Zeitschrift: Pionier : Zeitschrift für die Übermittlungstruppen

Herausgeber: Eidg. Verband der Übermittlungstruppen; Vereinigung Schweiz. Feld-Telegraphen-Offiziere und -Unteroffiziere

Band: 48 (1975)

Heft: 7

Artikel: Elektronik als Waffe

Autor: [s.n.]

DOI: https://doi.org/10.5169/seals-562818

Nutzungsbedingungen

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Mehr erfahren

Conditions d'utilisation

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. En savoir plus

Terms of use

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. Find out more

Download PDF: 02.07.2025

ETH-Bibliothek Zürich, E-Periodica, https://www.e-periodica.ch

11. Jahresrapport der Offiziere der Uebermittlungstruppen

Gegen 300 Offiziere der Uebermittlungstruppen reisten am 24./25. Mai 1975 nach Locarno, um diesmal im Kreise ihrer Tessiner Kameraden am 11. Jahresrapport der Offiziere der Uebermittlungstruppen teilzunehmen. Unter den zahlreichen Gästen konnte Divisionär A. Guisolan, Waffenchef der Uebermittlungstruppen, Mitglieder von Behörden, Vertreter der Armeeleitung sowie der Wirtschaft, Verwaltung und Presse begrüssen und willkommen heissen. Zu Beginn seines Vortrages hatte Divisionär A. Guisolan an seine Ausführungen über Kommunikation am Jahresrapport 1974 angeknüpft und festgehalten, dass auch das diesjährige Thema zu einer umfassenden Kommunikation beizutragen habe, ohne welche die Probleme unserer Zeit nicht mehr bewältigt werden könnte.

Das Schwergewicht des Rapportes galt dem Thema «Elektronik als Waffe». Wir veröffentlichen den Vortrag des Waffenchefs nachfolgend in vollem Wortlaut.

Im 2. Teil der Ausführungen stellten Mitarbeiter der Abteilung für Uebermittlungstruppen in Kurzvorträgen und Demonstrationen die heute im Studium, in Entwicklung oder Beschaffung stehenden Geräte und Systeme vor.

Kernstück war die Präsentation der neuen Chiffriergerätefamilie mit den sehr verständlich dargestellten Grundprinzipien der zwei zur Verfügung stehenden Möglichkeiten für den Schutz geheimer Information während der Uebermittlung. Die mit relativ wenig Aufwand realisierbare Verschleierung — eine teilweise Zerlegung der Nachricht in möglicherweise nicht gleichartige Bestandteile — bietet dabei weniger Sicherheit als die eigentliche Chiffrierung.

In einem weiteren Themenkreis wurde auf die Erneuerung und Erweiterung des heutigen Richtstrahlnetzes der Armee eingegangen. Dass dazu neben modernen Uebermittlungsgeräten auch ein leistungsfähiges Vermittlungssystem gehört, wurde klar ausgedrückt. Die heutigen Verbindungen basieren zum Teil auf dem zivilen PTT-Netz. Das geplante neue Netz für die 80er Jahre soll hingegen ein unabhängigeres, sicheres und flexibles Arbeiten gestatten. Neben den Projekten der Bildübertragung wurde vor allem auch auf die Nutzbarmachung der Elektronischen Datenverarbeitung für die Armee hingewiesen. Die Bedürfnisse nach aktueller und vollständiger Information sowie die zunehmende Verbreitung der EDV in militärischen und zivilen Bereichen verlangen die Erarbeitung eines Konzeptes für die gesamte Armee. Grosse Subsysteme, wie das Versorgungs-Informations-System (VISA) und das Personal-Informations-System (PISA) stehen ebenfalls in Bearbeitung.

Auf dem Gebiet der Funkgeräte wurden die verschiedensten Systeme vorgestellt. Vom kleinen Notsender und Peilempfänger zur Ortung von Lawinenverschütteten über die leistungsstarke Kurzwellenstation bis zum modernsten, tragbaren Funkgerät für die taktischen Verbindungen auf unterer Führungsstufe wurde das ganze Spektrum der in Bearbeitung stehenden Projekte aufgezeigt.

Mit einem letzten Kurzreferat über die Elektronische Kriegführung, die einerseits durch Aufklärung Nachrichten beschafft und anderseits durch Störung und Täuschung den Gegner in der Anwendung seiner elektronischen Geräte beeinträchtigt, wurde der Ueberblick über die zukünftigen Uebermittlungssysteme der Armee abgeschlossen. Die Rapportteilnehmer waren durchwegs von der Vielfalt und Komplexität der vorgestellten Projekte beeindruckt.

