http://www.globalsecurity.org/wmd/library/congress/1999_h/99-10-07graham.htm

Statement of William R. Graham, Ph.D.

RESUME'

William R. Graham

1997-Present: Chairman of the Board and President of National Security Research, Inc.

1998-1999: Served as a Commissioner on the Congressionally-established Commission on the Ballistic Missile Threat to the United States (The Rumsfeld Commission) and is a former Chairman and current member of the Department's Ballistic Missile Defense Advisory Committee.

1994-1997: Senior Vice President of the Defense Group Inc., headed the corporate programs in counter-proliferation and other related defense activities. Served as a member of the Department of Defense's Defense Science Board Task Force on Theater Ballistic Missile Defense.

1990-1993: Chairman of the Defense Department's Strategic Defense Initiative Advisory Committee and member of the Defense Science Board.

1986-1989: Dr. Graham served as Science Advisor to President Reagan and was confirmed by the Senate to serve concurrently as Director of the White House Office of Science and Technology Policy. During that time he was also Chairman of the Federal Coordinating Committee on Science, Technology, and Engineering, which provides high-level coordination for federal research and development programs, and the U.S. Joint Telecommunications Resources Board, which is responsible for joint emergency telecommunications planning and operations between the federal government and U.S. commercial telecommunications companies. As Science Advisor, his responsibilities included developing and staffing presidential initiatives in science and technology, serving as a member of the U.S. Arms Control Experts Group that negotiated with the Soviet Union during U.S. - U.S.S.R. Ministerial and Summit meetings, and serving as counterpart to foreign ministers of science and technology. In the latter role he lead the successful negotiation of U.S. bilateral science and technology cooperation agreements with Japan, India, and the Soviet Union, as well as a multilateral agreement with the 24-nation Organization of Economic Cooperation and Development. He was Co-Chairman of the U.S. - China Council on Cooperation in Science and Technology, led U.S. delegations to the Organization of Economic Cooperation and Development's Science and Technology Minister's Meeting in Paris in 1987, and to Japan, India, and the Association of Southeast Asian Nations in 1988. He left government service as a Presidential Appointee at the end of the Reagan Administration to return to private industry.

1985-1986: Confirmed by the Senate to serve as the Deputy Administrator of the National Aeronautics and Space Agency. He left to become Science Advisor to President Reagan.

1**982-1985:** Dr. Graham was confirmed by the Senate to serve as the Chairman of President Reagan's General Advisory Committee (GAC) on Arms Control and Disarmament. At the President's request, Dr. Graham led the GAC in preparing the first and to date only comprehensive review and analysis of the Soviet Union's arms control compliance record. The report, issued in October 1984, was entitled **A Quarter Century of Soviet Compliance Practices Under Arms Control Commitments: 1958 - 1983**. He subsequently briefed the report to the President, the other members of the National Security Council, and to congressional committees involved in national security affairs. This report was instrumental in changing the focus of arms control from verification to compliance in the 1980s.

1971-1985: Dr. Graham was a founder of R&D Associates, a high-technology defense firm. He managed the largest of five divisions of RDA, and was Director of Computing Operations. As Division Manager, he was responsible for all aspects of the Defense Nuclear Agency (DNA) Base Contract, and oversaw research in all aspects of DNA's technical program. While at RDA, he also made technical contributions to the theory of nuclear weapon-generated EMP phenomenology, its coupling to military and civilian systems, and the design of strategic systems for surviving nuclear attack. Developed the method used by DNA to generate and measure EMP phenomenology and effects on underground nuclear tests. He left RDA to become Deputy Administrator of NASA.

1965-1971: Member, Professional Staff, Physics Department of the RAND Corporation, Santa Monica, California. While there he developed the theory of the nuclear weapon-generated EMP near the surface of the ground in the high overpressure region, including the Graham-Schaefer effect subsequently observed on underground nuclear tests, and developed a method for increasing the EMP output of high altitude nuclear explosions. He also conceived and designed the large-scale ARES high altitude nuclear EMP simulator that is still in use at Kirtland Air Force Base. He left to form RDA.

