Elektronik als Waffe

Elektronik als Waffe

Wer Waffe sagt und dabei die Kriegführung vor Augen hat, denkt vor allem an Feuerwaffen in allen Erscheinungsformen, vielleicht aber auch an die althergebrachten blanken Waffen, wie Säbel und Bajonett. Aber wer vermutet schon, dass die Elektronik eine wirksame Waffe sein könnte?

Nun, Waffen haben ganz allgemein zum Ziel, im Kampf zur Vernichtung oder Schädigung des Gegners eingesetzt zu werden. So gesehen, eröffnet sich dem phantasievollen Betrachter sehr wohl ein ertragreiches Betätigungsfeld der Elektronikwaffe. Warum? Ganz einfach, weil seit der Erfindung des Transistors und weiterer verfeinerter Technologien der Siegeszug der elektronischen Übermittlungsmittel eingesetzt hat und im Militär wie im Zivilbereich aus unserer Gesellschaft nicht mehr wegzudenken ist. Überall sieht man Sender, Empfänger, elektronische Waffen- und Lenksysteme, Radar, Richtstrahlanlagen, Fernmeldeeinrichtungen, Flugzeuge, die bald mehr Elektronik an Bord haben als Triebwerke. Nicht, dass diese Erscheinung zu verdammen wäre, im Gegenteil, sie hat eine bedeutende Mehrleistung gebracht, die sich früher niemand hätte träumen lassen. Aber, wie so oft, wenn auf einem Sektor eine übergewichtige Entwicklung stattgefunden hat, sind Kräfte am Werk – das ist fast ein Naturgesetz –, die dafür sorgen, dass auch die «elektronischen Bäume» nicht in den Himmel wachsen. Und die Konkurrenz kommt gar aus den eigenen Reihen: **Elektronik wird mit Elektronik geschlagen, Übermittlung mit Gegenübermittlung.** Elektronik wird eingesetzt, um auf die gegnerischen Übermittlungsmittel schädigende Wirkung auszuüben, sei es direkt durch Funkstören, sei es durch Peilen und nachfolgendes Belegen mit Feuerwaffen, sei es indirekt durch elektronische Aufklärung. Denn man kann dem Feind auch schaden, wenn man seine Übermittlungsmittel im «Äther» anzapft und nicht für die eigenen Ohren bestimmtes Material erfasst.

Um etwas konkreter und systematischer die Hintergründe der Elektronikwaffe zu sehen, sei beispielsweise folgendes Modell entworfen (Fig. 1). In diesem Modell sind in logischer Folge die **Sequenzen** aufgeführt, die zu einem Waffeneinsatz führen. An erster Stelle: Hören, Sehen, Information gewinnen, diese Information der entscheidenden Stelle übermitteln (zweite und dritte Sequenz). Die getroffenen Entscheide als Befehle übermitteln (vierte Sequenz) und den Waffeneinsatz durchführen, seien es Feuerwaffen oder eigene elektronische Störungswaffen (fünfte und sechste Sequenz).

Wenn dieses Modell auch im Prinzip allgemeine Gültigkeit hat – denn auch ein Füsilier durchläuft bei sich selber vom Erkennen über Vergleichen mit seinem Auftrag bis zum Finger krümmen diese Sequenzen –, so bietet sich doch erst ab einer gewissen Stufe der **lohnende Gegeneinsatz von elektronischen Mitteln.** Lohnend in dem Sinne, dass die Informationskette unterbrochen oder durch Anzapfen zur schädigenden Wirkung ausgenutzt wird. Diesen möglichen Angriffsflächen sei nun im einzelnen nachgegangen. Mit anderen Worten: Wo bieten sich im komplexen Systemablauf des Waffeneinsatzes dem Spezialisten für elektronische Kriegführung Ansatzflächen für den Einsatz seiner Waffe?

