F-Flagge

MAGAZIN FÜR DEN FERNMELDERING e.V.

Foto:
Wolfgang Schmidt

45. Jahrgang / Nr. 1 - 2018

Führungsunterstützung
Informationstechnik
Führungsdienste
Fernmeldetruppe
Elektronische Kampfführung

Anmeldeschluß für Hotelbuchung: 5. März!

Jahrestreffen 2018
vom 20. bis 22. April in Potsdam
Programm und Anmeldeformular in dieser Ausgabe

Der FERNMELDERING in Zahlen

Mitglieder . . .

. . . nach Dienstgrad

	2013		2014		2015		2016		2017	
Generale	23	2 %	25	2 %	26	2 %	26	3 %	26	3 %
Oberste	136	14 %	144	15 %	145	15 %	145	15 %	150	15 %
Stabsoffiziere	438	45 %	428	43 %	424	43 %	410	43 %	431	43 %
Offiziere	213	21 %	213	22 %	207	22 %	205	21 %	180	21 %
Unteroffiziere	93	9 %	94	10 %	96	10 %	91	10 %	78	10 %
Mannschaften	18	2 %	15	1 %	10	1 %	10	1 %	16	1 %
Sonstiges	64	7 %	70	7 %	64	7 %	71	7 %	69	7 %
	985	**100 %**	**989**	**100 %**	**972**	**100 %**	**958**	**100 %**	**950**	**100 %**

. . . nach Status

	2013		2014		2015		2016		2017	
Aktive	458	46 %	457	46 %	450	46 %	438	46 %	435	46 %
Reservisten	129	13 %	124	13 %	122	13 %	122	13 %	131	13 %
Ehemalige	339	35 %	343	35 %	337	35 %	330	34 %	320	34 %
Zivilisten	59	6 %	65	6 %	63	6 %	68	7 %	64	7 %
	985	**100 %**	**989**	**100 %**	**972**	**100 %**	**958**	**100 %**	**950**	**100 %**

. . . nach Alter

	2013		2014		2015		2016		2017	
90 Jahre +	13	1 %	15	1 %	12	1 %	13	1 %	8	1 %
65 - 89 Jahre	321	33 %	323	33 %	328	33 %	340	36 %	350	36 %
50 - 64 Jahre	297	30 %	310	31 %	317	31 %	301	32 %	300	32 %
30 - 49 Jahre	300	31 %	290	30 %	271	30 %	261	27 %	251	27 %
30 Jahre -	43	4 %	36	4 %	32	4 %	29	3 %	27	3 %
keine Angabe	11	1 %	15	1 %	12	1 %	14	1 %	14	1 %
	985	**100 %**	**989**	**100 %**	**972**	**100%**	**958**	**100%**	**950**	**100%**

. . . nach Dauer

	2013		2014		2015		2016		2017	
30 Jahre +	52	5 %	56	6 %	62	6 %	66	7 %	67	7 %
20 - 30 Jahre	97	10 %	108	11 %	131	13 %	160	17 %	179	17 %
10 - 20 Jahre	436	44 %	479	48 %	484	50 %	485	50 %	472	50 %
10 Jahre -	387	40 %	327	33 %	279	29 %	229	24 %	213	24 %
keine Angabe	13	1 %	19	2 %	16	2 %	18	2 %	19	2 %
	985	**100 %**	**989**	**100 %**	**972**	**100 %**	**958**	**100 %**	**950**	**100 %**

. . . nach PLZ

	2016		2017		2017		2016		
0	32	3 %	33	3 %	37	4 %	38	4 %	6
1	67	8 %	73	8 %	33	4 %	32	4 %	7
2	87	9 %	89	9 %	194	20 %	198	20 %	8
3	56	6 %	56	6 %	55	6 %	54	6 %	9
4	47	5 %	49	5 %	52	5 %	51	5 %	Ausl.
5	286	30 %	289	30 %					
					950	**100 %**	**958**	**100 %**	

Entwicklung der Mitgliederzahlen 1963 bis heute (jeweils zum 31. Dezember / sofern vorliegend)

1962	144
1963	193
1964	264
1976	160
1986	300
1989	306
1990	317
1992	319
1995	375
1996	418
1997	465
1998	495
1999	525
2000	557
2001	600
2002	
2003	725
2004	789
2005	879
2006	894
2007	912
2008	955
2009	950
2010	963
2011	958
2012	991
2013	985
2014	989
2015	972
2016	958
2017	950

Impressum

Herausgeber
Fernmeldering e.V.
vertreten durch den Vorsitzenden
Brigadegeneral a.D.
Helmut Schoepe
Waldschmidtstraße 16
82327 Tutzing

Redaktion
alle Mitglieder des Fernmeldering e.V.

Layout
Hella Schoepe-Praun

Schluss-Redaktion
Hauptmann d.R. Uwe Lünsmann

Freie Mitarbeiter
siehe Beiträge / Autorenzeilen

Druck
Druckerei Fuck Koblenz
www.f-druck.de

Erreichbarkeit Redaktion
h.schoepe-praun@arcor.de
redaktion@fernmeldering.de

Nächste F-Flagge
Redaktionsschluss: **30. April 2018**
Geplantes Erscheinungsdatum:
15. Juni 2018

Bankverbindung
Raiffeisenbank Rheinbach Voreifel e.G.
IBAN: DE87 3706 9627 0028 1280 10
BIC: GENO DED 1RBC

ISSN 1614-1334

Der Fernmeldering im Netz
www.fernmeldering.de

Webmaster
Oberstleutnant
Ulrich Graf von Brühl-Störlein
webmaster@fernmeldering.de

Bezug der F-Flagge
Einzelbestellungen der F-Flagge über die Redaktion. - Für Mitglieder des Fernmeldering ist der Preis für die F-Flagge im Mitgliedbeitrag enthalten.Für Nichtmitglieder beträgt der Bezugspreis im Jahresabonnement (4 Ausgaben) 22,- €. Mitgliederliste geht nur an Mitglieder.

Beiträge
Namentlich gekennzeichnete Beiträge geben nicht unbedingt die Meinung der Redaktion wieder. Übersandte Beiträge werden vorbehaltlich einer redaktionellen Bearbeitung veröffentlicht.

Anzeigen in der F-Flagge
In der F-Flagge können Werbung veröffentlicht/Anzeigen geschaltet werden. Bedingungen und Preise sind der aktuellen Anzeigenpreisliste (Ausgabe 2018) zu entnehmen, die auf *www.fernmeldering.de* abgerufen werden kann.

Inhaltsverzeichnis

Titelfoto: Erzengel Gabriel wacht nun auch über die Militärhistorischen Lehrsammlung Nachrichten-/Fernmeldetechnik e.V. in Feldafing

Liebe Kameradinnen und Kameraden,
sehr geehrte Mitglieder des Fernmelderings!

57 Jahre jung wird der Fernmeldering e.V. dieser Tage – damit hat er viele Veränderungen und Reformen bei der Bundeswehr miterlebt: Von den Streitkräften der ersten Stunde über die Bundeswehr im "Kalten Krieg" und der Armee der Einheit hin zu Streitkräften im Einsatz auch außerhalb des NATO-Vertragsgebietes.

Dass es den Fernmeldering heute wie vor 57 Jahren gibt, hieran haben insbesondere Sie, die Mitglieder, maßgeblichen Anteil: Immerhin begleiten 116 unserer derzeit 950 Mitglieder seit mehr als 25 Jahren den Fernmeldering (darunter Brigadegeneral a.D. Konrad Bader, Oberstleutnant a.D. Wolfgang Dietze und Major d.R. Kay Kuntzen seit dem 20. September 1963 als „Dienstälteste“, gefolgt von unserem Ehrenvorsitzenden Oberst a.D. Dieter Schwatlo, der am 27. Dezember 1963 beigetreten ist), 346 Mitglieder halten dem Fernmeldering seit nunmehr 15 Jahren die Treue – und 410 Mitglieder verstärken seit mindestens 5 Jahren unsere Gemeinschaft.

Brigadegeneral a.D.
Helmut Schoepe
Vorsitzender
Fernmeldering e.V.

In Würdigung dieser Treue, ohne die es den Fernmeldering e.V. nicht geben könnte, hat der Vorstand beschlossen, Ehrennadeln in Gold, Silber und Bronze zu schaffen und damit jedem einzelnen zu ehrenden Mitglied zu zeigen, dass seine jahrelange Vereinstreue vom Vorstand sehr wohl wertgeschätzt wird. Alles in Allem also ein "Danke schön" für Jahre/Jahrzehnte lange Mitgliedschaft. Es freut den Vorstand und mich ganz persönlich natürlich besonders, dass diese Mitgliederehrung Ihrerseits auf eine so große Resonanz gestoßen ist, wie uns Ihre zahlreichen Briefe/ eMails und Telefonanrufe gezeigt haben.

Ein großes Danke!
Unsere Geschäftsstelle zeichnete für die Umsetzung des Vorstandsbeschlusses verantwortlich, wofür die Ehrennadeln bestellt, die beigefügten Briefe/Urkunden erstellt -wenn auch leider mit Tippfehlern (nobody is perfect)- und ausgedruckt, die Adressetiketten geschrieben und alles in die Versandkartons verpackt sowie waschkörbeweise zur Post gebracht wurden.

Natürlich würde ich mich sehr freuen, falls Sie diese Ehrennadeln zu Recht mit Stolz bei entsprechenden Gelegenheiten, wie unserem Jahrestreffen oder anderen Zusammenkünften zB. der bundesweiten "Gelben Kreise" tragen würden.

Nun liegt mir nur noch die Resonanz auf unser traditionelles Jahrestreffen, das in diesem Jahr vom 20. bis 22. April in Potsdam stattfinden wird, am Herzen. Wenn diese Zeilen erscheinen, werden sich die meisten Teilnehmer bereits angemeldet haben. Für alle anderen wird es nun höchste Zeit, denn Hotelzimmer-Reservierungen können nur noch bis zum 9. März garantiert werden (da anschließend die reservierten Zimmer freigegeben werden müssen, um spätere Storno-Gebühren zu vermeiden). -
In diesem Zusammenhang: Diejenigen von Ihnen, die sich schon angemeldet, aber bislang keine Anmeldebestätigung erhalten haben, bitten wir baldmöglichst telefonischen Kontakt mit der Geschäftsstelle aufzunehmen, um Ihre Unterkunft etc. sicherzustellen.

