OFFPRINT FROM *STRATEGIC OUTLOOK 8*

Antagonistic electromagnetic threats to civil defence systems

Sten E. Nyholm, Tomas Hurtig, Kia Wiklundh and Sara Linder

Many of today's vital societal functions rely on electronic control systems and wireless communication systems, such as GPS, mobile phones, and Wi-Fi. Cyberattacks with malicious code have become frequent, but since wireless communication systems and unprotected electronics can also be sensitive to electromagnetic (EM) threats, such as jammers and microwave weapons, intentional EM interference constitutes a tangible threat to civil defence capabilities and their potential to support military defence. It is therefore important that EM threats are considered in the risk and vulnerability analyses that authorities, municipalities, county councils, regions, and private enterprises with operations within civil defence are obliged to perform on their undertakings, especially concerning operative capability during a heightened state of alert.

A plausible EM-threat scenario

Imagine the following: the last few months have been characterised by an increasing international split and an escalating number of confrontations between military vessels and aircraft in the Baltic Sea area. Many servers at central government institutions, news agencies and private companies are at risk of advanced cyberattacks and false information is spread daily in social media. The Swedish government considers a mobilisation of the total defence to cope with the situation.

At this time, a large number of societal systems experience EM interference and some cease to work entirely. The communications centres of the emergency services lose contact with field units. Passage and alarm systems at several power plants and government buildings are inoperative. Power grid disruption forces the engagement of emergency power facilities at hospitals and alarm centres. There is traffic chaos in the major cities when traffic lights stop working. Trains remain immobile on railway lines when signals and electric power are lost. Landline telephones and mobile phones only function intermittently. Water distribution fails since pumps do not have electric power. Citizens cannot buy food or refuel their cars since electronic payment systems are not working. The public is unable to receive radio or TV broadcasts to find out what has happened or what to do. Transportation of food, fuel, etc. is so difficult that food shortages arise and private vehicles are immobilised.

What has happened? It soon turns out that there are a large number of jammers placed in cars, bags, baby strollers, etc. in the proximity of communication centres, government buildings, and switching stations for electricity and telecommunications. Jamming equipment on unmanned aerial vehicles circulating over the larger cities and airports paralyse all wireless communication. Furthermore, electronic components inside vital devices have somehow been burnt in radio and TV transmitters, in control equipment of switchgear stations, and in government offices.

How is an EM attack mounted?

An electromagnetic attack is mounted using equipment that emits EM radiation at radio frequencies, which in its simplest form can be a common radio transmitter, mobile phone, etc. The attack can occur with narrow band radiation on only one or a few frequencies, or with broadband radiation covering all frequencies within a wide frequency interval.

A simple method is to use jammers transmitting inaudible radio frequency noise. This drowns out

FOI Memo 6868
Project Nr I181103
Approved by Mike Winnerstig

October 2019

computer communication signals in the noise, and wireless communication in one or several frequencies is inhibited or impaired. The more powerful radiation from microwave weapons can disrupt the operation of electronic components, such as transistors or microprocessors, making them either temporarily malfunction or lose their function altogether, or actually frying components via currents induced in the circuits by the EM-radiation. The difference between these modes of attack is that jammers mainly affect wireless communication, while microwave weapons can affect all electronics, even stand-alone non-communicating devices. Common to both forms of attack is that the effect is local within its range, which can vary between a few metres and several kilometres.

EM attacks strike at the hardware in electronic systems, in contrast to cyber threats, which attack software in digital communication systems. Note that other technological systems may depend on a system that is impaired by an EM attack, which can be very serious and lead to cascade effects spreading through society. For example, water distribution and traffic signals fail if electric power distribution is interrupted. Hence, particular attention should be paid to dependencies between different vital societal systems.

Among potential antagonists who may use EM threats are foreign powers, terrorists and criminals. A civilian society, which, for its vital functions, relies on wireless communication and satellite-based navigation systems, such as GPS and its European counterpart Galileo, is highly vulnerable to modern electronic attacks in a military conflict. The introduction of the Internet of Things (IoT) will most likely further increase this vulnerability.

Society's increased dependence on electronics and communication

The scenario above could occur since all sectors of society have undergone a rapid development of electronic equipment for the control of various functions, data processing, and communication during recent decades. At the same time, advanced commercially available jammers have emerged with the capability to jam several frequency bands simultaneously, although such devices are illegal to possess or use in Sweden. Several countries are developing microwave weapons, which can disturb or physically destroy electronics. These threats to Sweden's civil defence are more tangible today than during the Cold War.

Military systems have often been equipped with protection against these types of effects, while civilian electronic devices are usually completely unprotected. Electronic Warfare (EW) emerged during the twentieth century as a means to achieve information superiority in military conflicts. EW consists of electronic surveillance (listening to an antagonist's signals, communications, and unintentional radiation from equipment), electronic attack (radiating EM energy to jam or confuse an opponent's electronics), and electronic protection (methods to reduce the effects of an opponent's EW operations). Military powers have spent decades developing methods, technologies and systems to cope with EW, not least for the protection of their own electronic systems and support functions.

