By Les Simmonds

Electronics – RF Weapons

In an earlier issue of Security Electronics Magazine (SEM) we highlighted the security threat of High Power Microwave (HPM). Now three years later and with the world reeling from a massive terrorist attack in the USA, I thought it might be appropriate for SE&N to revisit HPM which is an effective terrorist and extortionist tool.

HPM is sometimes called a directed energy weapon. HPM uses high power microwave energy to disrupt victim electronic systems. HPM energy is aimed at the victim by using a directional antenna, similar to that used by radar. Another similarity between HPM and radar is the inability for a target to tell it is being "illuminated" without special detectors.

HPM technology was merely a theoretical possibility until the 1970s. In the last thirty years advances in plasma physics, energy storage and fast switching devices have made HPM systems effective and the technology is migrating outside classified government research and development laboratories.

Since the technology is relatively new, and was closely guarded until the demise of the Soviet Union, the societal ramifications of HPM have received little analysis. Within the past few years non-military applications have been sought for HPM and these applications are often referred to as "non-lethal technologies." One such employment is the use of HPM by police to disable automobiles in a high-speed chase. Discussions have further highlighted the capability of HPM and presumably raised the general awareness of the technology capability.

The most widely acknowledged effect of HPM energy is disruption of electronic systems. This perturbation is extremely short in duration, generally in the order of a few hundred nanoseconds. This brief disturbance can be sufficient to reset computers, cause complete loss of stored data and/or cause microprocessors to switch operating modes.

Advanced electronic systems are increasingly vulnerable to upset by electromagnetic radiation. Many overseas defence studies indicate Radio Frequency (RF) power is a threat to the proper operation of modern systems. As circuits have become more densely packaged, more energy efficient and operate at higher speeds they have experienced an associated increase in vulnerability and susceptibility to radiation.

This vulnerability to RF power has started international research in optimising transmitters for use as weapons. NATO and former Soviet nations have apparently developed HPM weapons and these weapons are designed to exploit this inadvertent vulnerability to RF power by concentrating as much power as possible into a controlled field.

The effects of a successful HPM weapon attack are unpredictable. The primary goal is merely disruption of the victim system, the results of which are of secondary importance. Consequently, the result varies widely depending upon the victim system. In some cases computers may be reset while in other cases, local oscillators may be driven off frequency, navigation systems misguided, safety sensors incorrectly set or reset, faulty data recorded and control systems given erroneous inputs.

The significance of the perturbation is proportional to the importance of the system corrupted. A portable compact disc player may react by garbling music or changing the track it was playing. A similar amount of energy directed at a commercial aircraft could corrupt the aircrafts control and navigation systems enough to cause a crash.

Another important similarity shared by vulnerable systems involves post-attack evidence. Typically, there is none although the perturbation of the victim system is indisputable while subjected to the electromagnetic field the affected circuits are rarely permanently damaged. This makes identification of the cause extremely difficult. Failures appear to be anomalies with no traceable cause. An interesting aspect of a successful HPM weapon attack is that no evidence remains to incriminate the perpetrator.

Another feasible effect of an HPM attack, under proper conditions, is an unexplained explosion. The ability of electromagnetic energy to create a spark is undisputed. Inadvertently leaving a metal "twist tie" on a package placed in a common microwave oven can present impressive evidence of this phenomenon. An even more impressive proof can be achieved by filling the oven with an explosive vapour before activating the magnetron with the twist tie in the oven. Whether there will be resulting evidence of a microwave-induced spark causing the resulting explosion is arguable.

Other experiments familiar to scientists and technicians further prove the ability of microwave energy propagating through space to transform to other forms of energy. Tossing steel wool into the main lobe of search radar's antenna can produce a spectacular explosion. Fluorescent light bulbs can be lit without any wired connection at a considerable distance from a radar emitter.

After transoceanic flights, airliners often have more vapour than fuel in their tanks. These tanks also have conductive wiring harnesses inside the fuel tanks and if any of the wires immersed in this explosive vapour has an imperfection resulting in a sharp point, all the conditions are set for an HPM induced spark resulting in an unexplainable explosion. The origin of such an explosion would likely be impossible to discover from residual evidence.

Conditions similar to these were present when TWA 800 exploded shortly after takeoff in 1996. The centre fuel tank contained mostly vapour for reasons based in weight and economics. Although the reason the fuel tank exploded has not been determined, investigators are certain that the forces of that ignition made the incident un-detectable. This has resulted in consideration within the aviation regulatory community of prohibiting the common practice of flying aircraft with mostly empty fuel tanks. Such a regulation might mitigate the risk on take off, but does not address the situation of tanks emptied in flight.

