Méthodes modernes de chiffrement de la voix

send an den Wettbewerb wird die Übung bis Sonntagmorgen unterbrochen.
Die neue Betriebsbereitschaftszeit ist auf Sonntag, 26. September 1982 um 0800 Uhr angesetzt. Dabei sollen die fünf Zentren Gelegenheit haben, je nach Art ihrer Netze zu den jeweiligen Aussensektionen eine eigene Übung zu verwirklichen. Ab Sonntag 1100 Uhr sind die Abbrucharbeiten in Angriff zu nehmen.
Sache der Übungsleitung ist es in der Folge, CAPITO 82 auszuwerten, Wettbewerbsgewinner zu ermitteln und Schlüsse aus der Übung zu ziehen.

Eingesetztes technisches Material

Telefon- und Drahtmaterial	
Telefonzentralen TF Zen 64	10
Telefonstationen A Tf 50/53	150
Feldkabel F-2E/20	50 km
Fernschreibmaterial	
Blattfernschreiber Stg-100	30
Kryptofunkfernschreiber KFF-58/68	30
Lochstreifensender LU-68	20
Funkmaterial	
Kurzwellenfunkstation SE-222	30
Sprechfunkgeräte SE-412 und SE-227	über 20
Richtstrahlmaterial	
Richtstrahlgerät R-902	10
Mehrkanalgeräte MK-5/4	10

Neben diesem Material gelangen Spezialempfänger und -Antennen, Kleinfunkgeräte SE-125 und SE-208 sowie ein beachtlicher Park von Militärfahrzeugen zum Einsatz.

Verbindungen

Das *Drahtnetz* bildet das eigentliche Rückgrat von CAPITO 82. Diese zuverlässigen und weitgehend störungsfreien Verbindungen laufen grösstenteils über das Leitungsnetz der PTT-Betriebe. In Absprache mit den TT-Betriebsgruppen werden die benötigten Verbindungen geschaltet und von den Anschlusspunkten im Truppenbau bis an den Übungsstandort verlängert.
Ausgebaut und überlagert wird dieses Drahtnetz mit *Kleinrichtstrahlverbindungen*. Diese Richtfunkverbindungen hoher Zuverlässigkeit sind im Gegensatz zu reinen Drahtverbindungen abhörgefährdet. Ein unverschleiertes Telefongespräch über Kleinrichtstrahl ist deshalb nicht zulässig.
Über beide Mittel – Draht und Kleinrichtstrahl – können *Fernschreib-* und *Telefonverbindungen* geführt werden. Für die Fernschreibverbindungen findet der *Blattfernschreiber Stg-100* Verwendung.
Mit dem *Funkfernschreiber KFF-58/68* wird in den Kurzwellenfunknetzen zwischen Stationen SE-222 gearbeitet. Solche Verbindungen bestehen landesweit; im Gegensatz dazu sind *Sprechfunkverbindungen* mit den Geräten SE-412 und SE-227 nur regional möglich. Die Dämpfung des elektromagnetischen Bereiches im Frequenzbereich zwischen 25 und 80 MHz ist vor allem durch Hindernisse in der Verbindungsstrecke so gross, dass überregionale Verbindungen nicht möglich sind.

In den Abb. 2 sind die Übermittlungsnetze ab Stufe Zentrum bis zu den jeweils angeschlossenen Aussensektionen wiedergegeben. Für den personellen und materiellen Einsatz in einem Zentrum ist natürlich noch zusätzlich der Aufwand für die Verbindungen der Zentren untereinander sowie zur Gesamtübungsleitung zu berücksichtigen (Abb. 1).
F. Engler leitet das Zentrum Zürich; an diesem Standort im Zivilschutz-KP Unterengstringen wird auch die Übungsleitung tätig sein.
Am Standort Lenzburg betreiben die Sektionen Aarau, Baden und Lenzburg zusammen ein Zentrum. Chef dieses Zentrums ist der Lenzburgische Sektionspräsident H.-P. Imfeld.
Das Zentrum der Sektion Bern wird in Schwarzenburg stationiert sein. Geleitet wird dieses Zentrum von P. Suter.
Das vierte Zentrum unter der Leitung des Sektionspräsidenten A. Furrer befindet sich in Luzern, und schliesslich haben sich, was uns besonders freut – auch unsere welschen Kameraden dazu entschlossen, in Lausanne ein Zentrum der Sektion Vaudoise, geleitet von J.-L. Jennet, zu betreiben.