1962-1965: Served on active duty with the Air Force as a project officer at the Air Force Weapons Laboratory, Kirtland Air Force Base, Albuquerque, New Mexico. He was in charge of the first test of a military system (the NORAD 425L Combat Operations Center) to the EMP fields produced by an electromagnetic simulator, and managed a research group carrying out experimental and analytical EMP research. He left when he completed his tour of duty with the Air Force.

Honors and Awards include membership in Tau Beta Pi and Sigma Xi, and receipt of the Air Force Commendation Medal and the American Defense Preparedness Association's Strategic Defense Award.

Statement for compliance with Rule XI, Clause 2(g) of the Rules of the House of Representatives of the 106th Congress:

William R. Graham has not received any Federal grants, subgrants thereof, contracts, or subcontracts thereof during the current fiscal year or the two previous fiscal years, and he does not represent any entity in his appearance today before the House of Representatives.

Electromagnetic Weapons and their Effects on Electronics Systems

Mr. Chairman distinguished Members of the Committee on Armed Services, thank you for inviting me to testify today on the threats to U.S. civilian and military infrastructure from electromagnetic pulse attacks. Today, I would like to address the threat from both nuclear and non-nuclear electromagnetic weapons, and limit my prepared testimony to a brief description of the range of effects that such weapons can produce in modern electrical and electronics systems.

The Electromagnetic Pulse Generated by A High Altitude Nuclear Explosion (EMP)

I would like to begin with a few examples of the circumstances in which another nation might wish to employ a nuclear weapon-generated EMP effect against the United States, and the benefits sought through such use. The possible scenarios cover both political and military use, and run from the tactical to the strategic level.

Like many important scientific discoveries, the intense electromagnetic pule produced by an exo-atmospheric nuclear weapon explosion was discovered by accident. It was first observed both directly and by its effects on civilian systems during the last U.S. exo-atmospheric nuclear test series, code-named FISHBOWL, conducted above the Pacific Ocean in the early 1960s. The generation and effects of nuclear EMP have been studied and simulated since that time.

One possible use of EMP would be against U.S. forces stationed overseas, for example on the Korean Peninsula or in the Persian Gulf. By exploding a nuclear weapon over the theater, the ability of U.S. and allied forces to make full use of their electronic systems, including communications systems, fire control systems, radar systems, and certainly the networked systems envisioned for our 21st-Century forces, would be degraded to some degree. Depending on the yield of the weapon, the height at which the weapon was detonated, and the degree of EMP hardening enjoyed by U.S. and allied systems, such degradation could range from a nuisance to a major hindrance in the employment of electronic systems throughout the theater.

Another possible use of a nuclear weapon would be against U.S. space assets supporting military forces in a theater. The detonation outside the atmosphere of even a small nuclear weapon, perhaps a few tens of kilotons, would produce sufficient direct and delayed radiation to degrade or

destroy satellites in line-of-sight, as well as producing EMP near the earth's surface that would interfere with the satellite ground components. U.S. satellite assets are a significant part of our military's overall capability, providing communications, surveillance, on-demand intelligence and database access, and GPS data. Interruption of satellite availability thus could pose a serious problem to our regional warfighting capability. A logical use of this option would be to disrupt U.S. satellite systems immediately prior to an adversary's attack on a U.S. ally, or to interrupt an impending U.S. attack.

Another possibility would be the use of EMP because an adversary does not have confidence in its ability to target precisely a U.S. asset. For example, an adversary might not be able to pinpoint a carrier battle group or amphibious ready group, but could produce an EMP effect over the presumed operating area of the group. The same approach could apply to an Army formation on the ground. Another possibility might involve an adversary with a long-range but relatively inaccurate ballistic missile, or a short-range ballistic missile mounted on a ship or submarine, and a relatively low-yield nuclear weapon. In this case, the weapon could more confidently be used for an EMP attack than a direct attack.

Another reason for employing EMP would be simply to demonstrate that the nation had both functional nuclear weapons and the ballistic missile capability to deliver those weapons. This demonstration might be sufficient to dissuade U.S. intervention in a region, to coerce regional allies into denying U.S. access to their facilities, or to weaken the coalition-building efforts of the United States in a regional crisis. One can easily imagine the effect an Iraqi nuclear demonstration might have had on our country, our allies in the Persian Gulf, and the Coalition nations that assisted our efforts to liberate Kuwait in 1990-91.

