BLACKOUT WARFARE

Non-Nuclear Electromagnetic Pulse (NNEMP) Attack On The U.S. Electric Power Grid

Dr. Peter Vincent Pry
Executive Director
EMP Task Force on National and Homeland Security
June 20, 2021

TABLE OF CONTENTS

KEY JUDGMENTS

Non-Nuclear Electromagnetic Pulse (NNEMP) weapons, more commonly known as Radio-Frequency Weapons, are non-nuclear weapons that use a variety of means, including explosively driven generators or high-power microwaves, to emit an electromagnetic pulse similar to the E1 HEMP from a nuclear weapon, except less energetic and of much shorter radius.

Unlike the nuclear HEMP threat, NNEMP weapons are much more readily available to and easily exploitable by terrorists and the least sophisticated state actors. NNEMP weapons can be built relatively inexpensively using commercially available parts and design information available on the internet.

EMP simulators that can be carried and operated by one man, and used as an NNEMP weapon, are available commercially.

Even random attacks using NNEMP weapons against less than 100 EHV transformer control substations located in all three U.S. grid systems—Eastern, Western, and Texas—would probably suffice to inflict a protracted nationwide blackout.

Special mention must be made of the ongoing technological revolution in Non-Nuclear EMP weapons, which are becoming more powerful, more miniaturized and lighter-weight, and deliverable by cruise missiles or drones. The marriage of NNEMP warheads to drones or cruise missiles, 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.

Dozens of nations reportedly have NNEMP weapons or are developing them. Some of these are Russia, China, North Korea, Iran, Pakistan, India, Israel, Germany, the United Kingdom, France, Australia, and Switzerland.

Non-Nuclear EMP weapons, as a cutting-edge military technology, are being developed largely clandestinely, with relatively little detailed open source reporting on specific national programs, let alone on what terrorists may be doing.

Relatively small numbers of NNEMP cruise missiles or drones—perhaps only one capable of protracted flight—could inflict a long nationwide blackout.

20 NNEMP trucks could damage 580 EHV transformer substations in 24 hours, 430 substations in the East, 120 substations in the West, 30 substations in Texas—29% of all substations nationwide. The “army” manning 20 NNEMP trucks would number just 40 men.

U.S. military power projection capabilities would be severely crippled or altogether paralyzed by a protracted nationwide blackout. CONUS military bases depend upon the civilian electric grid for 99% of their electric power.

BLACKOUT WARFARE
Non-Nuclear Electromagnetic Pulse (NNEMP) Attack
On The U.S. Electric Power Grid

BACKGROUND

Non-Nuclear Electromagnetic Pulse (NNEMP) weapons, more commonly known as Radio-Frequency Weapons, are non-nuclear weapons that use a variety of means, including explosively driven generators or high-power microwaves, to emit an electromagnetic pulse similar to the E1 HEMP from a nuclear weapon, except less energetic and of much shorter radius. The range of NNEMP weapons is rarely more than ten kilometers.[1]

International scientific and electronic engineering organizations describe the NNEMP threat as "Electro-Magnetic (EM) Terrorism" and, less dramatically, as "Intentional Electro-Magnetic Interference" (IEMI).[2] Non-Nuclear Electromagnetic Pulse (NNEMP) weapons is the term used here to emphasize that the NNEMP threat has significant similarities to nuclear HEMP, similar technical solutions, and poses a much greater threat than implied by the word "Interference" in IEMI.

"There is enormous diversity in possible electromagnetic weapon designs, for both large scale and highly focused attacks, both against civil and military targets," according to Dr. Carlo Kopp, one of the world's leading experts on NNEMP weapons, "There are many possible taxonomical divisions for electromagnetic weapons":

--"Directed Energy Weapons vs. 'one shot' E-Bombs;"
--"Nuclear (HEMP) E-Bombs vs. Non-nuclear E-Bombs;"
--"Narrow Band Weapons vs. Wideband or UWB [Ultra-Wide Band] weapons;"
--"High Power Microwave vs. 'Low Band' weapons;"
--"Persistent Area Denial (AD) weapons vs. Non-Persistent weapons;"
--"Explosively pumped vs. Electrically pumped weapons."[3]

Unlike the nuclear HEMP threat, NNEMP weapons are much more readily available to and easily exploitable by terrorists and the least sophisticated state actors.

---

[1] U.S. FERC Interagency Report, Wiliam Radasky and Edward Savage, *Intentional Electromagnetic Interference (IEMI) and Its Impact on the U.S. Power Grid* (Meta-R-323) Metatech Corporation (January 2010). Carlo Kopp, *The Electromagnetic Bomb—A Weapon of Electrical Mass Destruction* (Melbourne, Australia). Jerry Emanuelson, "Non-nuclear Electromagnetic Pulse Generators" www.futurescience.com. Tom Harris, "How E-Bombs Work" www.science.howstuffworks.com.

[2] Ibid, U.S. FERC Interagency Report, pp. 1-2. R.L. Gardner, "Electromagnetic Terrorism: A Real Danger" Proceedings of the XIth Symposium on Electromagnetic Compatibility" (Wroclaw, Poland: June 1998).

[3] Dr. Carlo Kopp, "E-Bombs vs. Pervasive Infrastructure Vulnerability" Briefing, Pacific Theater Air, Sea, Land Battle Concept: IO/EW/Cyber Operations International Conference (Monash University/Air Power Australia) carlo.kopp@monash.edu.

NNEMP weapons can be built relatively inexpensively using commercially available parts and design information available on the internet. In 2000, the Terrorism Panel of the House Armed Services Committee conducted an experiment, hiring an electrical engineer and some students to try building an NNEMP weapon on a modest budget, using design information available on the internet, made from parts purchased commercially, available to anyone.[4]

They built two NNEMP weapons in one year, both successfully tested at the U.S. Army proving grounds at Aberdeen. One was built into a Volkswagen bus, designed to be driven down Wall Street to disrupt stock market computers and information systems and bring on a financial crisis. The other was designed to fit in the crate for a Xerox machine so it could be shipped to the Pentagon, sit in the mailroom, and burn-out Defense Department computers.[5]

EMP simulators that can be carried and operated by one man, and used as an NNEMP weapon, are available commercially.

For example, one U.S. company advertises for sale an "EMP Suitcase" that looks exactly like a metal suitcase, can be carried and operated by one man, and generates 100,000 volts/meter over a short distance. The EMP Suitcase is not intended to be used as a weapon, but as an aid for designing factories that use heavy duty electronic equipment that emit electromagnetic transients, so the factory does not self-destruct.[6]

But a terrorist or criminal armed with the "EMP Suitcase" could potentially destroy electric grid SCADAs, possibly shutdown transformers, and blackout a city. Thanks to NNEMP weapons, we have arrived at a place where the technological pillars of civilization for a major metropolitan area could be toppled by a single madman.

The "EMP Suitcase" can be purchased without a license by anyone.

According to the Wall Street Journal, a classified study by the U.S. Federal Energy Regulatory Commission found that damaging as few as 9 out of 2,000 EHV transformers could trigger cascading failures, causing a protracted nationwide blackout of the United States.[7] Terrorists armed with NNEMP weapons might use unclassified computer models to duplicate the reported U.S. FERC study and figure out which nine crucial transformer substations need to be attacked in order to blackout the entire national grid for weeks or months.

---

[4] Kenneth R. Timmerman, "U.S. Threatened With EMP Attack" ktimmerman@InsightMagazine.com and EMPwar.com U.S. Congress, "Radio Frequency Weapons and Proliferation: Potential Impact on the Economy" Hearing before the Special Oversight Panel on Terrorism, House Armed Services Committee (February 25, 1998) www.house.gov/jec/hearings/02-25-8h.htm.

[5] Ibid.

[6] Applied Physics Electronics, "High-Power RF Suitcase EMP Pulse Generator" www.apelc.com/rf-suitcase. Dr. Peter Vincent Pry, *Electric Armageddon* (EMP Task Force on National and Homeland Security, 2013) p. 13.

[7] Rebecca Smith, "U.S. Risks National Blackout From Small-Scale Attack" Wall Street Journal (March 12, 2014).

Big blackouts in the U.S., including the Great Northeast Blackout of 2003 that put 50 million people in the dark, caused by a tree branch, and the 2021 Texas blackout, caused by an ice storm, highlight the fragility of the national power grid. Malevolent actors are surely cognizant of this fragility.

Even random attacks using NNEMP weapons against less than 100 EHV transformer control substations located in all three U.S. grid systems—Eastern, Western, and Texas—would probably suffice to inflict a protracted nationwide blackout.

NNEMP weapons could offer significant operational advantages over assault rifles and bombs. Something like the "EMP Suitcase" could be put in the trunk of a car, parked and left outside the fence of an EHV transformer or SCADA colony, or hidden in nearby brush or a garbage can, while the bad guys make a leisurely getaway. Or a single NNEMP weapon could be driven from one transformer substation to another (the substations are unguarded) to knock-out enough SCADAs and transformers to cause a regional or even national protracted blackout.