Anmerkung der Redaktion

Die französische Fassung dieses Artikels über die gesamtschweizerische Übung CAPITO 82 folgt in der nächsten Ausgabe.

Organisation der Zentren

Zentrum Zürich	
Sektionen:	Zürich Zürichsee rechtes Ufer
Standort:	Unterengstringen
Leitung:	F. Engler
Zentrum Lenzburg	
Sektionen:	Aarau Baden Lenzburg
Standort:	Lenzburg
Leitung:	H.-P. Imfeld
Zentrum Bern	
Sektion:	Bern
Standort:	Bern
Leitung:	P. Suter
Zentrum Luzern	
Sektion:	Luzern
Standort:	Luzern
Leitung:	A. Furrer
Zentrum Lausanne	
Sektion:	Vaudoise
Standort:	Lausanne
Leitung:	J.-L. Jennet

TÉLÉCOMMUNICATIONS CIVILES

Crypto SA., Zug

Méthodes modernes de chiffrement de la voix

Il est évident que le but d'un équipement de chiffrement de la voix est de trouver un système présentant les caractéristiques suivantes:

- **sécurité maximale**
- **capacité de duplex intégrale**
- **bonnes performances en dépit de mauvaises conditions de communication**
- **poids réduit**
- **dimensions compactes**
- **et prix bas.**

Il est également clair qu'une telle unité n'est pas disponible sur le marché d'aujourd'hui et l'on peut supposer qu'elle ne le sera pas dans un proche avenir.
Compte tenu de la grande diversité des systèmes de sécurité de communication, de leur évolution rapide et de la sophistication des réseaux et des dispositifs de communication, l'évaluation des équipements disponibles est devenue une tâche assez ardue.

Quels sont donc les critères essentiels pour le choix du meilleur équipement à acquérir? Ce sont, à notre avis, les suivants:

Degré de sécurité

La décision la plus fondamentale que l'utilisateur doit prendre concerne la définition du niveau de protection; en d'autres termes, quel genre d'informations nécessite quel degré de sécurité et pour quelle durée? Evidemment, cette décision doit être prise avant d'identifier la technologie du produit.
La seconde décision, tout aussi importante, concerne le maniement de la clef – c'est-à-dire la génération, la distribution, l'introduction et la vérification de l'information – qui doit être pris en considération comme composant intégral de n'importe quel système de chiffrement de la voix.
De plus, un équipement moderne de chiffrement de la voix présentera – à l'intérieur du système de maniement de la clef – de grandes

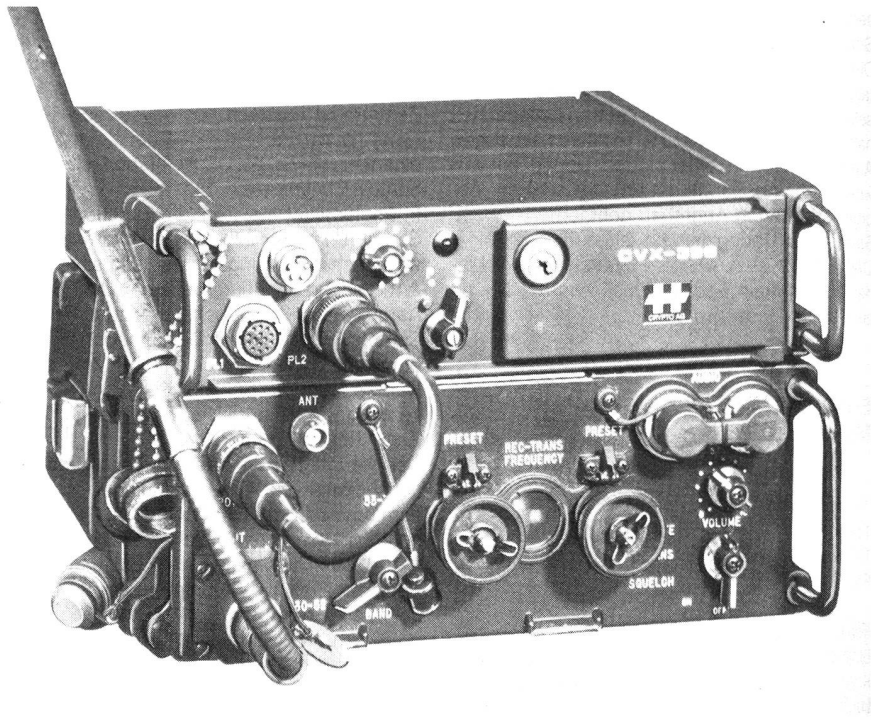
facilités pour l'identification positive de l'utilisateur afin d'éviter les violations de la sécurité des communications par des imposteurs.

