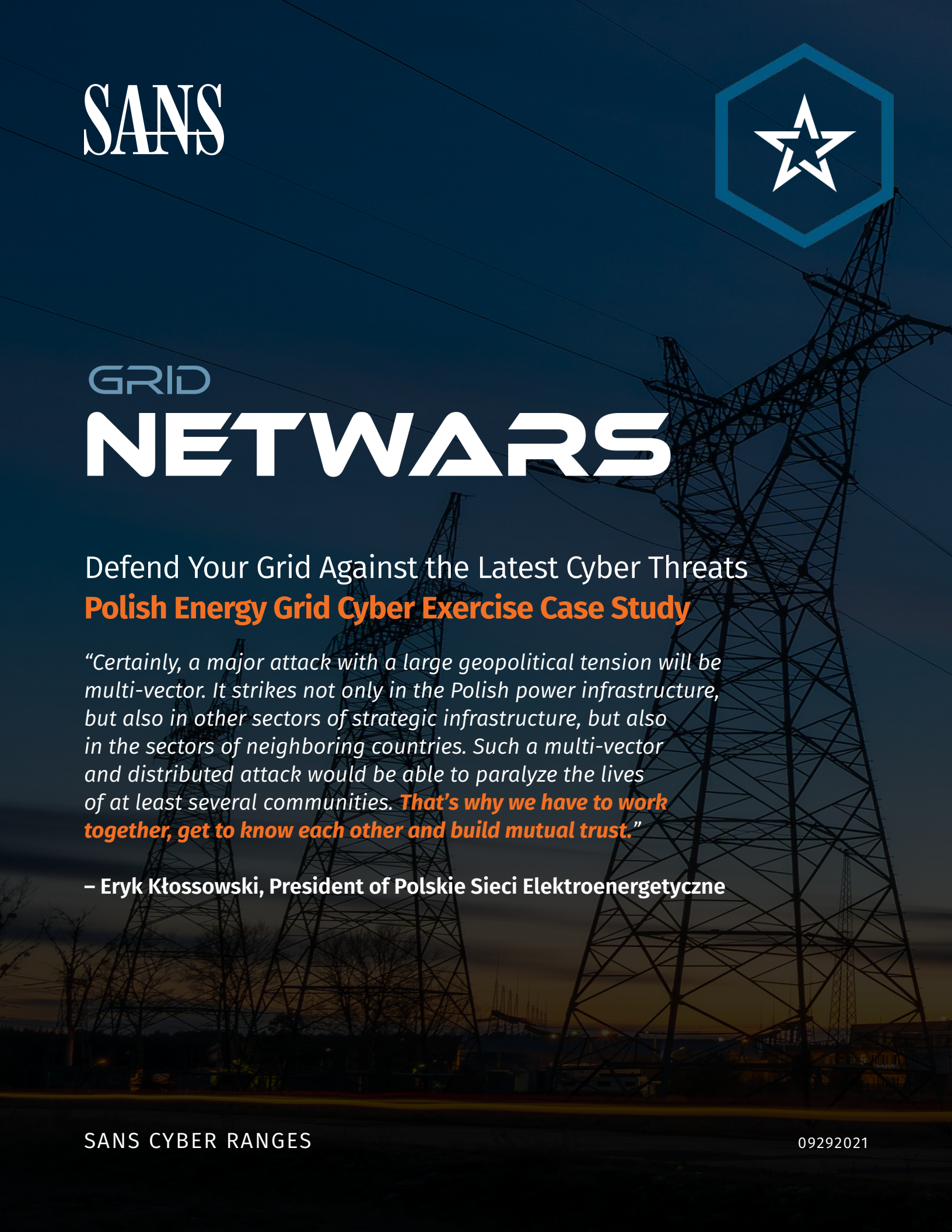


SANS

GRID
NETWARS

Defend Your Grid Against the Latest Cyber Threats
Polish Energy Grid Cyber Exercise Case Study

"Certainly, a major attack with a large geopolitical tension will be multi-vector. It strikes not only in the Polish power infrastructure, but also in other sectors of strategic infrastructure, but also in the sectors of neighboring countries. Such a multi-vector and distributed attack would be able to paralyze the lives of at least several communities. ***That's why we have to work together, get to know each other and build mutual trust.****"*

– Eryk Kłossowski, President of Polskie Sieci Elektroenergetyczne

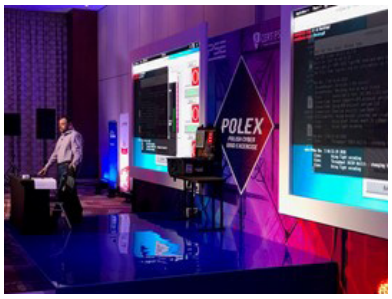
SANS CYBER RANGES

09292021

EXECUTIVE SUMMARY

PolEx is an annual event, run in collaboration with SANS Institute, for Information Technology (IT) and Operational Technology (OT) professionals from Polskie Sieci Elektroenergetyczne (PSE), other companies from the energy sector in Poland, other partnering countries in Europe, and industry solution providers.

