

U.S. risking cybergeddon with Russia

One coordinated cyberattack could shut down 80% of U.S. electrical grid

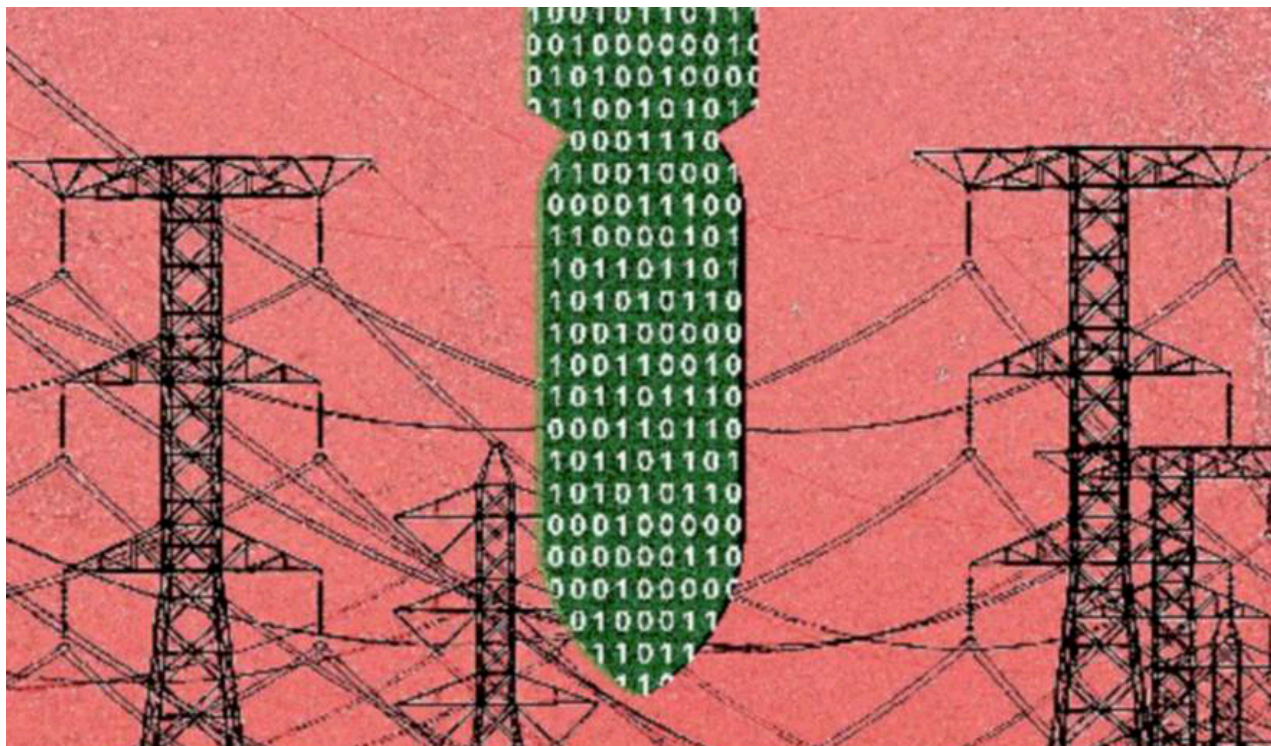


Illustration on the electrical grid and cyberattacks by Linas Garsys/The Washington Times [more >](#)

By Peter Vincent Pry - - Tuesday, January 18, 2022

OPINION:

"Fools rush in where even angels fear to tread."

— Alexander Pope (1711)

"Be afraid and expect the worst" is Russia's cyber-warning to Ukraine, flashed to Ukrainian government websites on Thursday, Jan. 13, just hours after U.S. and NATO meetings with Russian officials failed to resolve an escalating international crisis that could become World War III.

Russia is postured to invade Ukraine and could overrun NATO's frontline states in eastern Europe in 72 hours. Simultaneously, China is postured to annex Taiwan and the South China Sea. On Jan. 9, with China's approval and support, Russian troops poured into mineral-rich Kazakhstan, like Ukraine, formerly part of the Soviet Union, in an alleged "peacekeeping mission."

Now and over the past year, both Russia and China have been hurling nuclear threats.

Foolishly, the Biden administration has been publicly threatening to retaliate for aggression against Ukraine by Cyber Warfare. Foolishly, on Friday, Jan. 14, in what should have been a covert operation, the Biden administration and NATO instead publicly announced they are sending cyber warriors to assist Ukraine.

