International Journal of Research Studies in Electrical and Electronics Engineering(IJRSEEE)
Volume 5, Issue 3, 2019, PP 36-40
ISSN 2454-9436 (Online)
DOI: http://dx.doi.org/10.20431/2454-9436.0503005
www.arcjournals.org

Cybernetic and Electromagnetic Impacts on Electronic Equipment: Do they have Anything in Common?

Vladimir Gurevich, Ph.D*

Central Electrical Laboratory Israel Electric Corp., Haifa, Israel

Corresponding Author:** ***Vladimir Gurevich, Ph.D., *Central Electrical Laboratory Israel Electric Corp., Haifa, Israel*

Abstract: *Recently, it has become very fashionable to unite cybernetic and electromagnetic threats for electronic equipment into one type: cyber-electromagnetic. The term "cyber-electromagnetic" occurred in US Army reports, extended into special technical literature, then moved into common literature and even into governmental decrees, names of agencies and organizations. Apparently, it may seem that selection of a proper term is not a major issue. For instance, if somebody likes the term "cyber-electromagnetic" to denominate contemporary threats for electronic equipment, just go ahead and use it! Does it really matter, which term to use? Actually, it is not that simple.*

Keywords: *cyber-electromagnetic; cyberspace; information environment; electronic equipment; high altitude electromagnetic pulse; HEMP*

1. Introduction

The issue of combining "cyber impacts" and "electromagnetic impacts" into a common concept eventually results in logical combination of potential threats and practical combination of efforts to prevent them and ensure protection against them. In these circumstances, some agencies and specialists aim to develop measures which ensure protection from both cybernetic and electromagnetic threats. Are these threats really so close that some agencies and specialists can successfully address them? Let us examine this issue.

2. Cyber-Electromagnetic Activities

Let us start with cyberspace. Initially this concept was introduced by American writer William Ford Gibson in his science fiction novel *Neuromancer* [1], Fig. 1.

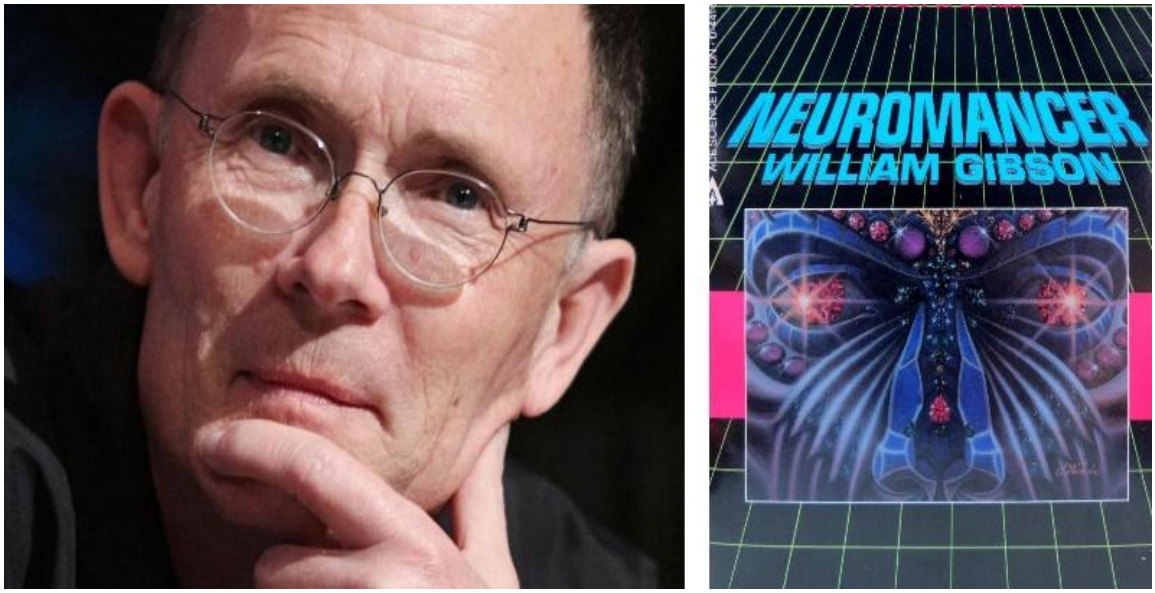


Figure1. *William Gibson and the cover of the first printing of Neuromancer (1984) [1].*

Today, though the concept has no common definition, it is widely spread in society. There are dozens of absolutely different definitions, from:

"Cyberspace – amorphous, supposedly "virtual" world created by links between computers, Internet-enabled devices, servers, routers, and other components of the Internet's infrastructure" (Encyclopedia Britannica)

to the definition of the US Department of Defense [2], Fig. 2:

"Cyberspace is a global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers."