Most HPM experts acknowledge that at the end of the Cold War the Soviet Union was ahead of Western laboratories in the development of HPM weaponry. This is logical since Western weapon systems (planes, missiles, etc.) tended to be more sophisticated than their Soviet bloc counterparts. Since HPM vulnerability tends to be proportional to a victim system reliance on microprocessors, the technology would be more attractive to NATO adversaries. Implementation of HPM against sophisticated weaponry transforms that sophistication from an asset to an "Achilles heel".

With the demise of the USSR the research and the scientists who performed it became less well controlled. This is particularly alarming since, unlike traditional weapons of mass destruction, there are no controllable components in an HPM weapon.

1995 saw the first known use of HPM technology by subversives. Chechnya rebels used HPM to defeat a Russian security system and gain access to a controlled area.

Traditional means of improving security are ineffective in preventing an HPM attack. HPM attacks use invisible electromagnetic energy as "ammunition". This implies speed of light velocity, a very "deep magazine", and an effective range that is limited only by the weapons effective radiated power and the victim system susceptibility.

It is generally unnecessary for attackers to expose themselves to the secure environment provided by traditional security measures. They can instead remain outside the sterile environment and still disrupt electronic systems a great distance away. While there are many variables that must be considered to determine the range of an HPM weapon a reusable system able to disrupt systems hundreds of meters away is certainly achievable.

The important point is that a clandestine attack can be mounted using HPM without having to breach or even account for existing security systems. A less obvious result is that there is very little risk involved in unsuccessful attacks or "dry runs." Unlike traditional attacks, precise execution and planning is unnecessary and tactics can be tested and refined until the perpetrators achieve the desired effect.

These weapons have proven successful against a wide range of victims. The vulnerability of an electronic system is directly proportional to its degree of sophistication and use of modern microprocessor technology. For example, while antiquated systems using vacuum tubes are almost impossible to victimise using HPM modern computers are easily disrupted.

The importance of the victim system, and therefore its attractiveness as a terrorist target is dependent on its intended purpose. Causing a malfunction in a sophisticated video game may annoy the player but will be of little value to a subversive. On the other hand, interfering with Government and/or Financial Institutions computers and critical control systems in aircraft will have more catastrophic results.

The recent publicity of disruption in aircraft navigation and control systems by passenger's laptop computers highlights the vulnerability of these systems to non-ionising radiation. The press further amplified the public awareness of the ability to disrupt modern aircraft without leaving any residual evidence and articles published in open literature have discussed the effects of RF emissions on airliners.

There has already been at least one crash whose cause cannot be explained by the US National Transportation Safety Board (NTSB). Data published by the NTSB is consistent with an attack using this new weapon. Besides the crash of United Airlines 585, the NTSB suspect high power RF energy may have caused several sudden and dramatic disruptions of aircraft autopilot systems.

HPM represents unique opportunities for subversives. Reusable systems used against an airliner can produce a "virtual windshear" on demand. Single shot expendable systems can produce "virtual lightning strikes" over a large geographic region. In either case, modern electronic systems are vulnerable to catastrophic disruption.

For centuries, security systems have concentrated on exclusion and detection of intruders. Sophistication has ranged from moats with drawbridges to infrared and laser motion detectors and other sophisticated detection devices. In today's world, intrusion detectors and other modern security devices may become as antiquated as the moat without supplemental detection of electronic attacks.

The technology to launch an HPM attack exists and is cost effective and easily obtainable. The security industry must consider appropriate detection for this threat. Until such detection technology is deployed, the opportunity endures to wreak tremendous havoc without fear of identification or recrimination – the perfect crime!

While researching this article I found the following US Navy Expression of Interest on the Web:

The U.S. Navy is interested in exploring the use of High Power Microwave (HPM) techniques and technologies for purposes including anti-ship missile defence (ASMD) and command and control warfare (C2W). The Naval Research Laboratory (NRL) is encouraging joint proposals wherein the project would be executed in an NRL/contractor team format to get the maximum amount of research in the most efficient manner. These proposals for research and development into HPM techniques and technologies may include, but not be limited to:

(1) Wideband (narrow-pulse) HPM sources. The sources of interest range from compact, lightweight devices that may be conventionally or explosively driven to larger, higher voltage devices that are suitable for shipboard installation. Marx generators are one example of several technologies being sought.

