

## Putin Cyberthreat

Vladimir Putin is one of the world's most dangerous men and evidence is mounting that he wants to solidify the number one position.

A U.S. research firm called FireEye has published a new report that links Putin's Russia to a cyberattack against an unnamed petrochemical plant. While FireEye declined to name the victim, other intelligence sources have identified the target as a facility in Saudi Arabia.

In the 2017 attack, the malware known as "Triton" gained control over a safety shut-off system that is considered critical to defending against catastrophic events. One can only imagine what kind of trouble Putin could be planning.

This is not an isolated incident. Intelligence services have identified Russia as the bad actor that has been probing digital networks of critical infrastructure for at least two years, including the U.S. electrical grid. Russia has also been identified as the instigator of two cyberattacks in Ukraine in 2015 and 2016 that caused large-scale blackouts.

The director of the cybersecurity firm, Dragos, said this about the people behind Triton: "They are active around the world, still focused on critical infrastructure and still pose a clear and present danger to innocent lives and their environments by affecting the safety of control systems."

While the U.S. press has been obsessed with Russia's clumsy and ineffective meddling in the 2016 election, this frightening issue has barely been mentioned.

It's our hope that while the media are focusing their attention elsewhere, cybersecurity experts in the U.S. and other free nations are laser-focused on stopping the critical threat posed by Putin's Russia.

For the Clear Energy Alliance, I'm Mark Mathis. Power On.