Stichwort Tradition: Wer bereits Gelegenheit hatte, die Lehrmittelsammlung der Schule für Informationstechnik in (noch) Feldafing, zukünftig in Pöcking, zu besuchen, wird voller Anerkennung festgestellt haben, dass hier ein besuchenswertes Museum herangewachsen ist, dass alle Facetten der Fernmeldetruppe, später Führungsunterstützungstruppe und heute IT-Truppe vorstellt.
Um diesem Projekt die Unterstützung zukommen zu lassen, die es zweifelsohne verdient, wurde gleich zu Beginn diesen Jahres ein "Förderverein der Lehrmittelsammlung" gegründet. Der Fernmeldering ist, vertreten durch den Vorsitzenden, diesem Förderverein als Gründungsmitglied beigetreten.

Zum Schluss noch drei erfreuliche Nachrichten:

Erstens: Die Teilnehmer des OL III 2016/2017 haben alle ihre Ausbildung zum IT-Offizier erfolgreich abgeschlossen und nunmehr ihre Erstverwendung in der Truppe angetreten. Unsere besten Wünsche begleiten sie!

Zweitens: Der OL III 2017/2018 hat seine Ausbildung aufgenommen und wird erneut vom Fernmeldering durch die kommenden Monaten begleitet.

Und drittens: Die Historischen Themen konnten wiederbelebt werden, nachdem Oberst a.D. Rudolf Grabau nochmals einen 5-teiligen Beitrag zu "Ideen und Planungen für eine militärische Funkaufklärung in Westdeutschland nach Ende des 2. Weltkrieges" der F-Flagge zur Verfügung gestellt hat (Teil 1 ab Seite 45). Hierfür ein herzliches "Danke schön"!

Nun freue ich mich aufs Wiedersehen beim Jahrestreffen und und verbleibe
mit wie stets kameradschaftlichen Grüßen

Ihr

Lange ist's her - Ehemalige UNOSOM II Teilnehmer treffen sich

Vor 25 Jahren beteiligte sich Deutschland mit 2 Kontingenten am UN Einsatz in Somalia

Der Bürgerkrieg in Somalia hatte zu einem Zerfall staatlicher Strukturen und einer humanitären Katastrophe dramatischen Ausmaßes geführt. Die Bundeswehr beteiligte sich mit der Einrichtung einer Luftbrücke sowie logistischer Unterstützung von Blauhelmtruppen.

Das Deutsche Einsatzkontingent war mit Masse in BELET-UEN stationiert.

Um den Einsatz nicht in Vergessenheit geraten zu lassen und die erbrachten Leistungen und persönlichen Erlebnisse in Erinnerung zu rufen, wollen wir am 9. Juni in Ingolstadt, eingebunden in den Tag der Bundeswehr, ein Treffen mit allen ehemaligen Angehörigen des 1. und 2. Einsatzkontingentes durchführen.

Leider gibt es kein Anschriftenverzeichnis mehr, so dass sich die Suche nach den Kameraden enorm gestaltet. Alle ehemaligen Soldaten 1. und 2. Kontingents mit Interessenten am Kontingenttreffen werden gebeten, den Organisator, Oberleutnant Jim Taverna, zu kontaktieren und noch bekannte Kameraden auf die Veranstaltung hinzuweisen.

Ansprechpartner / POC:
Oberleutnant Jim Taverna
Tel.: 0841 / 88660 - 2310 (Bw: 6610 - 2310)
Fax: 0841 / 88660 - 2309 (Bw: 6610 - 2309)
Email: tagderbundeswehr2018ingolstadt@bundeswehr.org
jimtaverna@bundeswehr.org

(Kurz-)Zusammenfassung der Vorstands-Aktivitäten

(Stand: Ende Januar)

Neben den Vorbereitungen zum Jahrestreffen, dem Versand der Ehrennadeln und der Teilnahme an der Gründungsversammlung des "Fördervereins Militärhistorische Lehrsammlung Nachrichten-/Fernmeldetechnik e.V." (siehe hierzu Vorwort des Vorsitzenden) stand der Berichtszeitraum vorrangig im Zeichen...

... der NeMa (i.e. "Neue Maschine" = Schweizer Weiterentwicklung der ENIGMA), einer Schenkung unseres Schweizer Mitglieds Adj. a.D. Christoph Biel. Die Maschine ist mittlerweile dank des Engagements unseres Mitglieds Manfred Kienzle gut in Deutschland angekommen und vom Fernmeldering der Lehrmittelsammlung zur Verfügung gestellt worden.

Annekdote am Rande: Die zunächst erhobenen Zollgebühren in Höhe von rund 350 Euro wurden mittlerweile von der Zolldirektion erstattet.

... des Antrags auf Aufnahme des Fernmelderings in den "Beirat Reservisten" (Dachorganisation der Kameradschaftsverbände der Truppengattung). Hierzu steht der Vorsitzende im engen Kontakt mit dem Beirat der Reservisten, der über die Aufnahme entscheidet und wird bei dessen nächster Sitzung zum Fernmeldering vortragen. Abhängig von der Aufnahme ist ua. die Uniform-Trageerlaubnis für unsere nicht mehr aktiven Mitglieder bei FmR-Veranstaltungen

Jahrestreffen vom 20. bis 22. April in Potsdam

Bitte beachten:

Die Reservierung von Hotelzimmern kann nur garantiert werden, wenn Ihre Anmeldung bis zum 9. März bei der Geschäftsstelle eintrifft.

Sollten Sie sich bereits angemeldet haben, aber keine Bestätigung erhalten haben, dann nehmen Sie bitte Kontakt zur Geschäftsstelle auf: 08158 / 90 44 100

Danke!

... der Frage, ob und ggfs. wo 2018 wieder ein Treffen junger Mitglieder stattfinden sollte. Die Entscheidung stand bei Redaktionsschluss dieser Ausgabe noch aus - sie wird beim Jahrestreffen ebenso bekannt gegeben, wie Ort und Zeitpunkt für das Jahrestreffens 2019 .

... der Sorge, dass Mails auf den Sammel-eMail-Adressen teilweise aufgrund technischer Gegebenheiten nicht ankamen. Unser Webmaster Oberstleutnant Ulrich Graf von Brühl-Störlein - Danke! - hat sich des Problems erfolgreich angenommen!

... der 500 gelben Kugelschreiber mit www.fernmeldering.de-Aufdruck, die kostengünstig als zukünftige Werbemittel erworben werden konnten.

... unseres Beisitzers Oberst i.G. Jürgen Schick, der im Januar seinen Dienst bei USCENTCOM (wieder) angetreten hat. Wir wünschen gutes Gelingen!

Unsere besten Wünsche gehen, wie stets, zu allen sich derzeit im Einsatz befindlichen Kameradinnen und Kameraden.

Gast-Beitrag

von Oberst Frank Schlösser,
Kommandeur der Schule für Informationstechnik der Bundeswehr
und Vorsitzender der Militärhistorischen Lehrsammlung Nachrichten-/Fernmeldetechnik e.V.

Am 16. Januar 2018 wurde im Casino Feldafing der Förderverein „Militärhistorische Lehrsammlung Nachrichten-/Fernmeldetechnik e.V.“ gegründet. Der Verein hat es sich zum Ziel gesetzt, Bildung und Erziehung, Kultur und Geschichte sowie die Erhaltung von historisch gewachsener Fernmelde- und Kommunikationstechnik zu fördern. Die Gründungsmitglieder stimmten einer entsprechenden Satzung zu und wählten den ersten Vorstand des neuen Vereins. Nach der notariellen Eintragung erarbeitet der Vorstand zunächst einen Haushaltsplan für das erste Geschäftsjahr.

Die Lehrsammlung wird auch nach dem Umzug in die General-Fellgiebel-Kaserne nach Pöcking ein eigenes Gebäude erhalten und Lehrgangsteilnehmern, aber auch vermehrt zivilen Gästen, zur Verfügung stehen. Mit etwa 1000 Besuchern im vergangenen Jahr erfreut sich die Lehrsammlung zunehmender Aufmerksamkeit. In Zusammenarbeit mit der Volkshochschule Feldafing werden zukünftig regelmäßig Führungen für zivile Besucher stattfinden. Interaktive Führungsanteile und funktionierendes historisches Gerät stehen im Mittelpunkt der museumsdidaktischen Überlegungen und sollen dem Besucher technische Entwicklungen über unterschiedliche Zeitepochen darstellen.

Mit der Gründung des Fördervereins wurde ein weiterer Schritt gegangen, um die Sammlung noch attraktiver gestalten zu können und die umfangreiche, mit viel Liebe gestaltete Ausstellung mit weiteren Ausstellungsstücken und notwendigen Restaurierungsarbeiten unterstützen zu können. Der Förderverein freut sich über Interessierte, Unterstützer jeglicher Art und besonders auch neue Mitglieder.

Mit kameradschaftlichen Grüßen aus Feldafing
Ihr Frank Schlösser

Der Vorstand des Förderverein Militärhistorische Lehrsammlung Nachrichten-/ Fernmeldetechnik e.V.

Vorsitzender:	Oberst Frank Schlösser
Stv. Vors.:	BrigGen a.D. Helmut Schoepe
Kassierer:	Oberstleutnant Igor Asl
Schriftführer:	OSFw Willibald Schuldes
Beisitzer:	Herr Hans D. Vogt Hauptmann Wolfgang Schmidt
Kassenprüfer:	Oberstlt. Renée Völkel Oberstl. a.D. Ernst Schmidhuber

Die Teilnehmer der Gründungsversammlung am 16. Januar

Bei Interesse kann die Satzung des Fördervereins kann auch über die Geschäftsstelle des Fernmelderings (geschaeftsstelle@fernmeldering.de) abgerufen werden!

