NATO “Article 4.5”: a new format for providing security against cyber attacks

Interviews

December 11, 2014



Like 2,299 people like this.

JTW Interview with Bakhtiyar Aslanbayli

Turkish Weekly team conducted an in-depth interview with Bakhtiyar Aslanbayli, lecturer at Baku State University, on the provision of cyber security to critical energy infrastructure in Azerbaijan, especially with respect to newly emerging alternative energy supply routes to the Europe.

Regarding critical energy infrastructure, what are the main problems and recent developments?

In the recent decade, energy has become one of the critical factors of international affairs and the role of energy resources in international affairs overall is dramatically increasing. The major reason for this is the increasing demand for energy resources throughout the planet, and in Europe specifically. The increasing demand for energy leads us to look for more opportunities related to energy resources. When we look at the statistics, around 30 percent of EU gas import is met by Russia. This fact makes the European gas market very dependent on Russian supply. Overall, currently Europe has three major sources of gas supply: the North Sea, North Africa, and Russia. What Europe

is trying to do these days is to bring gas to Europe from new sources such as the Caspian Sea. Europe is also looking to diversify the export routes of such energy resources. To bring Caspian gas to Europe, a new transit corridor has been proposed, namely the Southern Gas Corridor. This corridor consists of three major pipelines: the existing South Caucasus Pipeline (from Baku to Turkish-Georgian border), TANAP (from the Turkish-Georgian border to Turkish-Greek border), and the third leg being the Trans-Adriatic Pipeline, which starts on the Turkey-Greece border and continues through Greece, Albania, and eventually reaches the Adriatic Sea and then Italy. Here it should be noted that the Southern Gas Corridor will provide opportunity for interconnectivity with some Eastern and Central European countries, for example Greece-Bulgaria interconnector may bring gas to Bulgaria, and once the infrastructure becomes operational, there might even be further interconnections. This is a brief introduction to the developments in the field of energy that can be seen in the region.

On the other hand, the need to protect critical energy infrastructure and the materialization of potential threats thereto have been highlighted in several NATO summit declarations. The emerging security vision of NATO is heavily focused on protecting critical energy infrastructure. However, energy experts somehow ignore cyber threats and overlook political factors. For some reason, the dimension of cyber security continues to evade the attention of many experts. I appreciate that the political factors surrender to the importance of protecting the critical energy infrastructure protection. However, if we completely ignore the cyber security aspect of energy security, it may cause serious damage to the system. And by saying “damage to the system”, the point I would like to underline is that energy infrastructure has a unique nature as it is constituted by several elements, from platforms to pipelines, from pumping stations to terminals, etc., and if any small facet of that infrastructure were to be isolated or to face a cyber-attack, the entire system could be blocked. That is the unique nature of energy infrastructure. If a small component of the system malfunctions or ceases to work, the entirety of the infrastructure cannot properly function. In this way it is important to ensure the maintenance of the security of the whole structure.

Providing security to each and every constituent part of the critical energy infrastructure is a significant feat. Also, you mentioned the increasing role of NATO in terms of protecting critical infrastructure. So, in terms of the Southern Gas Corridor, whose burden is it to provide protection from cyber-attacks?

Obviously, maintaining security assurances falls within the responsibilities of the national governments. Each national government, whether Azerbaijani, Georgian, Turkish, etc., has to take protective measures and provide security for each respective part of the pipeline. However, in the 21st century there are certain issues that exhibit an internationalized nature. Therefore, states have to cooperate at a certain level in order to properly protect themselves and the infrastructure located within their territories from external threats. We could talk about political and geopolitical threats, but one threat I would like to highlight is found in the format of such cooperation itself. There are of course bilateral and multilateral formats for cooperation, but in order to more efficiently ensure the security of the energy infrastructure, countries in the region need to be more

involved with the EU and NATO. There is dialogue platform to this end, but I want to bring up a more tangible and substantial format of cooperation.

Turkey, as a NATO member country, can easily use existing NATO protection formats, but for Azerbaijan and Georgia this is not possible even though both countries are members of NATO’s Partnership for Peace program. Gaining access to the existing NATO protection platforms and instruments is basically impossible for Azerbaijan and Georgia. Therefore, what is needed to increase and intensify this cooperation is to discover and formulate a new format for Azerbaijan and Georgia, bearing in the mind that both of these countries are located on this energy corridor which is critical for supplying energy to Europe. Today, oil transported by the Baku-Tbilisi-Ceyhan pipeline meets approximately 4% of EU oil imports. If there were to be a cyber-attack against these systems, thus causing the pipeline to stop functioning, the failure to supply energy to the European market through this route may severely damage both European and global energy markets.

A new format against cyber-attacks… Could you further elaborate on this term with respect to cyber threats and NATO’s approach to cyber-attacks?

If everything goes according to plan, the Southern Gas Corridor should be completed and begin transporting energy resources at the end of 2018 or beginning of 2019. Through this corridor, at first stage 10 billion cubic meters of gas per year will be transported to Europe Shah Deniz field in Azerbaijan, with possibility of bringing some more volumes from other sources at a later stage. Yet, this massive volume could be interrupted by a cyber-attack that paralyzes the whole system.

NATO now equates cyber-attacks to military attacks, as the Wales Summit leaders decided that such an attack could be used as a reason to evoke Article 5 of the Washington Treaty. A decision as to when a cyber attack would lead to the invocation of Article 5 would be taken by the North Atlantic Council on a case-by-case basis. Turkey can take advantage of that mechanism but Azerbaijan and Georgia cannot. On the other hand, Article 4 of the Washington Treaty regulates the existing format of consultation in an emergency between partner countries. Article 4 provides consultation or dialogue, whereas Article 5 provides the possible deployment of military support.

Because of the well-known geopolitical realities in the Caucasus, the measures outlined in Article 5 are too much for Azerbaijan and Georgia, but at the same time, the measure outlined in Article 4 is insufficient. So we need to find a ground between these two proposed measures, a ground I call the “Article 4.5” format. This format proposes activity that is more than just “talking and consultation” but less than “boots on the ground”. Such a framework could assess defense capabilities in terms of cyber security. Here, gaps of the cyber system could be determined and improvements could be made to the security of critical energy infrastructure in terms of cyber security by addressing these gaps. Thus, a cyber-ring could be created to protect the infrastructure of the Southern Gas Corridor and to provide a common security system which would minimize and mitigate external cyber-attacks.

The cyber security perspective would be a good starting point from which protection of the energy infrastructure could become more reliable. This framework is also in the best interest of partner countries when it comes to furthering their relationships with NATO. This would also be helpful for NATO, as it would help to rebuild the already decreasing trust in the alliance that is seen within the societies of Azerbaijan and Georgia.

By Oğuz Kaan Pehlivan
Source: Journal of Turkish Weekly



0 Comments Sort by Top

Add a comment...

Facebook Comments Plugin