Elektromagnetische Bedrohungen

Ein KIRAS-Projekt befasste sich mit Maßnahmen gegen elektromagnetische Bedrohungen kritischer Infrastruktur.

In den letzten zehn Jahren hat die Bedrohung durch elektromagnetische Quellen für kriminelle oder terroristische Zwecke zugenommen. Während diese Bedrohung in den 1980er- und 1990er-Jahren auf den militärischen Bereich beschränkt war, ist seitdem auch eine Zunahme des Einsatzes von elektromagnetischen Waffen im zivilen Bereich zu beobachten. Dies führte international zu zahlreichen Projekten, die den Einsatz solcher Systeme untersuchen. Gestützt auf den internationalen State-of-the-Art wurde im Rahmen des österreichischen Sicherheitsforschungsprogramms *KIRAS* das Projekt „Sicherheit gegen elektromagnetische Bedrohungen kritischer Infrastruktur" (SEMB)[1] durchgeführt.

Angriffsmöglichkeiten mit elektromagnetischen Waffen sind wenig dokumentiert, da solche Vorfälle meist unter Verschluss gehalten werden. Bisherige Beispiele für zivile Angriffe betrafen

- die Ausschaltung von Sicherheits- oder IT-Systemen,
- das Blockieren von Sicherheitssystemen von Autos,
- die Deaktivierung von Alarmanlagen von Geschäften, wie Juwelieren,
- die großflächige Störung von Telefonnetzen und TV-Sendern mit bis zu einigen 100.000 betroffenen Menschen.

Im militärischen Bereich sind durch elektromagnetische Einflüsse Flugzeug- und Hubschrauberabstürze, Zerstörungen von großen Computersystemen und ein Unfall auf einem Flugzeugträger mit mehr als 100 Toten bekannt geworden. Dabei handelte es sich aber nicht um Angriffe, sondern um unbeabsichtigte Störungen.

Für den Konvoischutz, z. B. für VIPs oder bei Staatsbesuchen sind vor allem *Remote Controlled Improvised Explosive Devices (RCIED)* eine zunehmende Bedrohung. RCIED bestehen aus einer Energieversorgung (z. B. Batterie), einem Auslöser, einem Zünder, explosivem Material und einem Gehäuse. Eine mögliche Gegenmaßnahme ist das Blockieren von häufig verwendeten Funkbändern, wie z. B. GSM mittels Jammern.[2] Auch die Störung oder Beeinflussung von Positionierungssystemen (z. B. GPS) hat in den letzten Jahren zugenommen. Weitere Beispiele sind das Blockieren von Sicherheitssystemen von Autos und die Verwendung von GPS-Jammern durch Lkw-Fahrer, um ihren Standort zu verschleiern. Dies führt in der Umgebung von Flughäfen zur Beeinträchtigung der Positionsbestimmung von Flugzeugen. Ermöglicht wird dies durch die relativ schwachen GPS-Signale, womit eine Störung bereits mit geringen Störpegeln erzielt oder verursacht werden kann. Ein Spezialfall der GPS-Blockierung ist das „GPS-Spoofing". Dabei werden die GPS-Daten nicht nur gestört, sondern dem Empfänger sollen falsche Positionsdaten übermittelt werden. Eine Vielzahl von Maßnahmen kann GPS-Spoofing entgegenwirken, wie z. B. die Bestimmung der GPS-Signalstärken oder die Identifizierung der jeweiligen Satelliten.

Bedrohungen kritischer Infrastruktur. Das Projekt SEMB erfolgte im Einklang mit dem „Österreichischen Programm zum Schutz Kritischer Infrastruktur" *(Austrian Program for Critical Infrastructure Protection – APCIP)*. Als erster Schritt wurde die besonders durch elektromagnetische Angriffe verletzbarer Infrastruktur in Österreich identifiziert, wie z. B. die Sektoren Energie, Kommunikation und Transport.

