

## ELECTROMAGNETIC TERRORISM: NEW HAZARDS

V. Gurevich, Ph.D

Israel Electric Corp., Central Electric Laboratory

POB10, Haifa 31000, Israel, fax: (++1) 603-308-5909, E-mail: gurevich2@bezeqint.net

*Спроба повернути увагу до небезпеки нового виду тероризму: електромагнітного. Приведені відомості з відкритих джерел про історію створення нового виду зброї, про країни, компанії і фахівців, що займають лідируюче положення в цій області. Показано, що сучасні електроенергетичні об'єкти дуже вразливі щодо навмисних електромагнітних впливів, враховуючи широке застосування мікропроцесорної техніки і комп'ютерів в умовах, коли вже сьогодні на ринку є технічні засоби, що дозволяють здійснювати атаки на такі об'єкти.*

*Попытка привлечь внимание к опасности нового вида терроризма: электромагнитного. Приведены сведения из открытых источников об истории создания нового вида оружия, о странах, компаниях и специалистах, занимающих лидирующее положение в этой области. Показано, что современные электроэнергетические объекты весьма уязвимы в отношении преднамеренных электромагнитных воздействий из-за широкого применения микропроцессорной техники и компьютеров в условиях, когда уже сегодня на рынке имеются технические средства, позволяющие осуществлять атаки на такие объекты.*

The theory behind the *E-bomb* was proposed in 1925 by physicist Arthur H. Compton not to build weapons, but to study atoms. Compton demonstrated that firing a stream of highly energetic photons into atoms that have a low atomic number causes them to eject a stream of electrons. Physics students know this phenomenon as the *Compton Effect*. It became a key tool in unlocking the secrets of the atom. Ironically, this nuclear research led to an unexpected demonstration of the power of the Compton Effect, and spawned a new type of weapon. In 1958, nuclear weapons designers ignited hydrogen bombs high over the Pacific Ocean. The detonations created bursts of gamma rays that, upon striking the oxygen and nitrogen in the atmosphere, released a tsunami of electrons that spread for hundreds of miles. Street lights were blown out in Hawaii and radio navigation was disrupted for 18 hours as far away as Australia. The United States set out to learn how to "harden" electronics against this electromagnetic pulse (EMP) and develop EMP weapons.

Now, intensive investigations in electromagnetic weapons field are being carried out in Russia, the USA, England, Germany, and China. In the USA such research is carried out by the biggest companies of the military-industrial establishment, such as TWR, Raytheon, Lockheed Martin, Los Alamos National Laboratories, the Air Force Research Laboratory at Kirtland Air Force Base, New Mexico, and many civil organizations and universities.

In the 1990's the U.S. Air Force Office of Scientific Research set up a five-year Multidisciplinary University Research Initiative (MURI) program to explore microwave sources. One of those funded was the University of New Mexico's Schamiloglu, whose lab is located just a few kilometers down the road from where the Shiva Star sits behind tightly locked doors.

The German company "Rheinmetall Weapons and Munitions" has also been researching E-weapons for years and has test versions.

The EMP shell was designed following revelations that Russia was well ahead of the West in the development of so-called radio-frequency weapons. A paper given at a conference in Bordeaux in 1994 made it clear that the Russians believed it possible to use such weapons to disable all of an enemy's electronic equipment. Written by Dr. A. B. Prishchepenko, Deputy Director of Scientific Center "Sirius", Member-correspondent of the Russian

Academy of Military Sciences and entitled "Radio Frequency Weapons on the Future Battlefield", it described Soviet research dating back to the late forties, provoking near panic among western military planners (A.B. Prishchepenko, V.V. Kiseljov, and I.S. Kudimov, "Radio Frequency Weapon at the Future Battlefield", *Electromagnetic environment and consequences*, Proceedings of the EUROEM94, Bordeaux, France, May 30-June 3, 1994, part 1, p. 266-271). It gave credence to the nightmare scenario of a high-technology war in which all the radio, radar and computer systems on which their weapons depended would be disabled, leaving them completely defenseless. Then two years ago it emerged that the Russians had developed an electro-magnetic device, a so-called *E-Bomb*, capable of disabling electrical and electronic systems, which could be carried in a briefcase. Amid intelligence reports showing that the Irish IRA had discussed the possibility of paralyzing the City of London with an E-Bomb, British research in that technology was stepped up.

