by Cyrus Farivar

TALLINN, ESTONIA—Estonian President Toomas Hendrik Ilves told assembled attendees on the final day of the International Conference on Cyber Conflict that the nature of the Internet itself forces countries with different political realities "into almost inevitable conflict," calling the present international geo-political situation a "cold peace."

"We are now entering a new period of struggle of competing systems of government and economic organization," he said. "There is, this time, no Iron Curtain, no statement of hostilities, no declared conflict of ideologies. Perhaps it will remain a global cold peace, but a cold one nevertheless. What is at stake in this struggle is the liberal-democratic model of an open society, and of market economies that are transparent and rule-bound. This time, the struggle will play itself out in cyberspace."

Indeed, the creation of this very conference, and its sponsoring institution, the NATO Cooperative Cyber Defence Centre of Excellence, was a direct result of Estonia being subjected to a nationalistic, politically motivated denial of service attack originating from Russia in 2007.

The Estonian president said that the Internet's openness is at once its greatest asset, but also its greatest weakness.

"During the Cold War, Communist leaders may have been frustrated by the freedom within Western countries, but there was a limit to what they could do about it," he said. "Today, they can deface your website; DDoS your servers; hack your e-mail; steal your data, identity, and financial information; spy on your friends; plant malware on your systems; exploit your ICS systems; and so on. Our strength—our openness—is at once also our greatest liability. This is the crux of the challenge we face."

Of course, Western powers, most notably the United States, engage in similar behavior, as evidenced most famously by Stuxnet, and possibly the more recently discovered Flame malware that is seemingly targeting Iran for espionage purposes. President Ilves himself told

Ars on Twitter just last week that Estonia and the European Union do not condone this type of behavior—despite the fact that American allies arguably benefit politically and militarily from such American covert operations.

Furthermore, Ilves pointed out that this openness itself can be used not only for offensive purposes, but also for defensive purposes as well.

"The Iranian CERT released the code for the Flame virus, and within some weeks, several European teams had analyzed the malware (PDF), reverse engineered it and designed patches, so that in effect, the Iranians, using openness, piggy-backed on the cooperative community that has developed in our free societies to increase their own security," he noted.

Still, Ilves seemed to suggest that the struggle for freedom of information—for information-sharing between nation-states, countries, and regional institutions like the European Union, as well as their political adversaries—cannot allow for the Internet to become even more balkanized than it already is. After all, some countries, like North Korea, are almost entirely offline, while China and Iran, most notably, operate extensive filtration and surveillance systems against domestic traffic on their own networks. The Estonian president also called for increased cooperation within the "liberal democratic West," and specifically warned against ceding more power to the International Telecommunications Union (an issue being discussed at the December 2012 Dubai meeting) and countries (notably Russia and China) that have called for more national-level control over Internet traffic.

"Fundamentally, we could go into two directions—either we can change the nature of the Internet by placing a Westphalian structure on Internet governance, or we can change the world."

Cyrus is the Senior Business Editor at Ars Technica, and is also a radio producer and author. His book, The Internet of Elsewhere, was published in April 2011.

Original article on the Ars Technica webpage .