Als Beispiel untersucht wurde die Situation eines Fahrzeugkonvois mit einer angepassten Risikoanalysemethode, der *Failure Modes and Effects Analysis (FMEA)*. Auf Basis von Expertenschätzungen ergab sich eine „Risikoprioritätszahl". Diese berücksichtigt die Auswirkungen eines Ereignisses, die Auftrittswahrscheinlichkeit sowie die Möglichkeit der Erkennung des Ereignisses.

Als untersuchte Schadensfälle wurden ein vorübergehendes sowie ein dauerhaftes Stoppen eines Konvois, die Beeinträchtigung der Funkkommunikation des Konvois sowie die Beeinträchtigung von in oder am Fahrzeug mitgeführtem elektronischen Gerät betrachtet. Als Szenarien wurden ein VIP-Konvoi im Stadtgebiet, ein militärischer Truppentransport zur Kaderübung sowie ein Feuerwehrkonvoi zum Katastropheneinsatz analysiert. Die Gefahrenquellen stellen Jammer, High-Power-Microwave- oder Ultra-Wideband-Quellen dar. Auf Basis der getroffenen Annahmen wurde das höchste Risiko für ein dauerhaftes Stoppen des Feuerwehrkonvois und das geringste Risiko für ein dauerhaftes Stoppen eines Militärkonvois ermittelt.

Analyse der Bedrohungen. Als Hauptkategorien elektromagnetischer Störquellen kristallisierten sich bei der Analyse Schmalbandquellen, Breitbandquellen und Jammer heraus. Bei Schmalbandquellen wird die Energie auf einen kleinen Bereich des Frequenzspektrums übertragen, während bei Breitbandquellen diese Energieübertragung über einen sehr weiten Frequenzbereich erfolgt. Schmalbandquellen kommen daher für Angreifer in Frage, die bekannte Komponenten einer Infrastruktur attackieren wollen. Wenn ein Krimineller oder Terrorist entweder geringe Kenntnisse über die anzugreifende Infrastruktur besitzt oder viele unterschiedliche Komponenten einer Infrastruktur gleichzeitig beeinträchtigt werden sollen, dann kommen Breitbandquellen zum Einsatz. Ist das Ziel nur eine Blockierung einzelner Frequenzbänder verschiedener Funkdienste und nicht die Zerstörung elektronischer Komponenten, werden Jammer eingesetzt.

Die elektromagnetischen Störquellen können nach folgenden Kriterien kategorisiert werden:

- erforderliches Know-how für ihren Bau und Betrieb,
- notwendige Energie zum Betrieb,
- erforderliche Kosten,
- Größe,
- Transportfähigkeit,
- Beschaffungsmöglichkeit der Komponenten zum Bau,
- Ausgangsleistung,
- Bündelung des elektromagnetischen Strahles,

Elektromagnetische Bedrohung: Bereiche wie Energie und Transport wurden durch elektromagnetische Angriffe als besonders verletzbare kritische Infrastrukturbereiche identifiziert.

- Signalform,
- Frequenzbereich und
- Reichweite.

Berücksichtigt man diese Kriterien, stehen auf der einen Seite Lowtech-Geräte, die entweder illegal zu erwerben oder mit relativ geringen Kenntnissen zu bauen, meist leicht zu transportieren sind, aber eine vergleichsweise geringe Reichweite haben. Andererseits gibt es Hightech-Geräte, deren Bau und Betrieb hohes Wissen und Aufwand erfordern, die groß und daher schwer zu verstecken sind, aber dafür eine große Reichweite aufweisen.

Die Abnahme der elektrischen Feldstärke für unterschiedliche Quellkategorien (z. B. Schmalband – Lowtech) ist mit einfachen Formeln zu berechnen. Als Angriffsszenarien kann unterschieden werden zwischen Outdoor, dabei befindet sich weder das Zielobjekt des Angriffes noch die Quelle in einem Gebäude oder einer anderen Umhüllung, und Indoor, wobei von einem Gebäude ausgegangen wird, das die Leistung des einfallenden Strahles um den Faktor 1.000 abschwächt.