(2) Narrowband HPM sources. The sources of interest are generally high duty, relatively long pulse transmitters. Very high peak power, high average power, and high efficiency are all desirable.

(3) Innovative conventional and non-conventional HPM based electronic attack
(EA) techniques and systems including anti-missile defence applications, special operations command applications and C2W applications.

(3) NRL more favourably will consider proposals offering initial increments comprised of short-term studies (6-8 man-months) which then can be used to decide if the research deserves further investment.

HPM is an ideal tool for terrorists. It presents a combination of (a) a proven vulnerability in one of terrorists' favourite targets-airliners; (b) ground based systems can allow a non-suicidal attack; and (c) cause of the attack cannot be identified.

Restrictions of personal electronic devices (PEDs) during approach and takeoff advertise when the aircraft is at greatest risk. Coincidentally, it also represents the terrorist's greatest opportunity. If on board systems are affected by inadvertent PED emissions of fractions of watts, an attack focusing billions of watts on the plane may also disrupt the systems.

As aircraft become more advanced their vulnerability increases. As aircraft electronics become more integrated with the actual control of the plane the results can be more catastrophic. Boeing claims that their 757 can take off, fly to its destination and land itself without pilot intervention if necessary. A single screen has mostly replaced the plethora of gauges formerly found in the cockpit.

On board computers decide what information the pilot needs to see displayed on the screen. The moment-to-moment decisions in flying the plane have been shifted to the built-in electronics. Disrupting these systems can cause the plane to execute erroneous commands resulting in a crash. Jets manufactured by Airbus are even more advanced, with computers overriding pilot decisions in many cases.

Laptop computers, portable video games and other electronics (PEDs) used by passengers in flight have been linked to flight control anomalies. Similar to an attack, no evidence of the disruption remains for analysis after the interfering signal stops and this has made locating failures very difficult. Cockpit personnel have resorted to going through the cabin and asking individual passengers to turn off their computers and games. Correlating the aircraft's return to normal operation with the disabled carry-on has been the most powerful tool in identifying the source of the problem.

During approach and takeoff, vulnerability is increased by low airspeed and altitude. Pilots have less time to react to system failures and have fewer options. During this critical phase the planes are over uncontrolled ground and at close range, providing terrorist access.
Washington's National Airport presents a prime example of a terrorist target. Many aircraft approach the airport along the Potomac River. As they pass over the Francis Scott Key Bridge they have altitude and airspeed consistent with final approach. The banks of the river, as well as the Key Bridge, are uncontrolled. The bridge has several traffic lanes and pedestrian lanes on both sides. The river offers an unobstructed view of approaching aircraft from many vantage points.

A terrorist can set up a portable RF Weapon on the bridge or riverbank attacking planes as they pass over. If successful, the victim aircraft may suddenly and inexplicably fall into the river. A successful attack will result in a crash leaving no evidence of sinister involvement.
Since the terrorist is able to remain on the ground and out of the sterile environment of the airport he can conduct his attacks without risk of injury or apprehension. The lack of residual evidence is critically important to terrorists. It increases the probability of success for subsequent attacks, since potential targets will not be able to identify the risk against which they must protect themselves. At the same time, it decreases the probability of apprehension during any attack.

Presidents of the USA have sent strong messages to subversives, in the form of air strikes and cruise missile attacks, that the United States will not tolerate terrorism. An unintended message was also sent, that if one is to attack US interests, there must not be residual evidence linking them to the crime. RF Weapons provide the insulation of deniability.

The most recent outbreak of terrorist activity has been based more on religion than nationality. Some religions view the United States as "The Great Satan." Unattributable catastrophes affecting U.S. assets can be very useful when linked to an angry deity.

By then publicly predicting another such attack, perhaps at a different airport and as a prophecy of their deity, the terrorist organization achieves their primary goal. They will have caused societal panic. The ripple effects of crippling commercial aviation will be international. There will be no way to prevent future attacks or even know when they have occurred apart from the catastrophes they cause. The world will be hostage.

Acknowledgements:

A. Pevler – Texas Engineering Solutions

C. Coop - Department of Computer Science Monash University

Les Simmonds is an independent CCTV consultant.

Email:
les@cctvconsultants.com.au

Web:
www.cctvconsultants.com.au

This article was originally published in Security Electronics and Networks Magazine Australia.