ÁGNES HANKISS dr.
Member of the European Parliament

dr. Hankiss Ágnes előadása a Security and Defence Agenda 2010. március 22-i, a transzatlanti kiberbiztonságról rendezett vitaestjén.

Speech given by Ágnes Hankiss dr. MEP at the evening debate arranged by Security and Defence Agenda on cybersecurity on 22 March 2010.

It is really a pleasure to be here at the SDA and an honour to be part of SDA's distinguished speakers. I am not a technical expert of cybersecurity and cyber-terrorism, I would approach cybersecurity from a broader and to an extent political point of view.

As you may know, I come from a post-communist country, Hungary. This country, along with other central European states, got rid of communism twenty years ago this year. During the four decades spent under Soviet umbrella made many of us in Central Europe much more vigilant than probably those who, luckily, did not have to experience communist dictatorship and internal secret services like Stasi, KGB and others.

Twenty years after changing the regime, all of the ex-communist countries are NATO and/or EU member states. It may not be obvious but Central European countries are still struggling with the afterlife of the communist era. Part of this is due to the fact the former empire still treats Central Europe as part of its sphere of influence.

The EU's eastern-most countries are the primary target of attempts made to increase influence relying mainly on those local people that were educated in the schools of KGB and are often still in influential positions.
A good example for such attempt is the hostile take-over attempt of Hungarian oil company MOL by its Austrian state-controlled competitor, OMV. The failed attempt was followed by a suspicious overnight sell-off of a large amount of MOL's shares to a virtually unknown Russian oil company whose ownership structure is not transparent. But we could name a number of such cases from the whole region, maybe from the whole continent.

Under such circumstances I have always been interested to know whether the EU is protected sufficiently from east. And, of course, this does not contradict the fact that we do need a dialogue and cooperation with Russia, whether it is about energy, cyber security or anything else. Russia is indeed an important partner of the EU.
However, the cyber attacks against Estonia and Georgia in the recent years have clearly shown that any country's cyber-infrastructure is exposed to a new kind of warfare.
The Estonian attacks opened another question as to what extent solidarity shall be defined when it comes to article five of the NATO Treaty. I think that it is time for discussing and agreeing upon a broader term of solidarity which would apply to cyberattacks against a member state's vital cyberinfrastructure.
Should a cyber attack against a country's vital network or infrastructure be considered as an attack against the country, so article five of the NATO Treaty would apply?

Now, let me focus on how the EU, together with the United States, could increase the effectiveness of combating cyberterrorism.
The US has made it clear recently that by founding USCybercom, a unified cyber command within the Pentagon, cybersecurity is regarded as part of its military capabilities.
It is beyond debate that the US and the EU must work together also in this field, and in order to do so ever more efficiently, harmonizing our approaches would make sense. Regardless of the motive and the form of the attack, the modus operandi are always the same. That means civil and military defence must come together to unite their forces.

I think priority should be given to prevention, also when it comes to cybersecurity, so that we should not run after terrorists.

This comes with the question: shall Europe also regard cybersecurity more as part of its Common Security and Defence Policy, mirroring to a certain extent the American way of thinking – or shall we make cooperation more difficult by letting cybersecurity taken care of in a fragmented way, handled by different institutions of the union? I think, while cooperation should increase with the United States in this field, it is time for the EU to reconsider its approach and unify its forces for the sake of the better security of all European citizens.

ENISA, Europol, European Defence Agency, the Commission: four EU-bodies dealing with the cybersecurity and there are obviously more than just that. Much more focus and concentrated approach is needed so that concrete goals can be set and results could be measured.

Does the EU need a cyber security action plan? Yes, we do, in a strong cooperation with the United States but a separate strategic plan is required.

With the entry into force of the Treaty of Lisbon, a new era has come, especially when it comes to the Common Security and Defence Policy. We have a new tool in our hands in Europe. It is time to exploit the situation.