Neuer Regionalbeauftragter Nord

Der Fernmeldering freut sich, den neuen Regionalbeauftragten Nord vorzustellen:

Leutnant Martin Hallmann ist Regionalbeauftrager Nord und in Hamburg stationiert. Nach dem Abitur trat er 2013, als Offizieranwärter der Fernmeldetruppe, in die Bundeswehr ein. Seitdem durchläuft er die Offizierausbildung und befindet sich derzeit im Masterstudium der Bildungs- und Erziehungswissenschaften an der Helmut-Schmidt-Universität in Hamburg.

Sie erreichen Leutnant Hallmann wie folgt:

Telefon 0152 / 51 33 34 44

martinhallmann@hsu-hh.de

IG Fernmelder (wieder)gegründet

Wiederbelebt wurde an der Universität der Bundeswehr in Hamburg die IG Fernmelder, die vor einigen Jahren bereits als „FFF“ (Freundeskreis der Fernmelder und Führungsunterstützer) sehr aktiv war. Unter Leitung von **Leutnant Sascha Klement** und **Leutnant Martin Hallmann** trafen sich die Interessierten zu Ihrer Gründungsversammlung (siehe unten).

Brigadegeneral a.D. Helmut Schoepe, Vorsitzender des Fernmeldering e.V., begrüßte die Initiative und wünschte den Organisatoren viel Erfolg für alle Vorhaben.

Wer kann helfen?

Mein Großvater war 1941 beim Trägerfrequenz Zug 4 (Trupp 11). Er war von 1942 bis 1944 in Krasnoje (Russland) stationiert. danach flüchtete er nach Deutschland und kam in britische Gefangenschaft beo Oldenburg (Holstein) auf dem Gut Farve.

Können sie mir nähere Informationen über diese Abteilung geben? Waren vielleicht Mitglieder von Ihnen in diesem Zug?

Ich wäre für Informationen sehr dankbar.

Daniel Koehler
info@radio-produzent.de

IG Fernmelder (neu)gegründet

Neu der Uni München hat sich, ebenfalls Ende vergangenen Jahres, – hier unter Leitung von **Leutnant Benjamin Mohtaschemi** (benjamin.mohtaschemi@unibw.de) **Leutnant Felix Leber** (felix.leber@unibw.de) und **Leutnant Tobias Krauß** (tobias.krauss@unibw.de) – eine Interessensgemeinschaft der IT’ler gegründet.

Brigadegeneral a.D. Helmut Schoepe, Vorsitzender des Fernmeldering e.V., bot natürlich auch hier die Unterstützung des Fernmeldering e.V. für alle Vorhaben an.

1.111,11 Euro für das Soldatenhilfswerk

v.l. OTL a.D. Karlheinz Mergner (Schatzmeister SHWBw), Stabsfeldwebel Holger Linz, Stabsfeldwebel Danny Thärigen, OTL a.D. Hans-Michael Ketterle (Geschäftsführer SHWBw)

In guter Tradition bot das Stabsquartier im Dezember 2017 den im Kommando Informationstechnik der Bundeswehr beliebten Glühweinstand an. Die Angehörigen des Kommandos und Gäste trafen sich auf eine Tasse Punsch oder Glühwein und läuteten die Weihnachtszeit in geselliger Runde ein. Den Höhepunkt des weihnachtlichen Treibens bildete das Jahresabschlussgrillen. Der Erlös dieser Aktionen diente traditionell dem guten Zweck.

Dank der großen Spendenbereitschaft der Gäste und Angehörigen des Kommando Informationstechnik der Bundeswehr unter dem Motto “Kameradschaft pflegen bei einer Tasse Glühwein" konnte somit ein stattlicher Betrag gesammelt werden.

Im Auftrag des Kommandeurs der Dienststelle, Generalmajor Heinrich Steiner, übergaben Stabsfeldwebel Holger Linz und Stabsfeldwebel Danny Thärigen einen Spendenscheck in Höhe von 1.111,11 Euro an das Soldatenhilfswerk e.V.

Hauptmann Max Graf von Merveldt

Ein Schal für "Herrn Käthe"

Mit großem musikalischem Erfolg gestaltete am 12. November 2017 der Kirchenchor der Evangelisch-Lutherischen Kirchengemeinde Tutzing / Bernried, “Herr Käthe”, den sonntäglichen Gottesdienst mit der Gloria-Messe von Johannes Matthias Michel. Der Chor wurde am Klavier von Schwester Franziska Lehmann begleitet. Komponiert als “Mit-Mach-Messe” wurden die Gottesdienstbesucher bei leicht jazz-rhythmischen Klängen durch den Leiter des Kirchenchores, Herrn Ulrich Graf von Brühl-Störlein, in die Musik mit eingebunden und sangen, gemeinsam mit dem Chor, die liturgischen Teile der Messe mit.

Aber nicht nur die Art der Darbietung machte den Gottesdienst zu etwas Besonderem. Erstmalig traten die Sängerinnen und Sänger mit einem brombeer-farbenen Schal als Zeichen der Gemeinschaft und des Zusammengehörigkeitsgefühls zum Gottesdienst an. Gestiftet durch den Fernmeldering e.V. unter Vorsitz von Herrn Brigadegeneral a.D. Helmut Schoepe, überzeugte er sich nebst Gattin, nicht nur von den klanglichen Qualitäten des Chores, sondern auch über das schmückende Accessoire – schließlich “singt das Auge ja mit”! Dem Fernmeldering e.V. an dieser Stelle nochmals einen sehr herzlichen Dank!

Oberstleutnant Ulrich Graf von Brühl-Störlein

A n k ü n d i g u n g

Jahrestreffen 2018
und Mitgliederversammlung 2018
des Fernmeldering e.V.

Berlin ...

... Berlin ...

Wann?
Freitag, 20. April bis Sonntag, 22. April 2018

Wo?
In Potsdam

Unterkunft
Kongresshotel Potsdam am Templiner See (****)
Am Luftschiffhafen 1
14471 Potsdam
www.kongresshotel-potsdam.de

Einzelzimmer: **Euro 80,--** pro Nacht
Doppelzimmer: **Euro 108,--** pro Nacht
jeweils inkl. Frühstücksbüffet, W-Lan und Benützung des Sportbereichs.

Bitte beachten Sie, dass vorgenannte Sonderpreise nur für die beiden Übernachtungen des Jahrestreffens (Freitag bis Sonntag) gelten. Aufgrund verlängerter Aufenthalte zusätzlich benötigte Übernachtungen kosten Euro 98,-- (EZ) bzw. Euro 126,-- (DZ) pro Nacht.

Programm
Schwerpunkt des Rahmenprogramms wird der Besuch des *Wald der Erinnerung* am Samstag sein.

Am Sonntagvormittag ist die Besichtigung der Friedenskirche Sanssouci mit anschließender Teilnahme am Gottesdienst geplant.

Teilnehmer, die Sonntagnachmittag noch in Potsdam bleiben wollen, können unter Führung und auf Einladung des erfahrenen Potsdam Erl(i)eben"-Teams, unseren langjährigen Mitgliedern Thomas Hirschhäuser und Reinhard Wilhelm, kostenlos die Stadt Potsdam weiter erkunden.

... wir fahren nach ...

... Potsdam !!!

A n k ü n d i g u n g

Teilnehmergebühr für das Jahrestreffen
Analog zum dann 57jährigen Bestehen
des Fernmeldering e.V.
beträgt die Teilnehmer-/Tagungsgebühr´
Euro 57,-- p.P.
(Euro 28,50 für Teilnehmer der Jahrgänge 1985 und jünger)

Berlin ...

... Berlin ...

Bitte beachten Sie, dass
persönliche Ausgaben
Getränke/Verzehr beim Kameradschaftsabend am Freitag
Getränke beim festlichen Abendessen am Samstag
Imbiss am Sonntag
nicht in der Teilnehmerpauschale enthalten sind.

Anmeldungen
!!! Je früher, desto besser (für die Organisation) !!!

Anmeldungen **mit** Hotelbuchung bitte bis zum 5. März 2018
Anmeldungen **ohne** Hotelbuchung bitte bis zum 30. März 2018
an
Hella Schoepe-Praun
geschaeftsstelle@fernmeldering.de

Ein Anmeldeformular finden Sie auf Seite 61 dieser Ausgabe.

Großes Danke
Unseren Mitgliedern
Oberstleutnant a.D. Thomas Hirschhäuser
und
Oberstleutnant a.D. Reinhard Wilhelm
(www.potsdam-erlieben.de)
für ihre Unterstützung des Jahrestreffens 2018.

Für weitere Informationen:
Geschäftsstelle
Hella Schoepe-Praun
Telefon 08158 / 90 44 100

... wir fahren nach ...

... Potsdam !!!

Programm

Jahrestreffen und Mitgliederversammlung 2018

Zeit	Programm	Ort	Hinweise
Freitag, 20. April 2018	**Anreise**		individuell
ab 14 Uhr	Einchecken im Hotel / Möglichkeit des Besuchs des Spa-/Sportbereichs	Kongresshotel Potsdam	
18 Uhr	Sektempfang für neue Mitglieder	Kongresshotel Potsdam	
19 Uhr	Kameradschaftsabend	Kongresshotel Potsdam	
	Gemeinsames Programm		
Samstag, 21. April 2018	Frühstück	Kongresshotel Potsdam	
	Mitgliederprogramm		
9.00 Uhr	Mitgliederversammlung - Begrüßung	Kongresshotel Potsdam	
9.15 Uhr	Mitgliederversammlung - Bericht des Vorstandes		
10.00 Uhr	**Kaffeepause**		
10.30 bis 12.30 Uhr	Mitgliederversammlung - Vorträge		
	Partnerprogramm		
9.30 - 12 Uhr	Potsdam Erkunden unter Führung von OTL a.D. Hirschhäuser und OTL a.D. Wilhelm		
	Gemeinsames Programm		
12.30 Uhr	Mittagessen	Kongresshotel Potsdam	
13.30 Uhr	Fahrt zur Henning-von-Tresckow-Kaserne		eigene PKW's/ Fahrgemeinschaften
14 Uhr	Führung durch den Wald der Erinnerung durch OTL a.D. Hirschhäuser und OTL a.D. Wilhelm mit anschließender Kranzniederlegung, anschließend Rückkehr ins Hotel		
19 Uhr	**Festliches Abendessen**	Kongresshotel Potsdam	
	Gemeinsames Programm		
Sonntag, 22. April 2018	Frühstück	Kongresshotel Potsdam	
9 Uhr	Besichtigung Friedenskirche Potsdam Sanssouci mit anschließenden Besuch des Gottesdienstes		
11.30 Uhr	Imbiss mit offizieller Verabschiedung	Café Theaterklause	
ab 13 Uhr	Möglichkeit zur Stadtbesichtigung Potsdam unter Führung von OTL a.D. Thomas Hirschhäuser und OTL a.D. Rainer Wilhelm		

Änderungen vorbehalten ! **Stand: Januar 2018**

Tag der Bundeswehr in Murnau - Hubschrauber, Haubitzen und Hägglunds

Oberstleutnant Max-Joseph Kronenbitter

Die Highlights beim Tag der Bundeswehr stehen fest - beim Informationstechnikbataillon 293 präsentiert sich die Bundeswehr am 9. Juni in einer Bandbreite, wie sie Murnau noch nicht gesehen hat.

