CRITICAL INFRASTRUCTURES

The Threat of

RADIO FREQUENCY WEAPONS

TO

CRITICAL INFRASTRUCTURE FACILITIES

TSWG & DETO Publication:
August 2005

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
AUG 2005		**00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
The Threat Of Radio Frequency Weapons To Critical Infrastructure Facilities	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Naval Surface Warfare Center,Dahlgren Division,17320 Dahlgren Road,Dahlgren,VA,22448**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

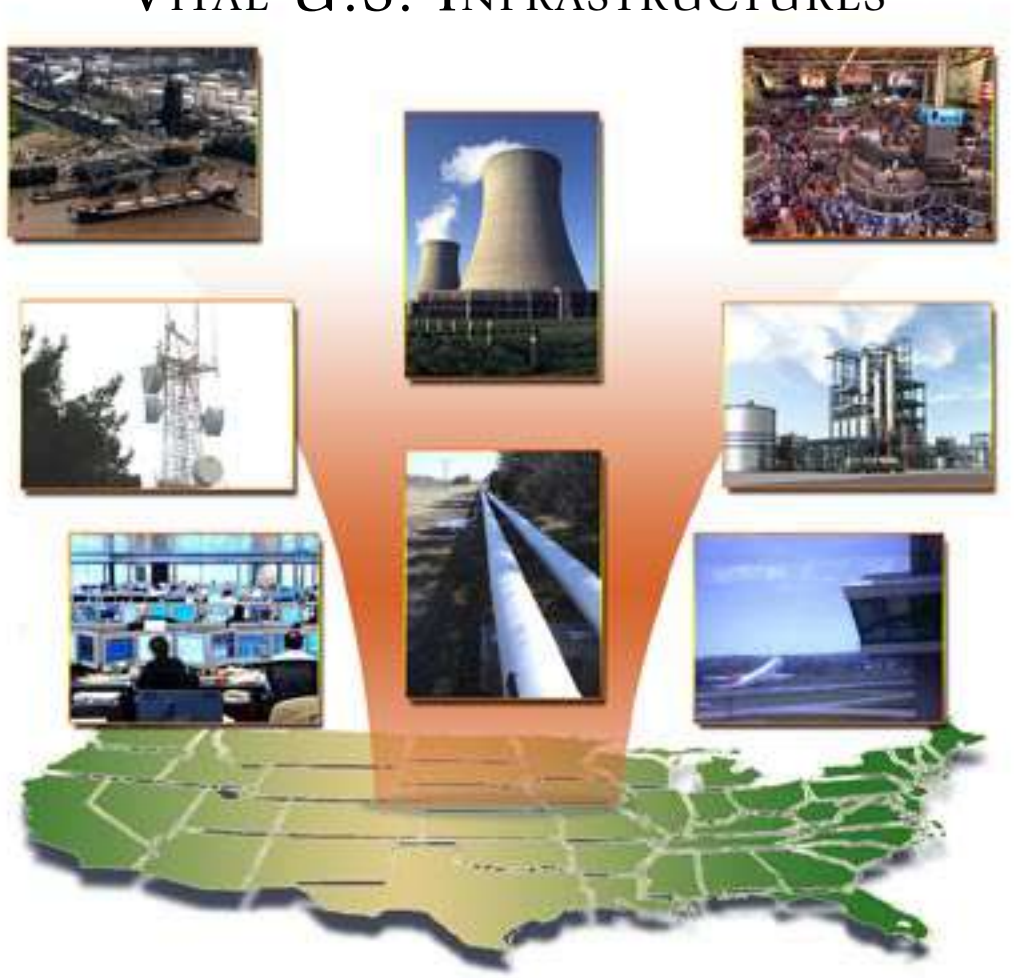
14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**13**	

Contents

Vital U.S. Infrastructures



Threat of Radio Frequency Weapons to Critical Infrastructure Facilities

Critical infrastructure facilities, as pictured above, support all facets of modern day life in the United States. By definition, they are the "...systems and assets...so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." [Section 1016 (e), U.S.A. Patriot Act of 2001] Critical infrastructure facilities include electric power facilities, oil refineries, water treatment plants, banking systems, pipelines, transportation systems, and communications facilities. Most critical infrastructure facilities depend on electrical and electronic systems to function. These systems can be susceptible to a little-known, yet significant and growing threat called ***radio frequency weapons (RFWs)***.

