ECCWS 2022

21st European Conference on Cyber Warfare and Security

16 - 17 June 2022, Chester, UK

Mini Track on Enhancing Critical Infrastructure Cybersecurity

Mini Track Chair: Dr Leigh Armistead, Peregrine Technical Solutions, VA, USA

In May 2021, the operators of the Colonial Pipeline were forced to proactively shut down operations and freeze information technology (IT) systems after becoming the victim of a ransomware attack. On May 10th, the FBI confirmed that this group was responsible for the pipeline attack, and on May 13th, Bloomberg reported that the Colonial Pipeline company paid a ransom demand of close to $4.4 million in return for a decryption key that enabled it to regain control of its business networks and data. All indications are that the Colonial Pipeline attack was a criminal operation—DarkSide operators targeted the company's business IT networks, rather than its IT and operational technology (OT) networks providing pipeline control. In the wake of the Colonial Pipeline incident, on May 28, the US Department of Homeland Security's Transportation Security Administration (TSA) issued new requirements for pipeline cybersecurity. On July 20th, the TSA issued a new cybersecurity directive requiring owners and operators of certain critical pipelines carrying hazardous liquids and natural gas to "implement a number of urgently needed protections against cyber intrusions."

The OT systems comprising ICS used to control a wide variety of critical infrastructure is ubiquitous and, in many cases, virtually unprotected.

Dr Edwin "Leigh" Armistead is the President of Peregrine Technical Solutions, a certified 8(a) small business that specializes in Cyber Security. A retired United States Naval Officer, he has significant Information Operations academic credentials having written his PhD on the conduct of Cyber Warfare by the federal government and has published three books, in an unclassified format in 2004, 2007 and 2010, all focusing on full Information Warfare. He is also the Chief Editor of the Journal of Information Warfare (JIW) https://www.jinfowar.com/ ; the Program Director of the International Conference of Cyber Warfare and Security and the Vice-Chair Working Group 9.10, ICT Uses in Peace and War. Shown below are the books on full spectrum cyber warfare and the JIW:

Submission details

In the first instance a 300-word abstract is required, to be received by **24th November 2021.** Please read the guidelines at
http://www.academic-conferences.org/policies/abstract-guidelines-for-papers/

Submissions must be made using the online submission form at
http://www.academic-conferences.org/conferences/eccws/eccws-abstract-submission/

If you have any questions about this track please email: Leigh Armistead
leigh.armistead@Goldbelt.com

See more about ECCWS at *http://www.academic-conferences.org/conferences/eccws/*