It should also be pointed out that a direct nuclear attack on U.S. forces could reasonably be expected to result in an overwhelming U.S. response, making EMP use a more attractive option for an adversary. If EMP use did not result in any U.S. or allied casualties, it might be safer for the adversary nation than a direct attack. Given the United States' greater reliance on sophisticated electronic systems throughout our military and civilian infrastructures, and the strong taboo against nuclear weapons use built up over a half-century, even our ability to respond in kind with an EMP attack would be problematic. These are just examples of possible EMP employment, but I believe they demonstrate the range of utility of an EMP attack to a U.S. adversary.

Finally, I would like to mention an aspect of the effect of nuclear EMP that is unique. While all electronics systems can fail spontaneously for a myriad of reasons, in the case of a reliable system these failures occur infrequently and even then only at single points. Therefore, experience is gained in dealing with single point failures during the normal operation of the systems. However, since the nuclear EMP from a single exo-atmospheric detonation covers a wide area of the ground and the atmosphere above it, nuclear EMP can produce electronic system failures at many widely distributed points simultaneously. Unless special nuclear EMP recovery preparation and training has been implemented, system operators will have no experience with recovering the system from simultaneous, widely distributed, nuclear EMP-induced multiple failures, and will have to discover how to do so at a highly stressful time.

Non-nuclear Electromagnetic Weapons: High Power Radio Frequency and Microwave Devices

Turning next to non-nuclear electro-magnetic weapons and their effects, there are again several characteristics of such weapons that could make them attractive to an adversary. Most such weapons are high-power, pulsed radio-frequency devices. They require varying degrees of technical competence to build, but can be as small as a briefcase or as large as a school bus, depending on their desired output.

Radio-frequency weapons, or RF weapons, have the potential disadvantage of requiring closer proximity to their targets to be effective than do nuclear EMP weapons. For example, a small RF device might have a range measured in feet, while a relatively large RF device might produce upset or damage in electronics systems at a range measured in hundreds of feet, and interference at a range of hundreds of miles. However, RF weapons are more suitable to covert use than are nuclear EMP weapons. A targeted asset may not realize that its problems are the result of an RF attack, or that an RF attack has taken place at all.

If used simultaneously against multiple sites, RF weapons could cause confusion and slow restoration efforts. The ability to use RF weapons selectively and intermittently, as well as the ability to disguise them as ordinary objects, could allow adversary covert operatives to interfere with U.S. or allied systems in a more controlled manner than a nuclear EMP attack.

Finally, RF weapons provide an opportunity for their users to escape detection and capture, and potentially can be used repeatedly against U.S. assets. A truck-mounted RF weapon, for example, likely would be large enough to act from a distance, and mobile enough to have a reasonable chance of escaping.

It should be noted that RF weapons are not as damaging over a large area as nuclear EMP weapons. However, in regard to the specific target against which they are employed, RF weapons can produce effects ranging from temporary interference, to the need to shutdown and re-start the system, to physical disablement of the targeted system by literally fusing or melting sensitive internal components. Especially due to their greater applicability for covert use within the United States, they must be given serious consideration.

Research on such devices has been underway in the U.S., Russia, and elsewhere for several decades. While the nuclear EMP from a single exo-atmospheric detonation can cover large areas of the country with intense electromagnetic fields, non-nuclear electromagnetic generators can use pulsed and continuous wave electromagnetic fields to expose systems to disruptive effects more surgically from distances that range from direct contact to several hundred miles. The following summarizes the type of effects that both nuclear and non-nuclear electromagnetic weapons can produce.

Types of Electromagnetic Weapon Effects

At the lowest electromagnetic field strengths, there is the complex world of electronic warfare (EW), which involves the non-nuclear generation and transmission of narrow to moderately broadband electromagnetic signals designed to interfere with or spoof enemy receivers. Examples include continuous wave (CW) jamming enemy transmission channels, spoofing enemy fire control radars, and blocking GPS receivers with locally generated signals. EW is a well-established field.