In other words, it refers to electronic equipment processing information and computer software installed in this equipment.

The Allied Joint Doctrine for Information Operations NATO AJP-3.10 [3] (Fig. 2) provides the following definition of "information environment":

"Information environment – the virtual and physical space in which information is received, processed and conveyed. It consists of the information itself and information systems."

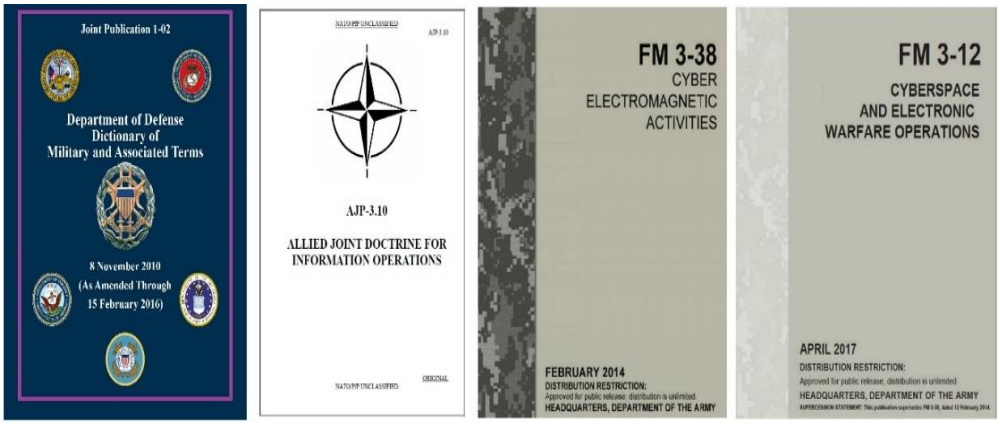


Figure2. *Documents of NATO and US Army regarding cyberspace and electromagnetic impacts.*

In this definition, "physical space" means electronic (computer) equipment, whereas "virtual space" means software environment. Joint work of both environments ensures reception, processing and conveying of information.

However, let us leave fierce philosophic debates regarding "cyberspace" definitions and continue. What is important for us is that this concerns two components of common the **information environment:** electromagnetic range (where information is physically processed by a computer) and virtual space (where information is processed by software). It should be stressed again: it is all about operations in the **information environment** and not elsewhere!

Operations in cyberspace are divided into several major types, which include multiple sub-types:

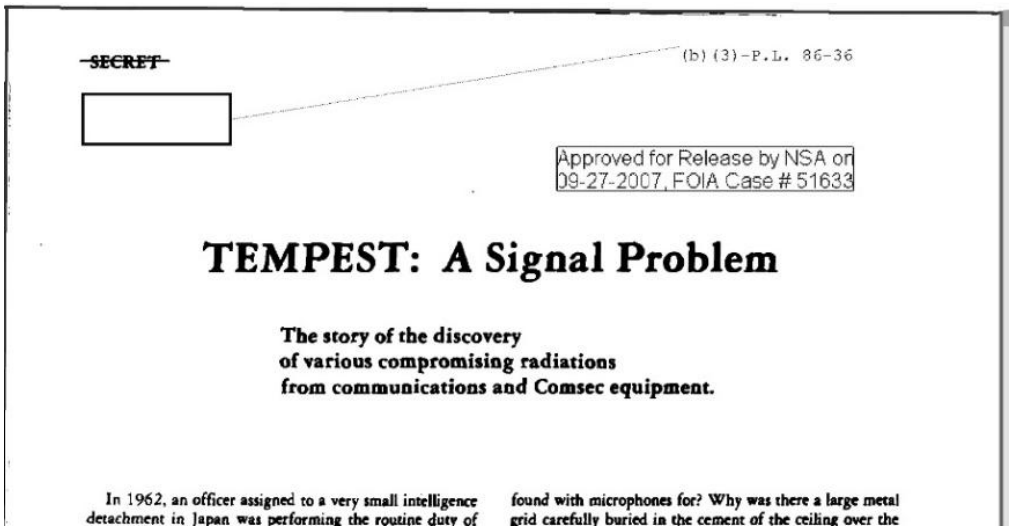
1. Data theft (information leak) by means of special software.
2. Intentional failures of equipment induced by special software.
3. Creation of fake data by fraudulent systems (fishing, clickjacking, information traps, etc.) operating on the basis of special software.

