based objectives). Their sub-goals include attacks on infrastructure for profit to competitors or other groups listed above, theft of trade secrets, and gain access and blackmail affected industry.
- **Hacktivists** – they form a small, foreign population of politically active hackers that pose a medium-level threat of carrying out an isolated but damaging attack. Their goal is to support their political agenda rather than damage to critical infrastructures.
- **Hackers** – the large worldwide population of hackers poses a relatively high threat of an isolated or brief disruption causing serious damage, including extensive property damage or loss of life. Their goals are: achievement; to gain access and deface web pages; notoriety; to cause disruption of networks and attached computer systems; profit.

🇺🇸 We consider the creation of **Joint Criminal Database** to be an important **long-term** objective that could lead to a peaceful and credible cooperation between the parties concerned.

As a mid-term action plan we suggest focusing rather on bilateral cooperation between countries in terms of joint database.



Today, we consider irrational to assume that all countries, including e.g. India and Pakistan are going to share willingly the specific data of cybercriminals threatening their national security without any negative impact.

Instead, we should stay more pragmatic, and at first focus on improving technology capabilities in order to sufficiently secure the future Joint Criminal Database, which will tend to be vulnerable due to its size and data sensibility as well.

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. For instance, the EU and the USA successfully conducted the first joint transatlantic cyber-attack simulation in November 2011. The exercise, entitled “Cyber Atlantic 2011”, involved more than 100 IT-security experts from both USA and EU, and consisted of two separate scenarios.

Moreover, the EU-U.S. Working Group on cybersecurity was established in 2010, and the first joint U.S.-Russian report on cyber conflict in February 2011.

However, China’s vast online censorship apparatus, known as the “Great Firewall”, contradicts basic American ideals of Internet freedom, and so further cooperation in this specific area is disabled.

- ❖ The United States consider establishment of new international organization – **CYBERPOL** - unnecessary due to its high requirements for time, finances, people involved, and creation of new legislative framework (where would be complicated to achieve a consensus, at least in a reasonable period of time).

Instead, in order to focus on short-term objectives, we propose to strengthen the powers of the **INTERPOL IT Crime Steering Committee**, which would be more effective. The Committee consists of law enforcement officials, representatives of major IT security companies and academia. The Committee aims to harmonize and provide guidance to regional working party activities, and to facilitate partnerships between the different sectors involved in the fight against cybercrime. At its first meeting, the Committee agreed that INTERPOL's cybercrime activities should revolve around three main pillars: operations, training and research and development.

- ❖ We support the development of **Best Practice Sharing** proposed by *The Forum for 21st Century*. 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. We believe the



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

developed countries could provide the necessary knowledge, training and other resources to the countries seeking to build technical and cybersecurity capacity.

Our goal is to help other states learn from our experience, and in particular to build cybersecurity into their national technical development. Our work has taken place bilaterally, through foreign assistance, as well in partnership with innovative public-private initiatives like the U.S. Telecommunications Training Institute. In recent years, we have helped make this work a priority at multilateral fora such as the OAS, APEC, and the U.N. The United States will expand these collaborations and work to build new collaborations in the coming years.

We have worked with dozens of other states and with numerous multilateral organizations to develop and share best practices designed to help states make wiser investments and develop more effective policies. The United States will continue to identify, develop and refine best practices and technical standards in collaboration and close partnership with industry, and will expand our efforts to promote awareness of and access to them.

🇺🇸 The United States highly appreciate the suggestion of the introduction of **voluntary Internet ID Numbers**.

In the current online environment, individuals are asked to maintain dozens of different usernames and passwords, one for each website with which they interact. It encourages behavior that makes online fraud and identity theft easier. At the same time, online businesses are faced with ever-increasing costs for managing customer accounts, the consequences of online fraud, and the loss of business that results from individuals' unwillingness to create yet another account. Moreover, both businesses and governments are unable to offer many services online, because they cannot effectively identify the individuals with whom they interact. Spoofed websites, stolen passwords, and compromised accounts are all symptoms of inadequate authentication mechanisms.

There is a compelling need to address these problems as soon as possible, making progress in the short- term and planning for the long-term.

Our vision is straightforward - individuals and organizations utilize secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation. To fulfill this vision we propose to create the user-centric “**Identity Ecosystem**” that will encourage trusted online transactions, provide privacy enhancements and support civil liberties, and reduce fraud. It is an online environment where individuals and organizations will be able to trust each other because they follow agreed upon standards to obtain and authenticate their digital identities—and the digital identities of devices.



The United States recognize four **Guiding Principles** to which the Identity Ecosystem must adhere:

- Identity solutions will be privacy-enhancing and voluntary
- Identity solutions will be secure and resilient
- Identity solutions will be interoperable
- Identity solutions will be cost-effective and easy to use

The Identity Ecosystem consists of the participants, policies, processes, and technologies required for trusted identification, authentication, and authorization across diverse transaction types.

The Identity Ecosystem should use privacy-enhancing technology and policies to inhibit the ability of service providers to link an individual's transactions, thus ensuring that no one service provider can gain a complete picture of an individual's life in cyberspace. By default, only the minimum necessary information should be shared in a transaction. In addition to privacy protections, the Identity Ecosystem should preserve online anonymity and pseudonymity, including anonymous browsing.

The complete Identity Ecosystem will take many years to develop, and the public and private sectors' engagement with international partners will be critical to the success of achieving this vision.

The United States suppose that the correct noticing of strange activity on PC by a common Internet user is hardly likely, therefore we don't see the relevant utilization of voluntary Internet ID Numbers as a new government counterterrorist measure, within the meaning of *The Forum for 21st Century's* statement.

- 🇺🇸 The United States consider every attack on national defense system and government body as an **act of aggression**. We will defend our networks, whether the threat comes from terrorists, cybercriminals or states and their proxies. In our entire defense endeavor, we will protect civil liberties and privacy in accordance with our laws and principles.

When a nation, terrorist group, or other adversary attacks the United States through cyberspace, the U.S. response need not be limited to criminal prosecution. 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 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

We strongly believe that 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.

- 🇸🇰 We, the United States, welcome the suggestion of cooperation in prosecution of illegal paramilitary or terrorist activity and groups, and exposure of individuals behind hacktivism.

However, we consider the proposal for setting a clear distinction between national defensive military units and organized individuals conducting operations in cyberspace as unsubstantial in consideration of expanded cooperation of such individuals with governments (e.g. in Great Britain, Israel, USA). Moreover, for instance the Identity Ecosystem can only be designed and built by the private sector with the aid of individual cyber-experts or even hackers.