Elektronik als Waffe

Ansprache von Divisionär A. Guisolan, Waffenchef der Uebermittlungstruppen am 11. Jahresrapport der Offiziere der Uebermittlungstruppen 1975 in Locarno

Am 14. Januar 1970 veröffentlichte «Pacific Stars and Stripes» eine Meldung unter dem Titel «Nordvietnamesische Funker brechen U. S. Code»: Kürzlich gaben nordvietnamesische Funker in fehlerfreiem Englisch eine Meldung an ein U.S. Feuerkoordinationszentrum durch, mit der sie Feuer auf einen grösserer amerikanischen Verband anforderten.

Diese List schlug nach amerikanischen Kommentatoren zwar fehl, hatte aber zur Folge, dass eine umfangreiche Suchaktion in allen Provinzen rund um Saigon gestartet wurde mit dem Ziel, die nordvietnamesische Abhorchzentrale auszuheben. Der Aktion war Erfolg beschieden. Ein Verband der 25. Infanterie-Division entdeckte ein unterirdisch angelegtes Abhorch- und Sendezentrum zirka 60 km nördlich Saigon, machte 12 Gefangene und stellte Geräte aller Art sicher, so unter anderem Empfänger primitivster Art, abgeänderte Sony-Transistorradios, erbeutete amerikanische Funk-Meldungen wurden aufgefunden. Jedesmal wenn die U. S. Funker anstelle des offiziellen, einen eigenen Privatcode benutzten, wurden von den kommunistischen Abhorchern Zeit-, Orts- sowie Truppenangaben eruiert und in Klarschrift auf dem Original rot eingetragen. Auf diese Weise waren die Nordvietnamesen in der Lage, sich amerikanischem Artilleriefeuer, Luftangriffen und Hinterhalten zu entziehen. Die Gefangenen bestätigten, dass sie praktisch alle Privatcode, die aus Bequemlichkeitsgründen dem offiziellen, sicheren vorgezogen wurden brechen konnten, wogegen die reglementarischen Verfahren den primitiven Dekryptiermethoden durchwegs Stand hielten. Was dann allerdings in der westlichen Presse als Schlagzeile erschien, lautete: «Nordvietnamesen knacken amerikanischen Code»!

Ein anderes Beispiel:

Im Verlaufe der Kämpfe entwickelten die Nordvietnamesen eine erstaunliche Fertigkeit auf dem Gebiet der Täuschung.
Ihre Operateure sprachen fliessend akzentfreies Amerikanisch, einige imitierten regionale Slangs, ohne dass dies bemerkt werden konnte.

Fall 1:

Ein Anrufer, der sich als Operateur der Station LIMELIGHT ausgab, verlangte von der Station LITTLE JOE ALFA Auskunft, wann die Helikopter am Morgen starten würden. Die Antwort lautete prompt: 0730! Zuspät dämmerte es dem Operateur von LITTLE JOE ALFA, dass LIMELIGHT die ganze Nacht über nicht in der Luft ge-

pionier

48. Jahrgang Nr. 7 Juli 1975

Zeitschrift für Verbindung und Uebermittlung

Offizielles Organ des
Eidg. Verbandes der Uebermittlungstruppen (EVU) und der
Schweiz. Vereinigung der Feldtelegraphen-Offiziere und -Unteroffiziere

Organe officiel
de l'Association fédérale des Troupes de Transmission et de l'Association des Officiers et Sous-officiers du Télégraphe de campagne

Redaktion:
Erwin Schöni, Hauptstrasse 50
Postfach 34, 4528 Zuchwil
Telefon (065) 25 23 14
Postcheckkonto 80 - 15666

Inserateverwaltung:
Annoncenagentur AIDA
Postfach, 8132 Egg ZH
Telefon (01) 86 27 03 / 86 06 23

Erscheint am Anfang des Monats
Druck: Buchdruckerei Erwin Schöni
4528 Zuchwil

wesen war und nie derartige Auskünfte verlangte. Beim nächsten Anruf verlangte er die Funkerkennung, damit schwieg dann die gegnerische Station prompt.

Fall 2:

In einem amerikanischen Unterstand klingelte das Telefon; der Gesprächspartner kündigte das Essen an. Die Mannschaft verliess die Waffen, begab sich ins Freie; was dann kam, war ein nordvietnamesischer Stosstrupp! Diese Falle kostete drei Amerikanern das Leben!