In Murnau geht's hoch her in diesem Jahr. Das neue Kommando Cyber- und Informationsraum, zu dem das Informationstechnikbataillon 293 Murnau gehört, die Luftwaffe, das Heer, die Streitkräftebasis und auch die Marine präsentieren sich beim Tag der Bundeswehr am Samstag, 9. Juni 2018 in der Werdenfelser Kaserne. Diese Öffentlichkeitsinitiative des Bundesministeriums der Verteidigung findet dann zum vierten Mal statt. Im vergangenen Jahr waren Penzing und Füssen die beiden Bundeswehr-Standorte in der Region, die über 63.000 Besuchern einen spannenden Tag geboten haben. Heuer erhalten die IT'ler in Murnau – neben 15 weiteren Standorten in ganz Deutschland - die Gelegenheit, Auftrag, Einsätze und Technik der Bundeswehr im Allgemeinen und des IT-Bataillons im Speziellen einer interessieren Öffentlichkeit zu zeigen.

Öffnet am 9. Juni seine Pforten: Das ITBtl 293 in Murnau

Die Besucher können in einem geländegängigen Einsatzfahrzeug der Bundeswehr mitfahren oder erleben, wie es in dem Feldlager im afrikanischen Wüstenstaat Mali, wo derzeit einige Murnauer Soldaten stationiert sind, zugeht. Das sind nur zwei der Highlights, die ein 20-köpfiges Projektteam unter der Leitung von Major Jan-Eric Foisner, eines der langjährigen Mitglieder des Fernmelderings, derzeit vorbereiten. „Wetterabhängig erwarten wir 12.000 Menschen an diesem Tag", so der Projektoffizier. Dazu müssen Parkplätze in der Region, Verpflegungsstationen, Ausstellungen und nicht zuletzt Sicherheitseinrichtungen organisiert werden.

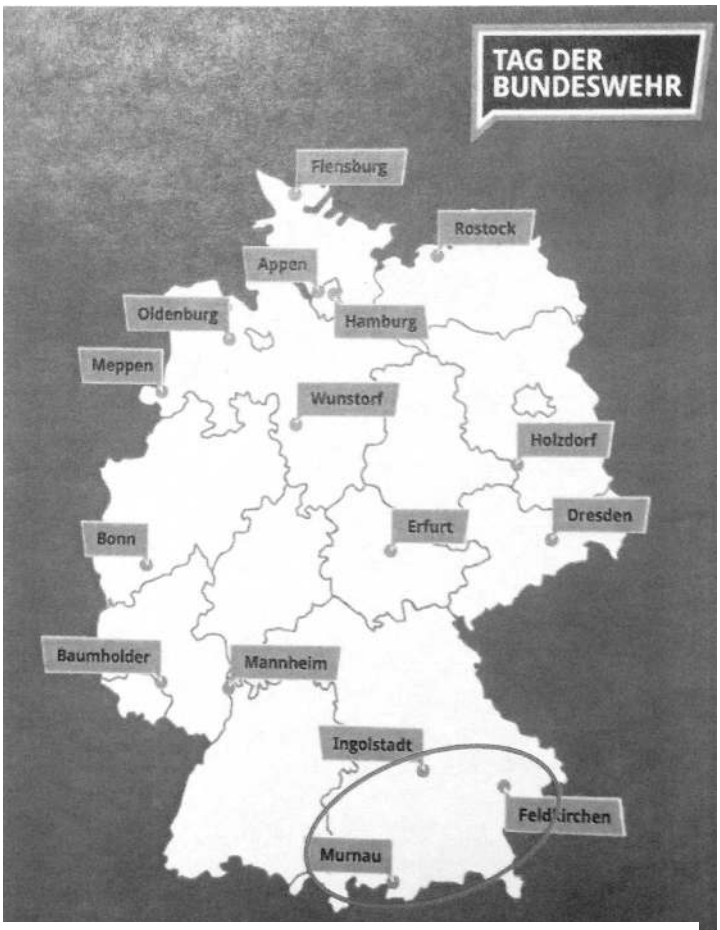
Der Zugang zur Kaserne erfolgt durch das große Torgebäude an der Weilheimer Straße. Zentraler Anlaufpunkt ist der zum Festplatz umgewandelte Exerzierplatz, auf dem eine große Bühne und ein Zelt mit Verpflegungsstationen stehen werden. Sternförmig vom Festplatz ausgehend geht's zum wüstenähnlich ausgebauten Teilbereich Bundeswehr im Einsatz, zur Blaulichtmeile und zum rollenden Museum mit historischen Bundeswehrfahrzeugen. Die Marine zeigt die anstrengende Arbeit in einem wassergefüllten Tauch-Container, die Luftwaffe einen Schleudersitz und das Heer Haubitzen und das Leben im Feld.

Freilich darf auch Großgerät nicht fehlen: Luftwaffenpiloten haben sich mit dem Hubschrauber H 145M angekündigt, auch die bayerische Polizei stellt einen ihrer Hubschrauber auf dem kaserneneigenen Sportplatz vor. Nicht weit davon entfernt bringt das deutsche Heer zwei ihrer Panzer in Stellung und demonstriert im Verbund mit anderen Waffengattungen seine Aufgabe in einem simulierten Gefecht.

Mindestens zweimal am Tag sind die Freifaller aus Altenstadt, die punktgenau auf dem Fußballplatz landen, zu beobachten.

"Es gibt viel zu tun..." - Projektoffizier Jan-Eric Foisner
Fotos: ITBtl 293

„Besonders froh sind wir, dass es uns gelungen ist, die Mulis von der Gebirgsjägerbrigade 23 aus Bad Reichenhall nach Murnau zu holen“, so Hautfeldwebel Kevin Janischewski. Die Kameraden des Einsatzzentrums für das Tragtierwesen bringen sogar eine komplette Schmiede mit, bei der die Besucher das Beschlagen mit Hufeisen beobachten können.



"Tag der Bundeswehr"-Standorte 2018

Stichwort beobachten: Die Bundeswehr-Erbsensuppe hat in der geneigten Bevölkerung längst schon Kultstatus erreicht. Was liegt näher, als beim Tag der Bundeswehr diese nicht nur zu verkaufen, sondern auch die Zubereitung in der Feldküche zu zeigen.

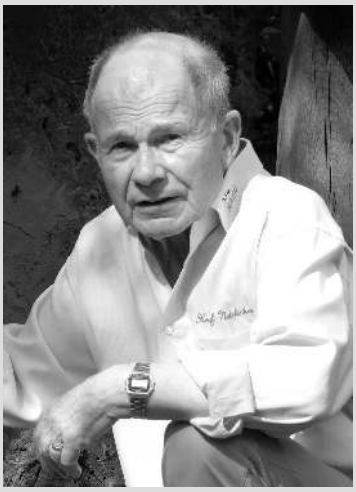
Breiten Raum im Veranstaltungsbereich nimmt freilich das bataillonseigne IT-Gerät in Anspruch. „Wir werden am Tag der Bundeswehr das gesamte Spektrum der IT-Truppen im Rahmen einer umfangreichen Leistungsschau darstellen“, berichtet Major Foisner, Kompaniechef der 4./ITBtl 293. Durch die vielen Beiträge anderer Teilstreitkräfte wird deutlich, dass es sich nicht um einen Tag der offenen Tür der „Murnauer“ handelt, sondern ein breites Spektrum der von der Präsenz- zur Einsatzarmee gewandelten Bundeswehr gezeigt wird.

Oberstleutnant Jürgen Eckert, Kommandeur des Informationstechnikbataillons 293, hat zudem entschieden, dass der 60. Geburtstag des Bataillons – leicht verspätet - auch an jenem 9. Juni 2018 gefeiert wird. Hervorgegangen aus der Gebirgsfernmeldekompanie 8 wurde das Gebirgsfernmeldebataillon 8 am 1. April 1958 in der Pionierkaserne Mittenwald in Dienst gestellt – und hat in den vergangenen 60 Jahren seiner Geschichte freilich einige Umbenennungen erlebt.

Informationstechnikbataillon 293
Werdenfelser Kaserne
An der B2
82412 Murnau am Staffelsee

Wir Bürger - Artenvielfalt - Glyphosat

Düstere Aussichten auch für das Jahr 2018 - Selbsttest schürt Besorgnis



Das Ehrenamt ist sein Vollzeitjob: Oberstleutnant a.D. Uwe Baumert (74) ist der stellvertretende niedersächsische NABU-Chef. Er sieht sich als Naturschutz-Lobbyist, sitzt in drei Begleitausschüssen der Landesregierung, dem Fachverband Biogas und setzt sich auch in Brüssel bei der Europäischen Union für den Umweltschutz ein. Baumert setzt sich vor allem gegen die „Vermaisung" der Landschaft ein und setzt sich für einen Energiepflanzenmix mit zusätzlich Sonnenblumen, Wild- sowie Blühpflanzen in dreigliedriger Fruchtfolge ein. 2012 erhielt er das Bundesverdienstkreuz für seine Umweltarbeit.