If the EMP fields are strong enough, an NNEMP weapon could be more effective, and far less conspicuous, than using explosives or small arms to attack transformers and controls at substations. Since all electronics within the field of the NNEMP could be damaged, precision targeting would be unnecessary, as is the case for firearms and explosives. Unlike firearms and explosive munitions, damage inflicted by NNEMP weapons might be mistaken as a freak accident or unusual systemic failure.

Some documented examples of successful attacks using NNEMP weapons, and accidents involving electromagnetic transients, are described by the Department of Defense:

--"In the Netherlands, an individual disrupted a local bank's computer network because he was turned down for a loan. He constructed a Radio Frequency Weapon the size of a briefcase, which he learned how to build from the Internet. Bank officials did not even realize that they had been attacked or what had happened until long after the event."
--"In St. Petersburg, Russia, a criminal robbed a jewelry store by defeating the alarm system with a repetitive RF generator. Its manufacture was no more complicated than assembling a home microwave oven."
--"In Kyzlyar, Dagestan, Russia, Chechen rebel commander Salman Raduyev disabled police radio communications using RF transmitters during a raid."
--"In Russia, Chechen rebels used a Radio Frequency Weapon to defeat a Russian security system and gain access to a controlled area."
--"Radio Frequency Weapons were used in separate incidents against the U.S. Embassy in Moscow to falsely set off alarms and to induce a fire in a sensitive area."
--"March 21-26, 2001, there was a mass failure of keyless remote entry devices on thousands of vehicles in the Bremerton, Washington, area...The failures ended abruptly as federal investigators had nearly isolated the source. The Federal Communications Commission (FCC) concluded that a U.S. Navy presence in the area probably caused the incident, although the Navy disagreed."

--"In 1999, a Robinson R-44 news helicopter nearly crashed when it flew by a high frequency broadcast antenna."
--"In the late 1980s, a large explosion occurred at a 36-inch diameter natural gas pipeline in the Netherlands. A SCADA system, located about one mile from the naval port of Den Helder, was affected by a naval radar. The RF energy from the radar caused the SCADA system to open and close a large gas flow-control valve at the radar scan frequency, resulting in pressure waves that traveled down the pipe and eventually caused the pipeline to explode."
--"In June 1999 in Bellingham, Washington, RF energy from a radar induced a SCADA malfunction that caused a gas pipeline to rupture and explode."
--"In 1967, the USS Forrestal was located at Yankee Station off Vietnam. An A4 Skyhawk launched a Zuni rocket across the deck. The subsequent fire took 13 hours to extinguish. 134 people died in the worst U.S. Navy accident since World War II. EMI [ElectroMagnetic Interference] was identified as the probable cause of the Zuni launch."[8]

North Korea used an NNEMP "cannon" purchased from Russia to attack airliners and impose an "electromagnetic blockade" on air traffic to Seoul, South Korea's capitol. The repeated attacks by NNEMP also disrupted communications and the operation of automobiles in several South Korean cities in December 2010; March 9, 2011; and April-May 2012.[9]

In July 2019, the USS Boxer downed an Iranian drone using a powerful new jammer, in the latest demonstration that the United States has incorporated Non-Nuclear EMP weapons into its armed forces.[10]

In 2019, the U.S. Air Force deployed at least 20 CHAMP cruise missiles, armed with NNEMP warheads, advertised as being capable of paralyzing North Korean or Iranian missiles and their military command, control, and communications: "The U.S. Air Force has deployed at least 20 missiles that could zap the military electronics of North Korea or Iran with high-power microwaves, rendering their military capabilities useless without causing any fatalities. Known as the Counter-electronics High Power Microwave Advanced Missile Project (CHAMP), the missiles were built by Boeing's Phantom Works for the U.S. Air Force Research Laboratory and tested successfully in 2012. They have not been operational until now."[11]

Since the Department of Defense clearly recognizes the utility of NNEMP weapons for offensive operations—and given the history of use of NNEMP weapons by criminals, terrorists, and North Korea—continued failure by the Department of Homeland Security to assign high priority to national EMP preparedness is inexplicable and intolerable.

---

[8] Department of Defense, *Pocket Guide for Security Procedures and Protocols for Mitigating Radio Frequency Threats* (Technical Support Working Group, Directed Energy Technical Office, Dahlgren Naval Surface Warfare Center).
[9] "Massive GPS Jamming Attack By North Korea" www.gpsworld.com (May 8, 2012).
[10] Ben Watson, "New U.S. Jammer Downs Alleged Iranian Drone in Gulf" Defense One (July 19, 2019).
[11] Ron Kessler "USAF Deploys New Champ Missile" (May 17, 2019) www.neogaf.com/threats/usaf-deploys-new-champ-missile. See also Dave Majumdar, "CHAMP: America's EMP Missile that Might Be Able to Fry North Korea's Nukes" National Interest (December 11, 2017).

NNEMP Technological Revolution

Special mention must be made of the ongoing technological revolution in Non-Nuclear EMP weapons, which are becoming more powerful, more miniaturized and lighter-weight, and deliverable by cruise missiles or drones. The marriage of NNEMP warheads to drones or cruise missiles, 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.[12]

A non-explosive 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 cruise missile, could follow the powerlines to attack numerous transformer and control substations, until its energy is exhausted.

Relatively small numbers of NNEMP cruise missiles or drones—perhaps only one capable of protracted flight—could inflict a long nationwide blackout. Reportedly, as noted earlier, 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.[13]

The "Cascade Failure" problem, warns Dr. Carlo Kopp, makes modern digital societies highly vulnerable to NNEMP attack: "Digital infrastructure is highly interconnected and thus interdependent." Because of: "Common reliance on power grid, telecommunications cabled and wireless connections, local and remote servers, single and multiple site Clouds and Grids," consequently, "A mass destruction effect in one geographical area can cause cascading failures as interdependent systems fail…*Damage effects are thus no longer localized in extant, e.g. destroying a server or Cloud in Washington DC may cripple dependent systems globally."*[14]

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

"The technology used in conventional E-Bombs is within reach of any nation capable of designing nuclear weapons and high power radars—e.g. China, Iran, DPRK, Russia," according to NNEMP expert Dr. Kopp:

--"OSINT source material very scarce on E-Bomb technology and designs, effort is usually well hidden from scrutiny;"
--"Potentially large area footprints of many square miles for GigaWatt class weapons, with the usual lethality prediction caveats—targets not tested may be unexpectedly resistant or susceptible at specific weapon frequencies/polarisations;"

---

[12] Carlo Kopp, *The Electromagnetic Bomb – A Weapon of Electrical Mass Destruction* (February 8, 2003). Though dated, Kopp is still among the best for background.
[13] Rebecca Smith, "U.S. Risks National Blackout From Small-Scale Attack" Wall Street Journal (March 12, 2014).
[14] Emphasis original in Dr. Carlo Kopp, "E-Bombs vs. Pervasive Infrastructure Vulnerability" Briefing, Pacific Theater Air, Sea, Land Battle Concept: IO/EW/Cyber Operations International Conference (Monash University/Air Power Australia) carlo.kopp@monash.edu.

--"Terrorist attacks predicated on the availability of proven designs or inventory of E-Bomb munitions—emerging risk;"
--*"The high payoff in using E-Bombs as disruptive or area suppression weapons points to common use in future nation state conflicts involving developed nations."*[15]

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.

As noted earlier, 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.[16] A German version of the "EMP Suitcase" weighs only 62 pounds, easily deliverable by a drone or cruise missile.[17]

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."[18]

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."[19]

Most NNEMP generators have limited range, less than 10 kilometers.[20] 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."[21] The U.S. Air Force has purchased CHAMP cruise

---

[15] Ibid, emphasis original.
[16] Applied Physics Electronics, "High-Power RF Suitcase EMP Pulse Generator" www.apelc.com/rf-suitcase.
[17] U.S. FERC Interagency Report, Wiliam Radasky and Edward Savage, *Intentional Electromagnetic Interference (IEMI) and Its Impact on the U.S. Power Grid* (Meta-R-323) Metatech Corporation (January 2010) p. 2-5.
[18] Global Research Institute Northeastern University, *Mobilizing a National Response to the Vulnerability of Critical Infrastructure to Non-nuclear Electromagnetic Pulse/Electromagnetic Interference Attacks* (April 2020) p. 4.
[19] Ibid.
[20] "Range of Russian EMP Weapons Increased to 10 km" Russia Today Military News TASS (July 5, 2020).
[21] "Boeing: CHAMP – Lights Out" www.boeing.com.

missiles, deployed to Japan, reportedly to prevent North Korean missile attacks by "frying" their missiles, command and control, and power grid electronics.[22]

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.[23]

Iran has demonstrated sophisticated cruise missiles and drones, using over 20 to make highly precise and coordinated attacks on Saudi Arabia's oil processing facilities on September 14, 2019.[24] Such delivery vehicles could easily be armed with NNEMP warheads, to make a less sophisticated version of CHAMP.