PSE turned to **SANS Institute's Grid NetWars** to create a multi-day simulated training exercise during PolEx for cyber security professionals to gain practical real-world experience about attacks and issues regularly encountered in Industrial Control Systems (ICS) infrastructure, Computer Emergency Response Teams (CERT), and Security Operations Centers (SOC).



"I believe that threats in cyberspace are one of the most important problems to be solved. We must act as a community. This is the only way to defend against cyber threats. We cannot act in isolation, we have to communicate between sectors. Energy infrastructure links them. This is the way to bring danger into the center of our system."

– Piotr Naimski, Government Plenipotentiary for Strategic Energy Infrastructure

WHAT IS SANS GRID NETWARS?

- A suite of hands-on, interactive learning scenarios focused on enabling OT security professionals to develop, test, and master the real-world, in-depth skills needed to defend real-time systems.
- Designed as a challenge competition consisting of multiple separate levels so that players at different skill levels can move through levels at their own pace.
- Themed for the electricity industry, the scenario has been previously used to support multiple electric sector exercises, enabling participation by players at all skill levels from any sector.

CHALLENGES

In partnering with SANS to create PolEx, the PSE was looking to provide learning opportunities for cyber security practitioners throughout the electric sector within Poland to improve incident response and information sharing capabilities. They needed to:

- Provide a safe, secure, and engaging experience for participants to develop and validate skills.
- Raise the level of practical skills of their employees by giving them the opportunity to put theory into practice.
- Ensure their personnel were prepared to handle potentially impactful attacks against their operational assets, especially given that adversary groups are increasingly targeting critical infrastructure entities around the world.

"The conference is a continuation of the successful PolEx exercises from autumn 2018. These exercises were successful because they showed a competence gap in solving cybersecurity problems. They showed that we were unable to solve all tasks on time. This is great news, because the bar was set high, and one should learn to jump through high crossbars, not to massage complexes, to be sure that in a real danger situation we will certainly manage."

— Eryk Kłossowski, President of Polskie Sieci Elektroenergetyczne

RESULTS

- Individual team managers and employees told PSE directly that their participation in Grid NetWars allowed them to acquire valuable knowledge and skills.
- The event allowed PSE to bring together multiple countries, critical infrastructure sectors, companies within a sector, and Government organizations speaking different languages, in a cooperative and engaging manner focused on individual and team learning.
- SANS Grid NetWars enabled international collaboration and contributed to the security and stability of power systems in Europe.
- Interest in and attendance at PolEx continues to grow significantly year over year.

LESSONS LEARNED

Participants and teams learned:

- The benefits of performing specific elements of the event annually, as well as the value of expanding table-top exercises across organizations within Poland.
- How beneficial it is to increase information sharing activities and capabilities across the critical infrastructure sectors within Poland and throughout Europe.
- Ultimately, how well they are prepared to combat risks to critical infrastructure, but under controlled conditions without the risk encountered in real-world scenarios.

BENEFITS

While the benefits across groups were significant and varied, PSE organizers benefitted from:

- Learning how well the information exchange path was working with accordance to the new national act on the Poland cyber security system.
- Checking how the resulting new standards and procedures will work in the case of complex attacks on critical infrastructure under changing legal and regulatory frameworks.
- Expanding the view of impact of cyberattacks and incident response procedures due to table-top exercises being attended by entities from outside the energy sector.

"The cyber threat landscape continues to evolve and it is essential that employees are kept up-to-date with the latest knowledge."

— Sylwia Kornaczewicz-Pieczoro, PSE, PolEx Event Organizer

"It is essential to utilize a training environment that blends the realities of IT, OT, operations, and adversary attacks with defender-focused learning objectives. I have seen firsthand how significant and impactful these hands-on training opportunities are for teams and individuals across multiple sectors and many parts of the world. There is nothing else like it to mature capabilities quickly."

