Facts

Cybersecurity and Secure Communications Department

Order no MSB1590 - June 2020

Recent activities in Sweden to counter antagonistic electromagnetic threats

The electromagnetic threat

Electromagnetic threats can disrupt information systems by affecting the electronics used to run the systems, and/or the wireless communications they often depend on.

Jammers, although generally illegal to use (in Sweden also illegal to possess), are readily available to the general public. High Power Microwave (HPM) generators are offered for sale to law enforcement as vehicle stoppers at short ranges, and knowledge of how to construct HPM devices is spreading online. Larger devices that can be hidden in a small truck can be used to disrupt the operation of unshielded IT-systems at ranges of up to several hundred meters (see table 1).

Susceptible systems are growing in number with the advent of industrial IoT and other systems relying on radio communications and low voltage electronics.

There is a lack of public data on incidents involving ICS, either for lack of incidents, lack of awareness as to the cause of an incident, or unwillingness to share/publicise information. That said, in Sweden in the recent past:

- a large electricity provider lost contact with distributed facilities due to a military exercise that disrupted wireless communication links that used the same frequencies as the military
- a major water producer suffered a similar effect for undetermined reasons, and
- a large port operator encountered simultaneous disruption of multiple radio-dependent systems.

Older international examples:

- in the late 1980:s a malfunctioning SCADA system caused a gas-pipeline to burst and explode. It has been hypothesised that the cause was a ship-radar in

Risk reduction

- Limit public access to information useful to an attacker, for example operating frequencies.
- Refrain from using wireless communications for mission critical systems. If that is not possible, then use robustness enhancing measures such as directional antennas.
- Protect using standoff distance: the further away the target is from a fence or other obstacle the lesser the impact of the EM-threat will be.
- Shielding: Install shielding around sensitive equipment. A concrete wall provides protection equivalent to increasing the distance to the transmitter by four. Vital equipment can be shielded within metallic enclosures (RF shielding). Use surge protectors and filters on all access points.

Contact:
Tel: +46 771-240 240
registrator@msb.se
www.msb.se/en

Swedish Civil Contingencies Agency

the port of Den Helder that caused the SCADA system to open/shut a valve with the same frequency as the rotation of the radar beam, causing a pressure spike.

- in 1999 radar transmissions from a ship at sea outside San Diego supposedly disrupted wireless communications with actuators in nearby water and gas/electricity facilities. These had to revert to manual operation during the incident.

Table 1. Swedish Defence Research Agency (FOI) estimates of range of HPM transmitters against unshielded civilian electronic equipment. Estimates are based on experience from testing of unshielded electronic equipment, cars, computers, communications-devices etc.

Type of Source	**Range**			
	A few meters	15 meters	50 meters	500 meters
HPM-weapon in van (Military grade)	Not applicable	Permanent physical damage	Permanent physical damage	Permanent physical damage
HPM-weapon in van (Engineered)	Not applicable	Permanent physical damage	Disrupted[1,2] /Damage	Disrupted[1, 2]
HPM-weapon in suitcase (Commercial)	Permanent physical damage	Disrupted[1,2]	Risk of disruption[1, 2]	No effect[3]

[1] Can cause residual errors.

[2] Equipment with antennas/sensors operating at the same frequencies as the weapon can suffer permanent damage at this and greater ranges.

[3] Equipment with antennas/sensors operating at the same frequencies as the weapon can suffer disruption at this and greater ranges.

Preventive measures taken in Sweden

Some of the activities undertaken in Sweden in recent years to mitigate electromagnetic threats:

- The Swedish Civil Contingencies Agency (MSB) is the seat of the Central Committee on Electromagnetic Threats (CBG EM-hot). Founded in 1980 by the Supreme Commander of the Swedish Armed Forces (ÖB) it is a forum for information sharing among Swedish national agencies. Originally focused on EMP, it changed to its current broader mandate in 2007.

- In 2018 the Swedish Fortifications Agency (Fortifikationsverket) published a "Guide for protection against intentional EM-threats". It is intended as a support for security coordinators when evaluating vulnerabilities and threats, and when deciding on physical protective measures for critical infrastructure vulnerable to EM-threats. The guide was produced in collaboration with an expert group at the KTH Royal Institute of Technology. An updated edition will be published in 2020.

- In 2018 MSB published a set of publications developed on its behalf by experts from the Swedish Defence Research Agency (FOI):

    - "Introduction to intentional electromagnetic threats to societally important services and critical infrastructure"

    - "Guide for risk and vulnerability analysis regarding antagonistic electromagnetic threats to societally important services and critical infrastructure"

    - "Execution of main study on electromagnetic threats to societally important services and critical infrastructure": It describes how the scenario based risk and vulnerability analysis methodology was validated with pilots on the Swedish railway signalling system and on RAKEL, the Swedish national Terrestrial Trunked Radio system.

- In 2019 the Swedish Security Service (SÄPO) published "Guidelines in protective security: physical protection", with a chapter on intentional electromagnetic threats.

- In 2019 MSB published an addendum on the use of wireless to its "Guide to increased security in industrial information and control systems".

- In 2020 MSB published a leaflet with contact information to various agencies in order to promote and facilitate EM incident reporting.

- In 2020 FOI published a report commissioned by MSB: "Electromagnetic threats against wireless systems". It contains examples of disruptions, attack scenarios and remedial suggestions.