Die Beispiele liessen sich beliebig vermehren. Sie sind allesamt vielleicht wenig spektakulär, in ihrer grossen Summe aber sind sie Zeugnis für sinnlos vergossenes Blut, grosse Materialverluste und Niederlagen im Gefecht!

Sie alle kennen die Verhältnisse in unserer Armee. Die Funkdisziplin, die Ausbildung weisen ebensolche Mängel auf, für welche die Amerikaner teuer bezahlen mussten. Zudem fehlen unseren Soldaten praktische Erfahrungen und Gewandtheit im Umgang mit gegnerischen Abhorch-, Stör- und Täuschungsstationen.

Ich will mit den eingangs genannten einfachen Beispielen aus der jüngsten Praxis nur andeuten, was im Titel des heutigen Vortrages steht, dass nämlich die Elektronik, die Uebermittlung — ganz allgemein — Information Waffe sein kann. Nicht einfach passives Hilfsmittel, technisches Gerät allein! Wir sind gerne geneigt, alles was nicht schiesst, was nicht explodiert oder brennt, als zweitrangig und nicht relevant im Sinne des Gefechtswertes zu betrachten. Dies ist ein gefährlicher Irrtum. Ohne echte, unverfälschte Information sind wir militärisch völlig machtlos. Kein vernünftiger Entschluss kann gefasst werden, wenn über den momentanen Gegner, seine Standorte, Stärke, Mittel, Absicht und Möglichkeiten keine oder nur unsichere Angaben vorliegen.
Aber in gleichem Masse sind wir machtlos, wenn wir unsere eigenen Vorhaben nicht in die Tat umsetzen können, weil wir unsere Untergebenen nicht erreichen, die Verbindungen unterbrochen sind!

Information ist Macht

«Information ist Macht!» gilt auch im militärischen Bereich. Je länger je mehr sogar! Je mehr nämlich der Informationsbedarf steigt, je rascher Information verfügbar sein muss, desto häufiger gelangen elektronische Hilfsmittel zum Einsatz. So begeben wir uns immer häufiger in die Abhängigkeit von Fernmeldeverbindungen, Bild- und Datenübertragungsmitteln sowie Datenverarbeitungsanlagen. All diese Mittel transportieren oder verarbeiten Information, sie sind deshalb Angriffspunkt höchsten Interesses für jeden Gegner. Elektronischen Systemen kommt nur mit anderen elektronischen Systemen bei. Letztere haben demnach den Charaker von eigentlichen elektronischen Waffen. Und über diese elektronischen Waffen möchte ich nun etwas eingehender sprechen.

Wenn wir Ansatzpunkte für elektronische Waffen suchen, müssen wir bei den Informationsquellen beginnen. Und die wichtigste Quelle ist bekanntlich der Mensch, dessen Schicksal es zu sein scheint, alles was er weiss, mitteilen zu müssen.

Die moderne Mikroelektronik wird deshalb auch dazu verwendet, dort Information zu gewinnen, wo sich der Mensch ungestört glaubt, nämlich in seiner Intimsphäre. Die Geräte sind unter dem Namen Minispione bekannt und stellen im wahren Sinne des Wortes elektronisches Ungeziefer dar, das im Dunkeln lauert und jederzeit zum Stechen und Saugen bereit ist.

Die Vorstellungen, welche man sich in der Oeffentlichkeit vom Einsatz solcher Geräte macht, sind zumeist unklar, ihre Wirksamkeit und Verwendungshäufigkeit werden unterschätzt. Überall wo heute Information entsteht, wo also Gespräche geführt werden, wo geschrieben wird, ist mit dem Einsatz elektronischer Waffen zu rechnen. Beliebtester Ansatzpunkt für das elektronische Ungeziefer ist einerseits das Konferenz-, anderseits das Schlafzimmer. Manchmal aus verschiedenen Beweggründen, häufig aus dem gleichen! Der Lauscher an der Wand ist durch diese Geräte allgegenwärtig geworden. Er gewinnt Staatsgeheimnisse, militärische Geheimnisse, Geschäftsinterna und Intimgeheimnisse ständig und überall.