1. Elektronik bei der Informationsgewinnung

Im Bereich der Informationsgewinnung gilt die Devise, dass Wissen Macht schafft. Die Verantwortlichen setzen demnach alles daran, möglichst früh möglichst viel über den Gegner zu erfahren. Und wenn die menschlichen Sinne zur umfassenden Informationsgewinnung nicht genügend taugen, werden andere, meistens elektronische **Mittel** eingesetzt, die sich dafür in reicher Form anbieten, etwa
- Satelliten,
- Radargeräte für die Flugwaffe, Fliegerabwehr und Gefechtsfeldüberwachung,
- Infrarot Nachtsichtgeräte,

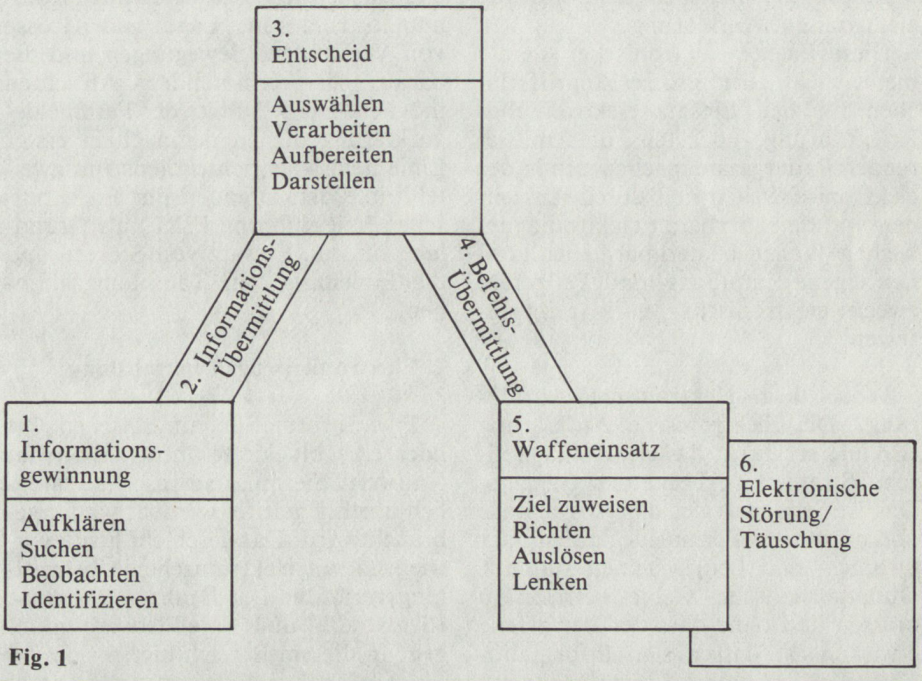

Fig. 1

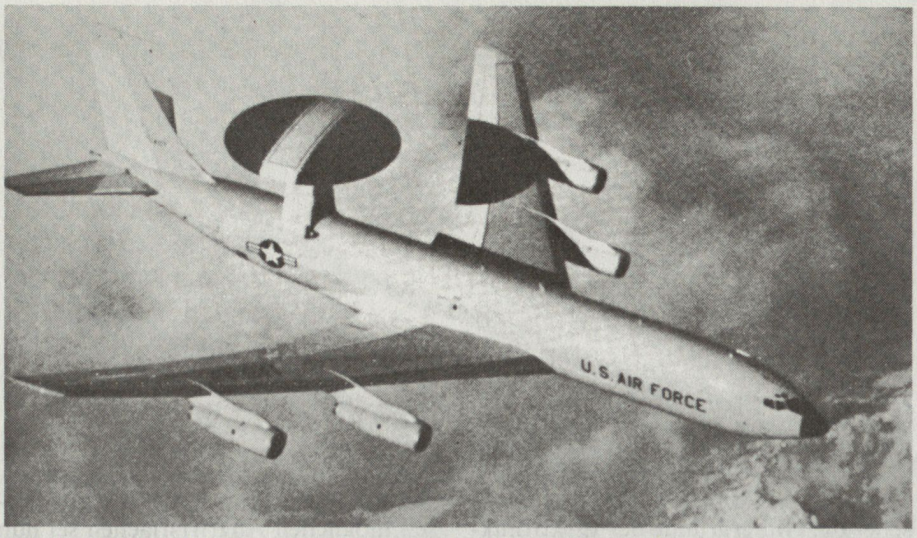

Bild 1. AWACS, das fliegende Frühwarnsystem in umgebauten Boeing-Flugzeugen.

