Energy Regulators from Armenia and North Macedonia Make Progress in Cyber Preparedness

January 2021 – Published in April and May of 2020, respectively, "*The Utility Regulator's Role in Promoting Cybersecurity: Resilience, Risk Assessment, and Standards*" and "*Evaluating the Prudency of Cybersecurity Investments: Guidelines for Energy Regulators*" are two publications meant to empower energy regulators to strengthen their cyber preparedness and increase grid resilience.

With funding support from the United States Agency for International Development (USAID) under the Energy and Infrastructure Division of the Bureau for Europe and Eurasia, the National Association of Regulatory Utility Commissioners (NARUC) developed these resources with the intention of arming regulators with the tools to understand and evaluate cybersecurity measures in a national and/or regional setting. Since 2016, USAID and NARUC have worked together to instruct national regulatory authorities in the Black Sea – Armenia, Georgia, Moldova, and Ukraine – and Southeast Europe – Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, and Serbia – on the fundamentals of cybersecurity, as well as the risk management principles that can be used to face these evolving challenges.

In this context, we followed up with regulators from both Armenia's Public Services Regulatory Commission (PSRC) and the Energy and Water Services Regulatory Commission of the Republic of North Macedonia (ERC) to track the progress they have made in relation to the key themes of each publication.

The Utility Regulator's Role in Promoting Cybersecurity

Regulators are charged with several core functions, such as ensuring security of supply, evaluating utility investment plans, and setting tariffs. In addition to these functions, "*The Utility Regulator's Role in Promoting Cybersecurity: Resilience, Risk Assessment, and Standards*" emphasizes regulators' leading role in protecting and advancing the energy sectors of their countries and provides a useful summary of international cyber standards. Through referencing the publication, regulators can better understand how to develop and implement appropriate, country-specific regulatory structures and mechanisms to safeguard critical infrastructure and ensure reliability and improved quality of service.[i]

Over the years, the role of the regulator in implementing cybersecurity standards in the energy sector has become more prominent as the nature of cyber threats continues to evolve. When asked about this role, representatives from the PSRC confirmed that they are increasing their monitoring efforts as they implement trade in the wholesale electricity market through an electronic platform in the next few years. Alongside this initiative, they will also introduce a supervisory control and data acquisition (SCADA) management program that will allow them to better monitor utilities remotely. Similarly, ERC representatives stated, "Energy companies' resilience to cyber-attacks has significant implications for the energy market and its consumers… the ERC aims to focus on preventing potential risks or disruption to the continuity of power supply through a supportive relationship with targeted utilities in implementing cybersecurity standards."

Both Armenia and North Macedonia have recently drafted legislation that aims to apply international cybersecurity standards. In the case of Armenia, the government, with contributions from the PSRC

and other relevant stakeholders, has developed a "*Draft of the Strategic Program for the Development of the Energy Sector of the Republic of Armenia (until 2040)*" as a means to ensure the digital transformation of the energy sector. Likewise, the ERC's "*Draft List of Cybersecurity Recommendations for TSO/DSO/GEN*[ii] *in the electricity sector*" includes cybersecurity frameworks and measures that are meant to contribute to the creation of a more secure digital ecosystem. This list of recommendations will be followed by the adoption of the first cybersecurity strategy for the electricity sector in the Republic of North Macedonia and an action plan with clearly defined steps for strategy implementation.

In addition to implementing cybersecurity standards for the benefit of the energy sector, regulators should also engage with utilities and other governmental institutions in coordination efforts to promote effective cybersecurity measures. For example, the ERC has made progress in coordinating with the National Centre for Computer Incident Response (MKD-CIRT) of the Republic of North Macedonia, the Personal Data Protection Agency, and with the Ministry of Information Society and Administration of the Republic of North Macedonia on cyber standards. By reaching across other sectors, regulators can become well positioned to coordinate and share knowledge, information, and best practices on cybersecurity related topics to the benefit of the entire country.

Evaluating the Prudency of Cyber Investments

On a related note, establishing a regulatory approach to enhance the cybersecurity stance of any power system requires reasonable, prudent, and effective investments. With this in mind, "*Evaluating the Prudency of Cybersecurity Investments: Guidelines for Energy Regulators*" is meant to serve as a practical tool that regulators can use to make tariff decisions in relation to their respective regulatory frameworks and vulnerabilities. By referencing the publication, regulators can get answers to questions such as "Is it possible to evaluate the effectiveness of cybersecurity investments?" and "Which regulatory frameworks are best suited to evaluate the prudency of cybersecurity expenditures?"

Some energy regulators are working to receive legal mandates so that they will be able to officially adopt a cybersecurity strategy and evaluate utilities' cyber investments. For example, the PSRC/Armenia is coordinating with other government institutions to contribute to defining roles and responsibilities with regard to cybersecurity. As of now, cybersecurity standards are expected to be implemented in the energy sector in late 2023. PSRC representatives specified that the topics covered in the *Guidelines* are very valuable as they work to that goal, and that the practical application of the publication will be frequent – especially concerning the evaluation of cyber-related expenditures and effectiveness metrics.

From another standpoint, energy regulators from North Macedonia have been able to move forward with evaluating utility cybersecurity expenditures on a legal basis. The Government of the Republic of North Macedonia adopted the National strategy for cybersecurity in North Macedonia (2018-2022) and an Action Plan for cybersecurity (2018-2022). ERC representatives underscored the importance of this advancement, stating, "This is crucial, since it enables us to be more proactive and efficient in various segments of our work, including activities related to strengthening cybersecurity preparedness in the energy sector."

They also added that their current tariff approval system – parts of which stem from the *Guidelines'* described method of performance-based regulation – requires utilities to provide detailed information on their planned costs for security/cybersecurity and define regulatory indicators and objectives that need to be reached. If an evaluation shows that the costs are reasonable and realistic, they are approved as part of the utilities' investment plans for the following regulatory period. Subsequently, an annual review of the plans functions to verify their implementation status and the reliability of the data received from the utilities.

In every country, progress in these areas is dependent upon many different stakeholders, often including various government ministries, utility companies, TSOs, and computer incident response

teams. Energy regulators are only one piece of the security puzzle, but they are an important one nonetheless given their role in ensuring quality of service and issuing licenses for utilities. In both Armenia and North Macedonia, it is clear that regulators are committed to exercising their leadership to help ensure that their electric grids are protected from and resilient against cyberattacks. Moving forward, NARUC will continue to support national regulatory authorities in the Black Sea and Southeast Europe as they craft customized regulatory policies that will determine their response to increasing energy security challenges.

This story is made possible by the generous support of the American people through the United States Agency for International Development (USAID). The contents are the responsibility of NARUC and do not necessarily reflect the views of USAID or the United States Government.

Photo Credit: © Song_about_summer / Adobe Stock

[i] "The Utility Regulator's Role in Promoting Cybersecurity: Resilience, Risk Assessment, and Standards." NARUC. https://pubs.naruc.org/pub.cfm?id=C3597EE6-155D-0A36-31AC-3F82F33A665B

[ii] Transmission system operator/distribution system operators/generators