India's Institute for Defence Studies and Analysis worries about being attacked with NNEMP weapons anonymously to defeat deterrence, but also sees possession of such weapons as a possible deterrent:

"EMP weapons could also be used clandestinely to take out important targets during peace time, when the use of conventional weapons would be considered outrageous, as it will be difficult to prove who exactly was responsible. Such incapacitating applications of EMP could also prove to be an effective deterrent against enemies contemplating military action."[25]

India's IDSA recommends: "Looking at the gross asymmetrical advantage it provides against adversaries, India should actively consider developing an offensive NNEMP capability."[26]

Dozens of nations reportedly have NNEMP weapons or are developing them. Some of these are Russia, China, North Korea, Iran, Pakistan, India, Israel, Germany, the United Kingdom, France, Australia, and Switzerland. Ukraine's Yuri Tkasch, Director of the Kharkov Institute of

[22] Ron Kessler, "USAF Deploys New CHAMP Missile" (May 17, 2019) www.neogaf.com/threats/usaf-deploys-new-champ-missile. Dave Majumdar, "CHAMP: America's EMP Missile that Might Be Able to Fry North Korea's Nukes" The National Interest (December 11, 2017).
[23] Dr. Peter Vincent Pry, "When Will DC Awaken To Putin's Nuclear Aim For US?" Newsmax (August 21, 2019).
[24] "Arms Seized by U.S., Missiles Used to Attack Saudi Arabia 'of Iranian Origin'" Reuters and New York Times (June 11, 2020).
[25] Group Captain Atul Pant, "EMP Weapons and the New Equation of War" Indian Defence Review (October 16, 2017).
[26] Ibid.

Helical FCG Operation

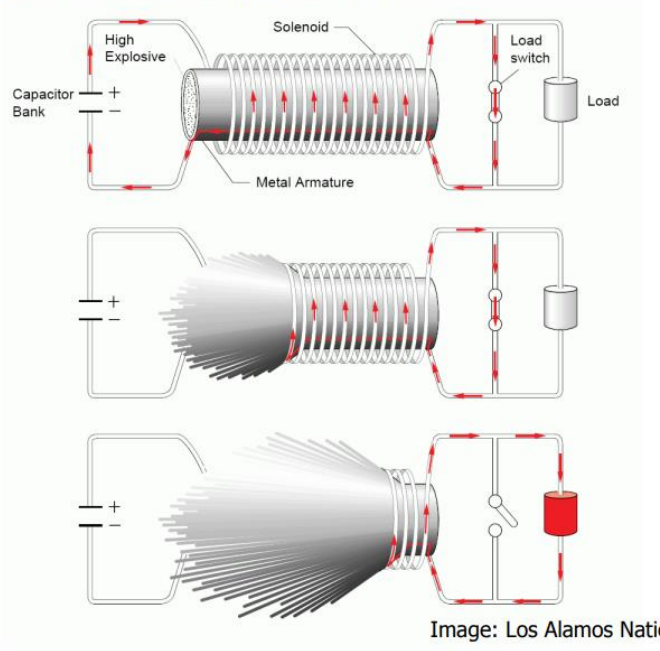


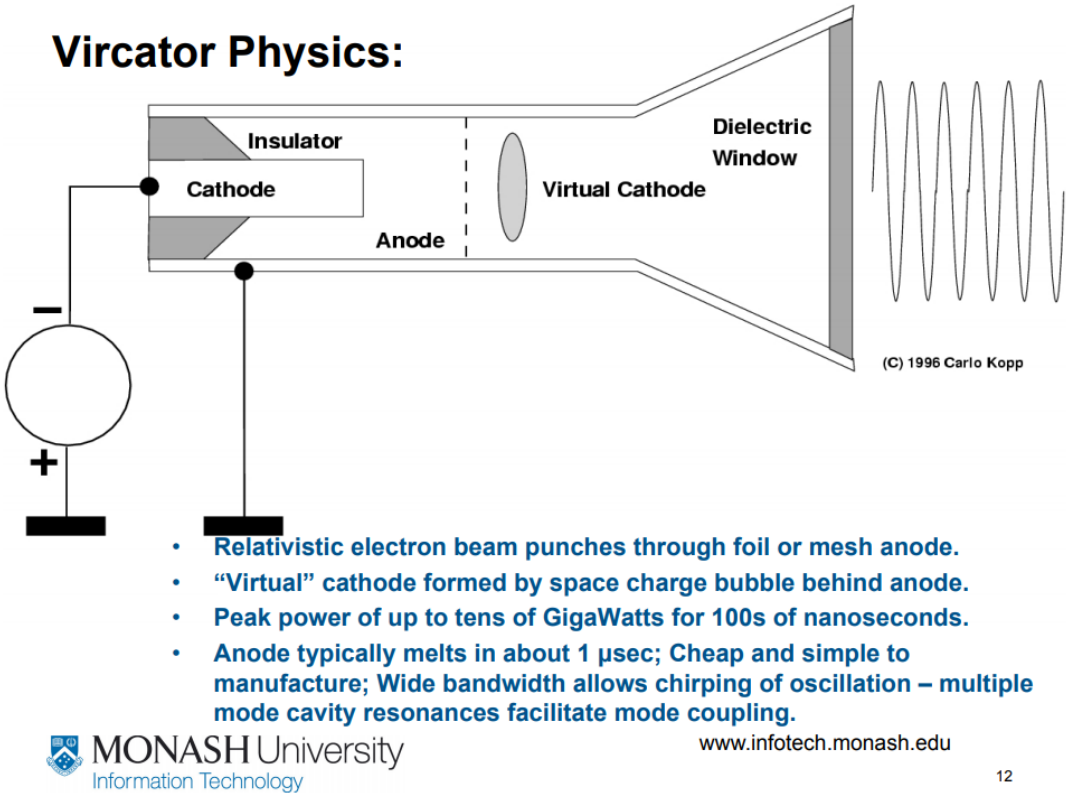
Image: Los Alamos National Laboratory

MONASH University
Information Technology

www.infotech.monash.edu

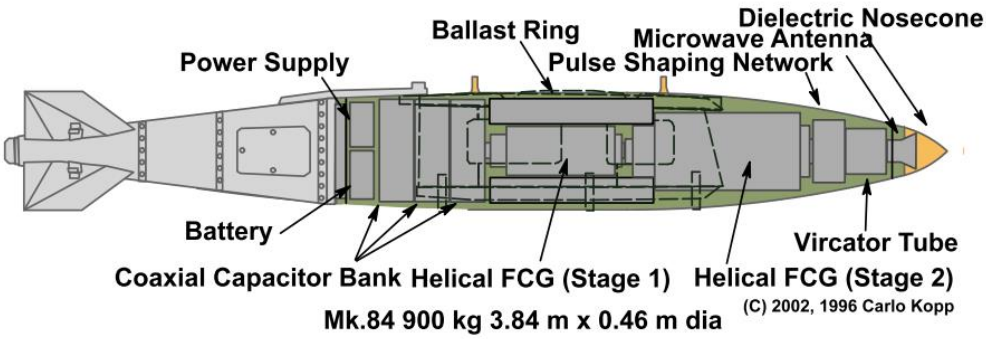
11

Source: Dr. Karlo Kopp, "E-Bombs vs. Pervasive Infrastructure Vulnerability" briefing to Pacific Theater Air, Sea, Land Battle Concept: IO/EW/Cyber Operations International Conference (Monash University, Air Power Australia) Carlo.Kopp@monash.edu.



Source: Dr. Karlo Kopp, "E-Bombs vs. Pervasive Infrastructure Vulnerability" briefing to Pacific Theater Air, Sea, Land Battle Concept: IO/EW/Cyber Operations International Conference (Monash University, Air Power Australia) Carlo.Kopp@monash.edu.