Nach einem Selbsttest bin ich besorgt, lasse Fakten sprechen und möchte warnen: **Immer mehr Bürgerinnen und Bürger, wenn nicht sogar alle Bürger, sind mit Glyphosat belastet, ihre Gesundheit ist bedroht.** Das Wildkrautvernichtungsmittel Glyphosat, bekanntester Markenname „Roundup", wird seit dem Jahr 1974 auf landwirtschaftlichen, öffentlichen und privaten Flächen eingesetzt. Nahezu viertausend Tonnen (2016 waren es 3.875 Tonnen) des Mittels werden auch im Jahr 2018 in Deutschland erneut ausgebracht werden. Auch Privatpersonen werden wieder mit rund 90 Tonnen Boden, Pflanzen, Tiere und Menschen gefährden. Glyphosat trägt auch bei zum Aussterben von Insekten und Vögeln. Ich habe einen **Selbsttest** gemacht, den **Glyphosatgehalt in meinem Körper über Urinproben** in einem unabhängigen Labor in Leipzig testen lassen.

Die Ergebnisse sind alarmierend, denn sie ergaben für **September 2015 einen Glyphosatgehalt von 0,68 Nanogramm pro Milliliter (ng/ml), im September 2016 sogar einen Gehalt von 1,28 ng/ml, und ähnliche Werte wieder im Jahr 2017.** Das Bundesamt für Risikobewertung (BfR) hat den Grenzwert für Ackergifte im Trinkwasser auf 0,1 Nanogramm pro Milliliter (0,1 ng/ml) festgelegt. Die Werte im Selbsttest sind also 7-fach und sogar fast **13-fach höher als dieser Grenzwert**. Deshalb wurde sowohl an den zuständigen Landkreis Rotenburg/Wümme (LK ROW) als auch an das BfR die Frage gestellt, ob unspezifisch vorliegende Symptome wie Infektanfälligkeit, Herzbeschwerden und Abgeschlagenheit mit der hohen Glyphosatbelastung zusammenhängen könnten?

Dazu Antwort durch den LK ROW: An der Trinkwasserversorgung kann es nicht liegen und es gebe ansonsten auch zu wenige Hinweise. Darüber hinaus wurde die Anfrage an das BfR weitergegeben, an das ich mich bereits persönlich gewandt hatte. Noch immer, seit Monaten steht die Antwort des BfR aus. Ich erwarte auch keine mehr; aber das wäre ein weiterer Artikel.

Kein Wunder; denn das für die EU und Bundesregierung maßgebende Gutachten, erstellt durch das BfR, beruhte u.a. auf Originalunterlagen der Fa. Monsanto!

Prof. Dr. Hensel, Präsident des BfR, hat zum Vorwurf „ Ganze Passagen von Monsanto im Gutachten für die Bundesregierung und die EU ohne Quellenangabe wörtlich übernommen zu haben" klargestellt: *„Das Vorgehen, Passagen aus eingereichten Dokumenten in Bewertungsberichte zu integrieren, sei üblich und anerkannt"*.

Meine Bewertung: Also *integrieren statt abschreiben* und ohne Quellenangabe; ist dann doch wissenschaftlich!! Eine Dienstaufsichtsbeschwerde wurde eingereicht.

Idealerweise sollten im menschlichen Körper keinerlei Rückstände von Ackergiften nachweisbar sein.

Sind sie aber und so auch Glyphosat.

Glyphosat tötet alle grünen Pflanzen ab, sorgt für gleichmäßige Kornreife und landet anschließend auch in Brotgetreide, Backwaren, Säften, Wein, Bier und Tierfutter. Glyphosat erleichtert die Bodenbearbeitung, tötet Froschlaich im Gewässer, führt zu Belastungen im menschlichen Urin und ist in den gesundheitsschädlichen Auswirkungen gefährlich unerforscht. Die Gefährlichkeit, bzw. das Risiko, wird noch erhöht, weil Beistoffe als Netzmittel (z.B. Tallowawine: sie können Keimzellen schädigen), beigefügt werden. Erinnerung: Bienensterben in Süddeutschland.

Todgespritzter Grünaufwuchs auf Maisacker
Fotomontage: Uwe Baumert

Allen glühenden Befürwortern von Glyphosat empfehle ich einen Urincheck. Dafür gibt es zertifizierte Labore und der NABU hilft gerne weiter. Auch der Bundeskanzlerin Angela Merkel sei ein Check, nach ihrer verniedlichenden Aussage *„Studien belegen, dass die Risiken nicht sehr groß sind“* (Boldekow, Mecklenburg-Vorpommern,18.08.2016) empfohlen. Glyphosat wird nicht gebraucht, auch nicht mit ein bisschen, geringem Risiko, (gibt es ein bisschen Krebs?). Es existieren erhebliche Forschungsdefizite sowie Risiken. Zur Verfügung stehen (ur)alte erfolgreiche alternative Methoden der Bodenbearbeitung. Für den Landwirt erhöht sich der Aufwand, der Gartenbesitzer und „Terrassenspritzer“ kann leicht verzichten und für den Verbraucher erhöhen sich die Preise. Das sollte uns die Gesundheit wert sein und vielleicht hilft ein Nachdenken über die Mehrwertsteuer.

Der NABU engagiert sich seit Jahren für ein Verbot und hat mit seinem Kooperationspartner REWE (einschließlich Penny, Merkur u.a) erreicht, dass bereits 2016 nicht nur Plastiktüten ausgelistet und durch Stoff- und Papiertüten ersetzt wurden, sondern auch Glyphosat in den zugehörigen TOOM-Baumärkten aus den Verkaufsregalen verschwand. Dazu eine satirische Anmerkung in der ZDF heute-show: „Glyphosatan“ vertrieben.

Mit kameradschaftlichen Grüßen

Ihr

Höchstes Ziel darf nicht die schnelle und kurzfristige Wildkrautvernichtung sein, sondern die langfristige Gesunderhaltung aller Lebewesen, Böden und Pflanzen. Frühling und Sommer werden dann nicht stumm sein, sondern uns mit Summen, Brummen und Zwitschern in einem vitalen Körper erfreuen.

Anmerkung aus der Wiener Zeitung „Neue Presse“, Österreich, November 2017.

(...) Wer keinen Zusammenhang zwischen der Entscheidung für Glyphosat (EU-Minister Schmidt) und der geplanten Übernahme des US-Konzerns Monsanto durch den deutschen Chemiekonzern Bayer erkennt, muss verwirrt sein. Monsanto`s Verkaufsschlager ist nämlich Roundup, das bekannteste Unkrautvernichtungsmittel mit Glyphosat. Es dürfte bald einer der attraktivsten Produkte für den in Deutschland beheimateten Bayer-Konzern sein. Nun bleibt alles beim Alten: Es gibt eine Verlängerung, die wieder verlängert werden kann. Es gibt keine Motivation, den natürlichen Kreislauf von Nützlingen und Schädlingen wiederherzustellen, der durch ein Übermaß an Chemieeinsatz schwer beeinträchtigt wurde (...)

Welche Reserve braucht das Land?
Gedanken zur zukünftigen Personalbedarfsdeckung der Bundeswehr

von Generalleutnant a.D. Peter Schelzig

Abdruck mit freundlicher Genehmigung von "Treue Kameraden",
Zeitschrift des Bayerischen Soldatenbundes 1874 e.V.

"Die Reservisten sind von jeher ein wichtiger Bestandteil unserer Bundeswehr. In meiner letzten Verwendung als Stellvertreter des Generalinspekteurs der Bundeswehr war ich auch der Beauftragte für die Reservistenarbeit der Bundeswehr. Was ich Ihnen im Folgenden darstellen möchte, beruht auf den Erfahrungen meiner aktiven Dienstzeit und meinem Interesse am Zeitgeschehen."

Generalleutnant a.D. Peter Schelzig

Sicherheitspolitische Herausforderungen und ihre Bewältigung

Das Weißbuch 2016 beschreibt das aktuelle sicherheitspolitische Umfeld Deutschlands, indem es feststellt, dass sich dieses im Umbruch befindet. Die Treiber sind Globalisierung und Digitalisierung, die zu einer weltweiten, alle gesellschaftlichen Bereiche durchdringenden Vernetzung geführt haben.
Neben den technologischen Vorteilen, die durch diesen Cyber- und Informationsraum für Politik, Wirtschaft und Gesellschaft entstehen, werden auch die Vernetzung und Verbreitung von Risiken und deren Folgewirkungen befördert. Dies reicht von Epidemien über die Möglichkeit von Cyberangriffen und Informationsoperationen bis zum transnationalen Terrorismus.
Gleichzeitig entstehen Kräfte der Antiglobalisierung, radikaler Nationalismus, gewalttätiger Extremismus und religiöser Fanatismus als Ausdruck von Identitäts- und Legitimationsdefiziten.
Weitere Schlagworte, die das Weißbuch in diesem Zusammenhang aufführt, sind:

- Infragestellung der euroatlantischen Friedens- und Stabilitätsordnung
- Europäisches Projekt unter Druck
- Zwischenstaatliche Konflikte
- Fragile Staatlichkeit und schlechte Regierungsführung
- Weltweite Aufrüstung und Proliferation von Massenvernichtungswaffen
- Gefährdung der Informations-, Kommunikations-, Versorgungs-, Transport- und Handelslinien und der Sicherheit der Rohstoff- und Energieversorgung
- Klimawandel
- Unkontrollierte und irreguläre Migration
- Pandemien und Seuchen

Ich werde nicht weiter zu diesen Schlagworten ausführen.

Vielmehr werfe ich einen kurzen Blick auf die sich daraus ergebenden strategischen Prioritäten Deutschlands:

- Die Gewährleistung gesamtstaatlicher Vorsorge
- Stärkung von Zusammenhalt und Handlungsfähigkeit in Nordatlantischer Allianz und Europäischer Union
- Ungehinderte Nutzung von Informations-, Kommunikations-, Versorgungs-, Transport- und Handelslinien sowie die Sicherheit der Rohstoff- und Energieversorgung
- Frühzeitiges Erkennen, Vorbeugen und Eindämmen von Krisen und Konflikten sowie
- Engagement für die regelbasierte internationale Ordnung.