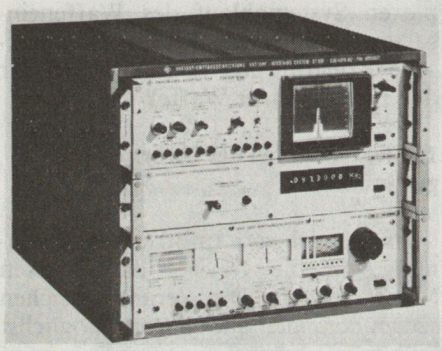

Bild 2. Aufklärungsempfänger mit Panoramaanzeige.

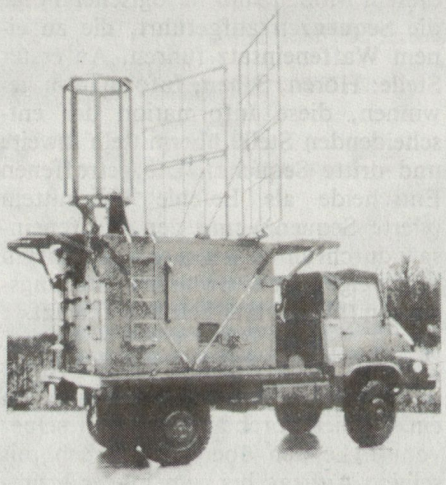

Bild 3. Ein hochwirksamer Störsender mit betriebsbereiter Antennenanlage.

- Restlichtverstärker,
- Gefechtsfeldsensoren jeder Art, und nicht zuletzt
- Empfangs- und Peilgeräte für die elektronische Aufklärung.

Diese Palette elektronischer Geräte bietet nicht eben grosse Angriffsflächen für den Einsatz elektronischer Kriegführung, höchstens die emittierenden Radargeräte machen sich in der elektronischen Umwelt durch Aussenden von detektierbaren elektromagnetischen Wellen bemerkbar. Hier können eigene Empfangs- und Peilgeräte zwecks elektronischer Aufklärung ansetzen.

Wozu dient elektronische Aufklärung? Die Elektronische Aufklärung (EA) liefert direkt das elektromagnetische Strahlungs-Abbild des Gegners. Das ist Sendeenergie, die grösstenteils von drahtlosen Fernmeldegeräten oder Ortungs- und Lenksystemen stammt. Ohne gegnerisches Gebiet betreten zu müssen und ohne dass der Betroffene etwas merkt, lassen sich Informationen über betriebliche, inhaltliche, technische und räumliche Gegebenheiten gewinnen. Damit werden nachrichtendienstliche Rückschlüsse auf Kommandostrukturen, Lage und Grösse von Verbänden, Bewegungen und die daraus zu vermutenden Absichten möglich. Die Resultate der Fernmeldeaufklärung dienen demnach in erster Linie dem Nachrichtendienst, in zweiter Linie den Organen der Elektronischen Kriegführung (EKF) als Grundlage für den Einsatz von Störern und die Einleitung von Täuschungsaktionen.

2. Elektronik in der Übermittlung

Eine Information am falschen Ort oder eine blockierte Information hat Nullwert. Sie muss so rasch als möglich dorthin geleitet werden, wo sie gebraucht wird. Das geschieht heute vorwiegend mit elektronischen Übermittlungsverfahren: **Draht-, Funk-, Richtstrahl- und Satellitenverbindungen.** In diesem Bereich bieten sich der elektronischen Kriegführung reiche Jagdgründe.

