Albania Establishes First-Ever Cybersecurity Regulation for the Electricity Sector

October 2020 – The Albanian Energy Regulatory Authority (ERE) has recently approved the country's first-ever cybersecurity regulation for the electricity sector, titled "Regulation on Cybersecurity of Electricity Sector Critical Infrastructure." In doing so, they have established incident reporting criteria and requirements that electricity system operators can use to assess and improve their cybersecurity maturity as well as their protection and response capabilities.

Under the United States Agency for International Development (USAID) Europe and Eurasia Cybersecurity Initiative, the National Association of Regulatory Utility Commissioners (NARUC) works alongside USAID to leverage the U.S. and European Union regulatory experience and assist Black Sea and Southeast European regulators in developing appropriate country-specific cybersecurity policies and tools. These tools can in turn be used as templates and models for regulators around the world.

As a testament to this initiative, ERE drafted their cybersecurity regulation, drawing upon two USAID/NARUC publications: the **Black Sea Cybersecurity Strategy Development Guide** and the **Cybersecurity Evaluative Framework for Black Sea Regulators**. The regulation was then peer reviewed by energy regulatory experts from the state of Connecticut, U.S., as well as the Agency for the Cooperation on Energy Regulators (ACER) in Europe.

The Importance of Cybersecurity in the Energy Sector

As societies become more interconnected, the need for improved cybersecurity measures to prevent and respond to threats targeting the security and data of operational systems is more important than ever. Since 2016, NARUC has responded to this need by providing technical assistance and conducting a variety of engagements and in-person workshops through the Europe and Eurasia Cybersecurity Initiative. These activities are meant to ensure regulators have the necessary tools and understanding to work with utilities and to cooperate with other government agencies to effectively strengthen the cybersecurity and resilience of their respective energy sectors.

Protecting the security of the energy sector is critical. As electric, gas, water, communications, and transportation systems become increasingly dependent on integrated systems to manage complex resources, they are exposed to additional vulnerabilities that can be exploited by cyberattacks. Notably, when cyber-attacks target the electric grid, the consequences can be dangerous – in addition to mass blackouts, banks, hospitals, government agencies, and a wide variety of other important institutions can be shut down, thereby shocking the economy.

Hisham Choueiki, NARUC's Principal Technical Advisor for Energy Regulation, stated, "While the implementation of cybersecurity measures is typically the responsibility of power system operators, national regulatory authorities (NRAs), such as ERE, have an obligation to protect the public interest by ensuring the security of supply. Cyber-attacks are more widespread these days, and the results of a successful attack can be very harmful to utility operations and the safety of the public at large.

Recognizing the seriousness of these attacks and encouraging the development of counter-defense measures are the first step that an NRA should pursue."

Albania's Efforts to Strengthen Cyber Preparedness

Similar to other countries in the Europe and Eurasia region, Albania acknowledges the need to prevent and contain cyber-attacks. Albania's National Security Strategy (2014) promotes the adoption and implementation of a National Cybersecurity Strategy, and the current Digital Agenda of Albania (2015-2020) includes cybersecurity as a recurring theme throughout its vision of "a society based on knowledge and information, through the consolidation of digital infrastructure in the whole territory of the Republic of Albania; improvement of the quality of online services, and increase of governance and transparency."[i] These measures to minimize digital vulnerability are needed to respond to the country's rapid advances in telecommunications and increasing access to the Internet.

As an example of Albania's success in progressing information and communications technology (ICT), 63.25% of the Albanian population had Internet access in 2015 compared, to 45% in 2010.[ii] However, efforts to manage and strengthen cyber preparedness in the energy sector have been met with some difficulty, namely due to the general lack of a cybersecurity mindset and a growing need to train more professionals in cybersecurity.