The President of the United States proclaimed it a national goal that "…the United States shall …[achieve]… and shall maintain the ability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of: the Federal Government to perform essential national security missions and to ensure the general public health and safety; state and local governments to maintain order and to deliver minimum essential public services; [and] the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services." [Presidential Decision Directive / NSC-63, dated May 22, 1998]

RFWs have already been used to defeat security systems, commit robberies, disable police communications, induce fires, and disrupt banking computers. Improvised RFWs have been demonstrated to jam satellites, cause a catastrophic failure in a locomotive and damage automobiles. Devices that can be used as RFWs have unintentionally caused aircraft crashes and near-crashes, pipeline explosions, large gas spills, computer damage, medical equipment malfunctions, vehicle malfunctions such as severe braking problems, weapons pre-ignition and explosions, and public water system malfunctions that nearly caused flooding.

What Are Radio Frequency Weapons?

Electromagnetic radio frequency (RF) emitters are common in everyday life. They work by sending invisible electromagnetic energy into the air or down a wire. RF emitters are used in a variety of applications, including wireless communication, navigation (e.g., Global Positioning System), radar, etc. Some familiar examples of RF emitters include broadcast radio transmitter towers, cellular phones, two-way radios, microwave ovens, weather radars, police radars, cable television, and local area networks. It is possible for electromagnetic energy from an emitter to adversely affect electronic devices not designed to work with the emitter. This is called Electromagnetic Interference (EMI). A common example of EMI is when a two-way radio, such as a walkie-talkie, transmits a signal near a television. The radio signal can be received through the television's antenna, distorting the picture and masking the sound with the radio operator's voice.

Figure 1 - Example of a Radio Frequency Weapon

Radio frequency weapons (RFWs), such as that shown in Figure 1, are devices that produce and emit electromagnetic energy for the purposes of intentionally disrupting or damaging the targeted electronics. Some RF emitters that are designed for non-hostile applications, such as radars and microwave communication transmitters, can be used as RFWs, if the intent is to cause disruption or damage.

Radio Frequency Weapons produce electromagnetic energy for the purpose of disrupting and/or damage electronic systems.

What Can RFWs Do to Infrastructure Facilities?

RFWs can damage electronics (see Figure 2) and/or cause them to malfunction, even in ways that compromise built-in, fail-safe mechanisms. The impact of the malfunction depends on what equipment is affected, how it is affected, when it is affected, and what function it is performing. If the affected electronics control critical processes, the impact may be significant, resulting in economic loss, reduced defenses, and infrastructure facility downtime.

For example, utilities and manufacturing facilities have become increasingly reliant upon automated control systems such as supervisory control and data acquisition (SCADA) systems and distributed control systems (DCS) to monitor, control, and regulate their processes. These automated control systems are basically composed of various electronic subsystems including a master computer called a Master Terminal Unit (MTU), a remote processor/controller called a Remote Terminal Unit (RTU), communications using wireless radio or telephone lines, electronic sensors (pressure sensors, current meters, etc.), and electronically controlled actuators (e.g. valves, circuit breakers, etc.) and relays, as shown in Figure 3. RFWs can potentially be used to affect any of these electronic devices and produce effects such as unintentional valve closures, disabled communications, false data transmissions, and damage to the electronic device itself. Further complicating matters, the data displayed on a control monitor (Figure 4) may

