NETL Impact
Vol. 04/ Spring 2018
A Publication of the U.S. Department of Energy's National Energy Technology Laboratory

Revolutionizing Energy Systems

DEVELOPING NEXT-GENERATION CYBERSECURITY TECHNOLOGIES TO STRENGTHEN NATIONAL ENERGY INFRASTRUCTURE

By Krista Baker
Technical Contact: Eddie Christy (Eddie.Christy@netl.doe.gov)

Reliable energy supports our prosperity and enables our quality of life. Delivering energy to our homes, hospitals, businesses, and beyond requires a vast network that produces, transfers, and distributes energy where it's needed. Resilient energy infrastructure requires robust energy delivery systems to provide timely and accurate information to system operators and automated control over a large, dispersed network of energy delivery components.

The Office of Electricity Delivery and Energy Reliability (OE) leads the U.S. Department of Energy's efforts to ensure a resilient, reliable, and flexible electricity system. OE works to develop new technologies to improve the infrastructure that brings electricity into our homes, offices, and factories, and the federal and state electricity policies and programs that shape electricity system planning and market operations.

A key aspect of OE's work is cybersecurity – advancing the research and development of innovative technologies, tools, and techniques to reduce risks to the nation's critical energy infrastructure posed by cyber and other emerging threats.*

Supporting OE's important mission in this area are NETL project managers within the Lab's Energy Technology Development directorate, who are applying their program management expertise to OE's Cybersecurity for Energy Delivery Systems (CEDS) Program. In this effort, NETL manages extramural research, development and demonstration of new tools and technologies to enhance situational awareness and cybersecurity of critical energy infrastructure, through research partnerships.

Critical energy infrastructure consists of hardware and software systems that monitor, protect and control processes. It also includes equipment that manages energy generation (electric) or production (oil and gas) all the way to energy delivery to the end user. Advances in communication and computing have enabled promising new benefits to be integrated into this infrastructure, such as improved automation, situational awareness, system performance, efficiency and reliability. However, these advances also brought unfamiliar problems and risks to the security and reliability of these cyber-physical systems. For this reason, OE has aimed its research and development efforts under its CEDS Program portfolio to supporting resilient energy delivery systems that are designed, installed, operated, and maintained to survive a cyber incident while sustaining critical functions.

CEDS research partnerships involve energy sector utilities, suppliers, government, universities and the Energy Department's national laboratories to advance cybersecurity capabilities tailored to the unique performance requirements and operational environments of energy delivery systems. These partnerships transition innovative cybersecurity capabilities from early-stage research to routine use, strengthening the resilience of real-world energy delivery systems. Examples of projects that have successfully transitioned to the energy sector include:

- Quantum Key Distribution (QKD) system that provides cutting-edge security while greatly simplifying the generation, maintenance, and distribution of encryption keys used in energy delivery systems. This uses quantum entangled photons to guarantee tamper detection and provides a secure encryption against even a quantum computing attack.
- Secure advanced metering infrastructure (AMI) and distribution automation (DA) wireless mesh networks with continuous monitoring, anomaly, and intrusion detection and prevention.
- Strong anti-malware and whitelist protection secures field devices that ensures only approved applications, services, and/or executables are ran and executed and all others are blocked.
- A solution to streamline the task of patching and updating devices used in energy delivery control systems. This is particularly important in cases when patches and updates mitigate security vulnerabilities that may be exploited by adversaries.
- Technology that enhances the cyber and physical security that protects both electronic and physical perimeter by monitoring and controlling device assets.
- Software Defined Networking technology for Energy delivery networks that keep working, even during a cyber-attack, by automatically redirecting communications along pre-selected, pre-engineered alternative paths.

"Each research partnership, whether led by industry, academia or national laboratories, is expected to establish a clear path toward industry acceptance and transition the research results to practice, from the earliest stages of the research," said Carol Hawk, Ph.D., the CEDS Team Program Manager.

The dynamic cyber threat landscape, continuous advances in energy delivery system technologies, and the use of legacy devices in ways not previously envisioned underscore the importance of transitioning the innovative CEDS R&D to practice. CEDS R&D helps secure our nation's energy infrastructure from cyber-attack, which is critical to national security, but for which an individual energy sector organization would likely be unable to support a business case.

