

By Elissar Harati, MALD 2014 candidate

"I should congratulate the United States for being number two in the world in Internet freedom," the President of the Republic of Estonia Toomas Hendrik Ilves joked during a recent talk at The Fletcher School of Law and Diplomacy. After a healthy pause he reminded the crowd that his country stands at number one.

President Ilves, an internationally recognized expert on cyber and information technology, spoke to a room packed with students, faculty and staff along with other members of the Tufts community in his September 26 lecture: [What Keeps Me Awake at Night: Worries and Challenges for a Small European Ally](#)

The Republic of Estonia is in fact a pioneer in information technology (IT) and e-governance; since regaining its independence, Estonia has steadily been earning a reputation as a leading economy in IT, innovation and connectivity in global markets. However, these innovations also created vulnerabilities—in April 2007, Estonia was the target of a sophisticated month-long denial of service (DDoS) attack that crippled the digital platforms of its parliament, banks, ministries and television stations.

But the crisis had a fortifying effect on Estonia's focus on cyber: in May 2008, a year after the DDoS attack, Estonia became home to the NATO Cooperative Cyber Defense Centre of Excellence.

"To horribly mix metaphors, Estonia has become a proverbial canary in a minefield," President Ilves said on his country's vulnerability to cyber attacks. "In our case we are the canary because in fact we are so reliant on IT—98% of bank transactions are done online, 98% of income tax returns are done online, 95% of prescriptions are refilled online, the last elections we had 25% of people voting online and the entire country is covered by WiFi."

President Ilves praised IT as a "great equalizer" in international relations, in which a small, poor country such as Estonia can take a leadership position in the global arena.

"I would argue it's a paradigmatic transformation of our world where the notion of a nation's size, wealth power, military might, population numbers, GDP relations all do not have the same relevance as it use to," he said.

To deal with this change in paradigm, President Ilves advocates a shift in mindsets, especially in the military. "You may have an F-35 jet fighter, the most modern, the best fighter in the world, but if the lights don't work it's not going to be much use," he pointed out.

And in regards to international regulations on cyber security, the president emphasized the need for more international norms and agreements such as the Convention on Cyber Crime and the International Telecommunications Union (ITU).

According to President Ilves, cyber security within NATO is mostly understood as intelligence gathering and espionage. He recommends a new approach within NATO that focuses on information sharing and inter-operability between intelligence agencies—that is, the ability for the system of one to work with another—in order to deal with these new threats.

"The problem in NATO today is that we have inter-operable rockets but we don't have inter-operable intelligence and systems dealing with cyber attacks," President Ilves explained.

The President of Estonia also expressed disappointment in fellow NATO members for failing to meet their financial obligations. According to President Ilves, only four European countries meet the agreed-upon figure of 2% of their GDP to defense spending—namely Estonia, Greece, UK, and Bulgaria.

"This is not sustainable politically," he concluded. "By not doing their share, by contributing too little either in the way of defense expenditures or in terms of boots on the ground in NATO operations, they are in fact weakening the transatlantic link and the ones who are making it easier for the United States to disengage from our side of the world."

Original article on the Fletcher School [webpage](#) .