Figure 2 - Integrated Circuit Damage Caused by an RFW

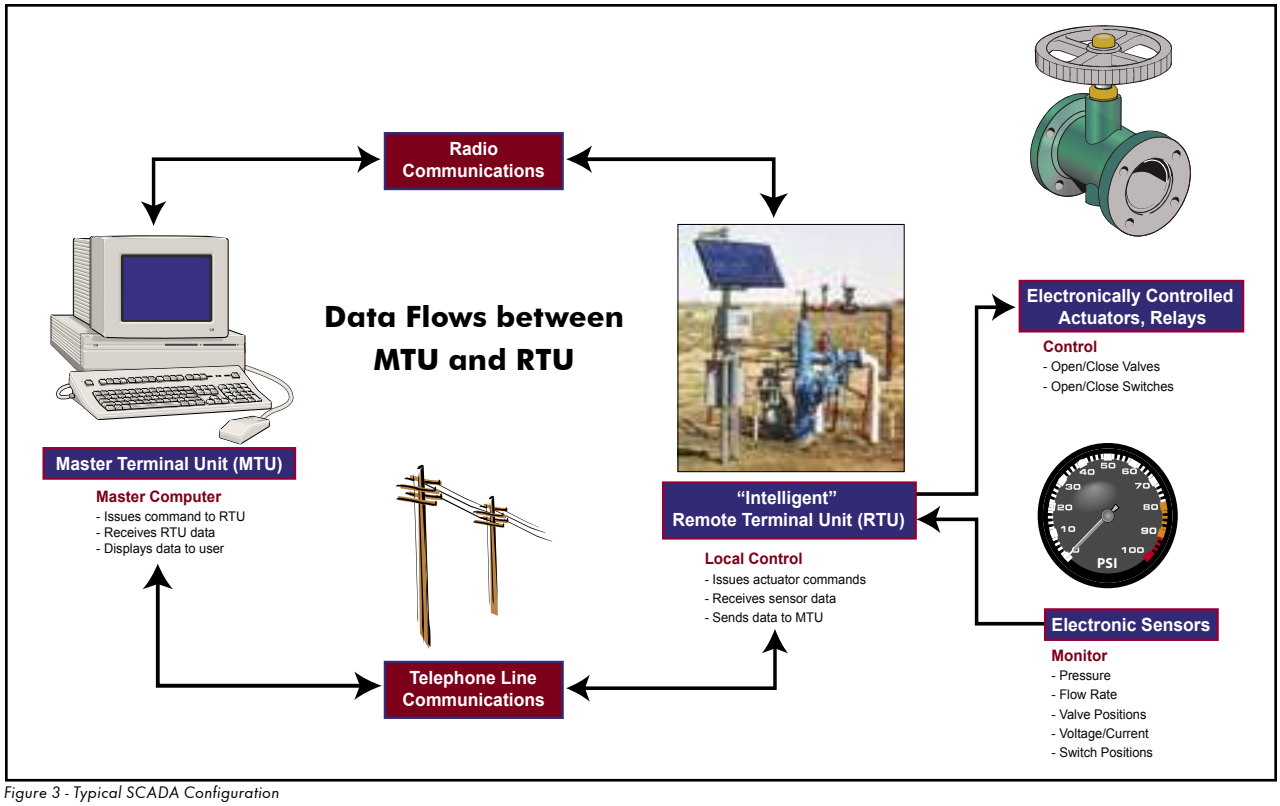


Figure 3 - Typical SCADA Configuration

not reflect the actual state of the system, which may hamper the operator's ability to correct the problems. Impacts from such effects can range from nuisance (e.g. having to send a technician to a remote site to reset equipment) to catastrophic (e.g. gas pipeline ruptures/explosions and mass electric power outages).

Other examples of how RFWs could be used to adversely affect critical infrastructures include disabling flight control systems for commercial aircraft, leading to loss of aircraft control and crashing; disruption of critical computers used for banking, stock exchange transactions, traffic light control, and train coordination; disabling security systems to hide a larger attack; and disrupting emergency communications.

Anything that uses electronics can potentially be affected by an RFW!

