WASHINGTON TIMES:
Lessons of the China-India Blackout War

Protecting the Power Grid Illustration by Greg Groesch/The Washington Times more >

By Dr. Peter Vincent Pry - - *Tuesday, March 16, 2021*
ANALYSIS/OPINION:

The future usually arrives before anyone is ready for it, especially in warfare.

China apparently blacked-out Mumbai, India, by cyber-attack — credibly threatening that Beijing could plunge all India into darkness through cyber warfare. Experts warn national electric grids are a technological Achilles heel.

The Mumbai blackout could be one of those "Monitor versus Merrimack" moments in military history when a revolutionary new way of warfare suddenly becomes recognizable, even to the dullest.

New military technologies that can change everything are often laughingly dismissed by establishments too busy planning for "business as usual."

From machine guns at the Somme (1916), panzer divisions in France (1940) and (Japanese) carrier aviation at Pearl Harbor (1941), nations learned the hard way. Obsolete thinking prevails until someone gets hammered, usually by an aggressor.

The Mumbai cyber-blackout, like Russia's annual cyber-blackouts of Ukraine, and blackouts in Mexico (2013), Yemen (2014) and Pakistan (2015) caused by terrorist sabotage of electric grids, are a new category of warfare.

These "blackout wars" foreshadow an existential threat that could end our civilization and kill millions of Americans.

Why did Beijing blackout Mumbai?

China and India are fighting over borders in the Himalayas, again. Ever since China swallowed Tibet in 1951, Beijing periodically tries expanding at India's expense.

But today China and India are both nuclear-armed, so fighting is deliberately "restrained" to avoid nuclear escalation.

Both refrain from a "shooting war" with modern weapons for control of the high Himalayas. Instead, their combat uses shovels, clubs and fists, the two nuclear powers fighting, on top of the world, with stone age tactics.

China evidently thinks threatening cyber-blackout of India could settle matters, without escalation to conventional or nuclear conflict. Protracted blackout of India's electric grid would be catastrophic for its economy, population and military capabilities.

Indian officials are understandably alarmed and now regretting that their national electric power grid and other critical infrastructures depend so much upon equipment imported from China — that likely increases their vulnerability.

"Military experts in India have renewed calls for the government of Prime Minister Narendra Modi to replace China-made hardware for India's power sector and its critical rail system," reports The New York Times in "China Appears To Warn India: Push Too Hard And The Lights Could Go Out" (Feb. 28, 2021).

The New York Times describes technical details of China's blackout war against India. But conspicuous by its absence is any mention of President Biden's suspension of President Trump's Executive Order 13920, "Securing the United States Bulk-Power System" (May 1, 2020), designed to reduce dependency on foreign-supplied equipment for the U.S. electric power grid, especially equipment from China.

Reportedly there are some 300 high-voltage transformers in the U.S. electric power grid manufactured in China. Moreover, the U.S. national grid depends upon an as yet unknown number of China-supplied control systems, called SCADAs, probably numbering in the thousands.

These China-supplied systems, critically important to the operation of the U.S. electric grid, could have built-in vulnerabilities to cyber-bugs and electromagnetic pulse (EMP). China's

version of cyber warfare includes attack by nuclear and non-nuclear EMP weapons (See my report "China: EMP Threat" June 10, 2020).

Mr. Biden would be wise to strengthen and reinstate Executive Order 13920. Electricity is foundational to U.S. national security.

Critical equipment necessary to the operation of the national power grid — that sustains the economy, military, and population — should be made in America.

The Biden administration deserves great credit for continuing implementation of the White House "Executive Order on Coordinating National Resilience to Electromagnetic Pulses" (March 26, 2019), designed to implement recommendations of the Congressional EMP Commission. One strategy for achieving resilience of electric grids and other critical infrastructures is to require through national manufacturing standards that transformers, SCADAs, and other vital equipment incorporate EMP and cyber-protection.

Most electric equipment is already manufactured resistant to lightning, a form of natural EMP. Standards could be upgraded to protect against "super-lightning" from EMP weapons.

Defense Department experience over 50 years manufacturing military equipment with nuclear EMP protection "baked-in" the original design increases costs only 1% to 6%.

Mr. Biden and the new White House "cyber-security czar" should compel electric utilities to protect themselves from cyber-attack and EMP. Hundreds are dead from California wildfires and a Texas ice storm because FERC and NERC failed to make utilities undertake simple preparedness for severe weather. They cannot be trusted to protect against cyber-attacks and EMP.

Utility lobbyists advocate retaliatory cyber-attacks by the U.S. government for "deterrence" instead of protecting electric grids.

Retaliatory cyber warfare cannot substitute for hardening critical infrastructures against cyber-attack and EMP — and is very risky. The U.S. is far more vulnerable than its adversaries. Russia and China make frequent cyber-attacks on the U.S. because they know we are vulnerable, and know they can hit back harder.

Moreover, Beijing apparently thinks blacking out India's national electric grid is less escalatory than a "shooting war" in the Himalayas. In 2020, China's strategists threatened EMP attack on the U.S. Navy in the South China Sea, as one of their "less escalatory" options.

Cyber warfare between nuclear-armed powers is not a good idea, for either side. 2021 could too easily become a nuclear version of 1914.

•Dr. Peter Vincent Pry, director of the Task Force on National and Homeland Security, served as chief of staff on the Congressional EMP Commission, and on the staffs of the House Armed

Service Committee and the CIA. He is author most recently of "The Power And The Light" (Amazon.com).
https://www.washingtontimes.com/news/2021/mar/16/lessons-of-the-china-india-blackout-war/