HPM (Microwave) E-Bomb Layout



HIGH POWER MICROWAVE E-BOMB - GENERAL ARRANGMENT MK.84 PACKAGING WARHEAD USING VIRCATOR AND 2 STAGE FLUX COMPRESSION GENERATOR

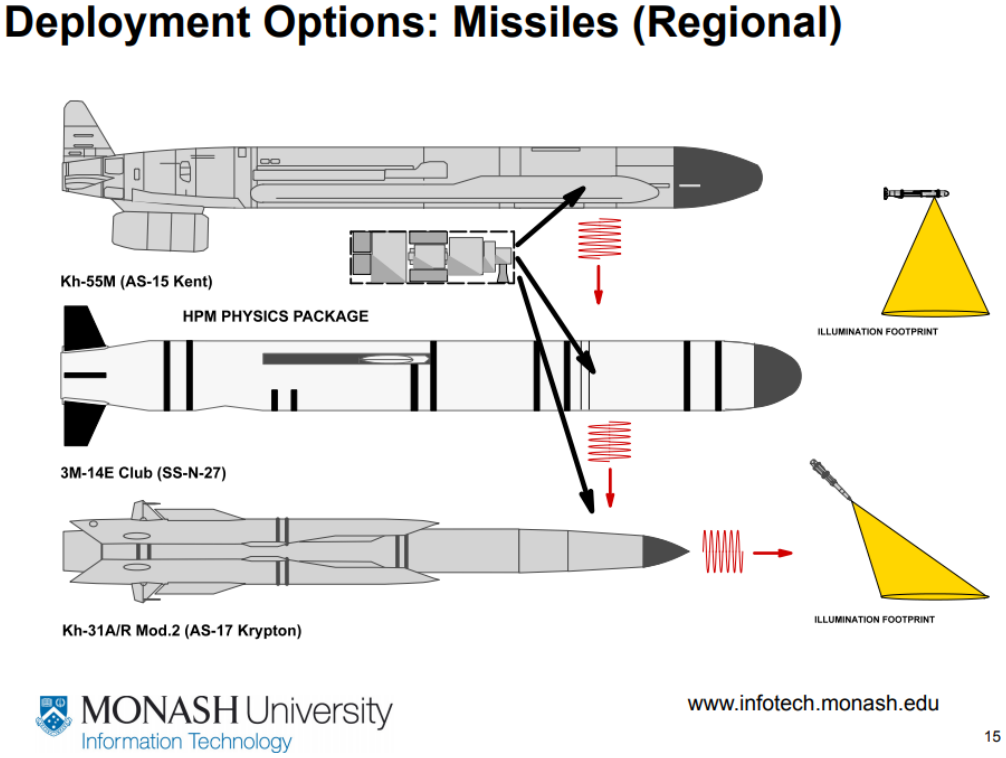
HPM E-BOMB WARHEAD (GBU-31/Mk.84 FORM FACTOR)

MONASH University Information Technology

www.infotech.monash.edu

13

Source: Dr. Karlo Kopp, "E-Bombs vs. Pervasive Infrastructure Vulnerability" briefing to Pacific Theater Air, Sea, Land Battle Concept: IO/EW/Cyber Operations International Conference (Monash University, Air Power Australia) Carlo.Kopp@monash.edu.



Source: Dr. Karlo Kopp, "E-Bombs vs. Pervasive Infrastructure Vulnerability" briefing to Pacific Theater Air, Sea, Land Battle Concept: IO/EW/Cyber Operations International Conference (Monash University, Air Power Australia) Carlo.Kopp@monash.edu.

Electromagnetic Research, which was the leading design bureau for the USSR's NNEMP weapons, is a one-man worldwide proliferator of NNEMP technology to any buyer.[27]

The technological revolution in NNEMP weapons 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.

"Since the term E-Bomb was coined in 1992, the scale of vulnerable infrastructure and systems has multiplied many times over, yet there has been no systematic effort to harden the infrastructure or military systems using COTS [Commercial Off-The Shelf] hardware," warns NNEMP expert Dr. Kopp:

--"Widespread skepticism and disbelief concerning weapon feasibility and infrastructure vulnerability, wholly a result of *technical illiteracy in electromagnetism;"*
--"The notion that a technology which is available and profitable to use in combat would not be used is wishful thinking."
--"*Legislation for electromagnetic hardening of infrastructure and systems for military, dual use and critical civil applications should be introduced immediately.*"[28]

NNEMP: A Clandestine Threat

Non-Nuclear EMP weapons, as a cutting-edge military technology, are being developed largely clandestinely, with relatively little detailed open source reporting on specific national programs, let alone on what terrorists may be doing. So the worldwide status of the NNEMP threat, the power and capabilities of NNEMP weapons in the inventories of state and non-state actors, is largely unknown.

However, the U.S., always more open than most nations, has demonstrated its CHAMP, noted earlier. This NNEMP cruise missile is clearly a threat to electric power grids. CHAMP is well within the technological capabilities of Russia and China. More primitive versions are well within the capabilities of North Korea and Iran.

China, as an example of the clandestine threat, has been working on NNEMP weapons for at least 20 years secretly.

Twenty years ago, the U.S. intelligence community detected China's NNEMP weapons program. According to a previously classified SECRET/NORFORN/XI U.S. defense intelligence report, now declassified, in April 2001: "The Chinese could assemble COTS [Commercial Off-the-shelf Technology] radiofrequency weapons at any time, and may have already done so without our

[27] "Kiev Gave Riyadh Technology To Create Microwave Weapons" en.topwar.ru (23 January 2019).
[28] Emphasis original in Dr. Carlo Kopp, "E-Bombs vs. Pervasive Infrastructure Vulnerability" Briefing, Pacific Theater Air, Sea, Land Battle Concept: IO/EW/Cyber Operations International Conference (Monash University/Air Power Australia) carlo.kopp@monash.edu.

knowledge since it is unlikely that fabrication of such devices would be detected by standard intelligence methods"[29]

Moreover, the U.S. intelligence report assesses that the first NNEMP weapon developed by China will likely be designed to attack critical infrastructures, like electric power grids: "…the first systems functioning as RF [Radio Frequency] weapons that the Chinese have the capability to deploy…could be effective for launching attacks at short range against critical elements of civilian and military infrastructure including electric-power distribution facilities, telecommunications networks and satellite ground terminals."[30]

Furthermore, according to the previously classified U.S. intelligence report, assessing the NNEMP threat from China 20 years ago:

--*"The Chinese are conducting research on high-power RF generation, susceptibility, and propagation that is relevant to the development of RF weapons."*

--*"…the Chinese have written about the use of radiofrequency (RF) weapons for waging information warfare and government officials have been quoted as stating that RF weapons that would defeat the enemy's electronics are among those weapons that China will need in the 21st century."*

--*"Clearly the purpose of the NINT [acronym for China research institute] measurements is to determine the optimum operating parameters for RF weapons designed to upset computers. In the same vein, an earlier paper from the National University of Defense Technology described experiments in which gigawatt HPM [High-Power Microwave] pulses from a VCO were used to induce upset and damage in computer components—a microprocessor, two sets of binary counters, and individual transistors and CMOs."*

--*"The NUDT [National University of Defense Technology] authors state explicitly that their purpose is to gain a better understanding of HPM effects on electronics in order 'to develop high-power microwave weapons and harden our vulnerable components.'"*

--*"The unclassified publications discussed above leave no doubt the Chinese are contemplating the development of RF weapons to defeat computers and electronic mines…for air defense and for antisatellite applications."*

--*[Illustration of a Chinese RF weapon] "concealed inside a truck so that it may be employed clandestinely."*

--*"…there is evidence of Chinese interest [in] a repetitively-pulse RF system deployed in a cruise missile or unmanned aerial vehicle flying at low altitude and that is used to attack ground targets such as air-defense sites and command and control infrastructure."*[31]

[29] Department of Defense, *Assessment of Chinese Radiofrequency Weapon Capabilities* National Ground Intelligence Center, NGIC-1867-0285-01 (April 2001) p. 9.
[30] Ibid.
[31] Ibid, pp. iii, 1, 5, 6, 7-9, 11.

The last quote above indicates that, 20 years ago, China was working toward an NNEMP cruise missile or Unmanned Aerial Vehicle (UAV) resembling the new U.S. CHAMP. China may have eclipsed CHAMP, as it has developed weaponized UAVs capable of evading radar and traveling intercontinental distances, 15,000 miles, from Beijing to Chicago and back, while carrying smart bombs, jamming radars, and conducting electronic warfare.[32]

Russia is proliferating NNEMP weapons technology worldwide, offering their Rosa-E and Ranets-E high-powered microwave "cannons" for sale at international arms shows as long ago as 2001, almost certainly not Russia's most sophisticated NNEMP weapons.[33]

Electric Grid Vulnerability To NNEMP Attack

Perhaps the best unclassified report on the vulnerability of the U.S. electric power grid to NNEMP attack is Metatech's *Intentional Electromagnetic Interference (IEMI) and Its Impact on the U.S. Power Grid* (January 2010). This interagency report, sponsored and coordinated with the U.S. Federal Energy Regulatory Commission (FERC), the Department of Defense and Oak Ridge National Laboratory, is based on comprehensive testing and analysis of SCADAs, PLCs and other electronics vital to electric power grid operations.[34]

The bottom-line is that the U.S. electric power grid is vulnerable, potentially highly vulnerable, to exactly the kind of electromagnetic fields that can be generated by NNEMP attack. Critical electric grid components experience upset and damage when exposed to NNEMP fields of 10,000 volts/meter (10 kilovolts/meter or 10 kV/m) or much less, in many cases less than 1,000 volts/meter (1 kV/m).