Voies de communication

De façon idéale, la sélection d'un équipement de chiffrement devrait précéder la conception d'un système de communication. Cependant, l'unité de chiffrement de la voix doit normalement être intégrée dans un réseau existant.
Les méthodes de transmission, c'est-à-dire HF-SSB, VHF/UHF, circuits téléphoniques, liaisons à large bande ou même toutes celles-ci à des moments différents, ont une influence directe sur la technique de chiffrement qui doit être appliquée.

Environnement d'opération

Les considérations normales ayant rapport à la facilité de montage, d'utilisation et d'opération sont applicables. Cependant, d'autres facteurs tels que l'adaptation de niveau, les raccordements et la commande à distance, l'installation fixe ou mobile, en semi-duplex ou duplex intégral, influencent la décision concernant le choix du système à retenir.
Le degré suivant dans le processus d'évaluation consiste à prendre en considération et à comparer les méthodes de chiffrement de la voix existantes. En principe, il y a deux méthodes de ce genre, à savoir: numérique et analogique.
Le traitement numérique des signaux offre la sécurité cryptologique la plus élevée, sans aucune intelligibilité résiduelle dans la voie de transmission. De nos jours, il est possible de transformer le signal de la voix en un signal digital (conversion A/D) avec un taux de bits allant normalement de 9,6 à 40 kbps, mais cette cadence de retransmission nécessite une largeur de bande spécifique de 10 KHz, ce qui est beaucoup trop élevé pour retransmettre dans un canal la bande vocale de 300–3000 Hz.



Le dispositif de chiffrage linguistique-numérique CRYPTOVOX CVX-396 garantit une sécurité de chiffrement maximale, et peut sans la moindre modification être branché directement sur le SE-227 et sur le SE-412. Il opère de manière entièrement automatique, également comme station de relais, et transforme chaque réseau radiophonique en un système de communication hautement protégé. Il exécute toutes les demandes exigées pour la sécurité de vos informations militaires.

Depuis peu de temps seulement, des unités de codage linéaire prophétique (LCP=linear predictive coding) ont été développées et fournissent une assez bonne qualité de reproduction de la voix à 2,4 kbps.
Par conséquent, le traitement analogique des signaux est la méthode de chiffrement la plus courante pour les canaux normaux de grade vocal (300–3000 KHz), tels que les lignes téléphoniques, les radiotéléphones VHF/UHF et les liaisons HF-SSB.
Il existe, en rapport avec les deux méthodes de chiffrement de la voix mentionnées ci-dessus, plusieurs alternatives. Leurs caractéristiques principales peuvent être définies comme suit:

Facteurs de comparaison	Besoins du canal				Mode d'opération			Encombrement et poids				Reconnaissance du speaker				Qualité de reproduction de la voix				Niveau de sécurité			Coûts		
Méthodes de chiffrement de la voix	40 kHz + (PCM)	9.6 – 20 kHz (V/UHF)	3 kHz (TF)	2.7 kHz (SBB)	Duplex	Quasi Duplex	Simplex	Grand (lourd)	Moyen	Petit (léger)	Très petit	Très bonne	Bonne	Acceptable	Mauvaise	Très bonne	Bonne	Acceptable	Mauvaise	Elevé	Moyen	Mauvais	Elevés	Moyens	Bas
Numérique à large bande > 6 kHz	(●)	●			●		●			●	(●)	●				●				●				●	
Numérique à bande étroite ≤ 3 kHz			●	(●)	●		●	●						●				●		●			●		
Domaine fréquence dynamique			●	(●)		(●)	●		●				●				●				(●)	●			●
Domaine temps			●	(●)		(●)	●		●				(●)	●			●				●	(●)		●	
Domaine fréquence/temps			●	(●)		(●)	●		●				(●)	●			●				●			●	
Transformation fréquence/temps			●	(●)		●	●		●				(●)	●			●			●				●	

Tableau de comparaison des méthodes de chiffrement de la voix.