Solche Geräte haben eine Reichweite von mehreren hundert Metern und übertragen alle Gespräche sehr klar und verständlich. Es gibt Modelle, welche nur senden, wenn gesprochen wird, andere lassen sich ferneinschalten, insbesondere Telefonabhörgeräte, die von einer Sprechstelle aus mit Hilfe von Pfiffen oder einer kleinen Mundharmonika in Betrieb gesetzt werden. Neben drahtlosen Geräten werden laufend anlässlich minutiöser Untersuchungen besonders gefährdeter Objekte, wie Botschaften, Konferenzräume, Hotelzimmer für illustre Gäste und dergleichen mehr auch eine Unzahl von Mikrofonen zutage gefördert, die im gleichen Haus oder vom Nachbargebäude her abgehört werden. Aber nicht nur der Ton wird aufgefangen, auch das Bild ist von Interesse. Zu diesem Zweck lauern auch Infrarot-TV-Kameras im Verborgenen. So wird Information an der Quelle gewonnen. Das Perfide an der Sache ist, dass die elektronischen Wanzen neuerdings in sehr hohen und sehr tiefen Frequenzbereichen tätig werden und sich so den heutigen Spürgeräten entziehen. In der Tat bedrohen Minispione das staatliche und private Geheimnis in vielfältigster Weise. Auch sind ingenieuse Varianten bekannt, die praktisch nicht eruierbar sind. Auch die neuen Gesetze zum Schutz der Privatsphäre haben diese Mittel nicht wesentlich zurückgedrängt, weil die Möglichkeien der Strafverfolgungsorgane eben sehr eingeschränkt sind.

Neben der Quelle wird aber auch die Verbindung mit Vorliebe zur Beschaffung von wichtiger Information angezapft. Am leichtesten ist dies bei der Funkverbindung möglich. Aber auch die Drahtverbindung wird nicht verschmäht.

Gefährdet sind alle Uebermittlungsmittel

In permanenten zivilen Netzen ist Anzapfung am leichtesten im Bereich des Teilnehmers, sekundär im Bereich der Zentralen und am schwierigsten unterwegs, bei den Kabeln möglich. Anzapfungen werden meist über kurz oder lang festgestellt. Pannen sind an der Tagesordnung.

Entweder treten Störungen im automatischen Betrieb der Fernmeldenetze auf oder dann wird die Montage, auch die Ueberwachung der Anzapfung festgestellt. Der vorsichtige Lauscher bevorzugt daher lieber die drahtlose Methode. In meinen bisherigen Ausführungen habe ich die aktiven Lauschmethoden mit Hilfe von Sendern behandelt. Das Gespräch zwischen zwei Partnern kann natürlich auch mit Hilfe von Spezialmikrofonen über mehr als 100 m aus dem Umgebungsgeräusch herausgehört werden. Wissen Sie aber, dass es sogar möglich ist, das Geräusch eines laufenden Fernschreibers zu analysieren und aus ihm den Text zu rekonstruieren? Das mit Hilfe einer einfachen Apparatur, die in die Steckdose gesteckt wird, der Klartext einer Fernschreibmaschine unter Umständen einen Häuserblock weiter wieder gewonnen werden kann? Wenn das allgemein bekannt wäre, könnten sich viele Leute, die heute Geheimnisse der Drahtverbindung anvertrauen, wie Ermittlungsbehörden, Banken, Versicherungen, Industrie- und Handelsfirmen, nicht mehr so wohl fühlen. Solche Einbrüche in die Intimsphäre sind äusserst gefährlich, weil die Einbruchsmöglichkeit unbekannt ist und im allgemeinen der Fernschreiber als sicheres Mittel angesehen wird. Selbst Chiffrieren nützt da nichts, wenn der Fernschreiber Klarsignale über Leitungen abstrahlt.

Erstaunlich ergiebige Quellen geben heute aber die modernsten Informationsverarbeitungsmaschinen, die elektronischen Datenverarbeitungsgeräte und ihre Fernübertragungseinrichtungen ab. Die Uebertragungsverfahren sind standardisiert und es macht keine besondere Mühe, den Verkehr der Ferndatenverarbeitung aufzunehmen. Datenverarbeitungsfirmen und Benützer bemühen sich heute gemeinsam, die Datensicherheit zu gewährleisten, doch können die getroffenen Massnahmen nicht als ausreichend für Fachspezialisten mit entsprechendem Gerät angesehen werden. Es scheint mir aus diesem Grunde vorderhand noch sehr gefährlich, hoch klassifizierte Angaben der Datenverarbeitungsanlagen und ihren Massenspeichern zu übergeben. Datenverarbeitungsanlagen selber können auch wieder als elektronische Waffen im vorerwähnten Sinne verwendet werden. Einerseits als unentbehrliches Hilfsmittel zum

Brechen von Codes, andererseits als Informationsbank. Zwar überschätzt der Nichtfachmann die Möglichkeiten des Computers in der Dekryptiertechnik gewaltig. Gut konzipierte elektronische Chiffriergeräte weisen Elemente auf, die einen modernen, schnellen Grosscomputer Tausende von Jahren beschäftigen würden, damit die nötige Transparenz erzielt würde, die Voraussetzung für das Brechen der Schlüssel ohne wesentliche Vorkenntnisse wäre.