The empirical results of *Intentional Electromagnetic Interference (IEMI) and Its Impact on the U.S. Power Grid* deserve quoting at length:

"While this report aims to inform the reader about the threat of IEMI against commercial electronic equipment and systems in general, it is clear that the biggest threat is against the civil infrastructure, as shutting down the control electronics associated with the power grid, the telecom network or other parts of the critical infrastructure could have widespread impacts."[35]

The *IEMI* report notes some examples of accidental electromagnetic transients causing: explosions and fire on a U.S. aircraft carrier that killed 134 sailors, the failure of anti-lock braking (ABS) systems on Germany's autobahn, and a death resulting from electromagnetically induced failure of a monitor and defibrillator in an ambulance, caused by the radio.[36]

---

[32] "China Reveals Chilling New 'Sharp Sword' Stealth Drone" www.mirror.co.uk (19 January 2017). "Losing World War III Inside America's Borders" Washington Times (8 September 2020).

[33] John Keller, "Russia Offers To Develop New Types Of Radio Frequency Weapons—If Buyers Pay For Research" Military and Aerospace Electronics (1 January 2002).

[34] U.S. FERC Interagency Report, Wiliam Radasky and Edward Savage, *Intentional Electromagnetic Interference (IEMI) and Its Impact on the U.S. Power Grid* (Meta-R-323) Metatech Corporation (January 2010).

[35] Ibid, p. 1-2.

[36] Ibid, p. 1-3.

While governments have ignored or been unaware of the threat from NNEMP, the *IEMI* report notes that, more than 20 years ago, in 1999, the International Radio Scientific Union (URSI) passed a "Resolution of Criminal Activities using Electromagnetic Tools" warning of:

--*"The existence of criminal activities using electromagnetic tools and associated phenomenon."*
--*"The fact that criminal activities using electromagnetic tools can be undertaken covertly and anonymously and that physical boundaries such as fences and walls can be penetrated by electromagnetic fields."*
--*"The potentially serious nature of the effects of criminal activities using electromagnetic tools on infrastructure and important functions in society such as transportation, communication, security, and medicine."*
--*"That the possible disruptions of the health and economic activities of nations could have major consequences."*[37]

Some important technical findings from test results and analysis in *Intentional Electromagnetic Interference (IEMI) and Its Impact on the U.S. Power Grid* are that even small electromagnetic generators like the "EMP Suitcase" are a potential threat:

--*"For radiated fields, it seems clear that frequencies above 100 MHz are of primary concern in that they are able to penetrate unshielded or poorly protected buildings very well and yet couple efficiently to the equipment inside of the building. In addition, they have the advantage that antennas designed to radiate efficiently at these frequencies are small."*[38]
--"*With regard to actual threat 'weapons'…Figure 2-6 illustrates a briefcase weapon (mesoband) developed by a German company for anti-terrorist actions."*[39]
--*"…existing briefcase test generators are sufficient to create operational problems, if the facility and its internal equipment are not properly grounded."*[40]
--*"For wideband radiated threat waveforms, buildings can be exposed externally to hyperband waveforms with peak field levels on the order of 10 kV/m. For briefcase devices, the same level of peak field in the hyperband to the mesoband range can be delivered and should be considered."*[41]

The *IEMI* report warns that, while non-nuclear EMP weapons can deliver thousands of volts on target: "The modern civil infrastructure is very dependent on computers, which operate at logic levels of a few volts. So an intentional interference can occur at a few volts in critical circuits, causing logic upset…If one raises the interfering signal to some tens of volts, then one may expect permanent damage to occur in the circuit elements by some type of breakdown, which in turn provides a path for the power supply to insert much more energy than provided initially by the

[37] Ibid, p. 1-4.
[38] Ibid, p. 2-4.
[39] Ibid, p. 2-5.
[40] Ibid, p. 2-8.
[41] Ibid, p. 2-10.

incident waveform."[42] Unprotected systems are vulnerable to "functional upset from radiated fields as low as 30 V/m [30 volts/meter]."[43]

The *IEMI* report notes that testing has proven the vulnerability of a wide range of modern electronic equipment, including: "cash machines, industrial control equipment, power supplies, Ethernet components, WIFI networks, automobiles, GPS electronics, cellular phones, PDAs and different types of sensors." Automobiles experience upset (engine stop) at 500 V/m and permanent damage at 15-24 kV/m.[44]

Intentional Electromagnetic Interference (IEMI) and Its Impact on the U.S. Power Grid finds from testing: "For conducted IEMI threats, it seems clear that if access to external telecom or power cables is not prevented, it is fairly easy to inject harmful signals into a building. Experiments have shown that narrowband voltages injected into the grounding system of a building can cause significant equipment malfunctions inside. Frequencies below 100 Hz and levels below 100 volts have been known to cause problems."[45]

Moreover: "While these failure values may seem low, they should not be a surprise. When one examines the EMC (Electro-Magnetic Compatibility] test requirements for immunity…it is unusual to see a narrowband radiated field level immunity requirement above 10 V/m [10 volts/meter]…This is also the current recommended immunity level for medical devices that are needed to support life."[46]

Summarizing the vulnerability of modern electronic equipment generally, the *IEMI* report finds:

--*"For narrowband, radiated fields, it appears that modern electronic equipment will have serious upsets at 0.5 kV/m for a frequency of 1 GHz. At 400 MHz upsets occur as low as 0.3 kV/m. Above 1 GHz, higher levels are required."*
--*"For wideband, radiated fields, the onset of upsets occurs at [about] 2 kV/m. Damage occurs at levels only a factor of 2-3 higher ([about] 5 kV/m)."*
--*"For conducted, wideband voltages, fast pulses with 5/50 ns pulse characteristics (rise time/pulse width), show serious malfunctions at peak levels of [about] 2kV/m and damage at [about] 4/kV. There is not much data for faster pulse injection waveforms at this time, so it is possible that the susceptibility levels could be even lower for faster pulses. Slower pulses (10/700 microseconds) have shown damage as low as 0.5 k/V with rare upsets."*
--*"For conducted narrowband voltages, only limited testing has been performed, but severe upsets have occurred when the grounding system of buildings were injected at levels of 100 V for frequencies below 100 Hz."*[47]

The *IEMI* report notes that, at much shorter range, non-nuclear EMP weapons are comparable to the effects of nuclear E1 HEMP: "It is clear that there are many similarities between the peak field

[42] Ibid, p. 3-1.
[43] Ibid, p. 3-2.
[44] Ibid, p. 4-1.
[45] Ibid, p. 4-3.
[46] Ibid, p. 4-4.
[47] Ibid, p. 4-5.

levels that can be produced by EM weapons at close ranges and by E1 HEMP. The IEMI waveforms tend to have higher frequency content than E1 HEMP, so they are likely to create equipment and system failures at lower peak levels than E1 HEMP."[48]

Assessing vulnerability of the U.S. electric power grid to non-nuclear EMP weapons, the *IEMI* report analyzed data testing:

1. High voltage substation controls and communication
2. Power generation facilities
3. Power control centers
4. Distribution transformers
5. Distribution line insulators

"Of these 5 portions of the power system, items 1-3 are of the biggest concern due to IEMI," according to the report.[49]

Intentional Electromagnetic Interference (IEMI) and Its Impact on the U.S. Power Grid found that high voltage substation controls and communication, crucial to the operation of the U.S. power grid, are most vulnerable, including:

1. "Computers, of various kinds."
2. "PLCs—programmable logic controllers—basically computers, but specialized with I/O ports, such as A/D and D/A converters (A=analog, D=digital) so that they can process controllers."
3. "Communication devices—modems, routers, switches, etc."
4. "Solid-state safety relays (increasingly used as replacements for the older electromechanical power relays)."
5. "SCADA systems (Supervisory Control And Data Acquisition)—this involves communication of data and controls between unmanned substations and manned control centers."[50]

Testing finds: "Such devices can be vulnerable to either upset or damage from IEMI pulses coming in on the connected wiring. (There is always the possibility that some functional upsets might actually lead to damage, in which the system's own energy is turned against itself, such as for devices controlling moving structures or burning of fuels, for example)."[51]

A few examples from the many test results that damaged critical electric grid equipment, from the *IEMI* report:

--*"The IRGC ports for both the SEL 331L and SEL 2032 [relays] were broken at a level of a few hundred volts (600 volts open circuit). The Ethernet connection on the SCADA unit was also*

[48] Ibid, p. 5-1.
[49] Ibid, p. 5-1
[50] Ibid, pp. 5-2-5-3.
[51] Ibid, p. 5-3.

damaged at the low level (1.2 kV open circuit). In this case we heard a 'bang' associated with the damage, and further testing showed that a resistor on the circuit board had blown up."[52]
--*"Figure 5-7 shows the Fisher ROC809 unit…The effects ranged from some that were localized to the port that was pulsed, up to effects occurring on other parts of the device. Damage was as low as 1 kV for the analog out port. The analog out card damage was subtle at first—its output was more and more inaccurate as the pulse level was increased, until finally (at 1 kV) the level was too high, and it would no longer work."*
--*"A computer was also tested…The Ethernet switch was upset (stopped working) at the 2.0-2.5 kV level. The full 8-port unit stopped communicating…On the computer two different network circuits were tried…These upset at the 4.5-5.0 kV level…The serial port on the computer died at a very low level—750 volts."*[53]

Intentional Electromagnetic Interference (IEMI) and Its Impact on the U.S. Power Grid bottom-line: "Given the vulnerability levels for such equipment, and the levels of coupled signal that IEMI can produce, it can be seen that the 'brains' and communication systems of any modern power facility could be vulnerable to IEMI. This applies to power substations, control centers, and power generation facilities…It is important to evaluate the IEMI threat to high voltage power networks throughout the world, and to develop protection methods against this threat."[54]

NNEMP Attack On The U.S. Electric Grid

Described here are two possible technical scenarios for Non-Nuclear EMP attacks on the U.S. electric grid, out of many possible scenarios. The political-military scenarios are also many.