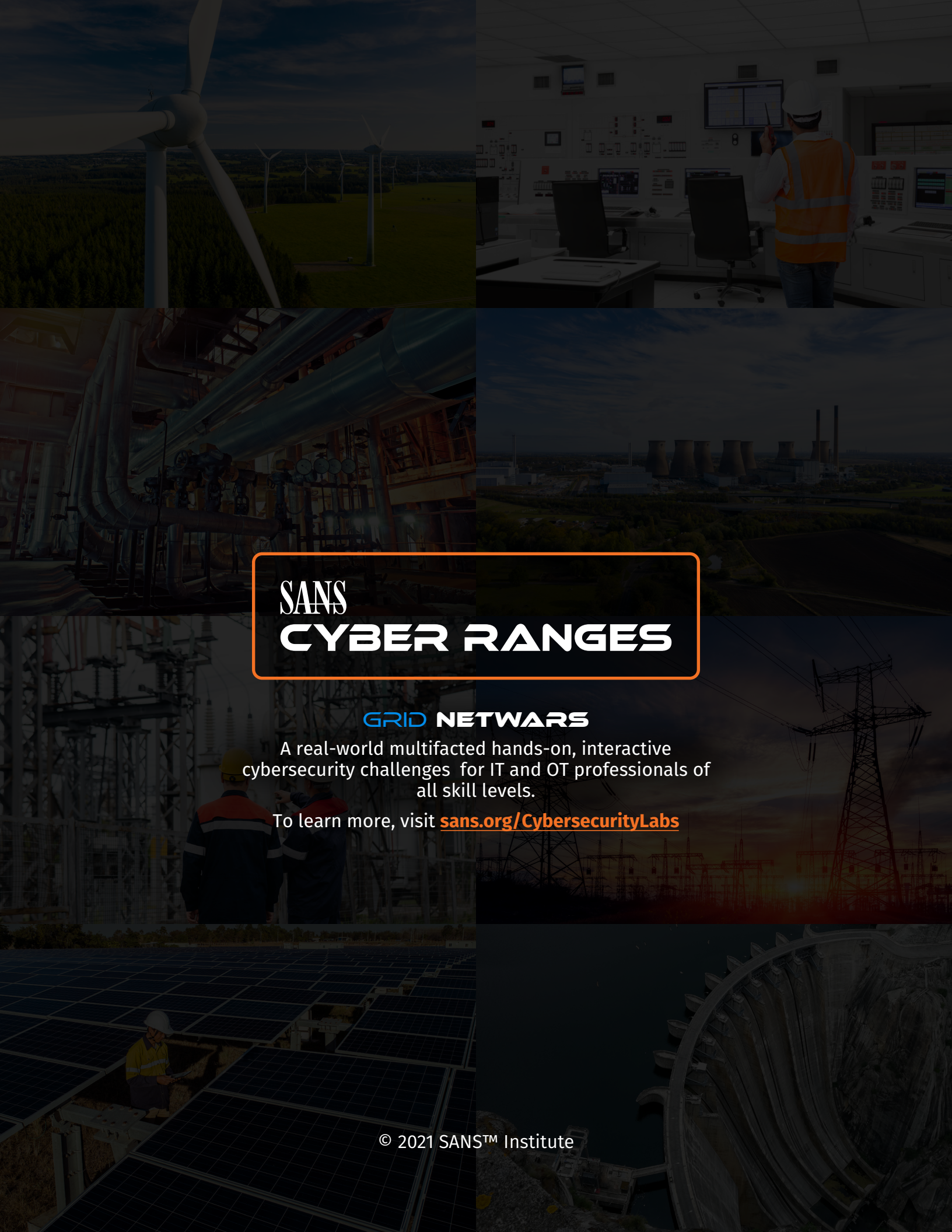
— Tim Conway, SANS ICS Security Curriculum Lead

"The SANS Grid NetWars simulation has an unparalleled realism and depth that is absolutely essential in preparing critical infrastructure defenders for their mission."

— Ed Skoudis, Director of SANS Cyber Ranges

LOOKING AHEAD

PSE will continue to organize annual cyber range exercises as well as a related conference, the Cybersecurity Conference for Energy Sector (CC4ES). SANS is also providing such exercises to other allied countries around the world.



SANS
CYBER RANGES

GRID NETWARS

A real-world multifacted hands-on, interactive cybersecurity challenges for IT and OT professionals of all skill levels.

To learn more, visit sans.org/CybersecurityLabs