Der Computer als Waffe

In unserer Armee ist der Computer als Waffe zwar bereits in Erscheinung getreten, allerdings nicht als einzeln dastehendes System, sondern als Herz von eigentlichen Waffensystemen. Denken Sie an Lenkwaffensysteme, FLORIDA, radarisierte Flab.

Wir sind heute in der modernen Waffentechnik soweit, dass wir uns je länger je mehr nicht nur mit dem ballistischen Schuss begnügen; wir fordern, dass unsere Waffen einem beweglichen Ziel folgen und es vernichten können. Ohne Elektronik geht das niemals, ganz einfach, weil mechanische Rechen- und Regeleinrichtungen viel zu träge und in ihren Möglichkeiten allzu beschränkt für diesen Zweck sind. Die Elektronik weist in ihrer Kompaktheit bei gleichzeitig hoher Zuverlässigkeit alle Eigenschaften auf, die in der modernen Kriegstechnik verlangt werden. Wir stehen gegenwärtig von einer neuen Aera, wo die Elektronik ihre Ecke im Bereich der Militärtechnik verlässt und sukzessive neue Bereiche erobert. Bald wird sie zum Huckepack des Infanteristen gehören, wie das Militärmesser zu seinem Hosensack. Obwohl diese Aussage für den Augenblick noch übertrieben erscheine mag, können Sie diese Entwicklung doch erahnen, wenn Sie sich vorstellen, mit welcher Selbstverständlichkeit Sie sich der zivilen Fernmeldeeinrichtungen, der Heimelektronik, des Tisch- und Taschencomputers bedienen.

Gerade das letztgenannte Gerät zeigt deutlich den Riesensprung, den die Elektronik in 15 Jahren genommen hat. Was Sie heute bequem aus der Tasche ziehen, einen wissenschaftlichen Taschenrechner zum Beispiel, hätte vor 15 Jahren einen Saal mit Röhrenelektronik gefüllt, einen Leistungsbedarf wie eine elektrische Grossküche erfordert und im übrigen gar nicht funktioniert, weil die mittlere Zeit zwischen aufeinanderfolgenden Defekten nur Minuten betragen hätte. Und so wird eben der Infanterist in Zukunft nicht mehr ein gewöhnliches Funkgerät mit sich herumschleppen, sondern einen Computer. In der Tat gleichen die neuesten Entwicklungen auf dem Funksektor eher einem Computer, denn einem Funkgerät. Weshalb das, wenn es anders auch geht, wird man fragen.

Die Antwort ist einfach. In Zukunft wird es eben ohne nicht mehr gehen, weil einerseits die Frequenzbänder gesättigt sein werden und andererseits zusehends mehr Abhör- und Störmittel in Erscheinung treten werden. Und Verbindung muss sein, besonders dann, wenn Führer und Truppe immer beweglicher werden oder werden müssen.

Die Elektronik als zuverlässiger Partner

An ein taktisches Funkgerät werden deshalb Forderungen gestellt, die nur mit zusätzlichem inneren Aufwand zu bewältigen sind. Einige Beispiele: Die Kanalvereinbarung und -Zuordnung hat zwischen den Geräten vollautomatisch zu erfolgen. Eine starre Zuordnung garantiert keinen sicheren Betrieb mehr. Wenn man aber diesen Automatismus einführt, wird eine Adresskennung nötig, ein besonderes, nicht konventionelles Uebertragungsverfahren und so ruft eine Massnahme die andere. Insgesamt hat dann das Funkgerät die Eigenschaften Kanalautomatik, Adressierung, automatische Relais, Simplex- und Duplexbetrieb, geringe Peil- und Störbarkeit sowie automatische Chiffrierung. Dies alles bedingt integrierte Elektronik, die weit über den Taschencomputer hinausgeht. Was ich ihnen hier sage, ist nicht Wunsch, sondern Tatsache — Prototypen stehen vor der Türe!