Political-Military Scenarios
Political-military scenarios for NNEMP attack on the U.S. national power grid include:

--Surprise attack "bolt from the blue" in peacetime, based on adversary calculation that war is eventually inevitable;
--NNEMP attack during a crisis but prior to outbreak of a "shooting war" as a warning and/or preemptive strike designed to cripple U.S. power projection capabilities;
--NNEMP attack coordinated with the outbreak of a traditional "shooting war";
--NNEMP attack as a last-ditch effort to reverse the tide of a losing war;
--NNEMP attack in the aftermath of a lost war, for revenge.

The scale of an NNEMP attack on the U.S. electric grid could include:

--Temporary blackout of a city to send a warning (as China did to Mumbai, India in October 2020 by cyber-attack)[55];

[52] Ibid, p. 5-4.
[53] Ibid, p. 5-5.
[54] Ibid, p. 5-13.
[55] "China Appears To Warn India: Push Too Hard and the Lights Could Go Out" New York Times (28 February 2021).

--Protracted blackout of a state or region to send a bigger warning and/or to cripple particular U.S. military capabilities;
--Protracted nationwide blackout of the U.S. electric grid to defeat the U.S. without a traditional "shooting war" and possibly to eliminate the U.S. as an actor on the world stage (as described in the military doctrines of Russia, China, North Korea, and Iran).[56]

There are many possible political-military scenarios. The focus here is on technical scenarios including adversary capabilities.

Technical Scenario: Nationwide Blackout
The most difficult technical scenario for the NNEMP threat is an attack on the U.S. power grid nationwide, against all three major parts comprising the national grid—the Eastern grid, Western grid, and Texas grid—that inflicts against all three grids simultaneously a protracted blackout, lasting weeks, months, or longer. As shall be demonstrated, since an NNEMP attack can achieve this worst-case scenario, all the lesser scenarios described earlier are also possible.

In both scenarios described here, the technical objective is to damage SCADAs and other vital electronics in EHV transformer substation control centers, of which there are 2,000 in the U.S. national electric power grid. EHV transformers themselves are unlikely to be damaged by NNEMP attack, but damaging the SCADAs and other control systems can stop transformer operations. As shown earlier, extensive testing of SCADAs and other control electronics proves they are highly vulnerable to the NNEMP threat.

In both scenarios, the tactical objective is to damage as many EHV transformer substation control centers as possible in a period of 24 hours. Near simultaneous damage of enough substations will at some point inevitably trigger cascading failures, as more and more load gets dumped on undamaged substations. Cascading failures result rapidly in a nationwide blackout, like the Great Northeast Blackout of 2003 writ larger and lasting much longer because of much deeper damage to the national electric power grid.[57]

A useful point of reference for assessing the likely effectiveness of the two NNEMP attacks described below is a classified study by the U.S. Federal Energy Regulatory Commission, leaked to the press, that found a protracted nationwide blackout could result from sabotage against EHV transformer substations that targets just 9 of 2,000 substations.[58]

Scenario #1: Lower-Tech NNEMP Attack
Scenario #1 is the kind of threat that is well within the technological and operational capabilities of Iran, North Korea, virtually any nation state, and major terrorist or criminal organizations.

---

[56] EMP Commission, *Nuclear EMP Attack Scenarios and Combined-Arms Cyber Warfare* (17 July 2017) pp. 1-11. "Russia: 'War Is Inevitable…Cyberwar'" Newsmax (19 April 2021).
[57] U.S.-Canada Power System Outage Task Force, *Final Report on the August 14, 2003 Blackout in the United States and Canada* (Canada: April 2004).
[58] Rebecca Smith, "Transformers Expose Limits In Securing Power Grid" Wall Street Journal (14 March 2014).

Scenario #1 entails a lower-tech NNEMP threat employing weapons which must be man-delivered by automobile or panel truck. The postulated NNEMP weapons are lower-tech also in power, requiring about 10 minutes to maximize damage against the electronics in unmanned electric grid control substations associated with EHV transformers.

Scenario #1 postulates that every panel truck armed with an NNEMP weapon has a two-man crew, one to drive and one to operate the weapon. The NNEMP weapon illuminates the target—an EHV transformer control substation—for 10 minutes. Then the panel truck moves to the next target, the nearest next substation, located on average 40 road miles away, traveling on average 50 mph.

Given these conditions, a single panel truck carrying an NNEMP weapon and 2-man crew can attack 30 EHV transformer control substations in 24 hours. Below find the capabilities for an NNEMP attack performed by up to 30 vehicles in 24 hours:

--1 NNEMP truck can attack 30 EHV transformer control substations in 24 hours;
--2 NNEMP trucks can attack 60 substations;
--3 NNEMP trucks can attack 90 substations;
--4 NNEMP trucks can attack 120 substations;
--5 NNEMP trucks can attack 150 substations;
--6 NNEMP trucks can attack 180 substations;
--7 NNEMP trucks can attack 210 substations;
--8 NNEMP trucks can attack 230 substations;
--9 NNEMP trucks can attack 260 substations;
--10 NNEMP trucks can attack 280 substations;
--11 NNEMP trucks can attack 310 substations;
--12 NNEMP trucks can attack 340 substations;
--13 NNEMP trucks can attack 370 substations;
--14 NNEMP trucks can attack 400 substations;
--15 NNEMP trucks can attack 430 substations;
--16 NNEMP trucks can attack 460 substations;
--17 NNEMP trucks can attack 490 substations;
--18 NNEMP trucks can attack 520 substations;
--19 NNEMP trucks can attack 550 substations;
--20 NNEMP trucks can attack 580 substations;
--21 NNEMP trucks can attack 610 substations;
--22 NNEMP trucks can attack 640 substations;
--23 NNEMP trucks can attack 670 substations;
--24 NNEMP trucks can attack 700 substations;
--25 NNEMP trucks can attack 730 substations;
--26 NNEMP trucks can attack 760 substations;
--27 NNEMP trucks can attack 790 substations;
--28 NNEMP trucks can attack 820 substations;
--29 NNEMP trucks can attack 850 substations;
--30 NNEMP trucks can attack 880 substations.

As noted earlier, reportedly a classified U.S. FERC study calculates that damaging 9 of 2,000 EHV transformer substations (0.45% of all transformers) is enough to cause a protracted blackout nationwide. Just one NNEMP truck could damage over three times this many (30) substations in 24 hours, but in only one of the three big grids.

At minimum, three NNEMP trucks would be required to attack the Eastern, Western, and Texas grids. These collectively could damage 90 substations, 30 substations damaged in each of the major grid systems, ten times the number of substations damaged in the U.S. FERC study.

The NNEMP attack would probably focus on areas that have the highest concentration of EHV transformer control substations, to maximize opportunities for inflicting the most damage in 24 hours.

In the Eastern grid, the seaboard area between Washington, DC and New York City has the highest concentration of substations. In Texas, substations are most highly concentrated around Dallas, Houston, and Austin. In the Western grid, substations are more geographically dispersed, but most concentrated around Los Angeles and Seattle and on the seaboard in between.

Since the Eastern grid generates about 75% of U.S. electricity, an NNEMP attack, or any other kind of attack, would probably focus most of its effort there. Logically, if the attack is proportioned to the percentage of the U.S. electric power supply, about 75% of the effort would attack the Eastern grid, 20% the Western grid, and 5% the Texas grid.

So in Scenario #1, if 20 NNEMP trucks are employed to attack the three big grids in proportion to their electric generating power, 15 would attack the Eastern Grid, 4 would attack the Western grid, and 1 would attack the Texas grid. Collectively, 20 NNEMP trucks could damage 580 EHV transformer substations in 24 hours, 430 substations in the East, 120 substations in the West, 30 substations in Texas—29% of all substations nationwide.

Scenario #1 requires very few operational personnel, just six men for three NNEMP trucks to attack all three big grids. The "army" manning 20 NNEMP trucks would number just 40 men. By way of comparison, al Qaeda's September 11, 2001, attacks on New York and Washington, that started the long War on Terrorism, was executed by 19 terrorists.

Scenario #1 and this chapter focuses exclusively on NNEMP attacks. But it is highly likely, if this scenario were to occur, the NNEMP attack would be supplemented by a kinetic attack on the EHV transformers too, using for example rocket propelled grenade launchers or a high-powered 0.50 caliber rifle firing explosive bullets, to destroy the EHV transformers while their control substations are also being attacked by NNEMP.

