Statement for the Record by Rafal Rohozinski,
Commission on Security and Cooperation Europe (U.S. Helsinki Commission).
15 July, 2011.

Chairman, distinguished members of the Commission,

I'd like to thank the Commission for the opportunity to appear and testify at today's hearing, which comes at a particularly important moment. The Internet has precipitated perhaps the fastest and largest expansion of rights in human history. And yet we are also at a constitutive moment - where our actions, and leadership can lead to two opposing outcomes. One promises a future of greater freedoms and transparency; the other threatens a return to a darker, more authoritarian past.

My name is Rafal Rohozinski, I am a senior scholar at the Canada Center for Global Security Studies, and the CEO of the SecDev Group and Psiphon Inc. For the past 10 years I've been a Principal Investigator of the OpenNet Initiative, a collaborative international research project between the University of Toronto, Harvard University, Cambridge University, and the SecDev Group, which has studied and documented the practice and policy of Internet censorship and surveillance worldwide. We have published more than two dozen case studies and thematic reports and are in the process of publishing our third volume documenting censorship practices in over 70 countries worldwide. The OpenNet Initiative has amassed the largest, most complete profile of how countries seek to shape access to cyberspace using a combination of regulation, repression, and technical means.

***

Just over 65 years ago, Winston Churchill warned an American audience of the danger of an Iron Curtain falling across Europe - casting a shadow of authoritarianism and depriving citizens of their democratic rights. Churchill spoke in 1946, at a time when the United States stood uncontested as a global power. He urged the creation of norms and institutions that would safeguard freedom, and actively oppose the forces of authoritarianism. For Churchill, the end of World War II was a constitutive moment: the choices made by the victorious Allies would have enduring consequences for the cause of freedom in Europe, and elsewhere.

Today, we stand at the threshold of a similar constitutive moment brought about by a revolution whose long-term consequences we are only now starting to grasp. For the past two decades, the emergence of the Internet and cyberspace has led to the largest sustained global expansion of knowledge, rights, and freedoms. Over a third of all humanity is connected to the Internet, and there are almost as many cell phones in circulation globally there are people. Significantly, we are now seeing the coming-of-age of the “digital natives” who have grown up knowing only a connected world. Two-thirds of those currently accessing cyberspace are under the age of 25, and over 80% use at least one form of social media.

But the numbers do not do justice to the social significance of this expansion. This revolution is so pervasive and so all encompassing that it's difficult to see just how fundamentally it has changed the exercise of individual human rights, how much it has added to the cause of basic

freedoms, and the ability of all peoples - no matter how small - to make their voices heard. We need not look further than the Color Revolutions of the Commonwealth of Independent States, or the recent Arab Spring, to witness the extraordinary power of the networked social movements.

But the tectonic plates of cyberspace are also shifting. The US - once the heartland of the Internet - now makes up approximately 13% of the global Internet connected population. Europe and the US together constitute approximately 40%. The center of gravity is fast shifting to the South and East. The consequences of the shift are of direct relevance to today's proceedings.

A **Digital Curtain** is descending across the globe that threatens to reverse the gains made possible through the emergence of the global commons of cyberspace. Just over half of the world's Internet-connected population live under one form on-line restriction or another, and that number is fast rising. Since 2003, when we first documented the emergence of the “Great Firewall” of China, more than 45 states worldwide have adopted similar means for turning the Internet from a global commons into a gated community.

Eurasia, and in particular the states of the former Soviet Union, are a petri dish of experimentation in new forms of online repression that deprive citizens of the means to demand transparency from their leaders, accountability from their governments, and the right to seek social and political change.

These new forms of restrictions, which we have documented as second and third generation controls, leverage the ability of governments to create restrictive legal environments that attempt to enforce self-censorship through fear of punishment. They also include the application of sophisticated technical means, just-in-time blocking, disrupting access to critical information resources at times when they are most needed, sowing disinformation, and otherwise manipulating information flows – as well as the use of targeted online attacks, denial of service, injecting false content, and sophisticated information operations turned inwards at the domestic populations. These controls are pervasive, but also applied selectively, such as during elections, in order to discredit legitimate opposition groups and deprive them of the right to free and unfettered speech.