As non-nuclear electromagnetic field strengths increase, carrier and modulation effects, usually involving CW electromagnetic field interaction in ways not envisioned in the design of the system, come into play. In addition to pickup on deliberate system antennas, the most likely coupling mechanism of these signals and those in the following three paragraphs is pickup on other conductors extending from the core of the system and acting like electromagnetic antennas. Examples of these effects include use of a CW carrier with audio modulation picked up on telephone lines attached to a computer, rectified, and interpreted as a telephone control signal; and the penetration of a microwave electromagnetic signal into a missile, where it is rectified and interpreted as a missile guidance and navigation command.

Electromagnetic field levels of sufficiently high amplitude to induce signals comparable in size to the normal signal levels in a digital system, injecting anomalous bits, corrupting data and/or producing system upset. Electromagnetic weapons can cause system upset by inducing pulses, on either external or internal signal lines, that digital systems interpret as proper binary signals, but which in fact corrupt digital information. Well designed systems anticipate noise in transmissions on external signal channels, and when these anomalous bits occur on such channels, for example telephone lines, they will usually be rejected; but when the anomalous bits are picked up by internal signal lines, such as computer mouse wires or hookup cables, they are usually interpreted as system signals and processed accordingly, resulting in data corruption and/or system upset. Upset may not cause permanent damage to the electronics hardware in the system, but often requires manual intervention to reload and restart the system, and data recovery or replacement to remove the corruption. Examples of this effect include computer lockup (which can be as benign as to only require rebooting in a PC or as fatal as complete system loss if it occurs in a missile guidance computer in-flight), and mis-routing of digitally switched communication channels that are being connected when the pulse arrives.

At electromagnetic field levels higher than those required to cause digital upset, signals induced on conductors can lead to semiconductor junction breakdown followed by system power supply-induced permanent damage. Electromagnetic weapon pickup "antennas" include power lines, communication cables, computer network cables, and computer peripheral cables. In this case, the electromagnetic weapon-induced signals do not contain enough energy to damage the system, but rather act as a triggering mechanism by breaking down a semiconductor junction that is in a reverse bias (and therefore high impedance)

state. A system power supply or other stored energy source then provides the much larger amount of energy that damages the junction by driving substantial current through it in the reverse direction. Circuits where this type of failure can occur are usually located near external interfaces, and include power supply rectifier diodes, telephone line modem interfaces, and PC peripheral line interfaces. These triggering effects require additional sources of energy beyond the electromagnetic weapon, and therefore occur only when the system is powered.

Finally, at still higher electromagnetic field levels, there are direct electromagnetic power-induced thermal effects, which can damage systems even when the system power is off and no sources of stored energy are present. These effects use the energy in the electromagnetic field to drive enough power into circuits for sufficient times to damage semiconductor junctions or other sensitive devices. As in the above cases, circuits at or near external conductor interfaces (that is, attached to electromagnetic pickup "antennas"), are the most likely to be subject to these effects. Such effects do not require other sources of energy, and therefore can occur when the system is unpowered as well as when powered. Examples of these effects occur when unpowered electronics components are placed near the source of the beam of a high-powered radar or are placed near a high amplitude pulser, such as a nuclear EMP simulator, or when directly exposed to nuclear EMP itself without benefit of electromagnetic shielding or other protection.

The effects described in paragraphs 1. and 2. above are produced primarily by CW non-nuclear electromagnetic sources, and the affected systems' electronics usually return to normal operation when the electromagnetic field is removed if the response of the system has not induced some consequent damage, such as a jammed GPS system causing an aircraft to crash.

The effects described in paragraph 3. are usually produced most efficiently by a pulsed field source, such as an ultra-wideband non-nuclear source or a nuclear EMP, since it is the introduction of individual pulses in a digital system that causes the system upset. In the first three cases, if the system survives the consequent effects of the electromagnetic-induced malfunctions, removal of the fields will leave the system hardware undamaged, although in the case of paragraph 3., the software and/or data may be permanently corrupted.

The permanent damage effects described in paragraph 4. are also usually produced most efficiently by a pulsed field source, since a single pulse can initiate the breakdown process. In the case of the permanent damage effects described in paragraph 5., either CW or pulsed electromagnetic fields can produce the effect. (End of Statement)