Scenario #2: Higher-Tech NNEMP Attack

Scenario #2 is the kind of threat that is well within the technological and operational capabilities of Russia and China, plausibly within the capabilities of North Korea and Iran, and even possibly within the capabilities of major terrorist or criminal organizations.

Scenario #2 entails a higher-tech NNEMP threat employing CHAMP-like drones or Unmanned Aerial Vehicles (UAVs) that can be preprogrammed or guided to attack EHV transformer control substations. The postulated NNEMP weapons are higher-tech also in power, requiring about 1-5 minutes to maximize damage against the electronics in unmanned electric grid control substations associated with EHV transformers.

Scenario #2 postulates an NNEMP drone or UAV that can fly 100 mph, locate the target, pause to make an NNEMP attack, and sustain these operations continuously for 24 hours. China's Pterodactyl UAV is exactly the kind of drone/UAV capable of such operations, if armed with an NNEMP warhead. Russia has similar UAVs, including the Skyfall cruise missile, powered by a nuclear reactor, that could conceivably energize a super-charged NNEMP warhead. Iran has demonstrated drones, UAVs, and cruise missiles capable of precision attacks on Saudi Arabian oil facilities, that could be modified to make an NNEMP attack.[59]

Scenario #2 postulates, after illuminating the target for 1-5 minutes, the drone or UAV moves to the next target, the nearest next substation, located on average 20 flight miles away, traveling on average 100 mph.

Given these conditions, a single drone/UAV armed with an NNEMP weapon, illuminating each target for 1 minute, can attack 110 EHV transformer control substations in 24 hours. If the time on each target lasts 5 minutes, a single drone/UAV can attack 85 targets in 24 hours. Below find the capabilities for an NNEMP attack, lasting 1-5 minutes on each substation, performed by up to 10 drones/UAVs in 24 hours:

SUBSTATIONS ATTACKED IN 24 HOURS

# DRONES/UAVs:	1	2	3	4	5	6	7	8	9	10
MINUTES ON TARGET										
1	110	220	330	440	550	660	770	880	990	1100
2	103	203	306	409	512	615	718	821	924	1027
3	96	192	288	384	480	576	672	768	864	960
4	90	180	270	360	450	540	630	720	810	900
5	85	170	255	340	425	510	595	680	765	850

[59] "China Reveals Chilling New 'Sharp Sword' Stealth Drone" www.mirror.co.uk (19 January 2017). "Losing World War III Inside America's Borders" Washington Times (8 September 2020). "When Will DC Awaken To Putin's Nuclear Aim For US?" Newsmax (21 August 2019). "Russia's Top Long-Range Attack Drones" airforce-technology.com (27 November 2020). "Drone Attacks Cripple Production At Giant Saudi Oil Plants" www.abc.net.au (14 September 2019). "2019 Abqaiq-Khurais Attack" en.wikipedia.org.

In the case of Russia or China, drones or UAVs could travel intercontinental distances, fly under radar, to make the NNEMP attacks. As noted earlier, China has a stealthy intercontinental UAV that can fly 15,000 miles, from Beijing to Chicago and back, to make attacks with missiles and conduct electronic warfare.[60]

NNEMP drones/UAVs could be launched off false-flagged freighters from U.S. coastal waters, for greater anonymity and plausible deniability. Freighter-launching would bring the U.S. in range of the kind of drones/UAVs currently available to Iran and North Korea. The freighter could carry all the technical personnel needed to perform the attack. Drones/UAVs could be disguised as cargo, hidden in and launched from shipping containers, like Russia's Club-K missile system, designed to convert ordinary freighters into missile launching platforms. The Club-K has been purchased by Iran.

Alternatively, NNEMP drones/UAVs could be shipped into the United States undetected, stored in warehouses located nearest targets in the electric grid, launched and operated from secure warehouses. This scenario would require three secure warehouses, one located in the Eastern grid, one in the Western grid, and one in the Texas grid.

For drones/UAVs that are range-limited, like those currently inventoried by Iran and North Korea, a minimum of three drones/UAVs would be required to make NNEMP attacks on the three big grids—Eastern, Western, and Texas. If NNEMP illumination on each substation lasts 1 minute, 3 drones/UAVs can attack 330 of 2,000 substations in 24 hours.

As noted earlier, a U.S. FERC study reportedly found that sabotaging just 9 of 2,000 EHV transformer substations could start catastrophic cascading failures, causing a protracted nationwide blackout.

10 drones/UAVs making NNEMP attacks, illuminating each target for 1 minute, could in 24 hours attack 1,100 substations, 55% of all EHV transformer control substations. If the NNEMP attack allocates 10 drones/UAVs roughly according to the percentage of electric power generated by each of the big grids, the Eastern grid would get 7 drones/UAVs, the Western grid 2 drones/UAVs, and Texas 1 drone UAV. Consequently, 770 substations would be attacked in the East, 220 substations in the West, and 110 substations in Texas.

A protracted nationwide blackout of the U.S. electric power grid, lasting weeks, months, or longer, would be inevitable.

Aftermath

Unlike the Great Northeast Blackout of 2003, the nationwide blackout from NNEMP attack will not be quickly recoverable because of widespread damage to numerous EHV transformer control substations. Many transformers, additional substations not attacked by NNEMP, and other electric

[60] Ibid.

grid equipment not attacked by NNEMP, may nonetheless be damaged by system-generated over-voltages as the grid collapses, as often happens during severe weather, like hurricanes.

Unlike hurricanes, that only have regional impact, a nationwide blackout induced by NNEMP attack will cause much deeper and more widespread systemic damage to all three parts of the North American grid—Eastern, Western, and Texas. Identifying damaged substations, locating and accurately diagnosing damage to equipment, will take time, probably many weeks. Replacing damaged equipment may not even be possible because of insufficient spares.

Acquiring replacement equipment and installation will require many weeks or months, if even possible when all critical infrastructures—communications, transportation, petroleum and natural gas, business and finance, food and water infrastructures—are inoperable or severely crippled due to protracted nationwide blackout.

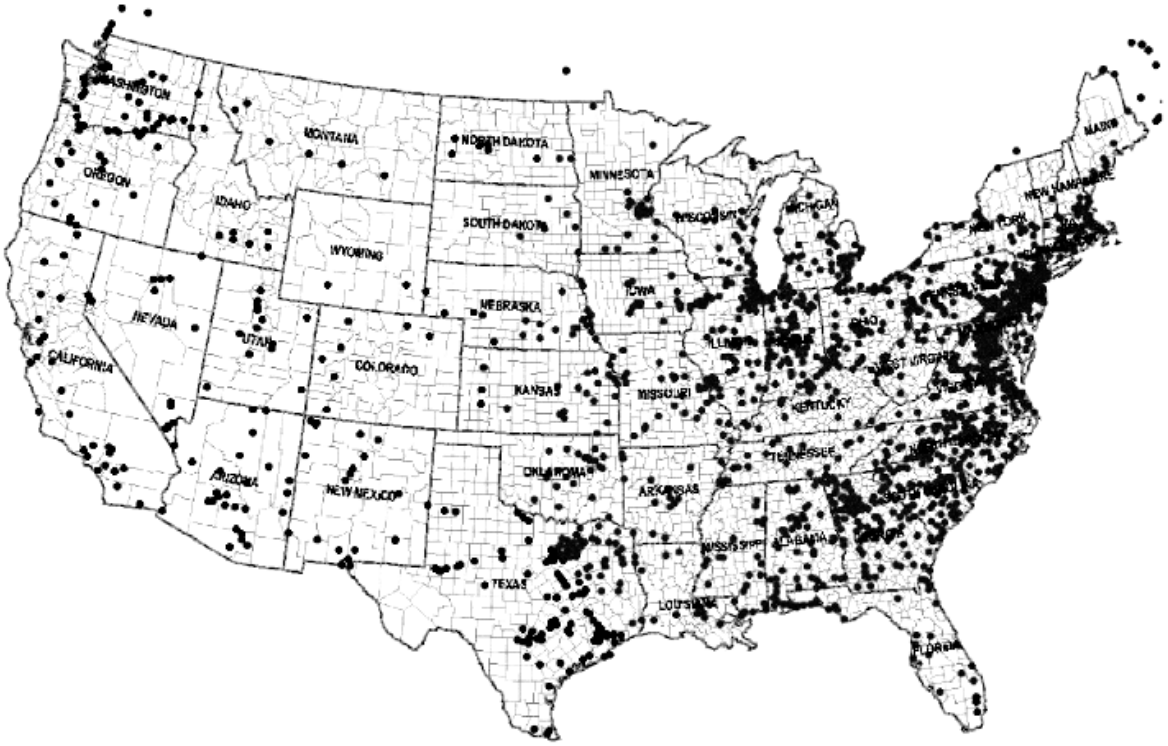
Utility emergency crews are typically too few and inadequately resourced to repair and recover electric grids from damage inflicted by hurricanes, let alone a nationwide NNEMP attack. Utility workers are not the police or firefighters, and may not even report to work from concern for their families as a nationwide blackout quickly becomes growing chaos. After Hurricane Katrina, many on duty police and firefighters stayed home with their families instead, 24 hours after the lights went out.