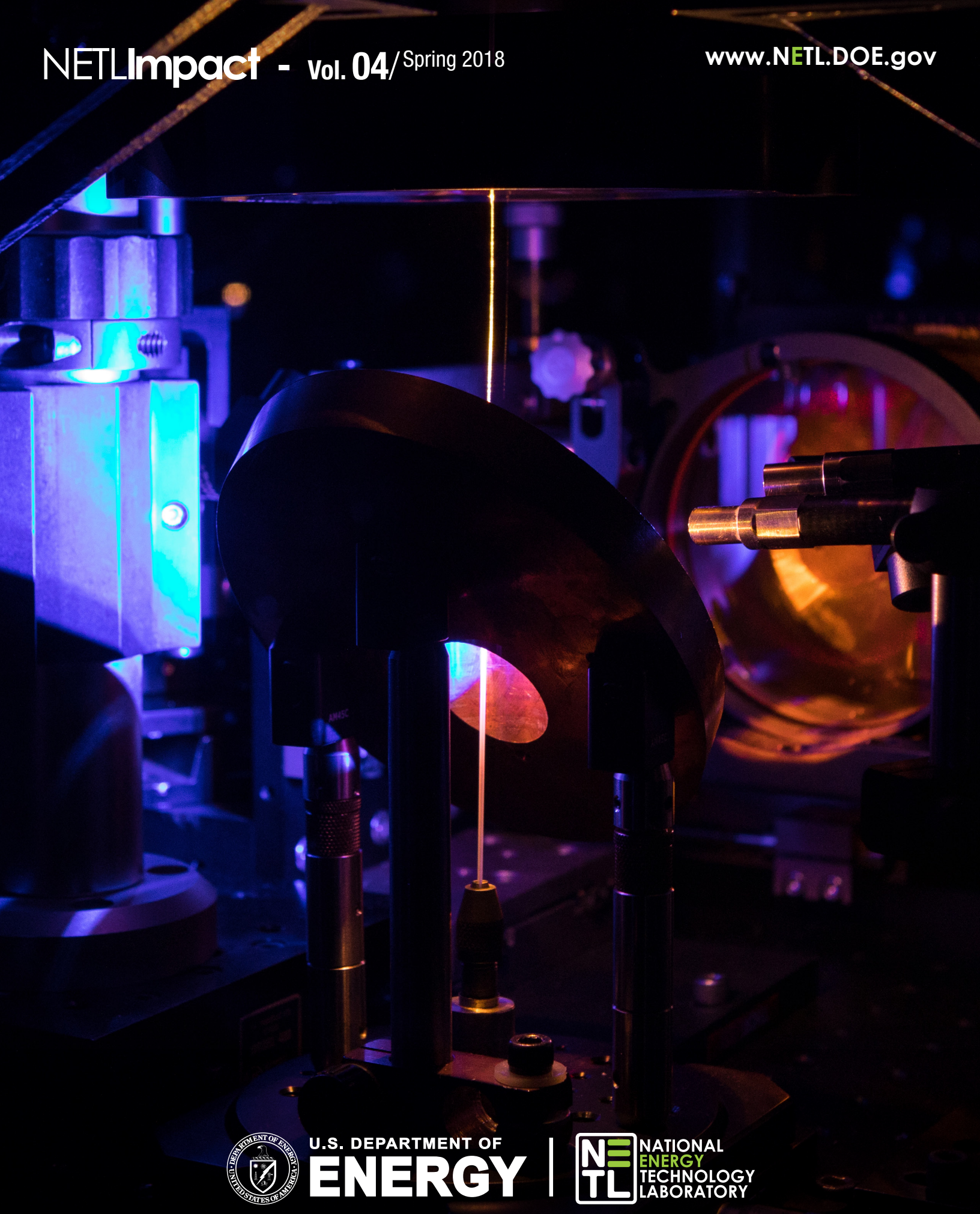
"More than 40 tools, including guidance documents, and technologies have been made available to the energy sector through CEDS-supported research partnerships," Hawk said. "I, along with the folks at NETL, am excited to be part of these research activities that have national significance to protect our critical energy infrastructure."

For more information on the CEDS program, visit the Office of Electricity Delivery & Energy Reliability's website at www.energy.gov/oe.

** Note: on Feb. 14, 2018, Secretary of Energy Rick Perry announced the establishment of a new Office of Cybersecurity, Energy Security and Emergency Response, which is intended to bolster DOE's efforts in cybersecurity and energy security.* ☰

NETLImpact - Vol. 04/ Spring 2018

www.NETL.DOE.gov



U.S. DEPARTMENT OF ENERGY | NATIONAL ENERGY TECHNOLOGY LABORATORY

DOE/FE-0599