These types of cyberspace operations are based on a common technique (method) of using special software, which intrudes into computers that process information. Thus, joining them into a common concept of "cyber activity" is rather evident and justified.

Operations in the electromagnetic range also consist of several major types which include sub-types:

1. Data theft (information leak) by means of specific highly unusual electronic equipment. Back in 1960s the US National Security Agency (NSA) gave a code name to this technology – "TEMPEST" – and everything related to this topic was classified for dozens of years (Fig. 3).

2. Intentional failures of equipment induced by a powerful directed electromagnetic emission with a local impact.
3. Creation of fake data and images by fraudulent systems which produce long-ranging powerful electromagnetic fields that deceive recognition and navigation electronic systems (spoofing, electromagnetic traps, fake targets).
4. Comprehensive and spacious physical damage of different electrotechnical and electronic (not only informational) equipment (electromagnetic pulse of high-altitude nuclear explosion - HEMP).



~~SECRET~~

(b) (3)-P.L. 86-36

Approved for Release by NSA on 09-27-2007, FOIA Case # 51633

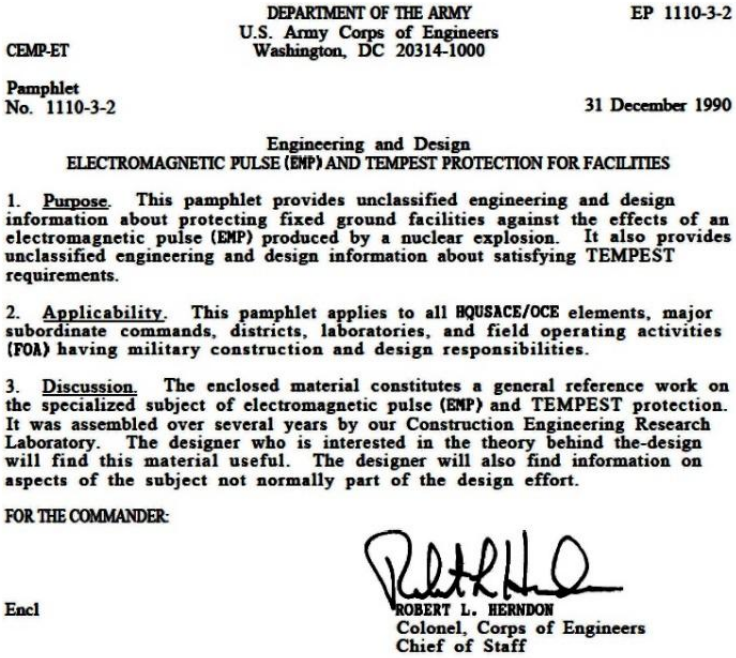
TEMPEST: A Signal Problem

The story of the discovery of various compromising radiations from communications and Comsec equipment.

In 1962, an officer assigned to a very small intelligence detachment in Japan was performing the routine duty of

found with microphones for? Why was there a large metal grid carefully buried in the cement of the ceiling over the

Figure3. *One of the documents from 1960s regarding TEMPEST was declassified by NSA in 2007.*



DEPARTMENT OF THE ARMY
U.S. Army Corps of Engineers
Washington, DC 20314-1000

EP 1110-3-2

CEMP-ET

Pamphlet
No. 1110-3-2

31 December 1990

Engineering and Design
ELECTROMAGNETIC PULSE (EMP) AND TEMPEST PROTECTION FOR FACILITIES

1. Purpose. This pamphlet provides unclassified engineering and design information about protecting fixed ground facilities against the effects of an electromagnetic pulse (EMP) produced by a nuclear explosion. It also provides unclassified engineering and design information about satisfying TEMPEST requirements.