Daraus ergeben sich für Deutschland entsprechende sicherheitspolitische nationale und internationale Gestaltungfelder. Besondere Schwerpunkte sind dabei unter anderem Deutschlands Engagement in den Vereinten Nationen, in der NATO sowie in der Europäischen Union.
Kurz gesagt, die Bundeswehr muss in Zukunft ihren Auftrag und ihre Aufgaben genau in diesen veränderten und nach wie vor dynamischen sicherheitspolitischen Umfeld erfüllen können.

Baustelle Neuausrichtung

Darüber hinaus befindet sich die Bundeswehr immer noch in der sogenannten Neuausrichtung.

Das Jahr 2011 war das Jahr für die Grundsatzentscheidungen dazu.

Im Jahr 2012 begann die Umsetzung der Neuausrichtung.

Seit dem Jahr 2015 arbeitet die neue Führungsorganisation in der Zielstruktur.

Seit dem Jahr 2016 sind die Masse der Verbände und Ämter umgegliedert.

Die Prägung der Neuausrichtung der Bundeswehr umfasst folgende Kernpunkte:

- Erhalt des gesamten Fähigkeitsspektrums bei Abstrichen an der Durchhaltefähigkeit („Breite vor Tiefe“)
- Aussetzung der Pflicht zur Ableistung des Wehrdienstes bei Einführung eines freiwilligen Wehrdienstes
- Reduzierung des Bundeswehrumfangs auf bis zu 185.000 Soldatinnen und Soldatinnen und 55.000 Stellen für zivile Mitarbeiterinnen und Mitarbeiter
- Stationierung nach den Grundprinzipien Funktionalität, Kosten, Attraktivität und Präsenz in der Fläche
- Konzentration des Ministeriums auf seine Kernaufgaben, damit zugleich Stärkung der Kommando-/Ämterebene
- Straffung der Führungsorganisation zugunsten der operativen Bereiche
- Konzentration von Aufgaben nach Möglichkeit in nur noch einem Organisationsbereich, dadurch
- Beschleunigung von Entscheidungsprozessen und Abbau von Doppelstrukturen
- Bürokratieabbau mit Hilfe eines Deregulierungsprogramms.

Die Umsetzung dauert derzeit noch an und fordert vor allem die Basis der Bundeswehr auf Verbandsebene.
Im Vergleich zu früheren Reformen fordert diese mehr als sonst vor allem Soldatinnen und Soldaten und zivile Mitarbeiterinnen und Mitarbeiter auf allen Ebenen durch Verlust des jeweiligen Standortes und damit die Perspektive in zum Teil sehr weit entfernten Standorten neu „Fuß zu fassen“.
Als ein Beispiel möchte ich nur meinen ehemaligen Verband – das Jagdbombergeschwader 32 Lechfeld – nennen, dessen einmalige Fähigkeit mit dem ECR Tornado in den Norden Deutschlands nach Schleswig Holstein verlegt wurde.
Deswegen standen eine ganze Reihe von Spezialisten vornehmlich in den Dienstgraden Feldwebel und Hauptfeldwebel vor der Situation dorthin umzuziehen oder eine heimatnähere dienstliche Alternative zu finden.
Fast 3600 Bundeswehrsoldaten beteiligen sich derzeit (Stand September 2017) an Einsätzen im Ausland. Dabei operieren Sie gemeinsam mit Soldaten der Bündnispartner und befreundeter Nationen.
Schwerpunkte sind Afghanistan, Kosovo, Syrien und Irak, Mali, Mittelmeer und Somalia.
Nicht zu vergessen die Anstrengungen, die die Bundeswehr im Bündnis mit Blick auf die Ukraine-Krise nicht unerheblich fordern.
Auch dieses „laufende Geschäft“ wird die Truppe auf absehbare Zeit weiter in Anspruch nehmen. Bleibt die Frage: Wie muss unsere Bundeswehr aufgestellt sein, um diesen Herausforderungen gerecht zu werden?
Reichen die Anstrengungen, die man bisher unternommen hat aus, um auch und gerade im Bündnis den angemessenen Teil einbringen zu können?
Nicht zuletzt die zukünftige Rolle der USA im NATO Bündnis – die übrigens nicht erst seit Donald Trump ein höheres Engagement der großen europäischen Partner bei der gerechten Lastenverteilung fordern – wirft die Frage nach dem künftigen angemessenen Beitrag Deutschlands und damit der Bundeswehr auf.
Ich wage die Prognose, dass dieser Beitrag eher größer wird.
Also muss die Bundeswehr über die richtige, moderne und ausreichende Ausstattung verfügen. Hier sind viele Weichen gestellt und Beschaffungen entsprechend eingeleitet.
Um nur einige zu nennen: Transportflugzeuge A400M, Eurofighter, Korvetten 130 und Fregatten 125, Schützenpanzer Puma, Infanterist der Zukunft, Hubschrauber NH-90 sowie Unbemannte Fliegende Systeme (Drohnen).
Allein, hier haben sich unerwartete Verzögerungen in der Auslieferung beziehungsweise in der Erfüllung der geforderten Spezifikationen ergeben, was zu Ungewissheiten bei der Truppe bezüglich der nun tatsächlichen Verfügbarkeit führt.
Derzeit fehlt es nicht an den notwendigen Haushaltsmitteln, sondern eher an den Produkten, die nicht vertragsgemäß ausgeliefert werden. Unser Haushaltsrecht sieht dabei vor, dass diese Mittel, wenn sie nicht ausgegeben werden können, wieder an den Finanzminister zurückgehen.
Auf der anderen Seite muss die Bundeswehr über das nötige Personal verfügen, um die vorher beschriebenen Aufgaben erfüllen zu können.
Die derzeitige Vorgabe der Neuausrichtung sieht bei den Soldaten einen Umfang von 185.000 Dienstposten vor. Derzeit sind von diesen Stellen circa 178.000 besetzt.
Die Ministerin hat im Mai letzten Jahres eine Erhöhung um 4.000 Dienstposten und darüber hinaus eine jährliche Betrachtung des Gesamtumfangs ins Spiel gebracht. Des Weiteren wird diskutiert, ob man zur Deckung des Personalbedarfs der Bundeswehr junge Menschen ohne Schulabschluss beziehungsweise EU-Bürger gewinnen und einstellen kann.
Auch ein breit angelegtes Attraktivitätsprogramm wurde aufgelegt und bringt den Aspekt „Vereinbarkeit von Familie und Dienst“ ins Spiel.
Die seit 1. Januar 2016 auch für die Soldaten der Bundeswehr geltende EU-Arbeitszeitrichtlinie (41 Stunden-Woche) bringt eine zusätzliche Herausforderung für den Personalbedarf.

Die Möglichkeit für aktive Soldaten, über sogenannte Arbeitszeitkonten auch längere „Auszeiten“ über Monate hinweg zu nehmen, erfordert die Kompensation durch zusätzliche Dienstposten für aktive Soldaten oder Reservisten.
Beides ist meines Wissens vorgesehen; so sind derzeit 2500 Dienstposten für Reservisten eingeplant. Entsprechende Untersuchungen laufen, um den tatsächlich benötigten Umfang zu ermitteln.
Wie auch immer das Ergebnis ausfallen wird, es entsteht ein eher wachsener Bedarf an vor allem qualifiziertem Personal.
Wie der zu decken sein wird, ist die Schlüsselfrage für unsere Streitkräfte. Und es sei mir erlaubt zu erwähnen, dass wir gerade mit Blick auf qualifiziertes Personal bereits seit einiger Zeit ein Defizit in unserer Bundeswehr zu verzeichnen haben.
Beispielsweise konnten wir im Jahr 2015 2800 Stellen für IT-Personal nicht besetzen; dieses Fehl ist meines Wissens noch nicht annähernd kompensiert. Dies ist mit Blick auf die Aufstellung einer unbedingt notwendigen Fähigkeit im Bereich Cyber ein nicht zu unterschätzender Aspekt.
Ein weiteres Beispiel ist das Fehl an qualifiziertem Personal im Bereich der Fluggerätemechaniker.
Waren es früher die fehlenden Haushaltsmittel, die den Mangel an Flugstunden für unsere Besatzungen begründeten, so ist es heute nicht das Geld, sondern auch und gerade das fehlende Personal.

Das „As im Ärmel“: Reservisten

Damit bin ich bei unseren Reservisten und stelle zunächst die Frage, ob unser derzeitiges Konzept den von mir umrissenen Herausforderungen gerecht werden kann?
Hier darf ich noch mal unser Weißbuch zitieren… Zur Sicherstellung des Bedarfs und auch zur Resilienzbildung in der Gesellschaft muss eine Durchlässigkeit zwischen Bundeswehr, Gesellschaft und Wirtschaft erreicht werden. Dafür gilt insbesondere,

- den Reservedienst insgesamt attraktiver zu gestalten
- ihn so weiterzuentwickeln, dass eine langfristige, verlässliche Unterstützung durch Reservistinnen und Reservisten sowie externes Personal, insbesondere im Bereich Cyber (Cyber-Reserve) ermöglicht wird;
- auch im Bereich des Reservistendienstes Austauschmodelle zwischen Wirtschaft und Bundeswehr zu schaffen, die eine bessere auf Zeit angelegte Kooperation mit externem Personal ermöglichen.

