SPEAKING NOTES FOR PANEL DISCUSSION ON CRITICAL INFORMATION INFRASTRUCTURE PROTECTION: HOW TO KNOW WHAT TO PROTECT

BY: AKVILE GINIOTIENE

VENUE: 5TH REGIONAL CYBERSECURITY SUMMIT

DATE: 31 NOVEMBER 2016

1. **YOU CANNOT PROTECT EVERYTHING**

   Internet has revolutionized how we interact with each other and the world around us. Increasing internet connectivity links people together and provides a growing and dynamic platform for communication, collaboration and economic growth.

   However, our increasing connectivity to and dependency on Internet-based platforms and services has significantly raised our exposure to risks. Cyberattacks and incidents are increasing in frequency and sophistication and do not recognize national borders. Government inability to effectively address emerging cyber threats can ruin people confidence and hamper economic growth.

   But can a government protect everything – all information infrastructures that are owned and operated in a country by public and private organizations? The answer is no, you cannot protect everything and it would be an impossible task for any government, no matter how advanced it is. Because no government is indefinetly rich and it needs to allocate resources to the most critical sectors.

2. **HOW TO KNOW WHAT TO PROTECT?**

   But how can a Government know which systems are most critical? Where the disruption of a system will have a greatest damage to the state? In other words, what information infrastructures are so important to the state that their incapacitation would cause havoc in a country within hours?

   One option – the Government just knows. And it says that in our country critical information infrastructures are a system A and a system B and we are going to protect them. And it can be true, to some point. But in today's world more and more information infrastructures are developed, owned and operated by private sector and the level of country's dependency on them cannot be fully appreciated. For example, a recent DDoS attack on Dyn Managed DNS infrastructure has not only not only brought down major internet sites, but also took down Swedish government's website used for informing Swedes in case of crises. And it happened because the Government relied exclusively on Dyn for the provision of DNS services.

That is why a more systematic approach to identification of national critical information infrastructures is another and smarter option. It enables the governments to conduct a comprehensive review of their information infrastructures, identify their dependencies and weak points and determine what is truly critical for the country. And take measures to protect and defend them, of course.

3. LITHUANIA'S EXPERIENCE IN IDENTIFYING NATIONAL CRITICAL INFORMATION INFRASTRUCTURES

Here, I would like to draw on Lithuania's experience in identifying our national critical information infrastructures. Lithuania has undergone a rapid digitization process in the last decade: most of the government services are now available online, businesses and utilities have become dependent on ICT systems and networks. So in 2015, a Law on Cybersecurity came into effective to address and govern Lithuania's cybersecurity. You can say that we followed the same path that many countries do: we digitized, made ourselves vulnerable and now are trying to deal with it.

The law on cybersecurity amongst other things introduced a notion of Critical Information Infrastructures and defined responsibilities for their protection and defence. The Law also defined CIIs identification process and required it to be executed in a comprehensive manner following the Methodology approved by the Government of the Republic of Lithuania.

NRD CS was awarded a contract to develop a methodology for identification of critical infrastructure and assist the Client in adopting is as a legal act.

The methodology for national CIIs identification, developed by NRD CS and approved as a Government resolution, adopted a top-down approach, meaning that no information infrastructure is critical per se unless it automates a service that is vital for the functioning of a state, its economy, health care, defence and security system and the disruption of which would have a grave damage on national security, economy, state and societal interests.

In Lithuania, we have identified 13 critical sectors and each sector has its own critical services. To name a few - energy sector, water sector, health sector, transport sector are among our critical sectors. In water sector we have two critical services – one of them is drinking water storage, distribution and quality control, another – wastewater collection and treatment. Because we think that if the provision of drinking water will be disrupted or our people will get water unsuitable for drinking, it would cause a major crisis in our country.

Based on these critical services, the responsible ministries had to identify infrastructures that are involved in the provision of a particular critical service and assess how critical they are. And here comes the dilemma: what determines the criticality of an infrastructure.

In Lithuania, we have established 9 criticality criteria for determining if a particular infrastructure is critical to our country. And we measure the effects of non-functionality or destruction of a particular infrastructure in terms of:

- Disruption effect on the provision of a critical service (in terms of population and area affected);
- Effect on human life and health (in terms of population and area affected);
- Disruption effect on the country's economy (in terms of lost working days);
- Environmental effect (in terms of financial damage);
- Effect on public trust to the State (subjective assessment);
- Effect on other infrastructures providing the same critical service (in terms of number of infrastructure affected);
- Effect on other infrastructures providing different critical service (in terms of number of infrastructure affected);
- Effect on public order (subjective assessment)
- Effect on other EU member states (in terms of number of the States affected)

For a particular infrastructure to be listed as critical, it should reach a certain threshold. Once critical infrastructures are identified, relevant ministries together with the operators of a particular infrastructure perform an assessment which information infrastructure is essential for the critical infrastructure to provide a critical service. The criticality of information infrastructures is determined by identifying all information systems, networks that are required for the provision of a critical service and assessing them against three basic questions:

- Is a network or information system essential for a critical infrastructure to provide a critical service?
- Can a cyber incident in a network or information system disrupt the provision of service by the critical infrastructure?
- If a network or information system is compromised/ disrupted, are there no alternatives to ensure the continuity of the provision of service by the critical infrastructure?

If answers to all three questions are positive, then a particular information infrastructure is listed as critical. In other words, if a part of the network breaks ups without compromising and entire system, it is ok to live with that and this network is not critical information infrastructure.

Lithuania is now in a final stage of compiling our critical information infrastructure list, which is again to be approved by the Government.

4. ROLE OF GOVERNMENT (REGULATION AND INCIDENT RESPONSE)

From my country's experience you can see that Governments do have a very important role to play in protecting their national information infrastructures. Firstly, because every government has a duty to protect their nations from cyberattacks, be they launched by the criminality, malicious actors, or other states. But Governments cannot protect everything, so they need to know which networks and

systems are critical to their countries. And truly knowing what is critical requires a comprehensive assessment and stocktaking of some form.

When the Government knows its critical information infrastructures, it can harden those networks and systems and make them less vulnerable to the attacks. In Lithuania, it is achieved through regulation – a compliance requirement to a number of technical and organizational security measures are established for the operators of CIIs, including mandatory cyber incident reporting. It helps to ensure that when malicious activity does occur, it is contained effectively and the consequences are reduced to a minimum.

On the other hand, the Government provides assistance to the operators of Critical Information infrastructures in incident detection, resolution and mitigation, if/ when they do happen. And use an extensive co-operation mechanisms with other CERTs to exchange information and provide warning.

And it is a balanced approach to protecting a nation from cyberattacks, I think.