2. Applicability. This pamphlet applies to all HQUSACE/OCE elements, major subordinate commands, districts, laboratories, and field operating activities (FOA) having military construction and design responsibilities.

3. Discussion. The enclosed material constitutes a general reference work on the specialized subject of electromagnetic pulse (EMP) and TEMPEST protection. It was assembled over several years by our Construction Engineering Research Laboratory. The designer who is interested in the theory behind the-design will find this material useful. The designer will also find information on aspects of the subject not normally part of the design effort.

FOR THE COMMANDER:

ROBERT L. HERNDON
Colonel, Corps of Engineers
Chief of Staff

Encl

Figure4. *Cover page of US Army's report # EP 1110-3-2, which combines absolutely different types of activity in the electromagnetic range, i.e. HEMP and TEMPEST [4].*

Unlike cyberspace operations, those performed in the electromagnetic range have no common grounds (technique, methodology). They differ from each other significantly and thus combining them into a common concept of "electromagnetic activity" is not feasible. For example, what is common between ultra-sensitive sensors of the electromagnetic field used for information retrieval from communication cables (TEMPEST), powerful generators of electromagnetic field with a frequency of dozens of gigahertz, and power rating of several million Watts in a directional antenna and nuclear explosion at the height of several hundreds of kilometers?

Table1. *Differences between TEMPEST and HEMP*

Differences	
TEMPEST	**HEMP**
SIGNALS POWER	
MICROVOLTS, MICROWATS	KILOVOLTS, MEGAWATS
FREQUENCY MARGIN	
UP TO 100 GHz	UP TO 100 MHz
MAIN PROTECTION MEASURES	
EMI FILTERS	VOLTAGE SUPPRESSORS
AREA OF USAGE	
LOCAL INSTALLATION	GLOBAL IMPACT
IMPACT ON CRITICAL INSTALLATION	
UNAUTHORIZED ACCESS TO CLASSIFIED INFORMATION	PHYSICAL DESTRUCTION OF INFRASTRUCTURAL OBJECTS
TESTING METHOD AND TEST EQUIPMENT	
VERY HIGHLY SENSITIVE COMPACT ELECTRONIC EQUIPMENT	VERY HIGH-POWER HIGH VOLTAGE BIG EQUIPMENT

However, 30 years ago the US Army Corps of Engineers compiled a substantial report about the results of an Engineer Research Lab operation, where an attempt was made to combine different types of activity in the electromagnetic range, taking HEMP and TEMPEST as an example [4] (Fig. 4). This combination is very strange due to significant differences between these types of activity in the electromagnetic range (Table 1).

Indeed, there is nothing common between these two types of activity, except for shielding requirements for equipment and cables.

Nevertheless, close connection between the electromagnetic range and virtual space in the information environment, as well as some logical similarity of selected operations both in cyberspace and the electromagnetic range, initiated an official introduction of a new concept: "cyber-electromagnetic activity", which would combine both types of activity into a single whole. The reasoning of authors of this concept is not clear, as the notion of cyberspace already includes electronic equipment working in the electromagnetic range. Introduction of a new concept would have been feasible if cyberspace included only the virtual space (i.e. software) and did not include physical processes of information processing by means of electronic equipment. But this is not the case.

Subsequently, how is this relatively new concept used in practice? Let us review some documents of the US Army (Fig. 2). The authors of FM 3-38 (2014) (Fig. 2) [5], which pretends to be the first in creation of a new military doctrine called "*Cyber-Electromagnetic Activities" (CEMA)*, suggest a necessity to "integrate and synchronize" operations in cyberspace and the electromagnetic range. One of the examples of such "integration and synchronization" has been discussed above based on US Army report # 1110-3-2.