Gerade für den zuletzt angeführten Aspekt bin ich dankbar, dass er seinen Eintrag ins Weißbuch gefunden hat. - Deswegen möchte ich Ihnen gerne etwas näher bringen, was ich darunter verstehe.
Zu dem erforderlichen, zukünftigen Personalbedarf der Bundeswehr vor allem mit Blick auf qualifiziertes Personal habe ich bereits ausgeführt.
Es ist schlichtweg unumgänglich, auch den sich abzeichnenden, grundlegenden Bedarf für die Gesellschaft beziehungsweise die Industrie, also den Bereichen, die mit der Bundeswehr im Wettbewerb um das qualifizierte Personal stehen, zu betrachten.
Darüber hinaus gilt es, die Entwicklung der Demographie unserer Gesellschaft zu berücksichtigen.
Im Wettbewerb um die besten Kräfte auf dem Arbeitsmarkt werden zunächst die finanzstärksten Arbeitgeber gewinnen. Allerdings am Ende alle verlieren, weil das Gesamtsystem Wirtschaft dann nicht mehr funktionieren würde.
Alleine die Zulieferindustrie bliebe als erstes auf der Strecke und damit kämen auch die Großkonzerne in Existenznöte. Als eine Lösung werden Kooperation sogenannter „Pools“ erwähnt, die das qualifizierte Personal projektbezogen einmal diesem und dann wiederum jenem Arbeitgeber zur Verfügung stellen.
Wie auch immer, wir brauchen neue Konzepte, die den Bedarf auch in Zukunft nachhaltig decken.
Für die Bundeswehr sehe ich im folgenden Ansatz nicht nur eine Chance, die Personaldeckung der Zukunft nachhaltig zu sichern, sondern ebenso die Chance, Attraktivität zu steigern.
Gelingen kann das aber nur zusammen mit allen Beteiligten im Wettbewerb: Industrie, öffentliche Arbeitgeber und natürlich auch der Bundeswehr und zwar am besten durch konkrete Vereinbarungen.

Das „Mehrphasen-Modell“

Ein Konzept, das ich „Mehrphasen-Modell“ nenne, könnte folgendem Ansatz nachgehen:
Die Bundeswehr gewinnt den jungen Mann, die junge Frau am Anfang des individuellen Berufslebens durch das Angebot folgender Perspektive:
In einer ersten Phase bildet die Bundeswehr den/die Berufsanfänger/in aus, indem sie ein Studium, eine Fachausbildung anbietet, was nach dem jeweiligen Abschluss zu einer vereinbarten Zeit im Dienst der Bundeswehr führt.
Zu einem vertraglich bestimmten Zeitpunkt folgt dann eine Beschäftigungsphase bei einem zivilen Arbeitgeber/Industrie. In dieser Phase käme es zu fest vereinbarten Zeiten der Reservedienstleistungen, die durchaus auch bis zu einem halben Jahr dauern können.
In einer dritten Phase erfolgt dann der vollständige Übertritt in die „zivile Welt“; die Bundeswehr zöge den Reservisten nur dann, wenn beispielsweise die Landesverteidigung dies erforderte.

Damit hätte man übrigens wieder ein zukunftssicheres Reservoir an Reservisten, das nach Aussetzung der Wehrpflicht auf lange Sicht sonst wohl verloren ginge. – So viel zur Grundidee.
Natürlich müsste man die Details mit allen Beteiligten, insbesondere was die zeitliche Länge dieser Phasen oder auch die Anzahl und Dauer der Wehrübungen angeht, intensivst abstimmen beziehungsweise mit Blick auf ihre Plausibilität besprechen.
Für den Bereich Cyber könnte ich mir Modelle vorstellen, die ähnlich wie bei der National Guard im Silicon Valley in den USA, IT-Fachleute in einer permanent geteilten Dienstleistung für die Bundeswehr und den zivilen Arbeitgeber vorsehen. Auch dies wäre mit Blick auf die konkrete Zeitaufteilung genau zu definieren.
Es bleibt abzuwarten, ob es gelingt, im gemeingesellschaftlichen Interesse zu plausiblen und umsetzbaren Lösungen zu kommen.
Bis dahin sind wir natürlich dankbar, dass unsere Reservisten bereits heute einen enorm wichtigen Beitrag für uns leisten: sei's im Ausland selbst, in den Dienststellen der Heimat, um die Vakanzen aktive Soldaten im Auslandseinsatz zu kompensieren oder durch das mindestens genauso wichtige Verbindunghalten zur Bevölkerung.

Zum Autor

Peter Schelzig, geboren am 10. Juni 1955 in Augsburg, ist Generalleutnant a.D. der Luftwaffe.

Er trat am 1. Juli 1977 in die Bundeswehr ein, absolvierte die Ausbildung zum Offizier des Truppendienstes, wurde zum Strahlflugzeug-Piloten (F 104G „Starfighter“ und „Tornado“) ausgebildet und durchlief zunächst verschiedene Truppenverwendungen im Jagdbombergeschwader 32 (Lechfeld).

Ab 1990 wurde er als Staffelkapitän im Jagdbombergeschwader 33 (Büchel) verwendet.

Nach der Generalstabsausbildung an der Führungsakademie der Bundeswehr in Hamburg durchlief er von 1994 bis 1996 Verwendungen als Dezernatsleiter A3a im Luftwaffenkommando Süd (Meßstetten), von 1996 bis 1997 als Referent „Konzeption und Planung Bundeswehr“ im Führungsstab der Streitkräfte (Bonn) und als stellvertretender Adjutant beim Bundesminister der Verteidigung (1997 bis 1998).

Während seiner Verwendung von 1998 bis 2001 als Kommodore des Jagdbombergeschwaders 32 führte er während der Operation Allied Force während des Kosovo-Konflikts das Einsatzgeschwader 1 der Luftwaffe.

Von 2001 bis 2002 leitete Schelzig die Stabsabteilung A3 im Luftwaffenführungskommando (Köln).

Befördert zum Brigadegeneral war er von 2002 bis 2003 Stellvertreter des Kommandeurs der 4. Luftwaffendivision; während dieser Zeit (2003) war er auch Deputy Commander Air im HQ ISAF (Kabul).

Von 2003 bis 2005 leitete Schelzig die Stabsabteilung III im Führungsstab der Luftwaffe (Bonn), bevor er 2005 das Kommando über die 4. Luftwaffendivision in Aurich übernahm.

Nach einer Verwendung als Befehlshaber des Luftwaffenführungskommandos (dabei Beförderung zum Generalleutnant) in Köln 2009 bis 2013 übernahm Schelzig am 1. Mai 2013 den Dienstposten des Stellvertreters des Generalinspekteurs der Bundeswehr, den er bis zu seiner Versetzung in den einstweiligen Ruhestand 31.10.2015 innehatte. In dieser Verwendung war er zugleich Beauftragter für Reservistenangelegenheiten der Bundeswehr.

Personalveränderungen

Stand: Ende Januar 2018

BMVG

Brigadegeneral Dr. Ing. Heinz Färber, Unterabteilungsleiter I Cyber/Informationstechnik im Bundesministerium der Verteidigung, Berlin, wurde Stellvertreter des Abteilungsleiters Cyber/Informationstechnik im Bundesministerium der Verteidigung, Berlin.

Oberst Wolfgang Ohl, Leiter der Leitungsinformationszentrale BMVg im Bundesministerium der Verteidigung, Berlin, wurde Unterabteilungsleiter Politik II im Bundesministerium der Verteidigung, Berlin.

Herr Eckart Meyer-Höper, Erster Direktor und Abteilungsleiter V im Bundesamt für das Personalmanagement der Bundeswehr in Sankt Augustin, wird Unterabteilungsleiter Personal II im Bundesministerium der Verteidigung, in Bonn.

SKB

Generalmajor Werner Weisenburger, Amtschef Streitkräfteamt, Bonn, trat in den Ruhestand. Sein Nachfolger wurde **Brigadegeneral Franz Weidhüner**, Unterabteilungsleiter Personal II im Bundesministerium der Verteidigung, Bonn.

Brigadegeneral Hartmut Pauland, zuletzt im Kommando Streitkräftebasis, Bonn, eingesetzt, trat in den Ruhestand.

CIT

Brigadegeneral Dietmar Mosmann wurde Kommandeur der Informationstechniktruppen, verantwortlich für alle IT-Bataillone der Bundeswehr, sowie Stellvertretender Kommandeur des Kommando Informationstechnik der Bundeswehr. Sein Vorgänger, **Brigadegeneral Ralf Hoffmann**, wird Director des NATO Advisory and Liaison Teams im Kosovo.

SANITÄTSDIENST

Generalarzt Dr. med. Jürgen Christian Hans Brandenstein, zuletzt im Kommando Sanitätsdienst der Bundeswehr, Koblenz eingesetzt und zuvor Kommandeur und Ärztlicher Direktor Bundeswehrzentralkrankenhaus Koblenz, tritt in den Ruhestand.

Generalarzt Dr. med. Norbert Weller, zuvor Direktor Wehrmedizinische Wissenschaft und Fähigkeitsentwicklung Sanitätsdienst und Stellvertretender Kommandeur Sanitätsakademie der Bundeswehr, München, wurde Kommandeur und Ärztlicher Direktor Bundeswehrzentralkrankenhaus Koblenz.

Ihm folgte **Oberstarzt Dr. med. Hans-Ulrich Holtherm**, Direktor Ausbildung/Lehre Gesundheitsversorgung der Bundeswehr Sanitätsakademie der Bundeswehr, München.

Brigadegeneral Hans-Dieter Poth, zuletzt im Streitkräfteamt, Bonn, eingesetzt, trat in den Ruhestand.

Blick zurück

Viel Soldatenglück in den zukünftigen Verwendungen gab im vergangenem November der FmR-Vorsitzende Brigadegeneral a.D. Helmut Schoepe den jungen IT-Offizieren mit auf den weiteren Berufsweg (siehe auch Bericht auf Seite 39)

Bedrohung aus dem Cyberraum – Wichtige Akteure, ihre Strategien und Ziele

Teil II: Die Russische Föderation

von Oberst a.D. Otto Jarosch

Es ist nur kurze Zeit her, da galt China als die größte Cyber-Bedrohung der USA. Wie ich im ersten Teil beschrieben habe, wurden über viele Jahre hinweg die Server großer amerikanischer Firmen immer wieder durch chinesische Hacker massiv infiltriert. Auch verschafften sich die Chinesen immer wieder Zugang zu IT-Systemen der US-Regierung. Nachdem Präsident Obama mit der chinesischen Regierung ein Abkommen ausgehandelt hatte, gingen diese Angriffe sehr deutlich zurück. Natürlich darf man nicht glauben, dass China deshalb sein Interesse an US-Informationen gänzlich verloren hat, die Situation hat sich aber deutlich entspannt. Besonders durch die Vorfälle im amerikanischen aber auch im französischen Wahlkampf ist nun Russland wieder mehr in den Fokus geraten. Offiziell bestreitet Russland zwar nach wie vor jegliche staatliche Beteiligung an den Hackerattacken und Desinformationskampagnen, es ist aber trotzdem sehr wahrscheinlich, dass politisch orientierte russische Hacker hinter diesen Operationen stecken. Ein Grund mehr sich einmal näher mit den russischen Cyberfähigkeiten zu befassen.