Today in Russia electromagnetic weapons are being developed by huge research and production institutions like the Scientific Association for High-Temperatures (OIVT), consisting of the following Moscow organizations: the Institute of High Temperatures of Academy of Sciences; the Institute of Thermal Physics of Extremal States; the Institute of Theoretical and Applied Electrodynamics; the Research-and-Development Center of Thermal Physics of Impulse Excitations, and the proving ground in Bishkek; in addition the All-Russian Scientific Research Institute of Experimental Physics in Sarov (Arzamas-16) in the Nizhni Novgorod region; the All-Russian Scientific Research Institute of Technical Physics in Snezhinsk (Chelyabinsk-70). In spite of the economic crisis in Russia and a lack of money for many military programs, the government allocates money to these institutions. For example, recently in Moscow for the Scientific Association OIVT, a new building with an area of 1.5 thousand square meters has been built.

As of late, many projects of past age have been declassified and are freely sold today. For example, the Institute of High Current Electronics of the Russian Academy of Sciences in Tomsk (HCEI SB RAS) offers at free sale ultra-wideband high-power sources of directional electromagnetic radiation (Fig.1).

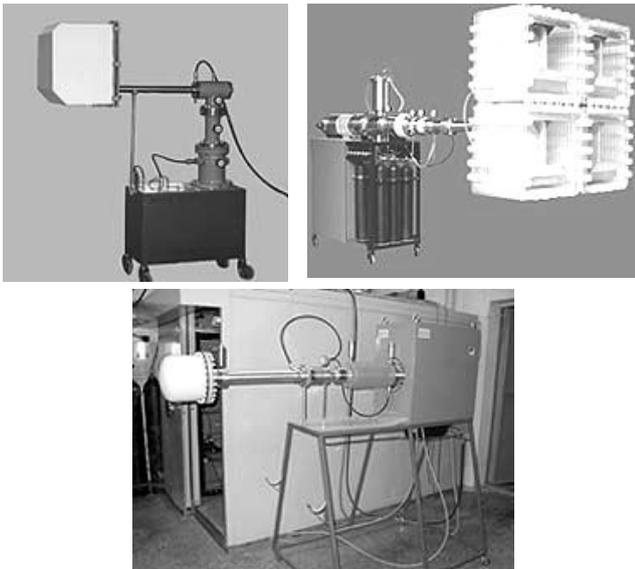


Fig. 1. Compact ultra-wideband generators of directional pulse electromagnetic radiation with power output of 100 – 1000 Megawatts (Institute of High Current Electronics, Russia)

As the technology of military RF weapons matures, such weaponry also becomes affordable and usable by criminals and terrorists. Both cheap low-tech and expensive high-tech weapons exist. High-power sources and other components to build EM weapons are available on the open market and proliferate around the globe, Fig. 2.

One potential ingredient made available by the military is old radars, sold when facilities close down. Anything that operates between 200 MHz and 4 or 5 GHz seems to be a real problem. The reason they are for sale is that they are not very effective. Radar technology has improved drastically, but the radar doesn't need to be the newest technology to cause problems to electronic equipment and systems that aren't prepared for an intentional EM threat. Intentional EMI includes both pulses and continuous-wave signals, in two basic forms. One is high-power microwave (HPM), a continuous-wave signal at a given frequency that continues for a microsecond or two at a Gigahertz, like radar. The other is ultra-wideband, which is essentially a fast pulse produced by a radar using pulse techniques rather than a continuous wave. These threats can be packaged in a mobile van or even a suitcase. The effective ranges decrease with size, but even a suitcase-sized threat is widely available. According to Peter Cotterill, managing director of MPE Ltd. (Liverpool, UK), an electromagnetic bomb in a suitcase with a range possibly as high as 500 m can be purchased on the Internet at the cost of only \$100,000. Terrorists could use a less expensive, low-tech approach to create the same destructive power. "Any nation with even a 1940's technology base could make them," says Carlo Kopp, an Australian-based expert on high-tech warfare. "The threat of E-bomb proliferation is very real." POPULAR MECHANICS estimates a basic weapon could be built for \$400.

Nowadays there are no measures preventing distribution of electronic weapons. Even if agreements on limitation of distribution of electromagnetic weapons are reached, they won't be able to solve the problem of accessibility of required materials and equipment.

One cannot rule out the possibility of leakage of electromagnetic weapons technology from countries of

the former USSR to third world countries, or to terrorist organizations, as the former really face great economic difficulties. The danger of distribution of electromagnetic weapons is quite real.