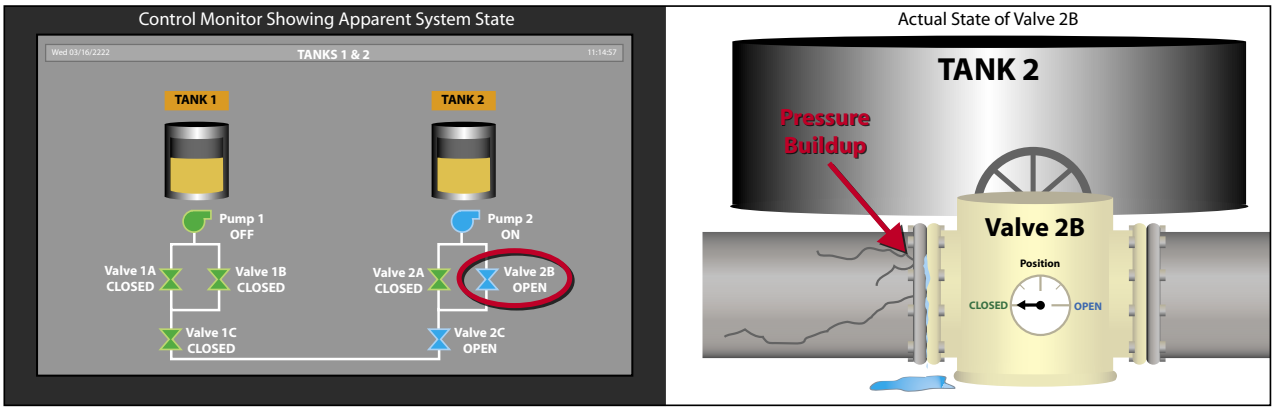


Figure 4 - Example of a Control Monitor Displaying Incorrect System State Caused by an RFW

How Might RFWs Be Used Against a Facility?

RFWs transmit electromagnetic energy in one of two ways: (1) radiation, which is the process of broadcasting a signal through the air using an antenna (see Figure 5), or (2) conduction, which is the process of transmitting electrical energy through a wire, such as a power line or a telephone line (see Figure 6). In either case, the energy can be transmitted continuously over a long period of time or transmitted in a burst over a short period of time.

If the RFW is a radiation threat, the transmitted electromagnetic energy can be received by the target, or by antennas and wires connected to it, and cause disruption or damage to the targeted electronics. A common example of radiated EMI occurs when cell phones are used in close proximity to computers. Typically, this causes distortion/interference effects on the monitor. Real RFWs are significantly more powerful and can cause more serious effects.

RFWs can easily be disguised in ordinary packages and they can be used in a variety of ways.

The electromagnetic energy from a radiated RFW can enter a facility by penetrating through walls and other barriers. Openings, such as windows, in the barriers will generally allow more energy into the facility. Typically, the more barriers, such as walls, that the electromagnetic energy has to penetrate, the harder it will be for the RFW to affect the targeted electronics. Another important factor for the radiation threat is that the energy from an RFW dissipates with distance, so the farther away an RFW can be kept from the facility; the harder it will be for the RFW to affect its target. Examples of radiated RFW use are provided on page 7.

If the RFW is a conduction threat, the attacker may connect it to a cable, such as a power or communication line, that leads into the facility. The RFW can discharge large surges of electrical energy into the line, which may enter the targeted equipment through its connection to the line and cause disruption or damage. A well-known example of conduction interference is seen on a television when a vacuum cleaner is operating. The vacuum cleaner introduces unwanted electrical noise through the power cord. The noise enters the television through its power cord and causes "snow" in the picture and audio noise in the sound. A real RFW source, such as that used in the Russian experiment described on page 8, can damage electronics.