"Several countries are developing microwave weapons, which can disturb or physically destroy electronics. These threats to Sweden's civil defence are more tangible today than during the Cold War."

The rapid development of electronics during the past few decades, with an enormous increase in computer control and wireless communication, both between humans and between machines, has resulted in many societal functions being based on this technology. Examples include the control and regulation of industrial processes and society's infrastructure via wireless networks, verification of entry permissions at vital plants, issuing warnings over radio and via SMS, payment systems, etc. The digitalisation of our society is progressing within all sectors, even critical services. This makes society dependent on the operation of electronics while at the same time there have been no incentives to introduce protection against antagonistic EM interference. Perhaps this is due to a lack of awareness of such threats to their own systems among those responsible, or not having deemed them as serious or probable, and hence in

the short-term the most cost-effective solutions have been chosen during procurement and installation. All commercial electronics must meet Swedish and international requirements regarding immunity to unintentional interference, which can be caused by natural phenomena or by other devices in the vicinity, but these interference levels fall far below the potential of intentional EM threats. Military systems face tougher requirements on resilience against jamming and interference, which gives much better protection but at a higher cost.

Sometimes electronic equipment is jammed by natural phenomena, such as lightning or solar flares, or unintentionally by other equipment nearby. But individuals with sufficient knowledge can also disrupt societal functions. An example is the Gothenburg riots in 2001, when police radio communication was jammed and false messages were sent. Such disruption is modest compared to the potential of military EW capability. There have also been reports of mobile communications and GPS being jammed as part of Russian EW during the conflicts in Ukraine and Syria.

The total defence concept is central in preparing Sweden to counter many different types of threats. A unified total defence means that civilian actors must consider adopting the same levels of protection as the armed forces. There is currently limited awareness and presence of EM protection within civilian sectors, while the armed forces have long since taken this into account. Increasing the awareness of antagonistic EM threats within civilian sectors is a matter of urgency, so that vital societal functions can be adequately protected.

How to reduce vulnerabilities to EM threats?

The formation of the new Swedish total defence means that many actors will face enhanced requirements for robustness against many different types of intentional or unintentional interference, including antagonistic EM threats. At the same time, the ongoing digitalisation of our society creates new risks of various types of EM interference. If the total defence is designed without this in mind, there is a risk that vulnerabilities will not be discovered and addressed. It is often far more expensive to protect sensitive systems retrospectively than to do so during the procurement or installation phases.

Those responsible for vital civilian functions usually do not have the same knowledge of EM threats and protective measures as is common within the military sector. Awareness of the EM threats faced today needs to increase so that the threats can be incorporated into risk and vulnerability analyses, and identified critical weaknesses can be addressed.

Wireless communication, which is transmitted through air, is much more difficult to protect than communication through metal wires or optical fibres. Hence, wireless communication solutions for vital societal functions need to be resilient against jamming, or have redundancy. This can be realised in different ways, e.g. using frequency hopping regularly or when disturbed; with several antennas in different locations; with several communication systems using different frequencies; or by supplementing with fibre solutions whenever possible.

Designing adequate protection against antagonistic EM radiation is no easy task. There are several strategies for protecting electronic equipment against EM threats. Depending on how critical the equipment is, and the level of protection selected, the protection can be designed in different ways. With regard to intentional EM threats against mission-critical systems, there are a few general recommendations for consideration:

- Do not spread information about critical electronic systems unnecessarily or information about how they operate, where they are located, and which frequencies are used. An antagonist can use this knowledge in an attack.
- When possible, do not use wireless communication between mission-critical systems. Wired communication is much less sensitive to jamming. Alternatively, equipment with EW protection or redundant systems should be used.
- Make sure that it is not possible to get close to critical systems. Since the effect decreases with distance between source and target, it is beneficial to move barriers and fences, or similar arrangements preventing unauthorised access to critical facilities, further away from the sensitive installation.

Securing access to spare parts and ensuring access to rapid service or repair if a system has been exposed to an EM attack is also a good strategy to help minimise

disruption in electronics-based societal functions. It is also possible to enclose critical equipment inside EM shielding walls and to install protective components, such as transient protectors or different types of filters, on connected wires.

It is important to realise that it is not possible to protect all communication and electronic equipment against EM threats. Priority should be given to vital systems, i.e. those whose loss would lead to major disruptions in important services. To achieve this, it is essential to carry out risk and vulnerability analyses, including the risks posed by EM threats to vital systems, on a regular basis. It is always a matter of balance regarding which weaknesses to fix and which level of protection to implement in order to obtain the resilience needed to continue operations when exposed to EM attacks in a severe crisis.

A first step when protecting communication solutions and electronic equipment is to obtain information about existing EM threats and how to incorporate those into a risk and vulnerability analysis, together with all other identified threats. The next step is to determine whether there is sufficient knowledge in-house to conduct a risk and vulnerability analysis and remedy identified weaknesses, or if external experts are needed. Finally, the analysis should be carried out, suitable protective measures implemented, and regular subsequent verifications that the protection is maintained should be performed. Do not forget the hardware!

FOI
Swedish Defence Research Agency
SE-164 90 Stockholm

Telephone: +46 8 5550 3000
www.foi.se