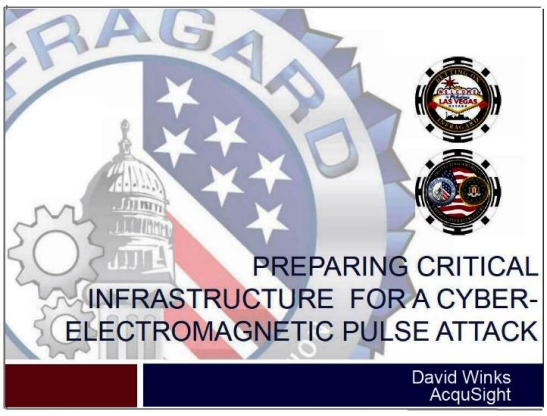


Figure5. *The document containing suggestions on how to prepare critical infrastructure to "cyber-electromagnetic pulse" attacks [8].*

In the attempt to follow a fashionable doctrine, the Department of Homeland Security (DHS) established the National Cybersecurity and Communication Integration Center (NCCIC), the purpose of which is to coordinate efforts in the field of cybersecurity, protection from HEMP, high-frequency directional electromagnetic weapons, and even from electromagnetic storms during solar flares.

The attempts to combine absolutely different (in physical essence) impacts on equipment give rise to really "strange" documents, such as the one shown in Fig. 5.

Another one is FM 3-12 [7] (Fig. 2), connecting cyberspace operations with HEMP, which are not associated with cyberspace, without addressing the TEMPEST problem, which should really be combined with cyberspace operations as one of the two components of a common problem of information protection.

3. CONCLUSION

1. Various operations in cyberspace have very much in common. Thus, it is rather logical and feasible to combine them into a common group of operations performed in the information environment.
2. Various operations in the electromagnetic range may significantly differ from each other. Moreover, not all of them are associated with the information environment.
3. The concept of cyber-electromagnetic activity covers only those operations performed in the electromagnetic range that relate to the information environment, i.e. the environment, where cyberactivity actually takes place.
4. It is not really feasible to combine absolutely different concepts, one of which relates to the information environment and the other which is not connected (e.g. Cyberactivity and HEMP) automatically. This results in confusion and incorrect allocation of efforts and resources aimed at protection from the destructive impact on critical electronic equipment and thus, this malpractice should be seized.

REFERENCES

[1] Gibson, William. Neuromancer. ACE, July 1984.

[2] JP 1-02 Department of Defense Dictionary of Military and Associated Terms. 2010.

[3] AJP-3.10 Allied Joint Doctrine for Information Operations. NATO Standardization Agency, 2009.

[4] EP1110-3-2 Engineering and Design Electromagnetic Pulse (EMP) and TEMPEST Protection for Facilities. Department of the Army, U.S. Army Corps of Engineers, 1990.

[5] FM 3-38 Cyber Electromagnetic Activities. - Headquarters, Department of the Army, 2014.

[6] Winks D. Preparing Critical Infrastructure for a Cyber-Electromagnetic Pulse Attack, AcquSight, GSX Infragard, 2018.

[7] FM 3-12 Cyberspace and Electronic Warfare Operations - Headquarters, Department of the Army, 2017.

AUTHOR'S BIOGRAPHY

Vladimir I. Gurevich, was born in Kharkov, Ukraine, in 1956. He received an M.S.E.E. degree (1978) at the Kharkov Technical University, named after P. Vasilenko, and a Ph.D. degree (1986) at Kharkov National Polytechnic University. His employment experience includes: teacher, assistant professor and associate professor at Kharkov Technical University, and chief engineer and director of Inventor, Ltd. In 1994, he arrived in Israel and works today at Israel Electric Corp. as a Senior specialist and Head of section of the Central Electric Laboratory.

He is the author of more than 200 professional papers and 15 books and holder of nearly 120 patents in the field of electrical engineering and power electronics. In 2006 he was Honorable Professor with the Kharkov Technical University.

Citation: *Vladimir Gurevich, Ph.D. (2019). "Cybernetic and Electromagnetic Impacts on Electronic Equipment: Do they have Anything in Common?". International Journal of Research Studies in Electrical and Electronics Engineering (IJRSEEE), 5(3), pp 36-40. DOI: http://dx.doi. org/10.20431/2454-9436. 0503005*