Einmal ist **Elektronische Aufklärung** (EA) über weite Distanzen sehr ergiebig. Dann kann mit eigener elektronischer Störung, also Sendern, welche **Feindfrequenzen** gezielt mit Signalen stören, die feindliche Tätigkeit unterbunden oder erschwert werden, und schliesslich können auch **Falschmeldungen** und irreführende Befehle, in Form elektronischer Täuschung, geschickt in feindliche Netze eingespiesen werden und dort Fehlaktionen auslösen. Solche Aktionen sind keineswegs utopisch, man kennt Fälle jüngeren Datums.

Wenn eingangs die Rede von üppigen Angriffsflächen für die EKF war, ist das zwar wahr, muss aber sofort relativiert werden, denn man weiss natürlich auf beiden Seiten, wo die schwachen Punkte liegen und sieht sich entsprechend vor. **Elektronische Schutzmassnahmen** (ESM) werden getroffen. Taktische Regeln, Sprechfunkregeln beschränken die freie Ausstrahlung von Sendeenergie, denn disziplinierte Netze sind schwerer aufzuklären als wilder Jedermannsfunk. Ausserdem werden seit längerer Zeit auch automatische Verschlüsselungsgeräte eingesetzt, die mindestens den Inhalt der Information vollumfänglich und sicher zu schützen vermögen.

3. Elektronik als Führungsmittel

Die **Elektronische Datenverarbeitung** (EDV) ist sicherlich heute nicht mehr neu, auch wenn sie in den Stäben kaum recht Fuss gefasst hat. Das hat verschiedene Gründe, einer der wichtigsten ist der, dass die für die zivilen Bedürfnisse entwickelten Computer nicht ohne weiteres für die Belange der Militärs Verwendung fanden. Auch im Ausland harzte es bei der Einführung der EDV in die Stäbe, und manche stürmischen und theoretischen Erwägungen über Führungssysteme fanden ihren Niederschlag in militärischen Fachzeitschriften. Mit der heute verwendeten Technologie aber wird aller Wahrscheinlichkeit nach eine Wende eintreten. Die ursprünglich grossangelegten EDV-Systeme machen handlicheren und übersichtlicheren Mikroprozessoren Platz.

Ansatzpunkte für elektronische Kriegführung, um auf das Thema zu kommen, bieten sich kaum, solange nicht **Ferndatenverarbeitung** betrieben wird.

4. Elektronik in der Befehlsübermittlung

Die Befehlsübermittlung benötigt (ähnlich der Ziffer 2) **Fernmeldeverbindungen,** in Zukunft vielleicht sogar abgesetzte **Terminals.** In diesem Bereich gilt alles, was bereits unter Ziffer 2 geschrieben wurde.

5. Elektronik beim Waffeneinsatz

Nicht jede Waffe bedarf zum Einsatz elektronischer Mittel, aber es gibt einige Waffensysteme, die nur wirksam sind, wenn die **elektronischen Hilfseinrichtungen,** Steuerungen, Lenkungsmittel und Rechner einwandfrei funktionieren. Es brauchen nicht immer Cruise missiles zu sein, auch die gezogene Artillerie kann ihre Schussbereitschaft erhöhen, wenn die artilleristischen Elemente von Mikroprozessoren gerechnet werden.

Die **elektronische Kriegführung** wird darauf bedacht sein, diese Systeme zu detektieren, aufzuklären und wenn möglich zu stören oder, nach erfolgter Aufklärung, mit Feuerwaffen zu zerschlagen.

6. Elektronik als direkte Waffe

Eine manchem unbekannte, mehrmals bereits angetönte Art des Waffeneinsatzes ist die **elektronische Störung und Täuschung.** Mit der elektronischen Störung im Fernmeldebereich wird die Absicht verfolgt, den Gegner durch Unterbrechen seiner Verbindungen zu behindern und seinen Informationsaustausch zu hemmen. Die elektronische Täuschung verfolgt das Ziel, in gegnerische drahtlose Netze einzudringen, Verwirrung zu stiften oder geplante Aktionen auszulösen. Unter elektronischer Täuschung versteht man auch eigene Blindaktionen, die Tätigkeiten vortäuschen, welche blosse Fernmeldefiktionen sind. Beide Arten, Störung und Täuschung, verlangen stets eine sorgfältige Planung und Abstimmung, wenn sie Erfolg haben sollen. Dann aber ist leicht einzusehen, dass mit relativ geringem materiellen Aufwand gegnerische Operationen stark beeinträchtigt werden können.