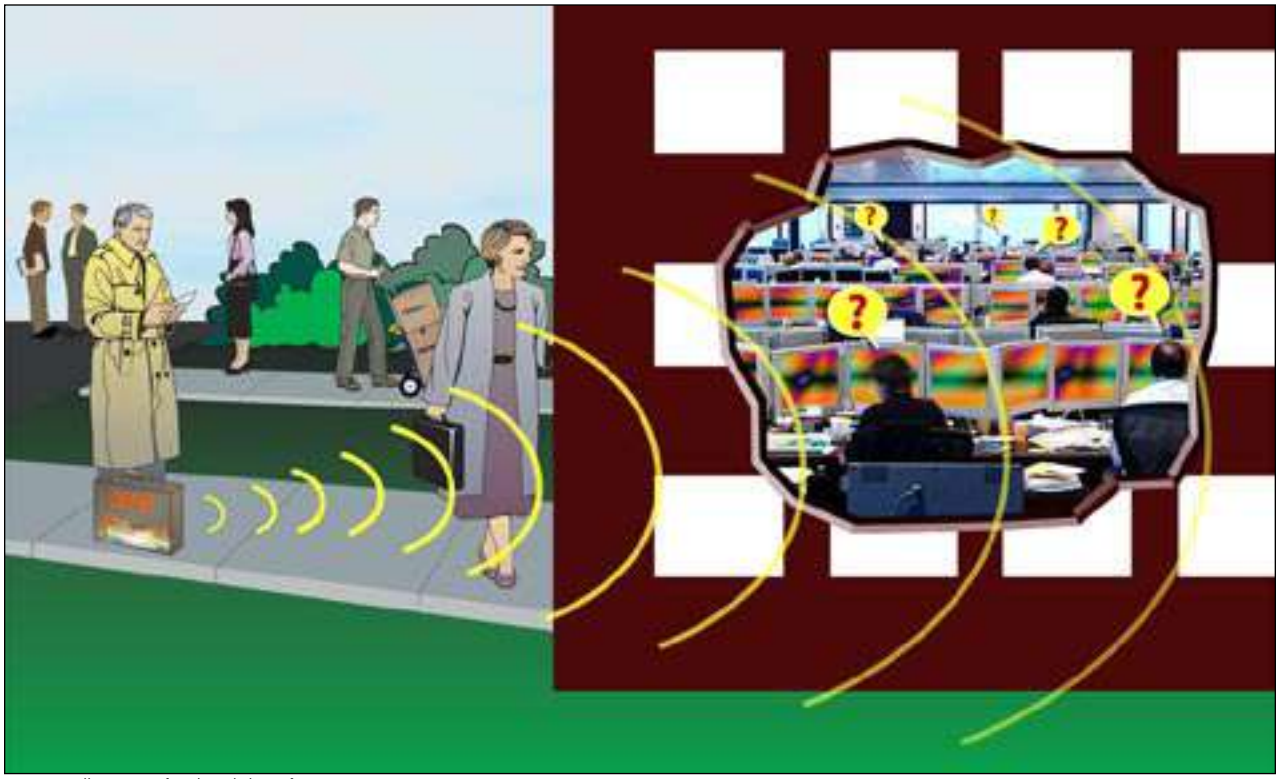


Figure 5 - Illustration of Radiated Threat from an RFW

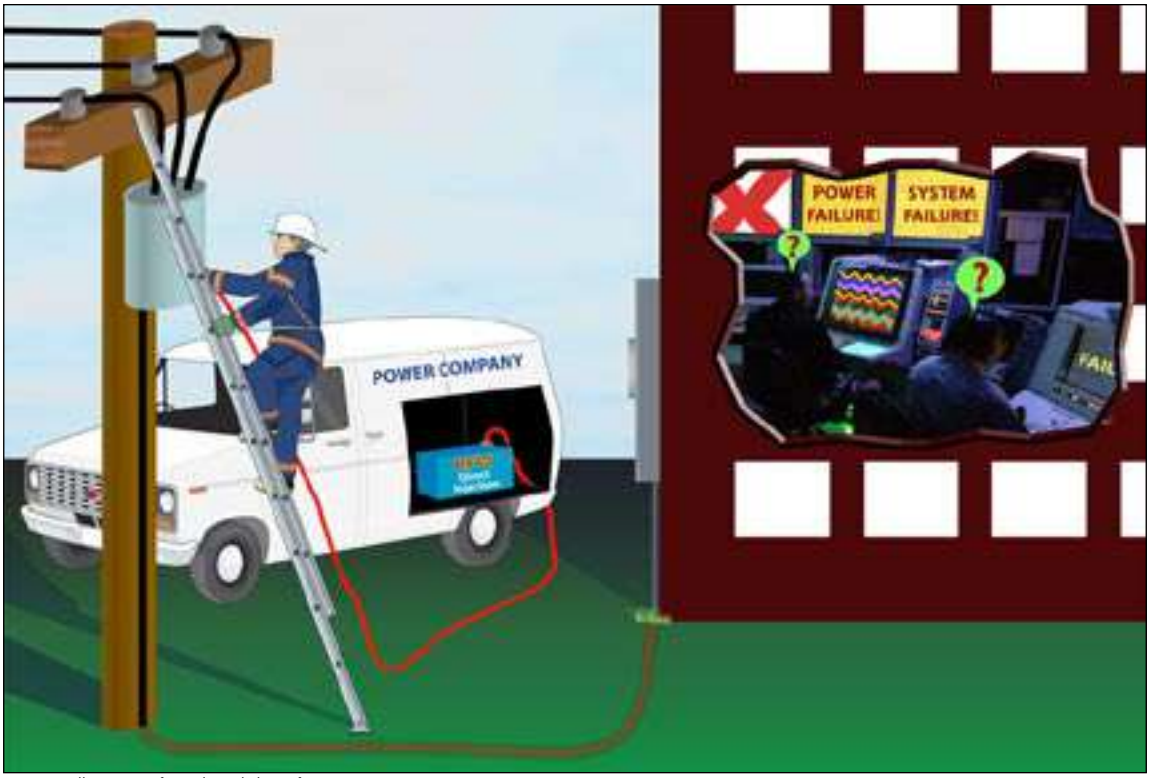


Figure 6 - Illustration of Conducted Threat from an RFW

RFW Sizes, Packaging, and Employment

RFWs can vary in size from a hand-held device to a large vehicle-born device. RFWs can be hidden in a truck, a briefcase, or even a package as small as a soda can (Figure 7). Small RFWs can be smuggled into a building with relative ease using inconspicuous packaging and then left behind. Large RFWs can be placed outside the facility, disguised as a utility truck, delivery truck, commercial vehicle, or even a small pickup truck. The presence of the RFW may go unnoticed for an extended period of time, well after the attacker has left the facility.

RFWs can be used to cause damage or to cause intermittent, temporary effects, such as locking up a computer or corrupting a data stream. If the computer is controlling an important process during a critical period, a "temporary" result could still lead to catastrophic impacts.

Figure 7 - RFW Hidden in Inconspicuous Packages

Truck-mounted RFW

Why Would an Attacker Use RFWs?

Attackers may choose to use RFWs over conventional weapons (i.e., explosives) for several reasons. Some of the most prevalent reasons are:

- ***Covert***
  Attacks can be carried out with little or no trace left by the attacker. Often, the only knowledge that the victim has is that their electronic systems suddenly stopped working properly—or entirely. The victim may not even realize that they had been attacked.
- ***Remote***
  Attacks can be initiated at a distance from the target (called stand-off distance). This may be useful if the attacker cannot get to the target. It also helps an attacker avoid suspicion and provides a head start for a get-away.
- ***No Ammunition Required***
  Unlike conventional weapons, RFWs do not require ammunition or separate rounds for multiple shots. RFWs require a power source, which is typically what limits its usage.