U.S. military power projection capabilities would be severely crippled or altogether paralyzed by a protracted nationwide blackout. CONUS military bases depend upon the civilian electric grid for 99% of their electric power.[61]

Any rational American president, faced with a ticking clock toward societal chaos and mass starvation, would likely give highest priority to mobilizing all remaining operating resources, including the Defense Department, to recovering the national electric grid and other life-sustaining critical infrastructures, instead of fighting World War III.

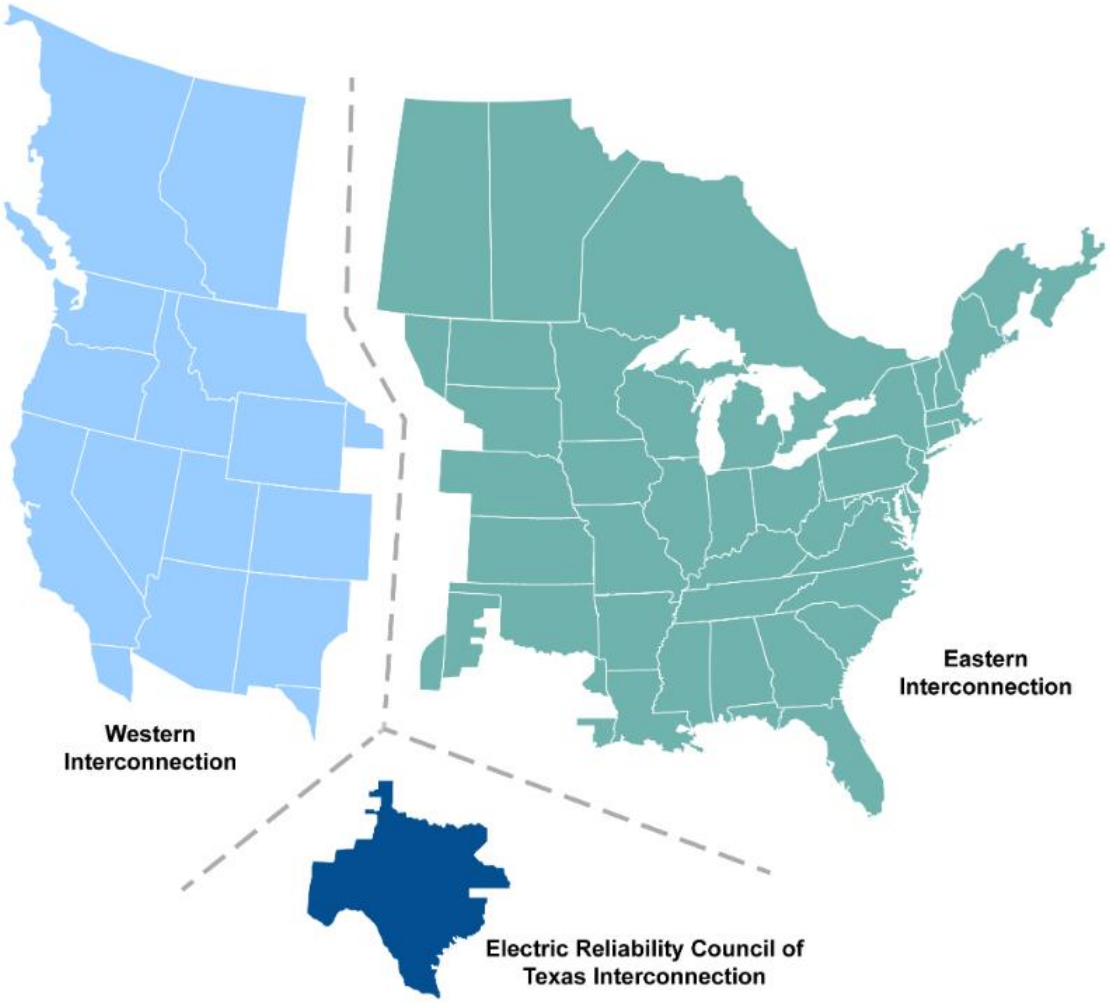
[61] Loren Thompson, "Critical U.S. Military Sites Can't Cope With A Prolonged Power Outage" Forbes (18 May 2018). Peter Huessy, "Electronic Doomsday for the U.S.?" Gatestone (13 January 2016).

LOCATIONS OF EHV TRANSFORMER SUBSTATIONS
345 KILOVOLTS OR HIGHER



Source: Adapted from Edward Savage, James Gilbert, and William Radasky, *The Early Time (E1) High-Altitude Electromagnetic Pulse (HEMP) and Its Impact on the U.S. Power Grid*, Meta-R-320 (January 2010) p. 7-20.

NORTH AMERICAN ELECTRIC GRIDS



The Eastern, Western, and Texas grids are called “interconnects” although they are not interconnected. The Eastern and Western North American grids include the USA and Canada.

DR. PETER VINCENT PRY

Dr. Peter Vincent Pry is Executive Director of the EMP Task Force on National and Homeland Security, a Congressional Advisory Board dedicated to achieving protection of the United States from electromagnetic pulse (EMP), cyber-attack, mass destruction terrorism and other threats to civilian critical infrastructures on an accelerated basis. Dr. Pry served as Chief of Staff of the congressional Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack (2001-2017); as Director of the United States Nuclear Strategy Forum, an advisory board to Congress on policies to counter Weapons of Mass Destruction; and on the staffs of the Congressional Commission on the Strategic Posture of the United States (2008-2009); the Commission on the New Strategic Posture of the United States (2006-2008); the House Armed Services Committee (1995-2001); and the CIA (1985-1995).

Dr. Pry served as Professional Staff on the House Armed Services Committee (HASC) of the U.S. Congress, with portfolios in nuclear strategy, WMD, Russia, China, NATO, the Middle East, Intelligence, and Terrorism. While serving on the HASC, Dr. Pry was chief advisor to the Vice Chairman of the House Armed Services Committee and the Vice Chairman of the House Homeland Security Committee, and to the Chairman of the Terrorism Panel. Dr. Pry played a key role: running hearings in Congress that warned terrorists and rogue states could pose an EMP threat, establishing the Congressional EMP Commission, helping the Commission develop plans to protect the United States from EMP, and working closely with senior scientists who first discovered the nuclear EMP phenomenon.

Dr. Pry was an Intelligence Officer with the Central Intelligence Agency responsible for analyzing Soviet and Russian nuclear strategy, operational plans, military doctrine, threat perceptions, and developing U.S. paradigms for strategic warning. He also served as a Verification Analyst at the U.S. Arms Control and Disarmament Agency responsible for assessing Soviet compliance with strategic and military arms control treaties.

Dr. Pry has written numerous books on national security issues, including: *Will America Be Protected? (Volumes I and II); The Power And The Light: The Congressional EMP Commission's War To Save America; POSEIDON: Russia's New Doomsday Machine; The Long Sunday: Nuclear EMP Attack Scenarios; Blackout Wars; Apocalypse Unknown: The Struggle To Protect America From An Electromagnetic Pulse Catastrophe*; *Electric Armageddon: Civil-Military Preparedness For An Electromagnetic Pulse Catastrophe*; *War Scare: Russia and America on the Nuclear Brink*; *Nuclear Wars: Exchanges and Outcomes*; *The Strategic Nuclear Balance: And Why It Matters*; and *Israel's Nuclear Arsenal*. Dr. Pry often appears on TV and radio as an expert on national security issues. The BBC made his book *War Scare* into a two-hour TV documentary *Soviet War Scare 1983* and his book *Electric Armageddon* was the basis for another TV documentary *Electronic Armageddon* made by the National Geographic.

DR. PETER PRY

This recognizes Dr. Peter Pry *for his outstanding accomplishments during his 10 years of service at the Central Intelligence Agency. A noted expert in his field, Dr. Pry conducted groundbreaking research that illuminated one of the most important issues of our time—the US-Soviet nuclear competition. On the vanguard of strategic intelligence analysis during the Cold War, he developed much of what the US Government knows about Soviet planning for nuclear war, including Soviet views of the character of war, perceptions of US intentions, assessment of the nuclear balance, and operational plans. In the post-Cold War period, his work has been central to the US Government's understanding of evolving Russian threat perceptions and military doctrine and the construction of new paradigms for strategic warning and stability assessments.*

Dr. Pry can take pride in knowing that his work has contributed significantly to the security of the United States. He has been a pillar of the Intelligence Community and will be sorely missed. Without a doubt, his continued public service on Capitol Hill will reflect the same expertise, professionalism, and dedication that have characterized his exemplary career at the CIA.

We wish him much success in his new endeavor.

Lawrence K. Gershwin *Charles E. Allen* *John E. McLaughlin*