7. Die elektronische Kriegführung

Die hier aus dem Modell mosaikartig zusammengetragenen Elemente der Elektronikwaffe haben schon lange zum Begriff der Elektronischen Kriegführung (EKF) geführt. Zusammengefasst lässt sich sagen, dass **jedes Einschalten eines Senders,** jedes Drücken der Sprechtaste, jede Aktivierung von Richtstrahlanlagen und schliesslich der Einsatz beinahe aller bekannter Elektroniksysteme die Ausstrahlung von detektierbaren elektromagnetischen Wellen zur Folge hat. Diese Ausstrahlung erreicht nicht nur den Adressaten, sondern andernorts interessierte Dritte.

Auf dieser Tatsache beruht die elektronische Kriegführung (Fig. 2). Sie ist im wesentlichen gegliedert in offensive **elektronische Gegenmassnahmen und defensive elektronische Schutzmassnahmen** und enthält die Elemente, die im entwickelten Modell eines Waffeneinsatzes erhellt wurden.

Nun ist trotz aller Technik die elektronische Kriegführung keineswegs nur ein Tummelfeld für Elektronik-Spezialisten. Im Gegenteil: **Jeder, der an einem elektronischen Gerät sitzt, und das ist in heutigen Armeen jeder zehnte Wehrmann, muss zugunsten der Gesamtheit in seinem kleinen Bereich elektronische Kriegführung betreiben,** insbesondere seine elektronischen Schutzmassnahmen treffen. Nur so kann auf breiter Front der Erfolg gegnerischer Aufklärung, Störung und Täuschung vermindert werden. Das gilt bereits in Friedenszeiten auch in der Ausbildung.

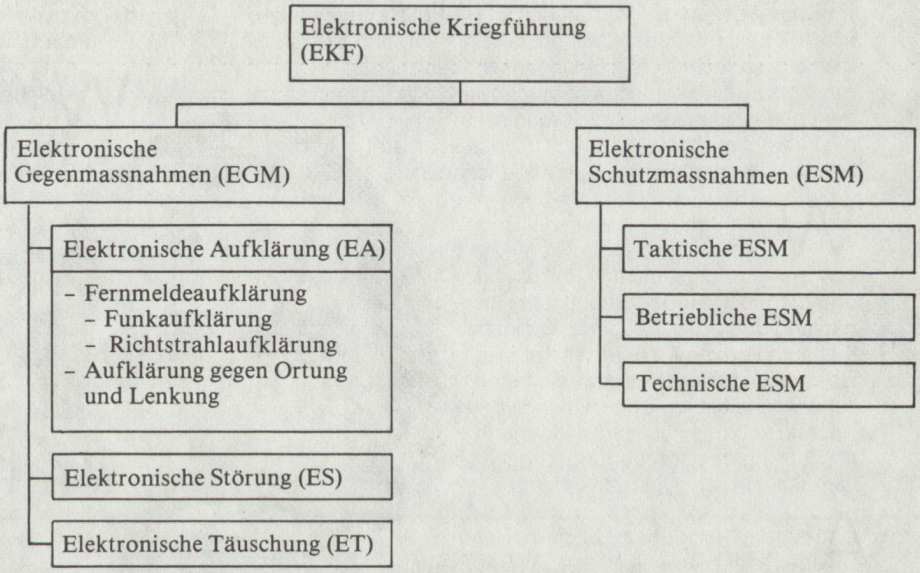

Fig. 2. Gliederung der Elektronischen Kriegführung (EKF).