- ***Penetration***
  RFWs energy can penetrate walls and go over/around obstacles.

- ***Area of Coverage***
  Attacks can cover a broad or narrow area, depending on how the energy is focused. If the energy is focused on a broad area, such as a whole building, many targets can be attacked simultaneously.
- ***Instantaneous***
  Target exposure and effects occur immediately after transmission because the RF energy travels at the speed of light. As a result, exposure can be timed to a specific instant. For example, if the attacker has the intelligence, an attack could coincide with another event, such as turning on a piece of equipment or an air conditioner. The victim's first response may be to blame the problems on the equipment turning "on" rather than considering an RFW. How quickly the attack leads to an impact on the operations of the critical infrastructure facility depends on the importance of the targeted equipment and how it is affected.

Have RFWs Been Used in the Past?

YES. For example:

- *In the Netherlands, an individual disrupted a local bank's computer network because he was turned down for a loan. He constructed a briefcase-size RFW, 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 Japan, two yakuza criminals were caught stealing from a Pachinko machine using a hidden high energy RF gun to interfere with the machine's computer and falsely trigger a win.*
- *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 home microwave ovens."*
- *In Kizlyar, Dagestan, Russia, Chechen rebel commander Salman Raduyev disabled police radio communications using RF transmitters during a raid.*
- *In Russia, Chechen rebels used an RFW to defeat a Russian security system and gain access to a controlled area.*
- *RFWs 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.*

Figure 8 - Robinson R-44 News Helicopter Nearly Crashed While Flying by a High-Frequency Broadcast Antenna

There have also been several documented incidents caused by devices that could be used as RFWs. For example:

- *On March 21-26, 2001, there was a mass failure of keyless remote entry devices on thousands of vehicles in the Bremerton, Washington, area (operating frequency: 150-500 MHz). The failures ended abruptly as federal investigators had nearly isolated the source. The Federal Communications Commission (FCC) indicated that a military presence in the area was the probably cause. (The U.S. Navy did not agree.) The problem coincided with the arrival of the USS Carl Vinson (CVN 70).*
- *In 1999, a Robinson R-44 news helicopter nearly crashed when it flew by a high frequency broadcast antenna (National Transportation Safety Board Identification #IAD99WA033).*
- *In 1992, a U.S. Navy ship passing through the Panama Canal left its radar on, damaging several nearby computer systems.*
- *In the late 1980s, a large explosion occurred at a 36-inch diameter natural gas pipeline in the Netherlands. A SCADA system, located about 1 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 pipeline and eventually caused the pipeline to explode. It took 6 weeks to discover the cause of the failure. A similar event occurred in June 1999 in Bellingham, Washington, when a SCADA malfunction caused a gas pipeline to rupture and explode.*
- *In 1967, the USS Forrestal was located at Yankee Station off of 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. Naval accident since World War II. EMI was identified as the probable cause of the Zuni launch. (The incident launched the Navy Hazards of Electromagnetic Radiation to Ordnance (HERO) program at the Naval Surface Warfare Center – Dahlgren Division.).*

Radio Frequency Weapons have been used and their potential impact can be significant!


Figure 9 - Gas Pipeline Explosion Caused by SCADA Malfunction


Figure 10 - EMI Identified as Probable Cause of U.S.S. Forrestal Incident

Who Might Attack My Facility?

There are several types of potential attackers, including:

- ***Terrorists***
- ***Criminals***
- ***Competitors***
- ***Disgruntled Employees***
- ***Protestors***
- ***Adversary Military/Special Forces***
- ***Others***


DEFENSE NEWS

Chinese Covet High-Technology Arsenal

DoD Report Reveals PLA Quest For Robotics, Cyber Warriors

Several countries have performed research into RFWs, including the United States, Russia, Ukraine, United Kingdom, China, Australia, France, Germany, Sweden, South Korea, Taiwan, Israel, and others.

The Department of Defense has demonstrated that an RFW can be developed with only modest financial means and technical capability. Furthermore, RFWs, as well as the components and knowledge to develop them, are available on the open market. For example, the Russians are selling the Ranets system (Figure 11) and the German firm Diehl sells various RF sources that can be used as RFWs, including a briefcase-size RF source (Figure 13).

Regarding the conductive threat, some countries have investigated the feasibility of injecting pulses into cables to cause damage to equipment inside of buildings. For example, the Russians performed an experiment in 1999, showing that personal computers in a building can be damaged using pulses injected through power lines (Figure 14).

Figure 11 - Russian Ranets-E RFW

Figure 12 - 1991 Prediction of RFW Threat

Many groups have the means and motivation to use Radio Frequency Weapons.


Figure 13 - Briefcase-sized RF Source by Diehl

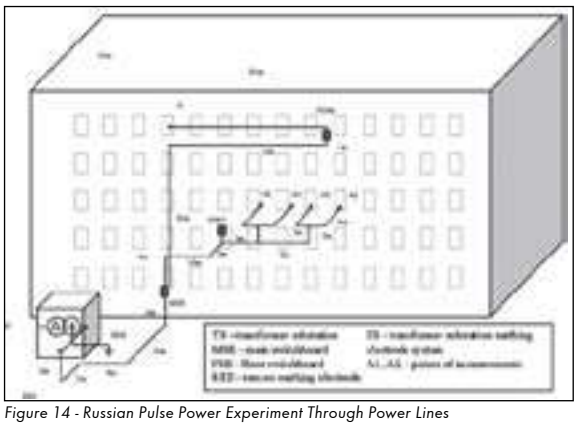


Figure 14 - Russian Pulse Power Experiment Through Power Lines

How Can I Protect My Facility?

Given the potential for disruption and/or damage by RFWs to critical infrastructure facilities; given the relative ease in acquiring the technical know-how and components at reasonable cost levels; given the level of dependence facilities have on electronics; and given that RFWs allow attackers to be covert, remote, and cover a broad area, there is a growing concern about the threat of RFWs to infrastructure facilities. To address this threat, the following basic steps should be performed:

(1) Perform a site assessment

(2) Develop a mitigation plan

(3) Implement mitigation techniques

Figure 15 - Site Assessment Guide to RFW

A site assessment should be conducted to get a general idea of what areas and equipment are most susceptible to an RFW attack. A top level approach is outlined in the RF Site Assessment Guide (Figure 15).