Today it is possible to find finished drawings and descriptions of generators of directional high frequency radiation based on household microwave ovens on the Internet (see: [www.powerlabs.org](http://www.powerlabs.org), [www.voltsamps.com](http://www.voltsamps.com), etc).

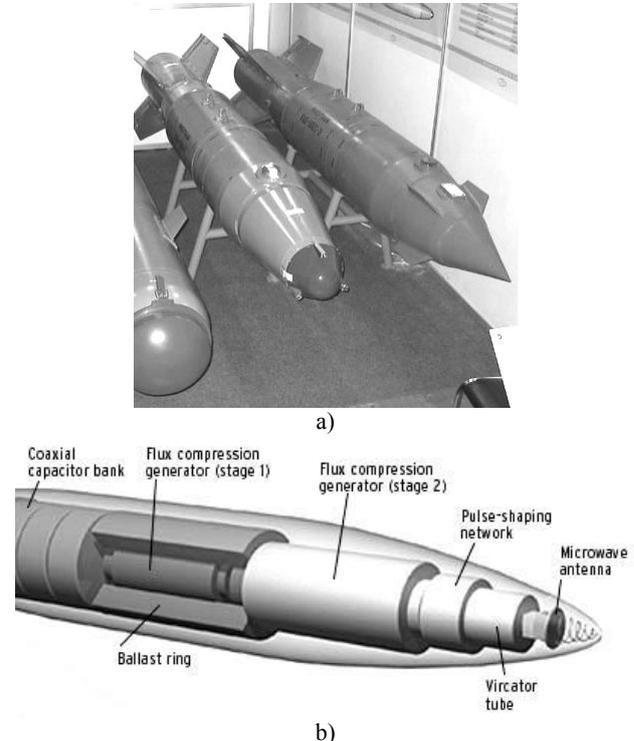


Fig. 2 Electromagnetic Bombs  
a - Russian GPS-guided KAB-500S type Electromagnetic Bomb (right); b - typical construction of an E-bomb

Problems of "electromagnetic terrorism" capable of causing man-caused accidents on a national scale similar to that which happened in New-York in August 2003, were formulated in an article by Manuel W. Wik (now chief engineer and strategic specialist on future defense science and technology programs at the Defence Materiel Administration, Stockholm) "Electromagnetic Terrorism – What are the Risks? What can be Done? ", Published in 1997 in the "International Product Compliance Magazine". Here is what that article says on the subject:

"Although electromagnetic terrorism is not often discussed in public, as it is potentially an extremely sensitive issue, there needs to be wider public awareness of the threats posed and a better understanding of the consequent risk-management strategies required. Nevertheless, with the gradual development of smaller equipment that can be used to produce short, intense electromagnetic pulses capable of damaging the controls of much electronic equipment, electromagnetic terrorism is increasingly something that needs to be considered during the compliance-planning route. Thus, although it is important that neither the details of electromagnetic (EM) interaction with particular systems nor specific vulnerabilities should be made public, public awareness of the potential threats and, indeed, a better understanding of the relevant risk-management strategies need to be more widely disseminated. Electromagnetic terrorism (EM terrorism) is the intentional, malicious generation of electromagnetic energy, introducing noise or

signals into electric and electronic systems, thus disrupting, confusing or damaging these systems for terrorist or criminal purposes. EM terrorism can be regarded as one type of offensive information warfare. EM terrorism needs to be considered more carefully in the future because information and information technology are increasingly important in everyday life".

Electronic components and circuits, such as microprocessors, are working at increasingly higher frequencies and lower voltages and thus are increasingly more susceptible to electromagnetic interference (EMI).

At the same time, there have been rapid advances in radio frequency (RF) sources and antennae and there is an increasing variety of equipment capable of generating very short RF pulses that can disrupt sophisticated electronics. Intentional electromagnetic interference (EMI) poses a significant threat worldwide. Until recently, industry has been resistant to addressing the issue, but the International Electrotechnical Commission (IEC) is beginning to develop methods to fight criminal EMI.

The possibility of intentional EMI has come under the scrutiny of the United States Congress. Representative Jim Saxton of New Jersey and Representative Roscoe Bartlett of Maryland have held several investigations concerning this threat and have lobbied Congress for funds for appropriate research. As early as February 1998, Saxton began holding hearings on the proliferation and threat of RF weapons.

