Energy Intelligence
Reproduced with permission by Energy Intelligence for Henry L. Stimson Center
Issue Vol. 12, No. 32, August 10, 2018

NUCLEAR INTELLIGENCE WEEKLY®

Vol. 12, No. 32

August 10, 2018

IN PERSPECTIVE

Cyber Risks Go Nuclear

With the threat of cyberattacks on critical infrastructure across the globe escalating every day, Stimson Center analysts Debra Decker and Kathryn Rauhut argue that the US and Russia must work together to establish a strong cyber-security regime. Washington-based Decker and Vienna-based Rauhut have co-authored publications including — along with other team members — Re-Energizing Nuclear Security.

The US Federal Bureau of Investigation (FBI) warned this spring that Russia had infiltrated critical US infrastructure, targeting nuclear and other power plants, along with homes and businesses. UK officials joined in the warning, noting the attacks were worldwide. In July, the US Department of Homeland Security (DHS) revealed more about Russia's sophisticated methods to target and infiltrate industrial control systems. As Russian surveillance of systems persists, a DHS staffer summed up the current Russian capability: "They have access to the button, but they haven't pushed it."

Ergo, the Trump-Putin discussion to establish joint cybersecurity initiatives sounds preposterous. After all, why consort with the enemy? Because in this particular area the two countries could work together to leverage purchasing power over the supply chain for computer software and hardware to demand higher standards that benefit everyone, including both countries' nuclear industries.

The Supply Chain Issue and Nuclear Development

In June the International Atomic Energy Agency (IAEA) held a weeklong meeting that grappled with quality assurance in the cyber supply chain. Dozens of participating countries acknowledged the magnitude of the issue, including the potential for unexpected plant shutdowns. Kremlin-sanctioned attacks have successfully penetrated industrial control systems through vulnerable supply chains. The nuclear supply chain relies on countless items from a vast and competitive global market. Operators must guard against procuring counterfeit, fraudulent or suspect items, even in their own countries. For example, in 2013 in South Korea, a scandal of fraudulent certification of local parts cost the country billions of dollars; it also proved a boon to antinuclear activists, who in turn prompted the new South Korean government to pursue a dramatic decrease in domestic nuclear capacity.

While fear and economics may be stemming the tide of nuclear power in some established countries such as Germany, an expansion of nuclear power is under way elsewhere. And both the US and Russia remain key stakeholders in the global nuclear energy sector. Russia's Rosatom is in the forefront of nuclear newbuilds around the world, and the US still houses more operating power reactors than any other country. Given US and Russian interests in nuclear, could a joint effort for computer supply chain security standards be one confidence-building area between the two countries?

The cyber supply chain is particularly hard to manage. Software complexities and hardware assets can be more difficult to assess than tensile strength of a cable. Tampering can occur in development, manufacturing, shipping, installation or operation. Software updates, a major issue, have caused problems for some operators in the past. Agreed best practices are needed. The IAEA just released good general technical guidance recommending clear supply chain practices, and next year it hopes to publish examples of quality assurance in the nuclear cyber supply chain.

Meanwhile, industry needs to independently assess and grapple with the best way to manage cyber supply chain risks. The DHS described intrusions from compromised vendors, integrators and other partners with relationships to the targets, and cautioned not to pre-approve "network traffic with trusted partners." At the IAEA conference, several law firms and insurers advised nuclear operators to think more proactively about their procurement strategies and to establish terms and conditions addressing prevention and risk mitigation. This would include having suppliers issue important representations and warranties about their own practices that could get certified quarterly.

Why Cooperation Can Work

Large commercial suppliers of off-the-shelf products, cloud providers and even managed service providers are fighting back against accepting liability for cyber breaches or performance. The nuclear sector hasn't established common purchasing requirements that require these. Even if it did, nuclear operators are just one small portion of the customers for many providers. These market-driven realities provide little leeway in negotiating contracts.

Thus, perversely, working on good practices through joint Russian-US cooperation could benefit everyone. Governments have the purchasing power to demand requirements and standards in their procurements and

(continued on page 2)

In Perspective *(continued from 1)*

potentially to shift the liability burden to technology service suppliers. The US government scrapped using Kaspersky Lab software after it was deemed to be a potential access route for Russian hacking, and now it is requiring better supply chain management practices. The size of government procurements can drive more responsible supplier behaviors. If Rosatom wants to compete against other potential nuclear suppliers, it must show it not only will abide by good standards for procurement and performance, but that it also wants to help develop them.

Countries as well as industries should learn from each other. A forthcoming rule from the US Federal Electric Regulatory Commission includes better supply chain risk management practices. A cross-industry voluntary consensus standard could be developed from this rule, which could seek a broader US SAFETY Act designation. Those complying with the standard would gain liability protections. Countries still working to develop appropriate regulations should take note – as everyone must worry about the other guy.

The warning lights "are blinking red again," Direct of National Intelligence Dan Coats said recently. "Today, the digital infrastructure that serves this country is literally under attack. Every day, foreign actors — the worst offenders being Russia, China, Iran and North Korea — are penetrating our digital infrastructure and conducting a range of cyber intrusions and attacks against targets in the US."

But, so far, those attacks have been manageable. One reason is that Russia is in surveillance mode and hasn't pushed the button — *yet*. No doubt the US could retaliate. Establishing discussions in a cyber area of mutual interest and potential benefit could perhaps lead to broader discussions about good state behavior in cyber space and help everyone move toward much needed international cyber norms.