Processus numérique

Numérique à large bande
- Niveau de sécurité très élevé
- Très bonne qualité de la parole
- Cadence de transmission spécifique de 16 kbps
- Largeur de bande nécessaire pour la voie de transmission spécifique de 10 KHz
- Seulement réalisable actuellement avec les émetteurs-récepteurs de modulation FM à large bande ou interface de modex
- Transmission par lignes téléphoniques irréalisable
- Applications militaires et civiles

Numérique à bande étroite
- Niveau de sécurité très élevé
- Assez bonne qualité de la parole
- Cadence de transmission de 2,4 kbps
- Transmission possible par lignes téléphoniques normales (avec modem)
- Système très complexe et, par conséquent très coûteux
- Applications stratégiques

Processus analogique

Analogique – domaine de fréquence
- Niveau de sécurité bas à moyen
- Bonne qualité de la parole
- Transmission possible par les circuits de grade vocal

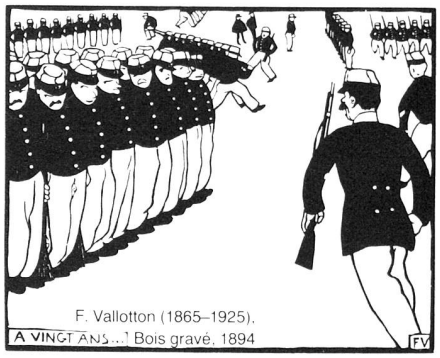
Analogique – domaine de temps
- Niveau de sécurité moyen
- Transmission possible par lignes téléphoniques
- A cause du délai d'assimilation et de syn

chronisation, utilisation en principe dans les applications semi-duplex

Analogique – domaine fréquence/temps
- Niveau de sécurité moyen à élevé
- Transmission possible par lignes téléphoniques et liaisons HF
- A cause du délai d'assimilation et de synchronisation en principe dans les applications semi-duplex

Analogique – transformation fréquence/temps
- Niveau de sécurité le plus élevé actuellement disponible
- Bonne qualité de la parole
- Transmission possible par radio HF et lignes téléphoniques
- Opération pseudo duplex intégral
- Application dans les forces de sécurité gouvernementales.

Dans le tableau qui suit, le lecteur peut identifier les différentes méthodes de chiffrement de la voix et leurs caractéristiques, avantages ou désavantages. Nous sommes convaincus que ce tableau aidera largement l'utilisateur potentiel à prendre un meilleure décision concernant le choix d'un équipement de chiffrement de la voix. ●



F. Vallotton (1865–1925). Bois gravé, 1894

PANORAMA

Stiftung zur Förderung der Übermittlungstruppen

Der Stiftungsrat hat am 9. Mai 1982 in Anwesenheit des Waffenchefs der Übermittlungstruppen seine ordentliche Jahresversammlung durchgeführt. Nach Kenntnisnahme des Berichtes der Kontrollstelle wurde die Jahresrechnung 1981 genehmigt.
Das Stiftungskapital beträgt zurzeit rund Fr. 190 000.–. Aus den Zinsen wurden im abgelaufenen Jahr folgende Aktionen finanziell unterstützt:
- Broschüre «Fernmeldematerial der Schweizerischen Armee seit 1875», 4. Folge
- Einweihungsschrift «Ausbau Waffenplatz Kloten-Bülach»
- Erinnerungsmedaille «Ausbau Waffenplatz Kloten-Bülach»
- Werbung Übermittlungstruppen.