In Albania, placing a priority on cybersecurity occurs mainly within the context of large commercial organizations, and is not necessarily a primary objective for utilities and government officials. This results from the fact that rural areas have limited access to the Internet, and existing cybersecurity awareness efforts are too limited in scale to provide a sufficient level of knowledge across society as a whole.[iii] On a related note, within most public institutions training for both general staff and ICT staff is limited. Regulators are often unfamiliar with topics such as how to assess utilities' cyber performance, how to work with utilities to block cyber-attacks, and how to develop a cybersecurity strategy.

USAID and NARUC Publications Meant to Increase Cybersecurity Proficiency

With this in mind, the USAID and NARUC publications that ERE referenced when writing their new cybersecurity regulation were created to help energy regulators address these obstacles. The **Cybersecurity Evaluative Framework for Black Sea Regulators** provides a framework that is designed to allow a structured way for regulators to assess what level of cyber-preparedness utilities have reached and identify areas for improvement. The framework is a companion to training provided at USAID/NARUC workshops in 2017-2018, which offered a comprehensive overview of cybersecurity fundamentals and outlined steps regulatory commissions can take to become effective partners with utilities in both preventing and mitigating cyber-attacks and supporting the overall security of the energy sector.[iv]

Subsequently, the **Black Sea Cybersecurity Strategy Development Guide** sets clear steps for regulators to follow as they develop their own cybersecurity strategies. Its contents include key questions that regulators must address in structuring their strategies, and lists examples of how regulators at U.S. commissions have approached each of the given questions. Altogether, these resources are meant to help regulators increase their cybersecurity proficiency and take action consistent with their respective needs and priorities.

Charting a Steady Path Forward

> "ERE has learned a lot from USAID and NARUC. Their cyber workshops – located in Latvia in 2018 and in Poland and North Macedonia in 2019 – publications, conference calls, and overall experience allowed us to prepare, consult, and approve the first cybersecurity regulation on critical infrastructure in the power sector. We tried to leverage NARUC's experience as much as possible to address this very complex and important issue, as well as the know-how of all the workshop presenters on both technical and financial matters related to cybersecurity.
>
> Following the workshops, we were able to gather and spread what we learned to our related staff and Commissioners as well as to the staff of the utilities operating Albania's critical infrastructure. As a result, they had the opportunity to express their thoughts and comments, which we took on board. The NARUC consultants also provided us with great support, and their comments and suggestions on the draft regulation helped make the document more consistent."
>
> - *Petrit Ahmeti, ERE Chairman*

Moving forward, NARUC will continue to assist ERE as they implement their new regulation and continue strengthening their cybersecurity preparedness. Ahmeti added, "We are looking forward to the continued support of USAID and NARUC in monitoring the implementation of the regulation from the operators of the critical infrastructures. In doing so, we aim to improve the regulation, and are aware that it will expand in the coming years as we set targets for instructing the operators to focus on this critical concern in their day-to-day business."

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 Caption: Albanian regulators receive training on designing an effective cybersecurity strategy at a USAID/NARUC workshop in Warsaw, 2019.

[i] "Albania Country Review Innovation June 2016." ITU. PDF file. 2016. https://www.itu.int/en/ITU-D/Innovation/Documents/Publications/Albania%20Country%20Review%20Innovation%20June%202016.pdf

[ii] "ICT Centric Innovation Ecosystem Country Review: Albania Report." ITU. PDF file. 2016. https://www.itu.int/en/ITU-D/Regional-Presence/Europe/Documents/Events/2016/Innovation%20Ecosystem%20Albania/Innovation%20Ecosystem%20Albania.pdf

[iii] "Report on Cybersecurity Maturity Level in Albania." National Authority on Electronic Certification and Cyber Security. PDF file. 2018. https://cesk.gov.al/Publikime/2019/AlbaniaCMMReport.pdf

[iv] "Cybersecurity Evaluative Framework for Black Sea Regulators." NARUC. https://pubs.naruc.org/pub.cfm?id=E3CE75B5-155D-0A36-31FD-1B268F7BD125