In Kazakhstan, Uzbekistan, Turkmenistan, Russia, and notably in Belarus, these techniques have been used with great success to silence opposition groups, driving them and their followers offline. In fact, the Internet is subject to some form of control in all post-Soviet states. Indeed, the mechanisms for control are getting deeper and more coordinated through regional bodies such as the Shanghai Cooperation Organization, and the Collective Security Treaty Organization, as well as via bilateral cooperation between governments and their security services.

Tragically, perhaps, we are complicit in this growing trend towards authoritarianism. Our own fears of cyber insecurity and terrorism make it easier for others to appropriate these terms to justify political repression.

The label "terrorists” can be applied to anyone inconveniently opposed to the political status quo; and calls for changing the Internet, introducing greater security, and the ability to identify users - helpful in tracking down hackers and cyber criminals - find their place in the arsenal of

repressive regimes as a means of selectively prosecuting human rights activists, journalists, or anyone seeking to struggle for social and political reform.

Our emphasis on harmonizing laws on cybercrime and seeking global solutions to cyber security paradoxically makes it difficult to assert and demand respect for freedom of expression and access to information online.

And security is not the only means by which rights can be suppressed. Net neutrality, copyright enforcement, and the empowerment of telecommunications carriers to "clean pipes" are convenient means for regimes with less than Democratic tendencies to offload and outsource policing and ultimately repression.

There are no simple solutions to these challenges, only difficult trade-offs. To paraphrase the words of the immortal Pogo, "we have met the enemy and he is at least **partially** us."

So what is to be done?

Future historians will look back at this time and see it as a constitutive moment. Before us are some hard choices - but also clear norms and ideals that have been core to the Euro Atlantic alliance over the past 50 years, and part of our shared cultural and historical heritage.

Leadership comes from the courage to make the hard decisions in pursuit of a greater common good. In this respect, a commitment to an open global commons of cyberspace is by far the most important far-reaching objective for the US and its like-minded partners worldwide to support.

Security is an important obligation of the state, but must be balanced against preserving the right to dissent, communicate, and act online - even if it comes at some costs. This is especially true as the new generation of digital natives find their own voice in the online world. New forms of protest, whether they come in the form of making public confidential information, as in the case of Wikileaks, or “hacktavism” as has been exercised by LulzSec and Anonymous, may be the necessary friction for preserving a global norm that enshrines the right to seek and access information. We carefully adjust our own laws to accommodate some of the new forms of dissent that will emerge. Is there a difference between picketing an employer during a labor dispute, and making his website and Internet systems inaccessible through a denial of service attack? These are important questions and we must pause before we consider how to address them, as the rules we apply will have repercussions well beyond their own borders. In a global world, there is no such thing as a purely domestic policy.

In specific terms, at the highest level this Commission should encourage our European partners to remain committed to a global commons of cyberspace.

- Calls such as those put forward by some members of the UN to end the multi-stakeholder engagement on the governance cyberspace should be strongly resisted.

- Pressure should be applied through bilateral agreements, as well as by organizations such as the WTO to ensure that restricted access to content is also framed as a trade issue, with consequences and sanctions against countries pursuing these practices.

- Access to an uncensored Internet should become a basic measure of freedom and democratic progress, and should be made a condition for recipients of preferential US trade relationships or development assistance;

- Access to political content via the Internet should become a central component of monitoring the freedom and fairness of national elections - as important as the right to assembly, and balloting.

Preserving the global Internet commons will not be easy, but the costs of not doing so are greater. The rise of new superpowers in the East is occurring just as the tectonic plates of cyberspace are shifting to the same region.

The historical moment in which we live and which have expanded the means for human expression made possible a quest for knowledge, and an ability to network and act on a planetary scale – which risks becoming a fading chapter in the future where the same technologies enable surveillance societies that far exceed those which George Orwell's 1984 could imagine.

The future is ours to lose, and as in those March days of 1946 when Churchill warned of the Iron Curtain, now is the time for us to courageously make choices so that our constitutive moment - the future of Cyberspace – furthers, rather than constrains, the universal values of dignity, freedom, and the right to choose.

Washington DC, July 15, 2011