Wer ein solches System besitzt, ist einem Widersacher gegenüber entscheidend im Vorteil. Sein Standort kann nur schwer bestimmt werden, das Gespräch kann nicht mitgehört, die Partner können nicht identifiziert, die Verbindungen nur sehr schwer gestört werden. Elektronik wird so zur Waffe.

Auch der Computer allein wird bald als modernes Artilleriefeurleitgerät Geschwindigkeit und Sicherheit des Artilleriefeuers verbessern.

Gross-Datenverarbeitungsanlagen sind im militärischen Verwaltungsbereich nicht mehr wegzudenken. Für den Verteidigungsfall wichtige Informationen, vorläufig meist im logistischen Bereich, werden in Datenbanken abgespeichert und stehen den Sachbearbeitern in jeder wünschbaren Form zur Verfügung. Der Logistik nachfolgen werden sicher das Personelle und der Nachrichtendienst. Informationssysteme im Verwaltungsbereich lassen bald den Wunsch aufkommen oder werden erzwingen, dass den höheren Stäben diese Computerdienste ebenfalls zur Verfügung stehen müssen. Die Datenverarbeitung zugunsten der Armee und ihrer grossen Verbände befindet sich gegenwärtig im Studium bei meiner Dienstabteilung. Ob sie jedoch eingeführt werden kann, lässt sich nicht vorhersagen, da die Bedürfnisfrage noch offen ist. Auch zwingen die finanziellen Engpässe zu einer rigorosen Prioritätenordnung. Wenig Anklang findet bei höheren Kommandanten auch der Gedanke, sich in Zukunft nicht nur mit Reglementen, Befehlen und Befehlssammlungen, sondern auch noch mit Computern herumschlagen zu müssen. Es wird aber verkannt, dass mit dem Computer eben viele dieser Papiergrundlagen in Wegfall kommen könnten, dass ein universell aufgebautes militärisches Informationssystem bessere Entscheidungsgrundlagen, verbunden mit Aufwand- und Zeitersparnis bieten könnte. Die Geschichte zeigt, dass sich neue Mittel gegen alle Widerstände durchsetzen. In diesem Sinne bin auch ich davon überzeugt, dass man in 20 Jahren darüber lächeln wird, was uns heute noch als Frage erscheint.

Einige Aspekte der elektronischen Kriegführung

Sie werden sich wundern, dass ich noch nicht auf die schärfste elektronische Waffe, die Elektronische Kriegführung eingetreten bin. Tatsächlich darf man hier nicht nur im übertragenen Sinne von Waffe sprechen.

Das wird durch die Tatsache bewiesen, dass sowohl die West-, wie auch die Ostmächte ausserordentlich hohe Investitionen auf diesem Gebiet tätigen. Beim elektronischen Krieg fliesst zwar unmittelbar kein Blut, hingegen wird sehr viel Gehirnschmalz verspritzt. In diesem Krieg messen sich die findigsten Köpfe. Jede Massnahme wird mit einer Gegenmassnahme gekontert.

Jedesmal, wenn eine Massnahme der Elektronischen Kriegführung zum Erfolg kommt, bedeutet dies den Ausfall eines Waffensystems von hohem Kampfwert. Das ist gleichbedeutend mit einer vorübergehenden Zerstörung. Ein gestörtes Lenkwaffen- oder Feuerleitsystem macht den Waffeneinsatz unmöglich. Das Elegante an der Elektronischen Kriegführung ist ihr hoher Nutzwert, das heisst, mit einem verhältnismässig geringen Aufwand werden teure Systeme ausser Gefecht gesetzt.

Ein weiteres hervorstechendes Merkmal ist die Wirkung über grosse Räume hinweg und die Unmittelbarkeit derselben. Die Elektronische Kriegführung ist die absolut schnellste Waffe, sie arbeitet mit Lichtgeschwindigkeit.

Sie hat zum Ziele, Information über gegnerische elektronische Systeme zu sammeln, diese in ihrer Wirkung zu beeinträchtigen und die eigenen Systeme zu schützen.

Sie gliedert sich folgerichtig in Elektronische Gegenmassnahmen (EGM), gemeint sind Aufklärung, Störung und Täuschung und in Elektronische Schutzmassnahmen (ESM), gemeint sind taktische, betriebliche und technische Vorkehren, um die eigenen Anlagen vor Aufklärungs- und Störeinwirkung möglichst zu schützen.

Die Elektronische Aufklärung ist die legale Spionagetätigkeit. Sie steht deshalb auch dem Neutralen zu. Ohne gegnerisches Gebiet betreten zu müssen, lassen sich wertvolle Informationen über Standort und Art von Sendestellen gewinnen; diese Angaben ihrerseits lassen wiederum Rückschlüsse auf Kommandostrukturen, Lage und Absicht von Verbänden zu.