Aus Normen und wissenschaftlichen Dokumenten kann abgeschätzt werden, bei welchen Feldstärken elektronische Geräte gestört oder zerstört werden können. Daraus kann für die unterschiedlichen Arten von Quellen bzw. Waffen (z. B. Schmalband Lowtech, Geräte relativ einfacher Bauart mit meist relativ geringer Sendeleistung) eine Störungsgrenze sowie eine Zerstörungsgrenze abgeleitet werden, also Distanzen bis zu denen mit einer Störung oder Zerstörung eines Zielobjektes bei Befeldung durch Störquellen der jeweiligen Kategorie zu rechnen ist. Da es sich hierbei um eine Abschätzung auf Basis der verfügbaren Informationen handelt, ist es durchaus möglich, dass bei störempfindlicheren Geräten als den getesteten auch bei höheren Distanzen Zerstörungen bzw. Störungen auftreten können.

Schutzkonzepte. Beim Schutz kritischer Infrastruktur unterscheidet man zwischen organisatorischen und technischen Maßnahmen, die sowohl bei der Errichtung als auch bei der Planung der Infrastruktur und während des Betriebes umgesetzt werden können.

Organisatorische Schutzmaßnahmen sind Schutzzonen und Alarmanlagen. Zu den technischen Maßnahmen zählt die Erhöhung der gestrahlten und leitungsgeführten Störfestigkeit. Dies ist zu erreichen mit technischen Maßnahmen, wie der Filterung für leitungsgebunden Störungen und Schirmung von Feldstörgrößen, optimierte Massekonzepte oder Überspannungsbegrenzungen. Eine Steigerung der Wirkung der Schutzkonzepte kann erreicht werden durch Kaskadierung von Maßnahmen auf verschiedenen Ebenen. Dabei können Schutzmaßnahmen beispielsweise auf der äußersten Ebene, etwa bei einem Zaun, beginnen und auf der Ebene des integrierten Schaltteiles (IC) enden. Dieser gestaffelte Schutz ist als Zonenkonzept bekannt. Bei einer Systemstörung muss sichergestellt sein, dass das System keinen unsicheren Betriebszustand einnimmt („Fail-Safe"-Prinzip).

Ausblick. Die relativ geringe Anzahl bekannter Ereignisse begründet sich durch die Geheimhaltung vieler Angriffe und Auswirkungen. Zerstörungen treten je nach Art der eingesetzten elektromagnetischen Waffen in Distanzen von bis zu 500 m auf. Störungen wurden in Distanzen von über 10 km vom Störsender beobachtet.

Der Schutz kritischer Infrastruktur erfordert ein Bündel an Maßnahmen. Den Betreibern dieser Infrastruktur ist anzuraten, ihre Systeme und Anlagen zu überprüfen und Schutzmaßnahmen zu setzen. Die Bereitstellung eines Handbuches, das beispielsweise den Betreibern kritischer Infrastruktur auf der *CIWIN-Plattform (Critical Infrastructure Web Information Network)* zur Verfügung gestellt werden kann, wäre als unterstützende Maßnahme wünschenswert.

Ein vorsorglicher Umgang mit elektromagnetischen Bedrohungen ist sehr empfehlenswert, da elektromagnetische Waffen verschiedene Grundprozesse der Wirtschaft und Gesellschaft wie Energieversorgung, Kommunikation oder Transport massiv beeinträchtigen können.

Thomas Gruber, Kurt Lamedschwandner, Georg Neubauer

[1]Die Studie SEMB wurde im österreichischen Förderprogramm für die Sicherheitsforschung KIRAS vom Bundesministerium für Verkehr, Innovation und Technologie (bmvit) finanziert. SEMB auf der KIRAS-Homepage: http://www.kiras.at/gefoerderte-projekte/detail/projekt/sicherheit-gegen-elektromagnetische-bedrohungen-semb/. KIRAS setzt sich zusammen aus den griechischen Wörtern kirkos (Kreis) und asphaleia (Sicherheit); siehe www.kiras.at

[2]Ein Jammer ist ein Störsender, der den einwandfreien Empfang einer Funknachricht (z. B. von Radio, Fernsehen, Mobilfunk oder GPS) schwierig bis unmöglich macht.

Fotos: Werner Sabitzer, Egon Weissheimer