The next step is to outline a cost-effective plan to help mitigate the risks. Several mitigation techniques are listed in Figure 16. The isolation techniques take advantage of the fact that, in general, the farther away an RFW is from its target, the larger it must be to achieve the same effect. In fact, the effective range for RFWs is typically on the order of tens to hundreds of meters and nearly always less than a kilometer. Also, since barriers such as walls or fences generally reduce the electromagnetic energy that pass through them, adding barriers between public areas and critical electronics can help to mitigate the threat. Other techniques include changing cable routing, increasing awareness of the problem to employees, and adding RF monitors to help detect an attack. Redundancy and hardening, such as placing the most critical equipment in shielded rooms, are other options. Note that all of these approaches have other benefits as well as reducing the susceptibility of the facility to RFWs. For example, security can help protect against other types of threats; better cable routing may reduce EMI; and redundancy adds reliability.

The final step is implementing the mitigation techniques in the plan. While both preventative and post-attack methods should be considered, the proactive approach to avoiding RFW attacks, disruption, and damage is preferred.

Additional details regarding RFWs and how to address the threat can be found in the RF Site Assessment Guide and the *Pocket Guide for Security Procedures and Protocols for Mitigating Radio Frequency Threats*, also called the Security Pocket Guide. If you have any questions, require any assistance, or wish to receive a copy of the Site Assessment Guide or Security Pocket Guide, contact the Technical Support Working Group or the Directed Energy Technology Office at the addresses and phone numbers shown on the back of this brochure.

There are techniques and procedures that can be used to mitigate the Radio Frequency Weapons threat.

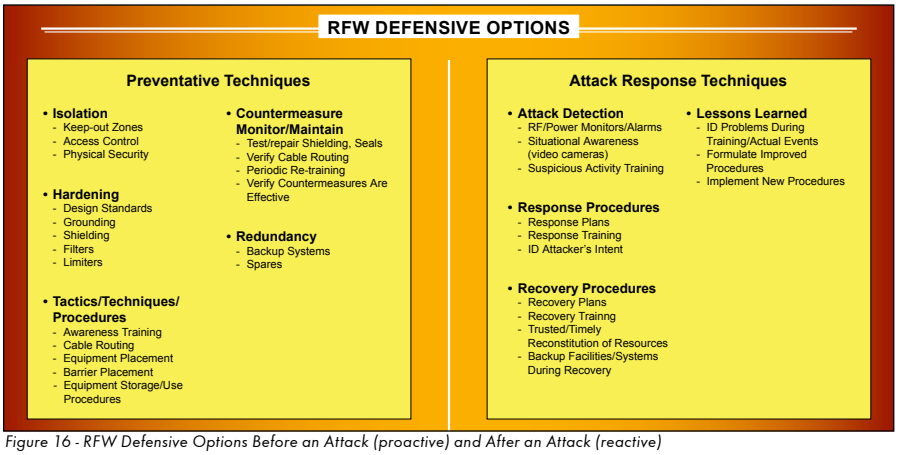


Figure 16 - RFW Defensive Options Before an Attack (proactive) and After an Attack (reactive)

Technical Support Working Group (TSWG)

The TSWG is the U.S. national forum that identifies, prioritizes, and coordinates interagency and international research and development requirements for combating terrorism. The TSWG rapidly develops technologies and equipment to meet the high priority needs of the combating terrorism community, and addresses joint international operational requirements through cooperative R&D with major allies.

Technical Support Working Group, Infrastructure Subgroup
PO Box 16224 • Arlington, VA 22215
Email: IPSubgroup@tswg.gov
http://www.tswg.gov

Directed Energy Technology Office (DETO)

DETO is a Department of Defense research & development organization that develops technologies and approaches to defend the United States against directed energy weapons, including radio frequency weapons.

Naval Surface Warfare Center, Dahlgren Division
17320 Dahlgren Road • Dahlgren, VA 22448
Telephone: (540)284-0878 • Fax: (540)653-1506
Email: DLGR_NSWC_DETOPMO@navy.mil