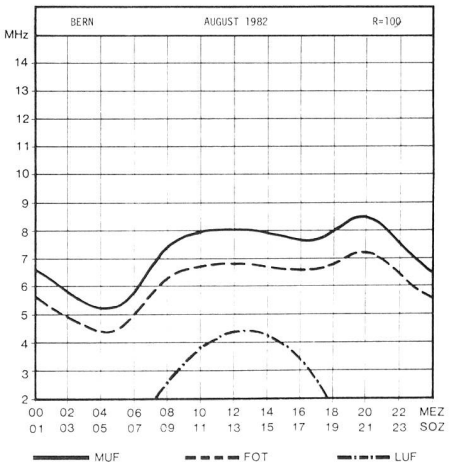
Donatoren 1981
Dr. H.P. Aellen, Spiegel-Bern; H.-P. Alioth, Bern; P. Arnet, Bern;, H. Bächler, Allschwil; G. Baggenstos, Bern; Major A.M. Banz, Hünenberg; Major A. Bassin, Neuchâtel; Dr. U. Baumgartner, Zürich; H. Benedetter, Zollikon; Divisionär J. Biedermann, Bern; M. Bonnard, St. Sulpice; K. Brunner, Wohlen; D.C. Cosandier, Biel; P. + B. Egger-Münst, Kilchberg; EVU Sektion Mittelrheintal, St. Margrethen; R. Fehr-Leserf, Schaffhausen; Oberst P. Folini, Schlieren; P. Füglister, Berikon; W. Gerber, Buchs; P. Gfeller, Eglisau; A. Jeschko, Spiegel-Bern; Oberstlt W. Kaufmann, Aarau; H. Keller-Abegg, Saanen; G. Kessler, Luzern; W. Markwalder, Würenlos; Oberst P. Maurer, Rüschlikon; A. Moser AG, Frutigen; B. Moser, Basel; B. Müller, Freiburg; Dr. W. Riedweg, Thörishaus; Hptm E. Roth, Gümligen; W. Rothlin, Wohlen; Dr. A. Schellenberg, Wettswil; H. Schwarber, Basel; D. Spinnler, Turgi; E. Steiger, Männedorf; Dr. W. Sulser, Zizers; A. Teuscher, Zweisimmen; K. Voegtli, Bern; R. Wyder, Schleinikon; St. Zürcher, Wettingen.

Als Dank und Anerkennung für alle Donatoren unserer Stiftung stehen auch dieses Jahr die dreifarbigen Grusskarten mit dem auf dieser Seite reproduzierten Signet zur Verfügung. Notieren Sie auf der Rückseite des Einzahlungsscheins die Anzahl der gewünschten Karten und auf der Vorderseite «Stiftung zur Förderung der Übermittlungstruppen der Schweizerischen Armee», Postscheckkonto 40-3089, Basel. *Ausschuss des Stiftungsrates*

21 Nationen am 23. schweizerischen Zweitage-Marsch

sp. Bei sommerlich warmem Wetter nahmen am 15./16. Mai 1982 rund 12 000 Teilnehmer am 23. schweizerischen Zweitage-Marsch in Bern teil. Leider sorgte eine Vielzahl von ausserdienstlichen Veranstaltungen an diesem Wochenende dafür, dass die Beteiligung aus der Schweiz um über 1600 Personen schrumpfte. Den Hauptharst der Teilnehmer aus dem Ausland stellten erneut die Niederlande, dicht gefolgt von der Bundesrepublik Deutschland. Auffallend war, dass bei den Ausländern weniger Leute die 20- und 30-km-Parcours bestritten, dafür aber sowohl bei der Zivilkategorie als auch beim Militär eine deutliche Zunahme der 40-km-Absolventen zu verzeichnen war. Bei den Schweizern dagegen führte der starke Rückgang zu einem Minus auf allen Strecken. Wie in den Vorjahren wurden die Marschierer der 30- und 40-km-Strecken mit Autobussen am Sonntag quer durch Bern zu ihren Standorten transportiert. Etwa 800 ehrenamtliche Funktionäre sorgten dafür, dass der vom Unteroffiziersverein der Stadt Bern organisierte Marsch, bei dem eine Gesamtdistanz von fast 644 000 Kilometern zurückgelegt wurde, reibungslos vonstatten gehen konnte. ●

Frequenzprognose August 82



Definition der Werte:

R Prognostizierte, ausgeglichene Zürcher Sonnenfleckenrelativzahl

MUF (Maximum Usable Frequency) Medianwert der Standard-MUF nach CCIR

FOT (Frequence Optimum de Travail) Günstige Arbeitsfrequenz, 85% des Medianwertes der Standard-MUF, entspricht demjenigen Wert der MUF, der im Monat in 90% der Zeit erreicht oder überschritten wird.

LUF (Lowest Useful Frequency) Medianwert der tiefsten noch brauchbaren Frequenz für eine effektiv abgestrahlte Sendeleistung von 100 W und eine Empfangsfeldstärke von 10 dB über 1 μV/m ●