Blacking Out Civilization With Robotic Terrorism

(Colicaranica/Dreamstime.com)

By Dr. Peter Vincent Pry Wednesday, 10 November 2021

My new book "Blackout Warfare" warns that drones or unmanned aerial vehicles (UAVs) can be used to black out national power grids.

Now, according to an FBI and DHS memo recently reported in the press, in July 2020 a drone made a failed attack on the Pennsylvania electric power grid. The drone, trailing electrical conductors intended to short out high-voltage powerlines at a transformer substation, crashed on a roof before reaching its target.

The perpetrator has not yet been identified.

A similar attack using a small manned airplane blacked out Canada's Hydro-Québec electric grid in 2014. According to The Washington Post:

"Hydro-Quebec, Canada's largest electric utility, was hit with a crippling blackout at the start of the winter. Traffic lights went dark, and more than 188,000 customers lost power, including Montreal's McGill University Health Center. ... Power exports to the Northeast United States were cut. Industrial users were asked to slash production ... " (See "The Power And The Light," 2020.)

Military drones and armed unmanned aerial vehicles are in the process of revolutionizing warfare.

In 2020, for the first time in history, an Air Force of UAVs defeated a traditional army of tanks, soldiers, and manned jets, giving Azerbaijan decisive victory over Armenia in the long inconclusive Nagorno-Karabakh war, waged on and off for over 30 years.

An ongoing technological revolution in non-nuclear electromagnetic pulse (NNEMP) weapons is making these more powerful, more miniaturized and lighter weight, and deliverable by drones or UAVs.

The marriage of NNEMP warheads to UAVs, preprogrammed or equipped with sensors to follow high-power electric lines and to target control centers and transformers, introduces a major new threat to national power grids.

A nonexplosive high-power microwave warhead, for example, can emit repeated bursts of electromagnetic energy to upset and damage electronic targets. Such a warhead, attached to a programmable drone or UAV, could follow the powerlines to attack numerous transformer and control substations, until its energy is exhausted.

Relatively small numbers of NNEMP drones or UAVs — perhaps only one capable of protracted flight — could inflict a long nationwide blackout. As reported in The Wall Street Journal, according to a classified study by the U.S. Federal Energy Regulatory Commission, disabling just 9 of 2,000 U.S. EHV transformer substations could cause cascading failures that would crash the North American power grid.

Thus, NNEMP unmanned aerial vehicles might be able to achieve results similar to a nuclear EMP attack in blacking out power grids, though the NNEMP attack would probably take hours instead of seconds.

The technology for non-nuclear EMP generators and drones is widely available for purchase as civilian equipment which can easily be weaponized, even by non-state actors.

For example, one U.S. company sells a NNEMP device for legitimate industrial purposes called the EMP Suitcase that looks like a suitcase,

can be carried and operated by one person, generates 100,000 volts/meter over a short distance, and can be purchased by anyone. NNEMP devices like the EMP Suitcase could become the Dollar Store version of weapons of mass destruction if turned against the national electric grid by terrorists.

A German version of the "EMP Suitcase" weighs only 62 pounds, easily deliverable by drone or UAV.

In 2020, Northeastern University's Global Resilience Institute (GRI) tested in an EMP simulator numerous electronic components vital to the operation of electric grids and other critical infrastructures. The GRI tests "confirmed the ability for non-state actors to outfit commercially-available platforms to conduct localized tactical EMI attacks against electronics that support critical systems ... identified the thresholds at which the functioning of representative electronics in common use across multiple infrastructures could become compromised, generating catastrophic outcomes.

"This includes, but is not limited to, disruption in cybersecurity safeguards for critical infrastructure to include key components of the electric power grid and telecommunications system."

GRI's tests of the non-nuclear EMP threat "confirm that a small EMI emitter that could be carried on a commercially-available drone or terrestrial vehicle, is capable of compromising electronic components, in common commercial use, at very low-energy levels from a considerable distance."

Most NNEMP generators have limited range, less than 10 kilometers. But if mated to a cruise missile or drone capable of protracted flight to target electric grid key nodes, the results can be spectacular.

For example, Boeing's Counter-Electronics High Power Microwave Advanced Missile Project (CHAMP) cruise missile can be viewed on the internet where CHAMP "navigated a pre-programmed flight plan and emitted bursts of high-powered energy, effectively knocking out the target's data and electronic subsystems." The U.S. Air Force has purchased CHAMP cruise missiles, deployed to Japan, reportedly to prevent North Korean missile attacks by "frying" their missiles, command and control, and power grid electronics.

Russia may still be the world leader in NNEMP weapons, as was the USSR during the Cold War. Russia's nuclear-powered cruise missile, the Burevestnik (Storm Petrel, NATO designation SSC-X-9 Skyfall), now under development, makes little sense as yet another missile to deliver nuclear warheads, as advertised by Moscow.

The Storm Petrel's engines, powered by a nuclear reactor, theoretically will give it unlimited range and limitless flying time for crossing oceans and cruising over the U.S. The Storm Petrel could be a nuclear-powered version of CHAMP, able to fly much farther and longer and armed with a more potent NNEMP warhead, electrically supercharged by the nuclear reactor.

Iran has demonstrated sophisticated UAVs and drones, using over 20 to make highly precise and coordinated attacks on Saudi Arabia's oil processing facilities on September 14, 2019. Such delivery vehicles

could easily be armed with NNEMP warheads to make a less sophisticated version of CHAMP.

Iran is the world's leading sponsor of international terrorism, and Iran's Islamic Revolutionary Guard is the world's most powerful and sophisticated terrorist organization. The advent of Blackout Terrorism by UAV is inevitable.

The technological revolution in NNEMP weapons and UAVs threatens to become an electromagnetic Pearl Harbor for nations, like the United States, that fail to fully comprehend the threat and have not protected civilian critical infrastructures and military systems.

President Joe Biden's infrastructure bill spending trillions to "build back better" the nation's critical infrastructures proposes spending millions for more EMP protection studies. Someday, perhaps soon, the infrastructure bill will prove to be a tragic missed opportunity.

What is needed is not more studies, but a crash program to protect the U.S. electric grid, and 320 million Americans, from the looming existential threat that is Blackout Warfare.

Dr. Peter Vincent Pry is executive director of the Task Force on National and Homeland Security.

https://www.newsmax.com/peterpry/military-drones-unmanned-aerial-vehicles-blackout-electromagnetic/2021/11/10/id/1044106/>