Sie wissen, dass sich die grossen Rivalen heute zu Lande, zu Wasser und in der Luft mit ungeheurem Aufwand elektronisch be-

lauern und bespitzeln. Ich erinnere nur an die ernsthaften Zwischenfälle, die aus dieser Aufklärungstätigkeit resultierten. Stichworte sind der Pueblo-Zwischenfall, die U2-Affäre, der Beschluss einer EC-130 durch libysche Jäger. Ebenso gut bekannt ist die Tätigkeit von gewissen sowjetischen Fischkuttern, die ihre Netze nicht unbedingt dort auswerfen, wo Fischgründe liegen.

Obwohl man nicht gerne darüber spricht — nicht umsonst ist der Schutzpatron der elektronischen Krieger ein Tierwesen der Schwarzmagier — darf hier gesagt sein, dass wir in unserer Armee doch seit dem letzten Weltkrieg dauernd Anstrengungen unternommen haben, um unsere Mittel und Verfahren auf dem Stande der Zeit zu halten.

Sie können sich vorstellen, dass wir mit unserem Milizsystem darauf angewiesen sind, für diese Sonderfunktionen des Funkaufklärers nur bestausgewiesene junge Leute zu rekrutieren. Seit 1973 sind wir dazu übergegangen, Funkaufklärungsspezialisten in einer eigenen Schule in der Nähe von Thun auszubilden.

Die aktiven Massnahmen, insbesondere die Elektronische Störung befindet sich bei uns noch im Versuchsstadium. Für Ausbildungszwecke setzen wir in Uebungen und Manövern von grösseren Verbänden den Störsender Grobian ein.

Möglichkeiten der elektronischen Kriegführung bei uns nicht ausgeschöpft

Es darf gesagt werden, dass die Möglichkeiten der Elektronischen Kriegführung bei uns noch längst nicht ausgeschöpft sind. Die gegenwärtige Entwicklungsrichtung läuft auf eine weitgehende Automatisierung der Bandüberwachung, Ortung und Signalanalyse hinaus. Diese Automaten vermögen das Aufklärungsrendement um einen Faktor 20—100 zu steigern. Gleichzeitig sind die Störanlagen mit den Aufklärungsanlagen zu integrieren und gewinnen damit beträchtlich an Wirksamkeit.

Es ist mir persönlich ein dringliches und wichtiges Vorhaben, der Elektronischen Kriegführung in unserer Armee zur Weiterentwicklung zu verhelfen. Eine diesbezügliche umfassende Studie mit konkreten Ausbauanträgen ist durch die oberste Entscheidungsinstanz behandelt worden.

Wir sind der absoluten Ueberzeugung, dass der Einsatz moderner elektronischer Aufklärungs- und Störsysteme für unsere Armee und ihren Abwehrerfolg entscheidende Beiträge zu leisten vermag. Bedenken Sie die Eindringtiefe der Elektronischen Aufklärung: Wir empfangen Signale aus vielen tausend Kilometern Entfernung, wir orten Sender in mehreren hundert Kilometern vor unserer Grenze, wir werten wichtige Meldungen unverzüglich aus und geben sie an den Nachrichtendienst weiter. Ein einziger Störsender moderner Bauart vermag den Funkverkehr eines gegnerischen mechanisierten Grossverbandes weitgehend zu lähmen. Ich frage: Welcher mechanisierte Gegner kämpft in unbekanntem Gelände, bezeichnet Ziele, manövriert ohne Funkkontakt?

Sie sehen also: Der Aufwand für elektronische Waffen in der geschilderten vielfältigen Art lohnt sich durchaus. Er kommt direkt oder indirekt der kämpfenden Truppe zugute. Sie hat bessere Nachrichten über den Feind, sie weiss seine Beweglichkeit und Feuerkraft beeinträchtigt.