Washington and the West still do not understand that cyber warfare is an existential threat that could explode the world powder keg, with catastrophic consequences.

In April 2021, Russia massed troops on Ukraine's border, threatening invasion, raising alarms in the U.S. and NATO. Ventriloquizing for the Kremlin, Putin intimate and director of Russia's state-run international media giants, RT and Sputnik, Margarita Simonyan, declared on TV: "Russia will invade Ukraine, sparking a conflict with the U.S. that will force entire cities into blackout. ... All-out cyber warfare, nationwide forced blackouts."

"War is inevitable," according to Russia's Ms. Simonyan, "I do not believe that this will be a large-scale hot war, like World War II, and I do not believe there will be a long Cold War. It will be a war of the third type: the Cyber War."

Russia's Ms. Simonyan: "In conventional war, we could defeat Ukraine in two days. But it will be another kind of war. We'll do it, and then [the U.S.] will respond by turning off power to [a major Russian city like] Voronezh."

She also stated: "Russia needs to be ready for this war, which is unavoidable, and of course, it will start in Ukraine." Continuing, "Russia is "invincible where conventional war is concerned, but forget about conventional war ... it will be a war of infrastructures."

Adding: "I've been agitating and even demanding that we take Donbas [eastern Ukraine]. We need to patch up our vulnerabilities as fast as we can, and then we can do whatever we want."

"We only lose if we do nothing," agreed Russian TV interviewer Vladimir Soloviev. He argued that "by absorbing parts of Ukraine — or the entire country — Russia would be able to remove the zone of American influence further from its borders."

Cyber warfare expert Edward M. Roche, in "Cyber-Attacking Electric Power Grids: A New Strategic Weapon" ("Blackout Warfare: Attacking the U.S. Electric Power Grid A Revolution in Military Affairs," 2021), warns that America is far more vulnerable and less prepared than Russia and China:

- "Russia is capable of launching a major attack that would shut down in one coordinated attack at least 80% of America's electrical grid";
- "Russia has likely experimented with placement of cyber logic-bombs in portions of America's electrical grid";

- “Russia is more capable than other countries in placement of assets (human agents) into critical parts of the management structure of the American electrical grid”;
- “During an extreme international crisis, a massive Russian cyber-attack against the entire U.S. electric grid prior to the outbreak of conventional or nuclear war is likely, to deter or defeat the U.S. with ‘gray-zone aggression’ instead of or prior to outbreak of a ‘real shooting war’ consistent with Russian military doctrine that Cyber Warfare is an unprecedented and decisive Revolution in Military Affairs”;
- “Russia’s response to a major cyber-attack made by the United States is likely to be at least proportional but more likely disproportional and massive, possibly even resulting in Russian nuclear retaliation as threatened in their military doctrine.”

Mr. Roche also warns that “In cyber, China Is A Mortal Threat To The United States ... China has the capability to disable all or at least very large parts of the electrical grid (Eastern, Western, Texas Grid Interconnects) as well as target specific areas, such as power in a single metropolitan area.”

“For U.S. relations with both nations, Russia and China, the emergence of viable paths to cyber-attacks against critical infrastructure as a new strategic weapon has lowered the barriers to conflict and presents a heightened danger with the potential to disrupt the long-standing balancing calculus dependent upon nuclear deterrence.”

Proving Mr. Roche prophetic, a member of the Russian Duma, equivalent to the U.S. Congress, proposes launching a hypersonic nuclear warhead to detonate in the Nevada desert nuclear test area, to demonstrate Ukraine entering NATO would start a nuclear war.

The U.S. is fast running out of time to harden its electric grid against cyber warfare and EMP.

When will President Biden learn that “climate change” and Trump voters are not the greatest threats to America?

• *Peter Vincent Pry is executive director of the EMP Task Force on National and Homeland Security, served as chief of staff of the Congressional EMP Commission, as director of the U.S. Nuclear Strategy Forum and on the staffs of the House Armed Services Committee and the CIA. He is author of “Blackout Warfare” (2021) and “The Power And The Light” (2020).*

Copyright © 2022 The Washington Times, LLC. [Click here for reprint permission.](#)

Please read our [comment policy](#) before commenting.

Advertisement