The issue of intentional EMI has also begun to be addressed at international conferences. The 1999 International Zurich Symposium on EMC held the first workshop on intentional EMI, with nearly 200 people in attendance. The 2001 Zurich Symposium was the culmination of several years of work in the field of intentional EMI. This symposium included the first refereed session on intentional EMI. The threat of intentional EMI is not limited to RF energy. Most of the emphasis in this area has been on radio-frequency fields but the issue of injecting directly into power and telecom systems has been overlooked. Yuri Parfenov and Vladimir Fortov, of the Russian Academy of Sciences Institute for High Energy Densities, recently experimented with injection of disturbances into power lines outside a building and found that the signals penetrate very easily and at a high enough voltage to cause damage to computers inside the building. Additionally, radiated fields often become a conducted threat due to coupling of RF energy to exposed wires.

It is astonishing that numerous research projects devoted to EM terrorism are concerned with the EMI impact on such objects as communication systems, telecommunications, air-planes, computers, but there are practically no projects devoted to investigation of resistance of microprocessor-based relays to EMI, malfunctioning of which can lead to high consequences. However, it is obvious without any investigations that microprocessor based relays are more prone to EMI impact than electromechanical and even analog electronic ones.

In addition, it turns out that "electromagnetic terrorism" is not the only form of modern remote terrorism to which microprocessor-based relays are prone. There are also electronic intrusions called *cyber-attacks*.

A cyber intrusion is a form of electronic intrusion where the attacker uses a computer to invade electronic assets to which he or she does not have authorized access. The IEEE defines *electronic intrusions* as:

*Entry into the substation via telephone lines or other electronic-based media for the manipulation*

*or disturbance of electronic devices. These devices include digital relays, fault recorders, equipment diagnostic packages, automation equipment, computers, PLC's, and communication interfaces.*

A cyber-attack can be an intrusion as described above, or a *denial of service attack* (DOS) where the attacker floods the victim with nuisance requests and/or messages to the extent that normal services and functions cannot be maintained. A DOS attack is also called a *flood attack*. A *distributed DOS attack* (D-DOS) is a flood attack launched simultaneously from multiple sites.

Tools for attacking computer-based control equipment by telephone and network connection are free and widely available over the Internet. There are literally dozens of Web sites devoted to hacking, usually providing downloadable programs or scripts to help the novice hacker get started.

Nowadays hackers' attacks are becoming terrorist weapons. Real cases of terrorist attacks of this kind are usually kept secret, but some are already known. For example, an attempt to damage the Israeli power system with the help of a hacker's attack was prepared by the "Special Services" of Iran for several months in 2003. Fortunately, the security service of the Israel Electric Corp. managed to block these attacks. As attacks of this kind to the main national computer systems of Israel have become more frequent, within Israeli Counter-Intelligence and Internal Security Service (SHABAK) there is a special subdivision for counteraction to such attacks.

But this problem is not only actual for Israel. The North American electric power network is vulnerable to electronic intrusions (a.k.a. cyber-attacks) launched from anywhere in the world, according to studies by the White House, FBI, IEEE, North American Electric Reliability Council (NERC), and National Security Telecommunications Advisory Committee (NSTAC). At the heart of this vulnerability is the capability for remote access to control and protection equipment used by generation facilities and Transmission and Distribution (T&D) utilities. Remote access to protective equipment historically has been limited to proprietary systems and dedicated network connections. Now, however, there is an increased use of public telephone services, protocols, and network facilities, concurrent with a growing, more sophisticated, worldwide population of computer users and computer hackers which is why special services of many countries had to create special subdivisions to fight this dangerous phenomenon. In Russia in particular, it is the Federal Agency of Governmental Communication and Information (FAQCI) that tackles these problems.

Is there a solution for this situation?

Probably yes, if:

- We completely replace all electric wires connected to microprocessor relays, including current and voltage circuits, with non-conductive fiber-optical wires;
  - Use opto-electronic CT and VT, instead of traditional instrument transformers;
  - Provide full galvanic separation from the power electric network by using a power supply of microprocessor relays to carry through the unit "motor generator";
  - The microprocessor based relays should be placed in a completely closed metal case made with a special technology, used for ultrahigh frequencies in which there are no other kinds of the electric equipment,
- This is the price necessary to pay for progress in the field of relay protection!

*Поступила 11.05.2005*