LATVIJAS VALSTS PREZIDENTS

Address by H.E. President of Latvia Raimonds Vējonis
at the Riga StratCom Dialogue 2019
11 June 2019

Since 2014 we have clearly seen that militaries fight in what is called "peacetime" while political and economic means are deployed in war. Whether we call this new generation, asymmetric or hybrid war, Mark Galeotti has correctly identified it as Political War. In the Baltic States we have felt this pressure since the early 2000s and are no longer surprised, for instance, by the information attacks which we regularly experience.

Latvia, which is a democratic country based on the rule of law, is accused of being a failed state with a faltering economy and incompetent governments. We are said to discriminate against our minorities, especially our Russian speaking ones. We are accused of failing to live up to international norms and, therefore, not to be worth defending.

Even though these narratives are self-evidently untrue, those who do not know Latvia may start to believe them if they are repeated often enough. Broadly, these same arguments are now being applied to the EU and NATO.

Frequently we have a tendency to look at specific parts of this peacetime hybrid conflict without acknowledging that it is one whole. In particular, we see the digital threat to our critical infrastructure as particularly dangerous. I would suggest that the threat is to a more vital part of our critical infrastructure than even our electricity or water supplies – it is to our minds through information operations. Coordinated inauthentic behavior can have a profound effect on democratic societies. In non-democratic ones what has been called digital authoritarianism is spreading.

Of course, this is nothing new. Most recently in the second half of the 20th Century we called it the battle for hearts and minds. But it is important that we should acknowledge that we are in a cognitive war where cyber is the means and STRATCOM is the method to defeat us. Therefore, both spheres must be viewed in combination.

I think we all agree that national security is a national responsibility. However, these information operations are aimed at splintering and destroying both the EU and NATO. For instance, the Canadian-led eFP battalion in Latvia is undermined not just in Latvia but also in Canada and other participating countries. Therefore, while maintaining national primacy, there are strong arguments for coordinating our response and sharing our insights, as we will

do during this conference. That is also the reason why the STRATCOM Centre of Excellence was created here in Riga.

You are all aware of the large amount of valuable work which has been done by the Centre during the last 5 years. But I would like to draw your attention to a short Non-paper written for NATO by the COE together with the Latvian Ministries of Defence and Foreign Affairs, which was distributed in March. It is about addressing the Alliance's digital security vulnerabilities and resilience.

New trends in hybrid warfare are intended to take target nations by surprise with a combination of new and old tools to undermine the country, its identity and resilience. Techniques primarily used in the marketing world are adapted for use in other areas. Vulnerable groups are targeted, monetarized and then weaponized for political purposes.

The STRATCOM COE's recent studies: "Responding to Cognitive Security Challenges" and "Black Market of Social Media Manipulations", demonstrate the increasing vulnerability of wider societies to data-based cognitive attacks.

Research conducted in military exercises demonstrated how open source data and social media infrastructure could be used not only to track our military, but also to manipulate behaviour to the point of disobeying orders.

Social media manipulation provides the infrastructure for hostile players to intervene in internal processes including elections. This infrastructure can also be used to undermine decision-making in individual states, in the EU and NATO.

These risks will increase with the development of Artificial Intelligence and big data gathering techniques. Democracies need to invest in countering these new challenges to mitigate potential future risks and improve cognitive resilience. Specifically, we could:

- Conduct regular risk assessments on digital security to expose and mitigate emerging vulnerabilities in the early stages;
- Conduct gap analysis assessing if and how the existing work can contribute to addressing these vulnerabilities;
- Develop technical tools that enable detecting cognitive attacks in the digital domain;

Most of all we should concentrate on increase digital security risk awareness in our general populations and especially in our political leaders. This must start with our education systems and aim at an overall improvement in our critical thinking.

If we do not respond to these emerging challenges, then we will face serious consequences for our nations, our international structures and for our democratic systems. I am sure that these and many other topics will be discussed during this conference. I wish you all a fruitful Dialogue and an enjoyable stay in Riga.