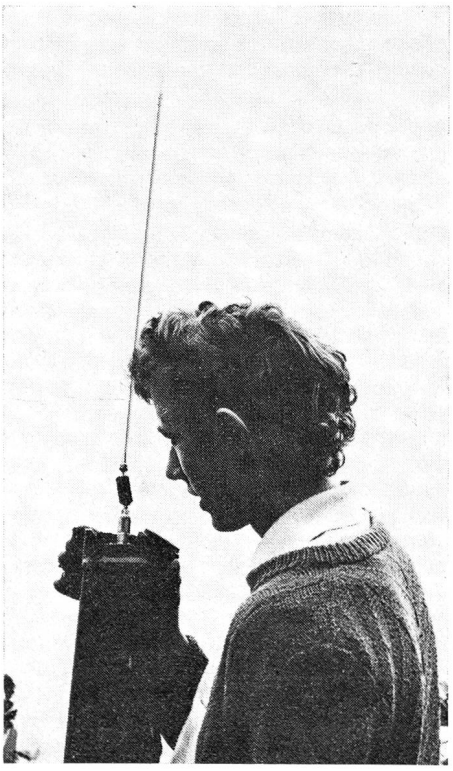
Etwas muss dafür bezahlt werden. Ich bin aber froh, wenn es mir gelungen sein sollte, zu zeigen, dass wir von der Uebermittlung nichts zum Selbstzweck tun dürfen; im Gegenteil, wir haben alles zu versuchen, um der kämpfenden Truppe die besten Voraussetzungen zum Erfolg zu verschaffen.

Massnahmen im Zusammenhang mit dem Jedermannfunk

Information der Sektion Zürichsee rechtes Ufer

Die Infomationstagung von Glattbrugg über den Jedermannfunk hat einige Schwierigkeiten mit diesem aufgezeigt. Auch wenn dies nicht die Zielsetzung der Tagung war, so sind wir den Organisatoren trotzdem dafür dankbar, dass sie das Problem aufgegriffen haben.

Die Sorgen mit dem 27-MHz-Band sind nicht neu. Bereits in der Sitzung der Technischen Kommission des EVU vom April 1974 wurde darauf hingewiesen, dass «die PTT darauf aufmerksam gemacht werden muss, dass die Benützer des 11-m-Bandes ihre Tätigkeit nicht kommerziell ausausnützen dürfen». Weiter wurde festgestellt, dass auf der Seite des EVU die Uebermittlungsdienste zugunsten Dritter vermehrt koordiniert werden sollten. Auch die Mietgebühren standen zur Diskussion. Inzwischen ist wiederum ein Jahr verstrichen, ohne dass ein Vorhaben auch nur teilweise verwirklicht worden wäre. Wir halten es aber für verfehlt, nun darüber zu lamentieren, vielmehr wollen wir die Massnahmen aufzeigen, welche die Sektion Zürichsee rechtes Ufer bereits eingeleitet hat.



Diskussionen und Streitereien sind kaum die geeigneten Mittel, die aufgetauchten Schwierigkeiten zu meistern. Nur ein qualitativ gutes und preislich günstiges Angebot vom EVU im Uebermittlungssektor wird Erfolg haben. Die technischen Mittel dazu — im Bild das moderne SE-125 — haben wir in der Hand. (evu-bild)

1. Funküberwachung

Seit einem Jahr verfügt die Sektion über Empfänger, mit denen der Funkverkehr überwacht werden kann. Diese Funküberwachung ist seit einiger Zeit intensiviert worden. Wir sind darüber im Bilde, dass Jedermannfunker illegale Einsätze leisten, dass nicht erlaubte Geräte verwendet werden und dass die PTT nicht eingreift.

2. Verbessertes EVU-Angebot

Wir haben seit eineinhalb Jahren die Ausbildung unserer Mitglieder verbessert. Ausgerüstet mit den SE-125 können wir den Veranstaltern Funknetze anbieten, welche dem kommerziellen Standard entsprechen. Für alle Funknetze leisten wir heute eine technische Funktionsgarantie. Wir wissen, dass die Jedermannfunker hier zurückstehen müssen.

3. Werbung

Wir bereiten neue Informationskampagnen vor. Damit möchten wir darlegen, dass es möglich ist, auf Sektionsebene sich der neuen Situation anzupassen.

Hansjörg Spring

Redaktionelle Ergänzung

Mit dem redaktionellen Artikel in der letzten Nummer des «Pionier» über die Glattbrugger Tagung sollte nicht der Eindruck erweckt werden, dass sich der EVU gegen die Jedermannfunker zur Wehr setzen sollte, um auf der andern Seite aber innerhalb des EVU das ganze Problem «Uebermittlungsdienste zugunsten Dritte» im bisherigen amateurhaften Rahmen weiterführen zu wollen. Das Gegenteil ist der Fall. Die Stellungnahme der Sektion Zürichsee rechtes Ufer zeigt auf, dass wir unsere Dienste in weit besserer Form der Oeffentlichkeit