Akteure der Staatsmacht oder Hacker als Cybersöldner

Bereits seit den ersten bedeutenden Cyberangriffen auf einen Staat des westlichen Bündnisses, die Angriffe auf Estland im Jahr 2007, stellt sich immer wieder die Frage, wer tatsächlich hinter den Cyberangriffen steckt, deren Spuren nach Russland führen. Nach der Verlegung eines russischen Kriegerdenkmals aus der Hauptstadt Tallin Ende April 2007 wurden Server der estnischen Regierung, von Banken, Zeitungen und anderen Unternehmen Ziel von Cyberangriffen. Sie dauerten mit Unterbrechungen zwei Wochen. Die estnische Regierung sprach damals von Cyberterrorismus, behauptete, dass sie den Ursprung der Angriffe bis auf Rechner des Kremls hätte zurückführen können, und beschuldigte die russische Regierung als Drahtzieher. Die estnische Regierung schaltete die EU und die NATO ein und forderte neben Konsequenzen auch die Entwicklung einer Strategie zum Schutz vor Cyberangriffen. Erwogen wurde gar, ob in solchen Fällen nicht für die Nato-Mitglieder der Verteidigungsfall eintreten müsse. Nach und nach stellte sich aber heraus, dass die Angriffe von weltweiten Bot-Netzen ausgegangen waren. Für eine Beteiligung der russischen Regierung gab es schließlich doch keine Hinweise, die Täter und ihre Absichten sind noch immer nicht bekannt. Abgesehen von den mehr oder weniger starken Distributed Denial of Service (DDoS) Angriffen, die teils über mehrere Stunden stattfanden, gab es keine Versuche, in Computer einzudringen, Daten zu stehlen oder Gelder zu erpressen.

Alleine aus diesem Beispiel wird deutlich, dass die von Russland ausgehende Bedrohung aus dem Cyberraum deutliche Unterschiede zu China aufweist. Dort handelt es sich um relativ klare militärische und geheimdienstliche Strukturen der chinesischen Cyberkrieger und die sich aus den chinesischen Strategien und Konzepten deutlich ergebende Zielrichtung, u.a. durch Daten- und Informationsdiebstahl eine stärkere wirtschaftliche aber auch militärische Rolle im internationalen Wettstreit zu erlangen. In Russland dagegen spielen vor allem die drei wichtigsten Geheimdienste eine maßgebliche Rolle bei Cyberangriffen. Der stärkste ist immer noch der FSB (Federalnaja Sluschba Besopasnosti, übersetzt: Föderale Inlandsabwehr und Sicherheitsdienst) der neben allen Arten von offensiven Informationsoperationen auch sehr stark in der Cyber-Sicherheit involviert ist. Der militärische Auslandsgeheimdienst GRU (Glawnoje Raswedywatelnoje Uprawlenije, übersetzt: Hauptverwaltung für Aufklärung beim Generalstab der Streitkräfte der Russischen Föderation) verfügt neben elektronischer Aufklärung, Satellitenaufklärung und Spezialaufklärungskräften (Speznaz) auch über hochentwickelte Cyber-Potenziale. Hinzu kommt noch der zivile Auslandsgeheimdienst SWR (Sluschba wneschnei raswedki, übersetzt: Dienst der Außenaufklärung, vergleichbar etwa mit dem britischen MI6). Dieser sammelt und analysiert nachrichtendienstlich bedeutende Informationen in Wirtschaft, Wissenschaft, Technologie und Politik (Wirtschaftsspionage). *Siehe Grafik auf der nächsten Seite.*

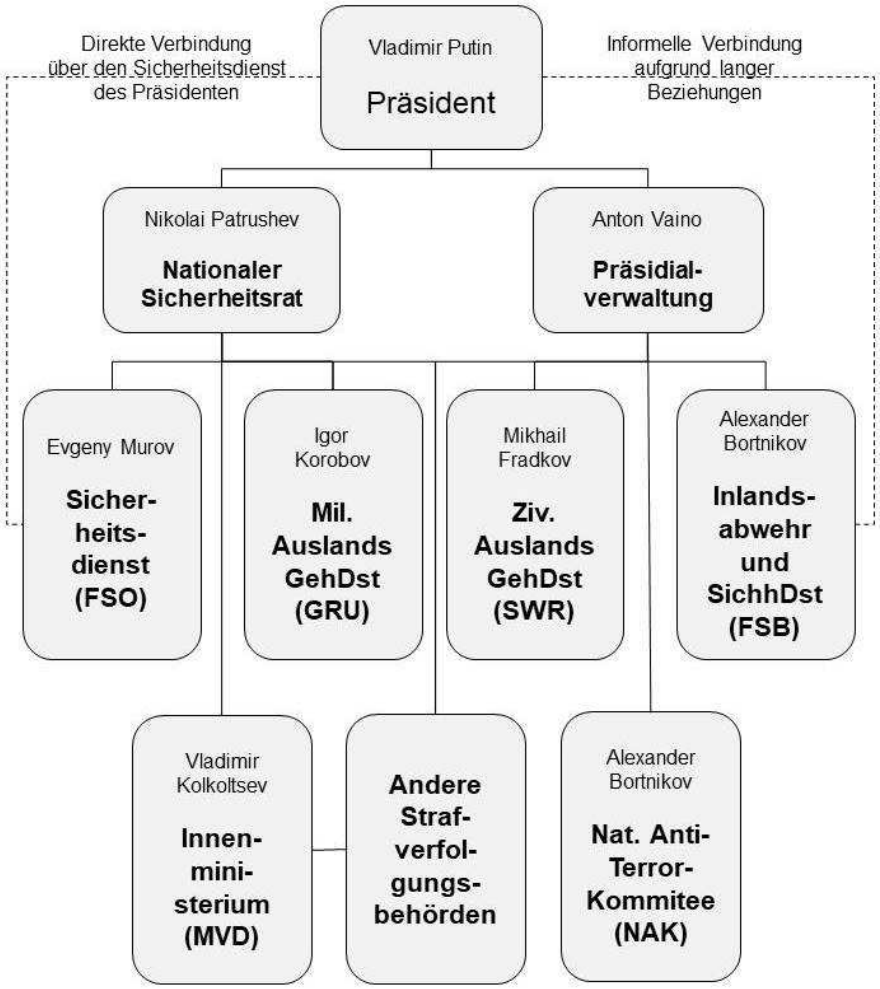
Nach meinen Recherchen verfügen diese drei Geheimdienste zusammen über geschätzt mindestens 4.000 Cyber-Agenten. Bei diesen Experten handelt es sich sowohl um militärisches als auch ziviles Personal. 4.000 klingt zunächst nicht viel, im Gegensatz zu China bedienen sich die Russen bei der Vorbereitung und Durchführung ihrer Cyberattacken vielfach aber auch der Zusammenarbeit mit professionel-

len Hacktivisten und kriminellen Vereinigungen sowie teilweise auch mit Technologiefirmen im Cyberbereich. Alle diese Akteure haben enge Verbindungen zu den russischen Geheimdiensten und werden von diesen auch finanziell unterstützt.

Die Entwicklung der russischen Cyberangriffe kann man in zwei Phasen einteilen. Bis etwa 2014 waren DDoS-Angriffe das am meisten genutzte Mittel. Mit diesem vergleichsweise einfachen Verfahren konnten beispielsweise regierungskritische Webseiten gezielt so überlastet werden, dass ein Zugriff darauf für die Zeit des Angriffs unmöglich wurde. Hinter diesen Angriffen standen häufig dem Kreml nahestehende Jugendbewegungen.

Danach wurden die Verfahren zunehmend technisch aufwändiger, konnten nicht so leicht erkannt werden und ermöglichten dadurch auch lange andauernde Spionageoperationen (Advanced Persistent Threat – APT). Dazu war selbstverständlich auch mehr und besser geschultes Personal erforderlich. Wie bereits beschrieben haben die Russen es dazu geschickt verstanden kriminelle Hacker, Aktivisten und sogar Mitarbeiter von IT-Firmen einzubinden und gleichzeitig die Möglichkeiten der Abstreitbarkeit einer Regierungsbeteiligung zu verbessern. Zwei Gruppen sind bei bekannten Angriffen besonders in Erscheinung getreten:

APT28 (auch „Fancy Bear“ oder Sofacy) ist seit mindestens 10 Jahren aktiv und vermutlich an umfangreichen Operationen zur Unterstützung strategischer Interessen Russlands beteiligt. Die höchstwahrscheinlich aus erfahrenen und produktiven Entwicklern und Hackern bestehende Gruppe hat in der Vergangenheit Informationen zu militärischen und geopolitischen Themen gesammelt. APT28 ist vermutlich für gezielte Eindringkampagnen gegen die Bereiche Luft- und Raumfahrt, Verteidigung, Energie, Regierungsbehörden und Medien verantwortlich, aber auch für Cyberspionage gegen Dissidenten und Personen, die der gegenwärtigen russischen Regierung ablehnend gegenüberstehen. Zielrichtung und Vorgehensweise lassen eine Zugehörigkeit zum Geheimdienst GRU vermuten. In den letzten Jahren hat Russland APT28 anscheinend zunehmend mit Spionageaktionen betraut, die zum Erreichen der strategischen militärischen Ziele des Landes beitragen. Nach der Infiltrierung der anvisierten Opfer stiehlt APT28 interne Informationen und lässt diese an die Öffentlichkeit durchsickern, um russische Interessen zu fördern. Diese Gruppe ist dafür bekannt, mit Phishing Seiten zu operieren, die auf gefälschte, aber legitimen Organisationen täuschend ähnliche Domains verweisen. Damit stehlen sie bei ihren Opfern Anmeldeinformationen zu E-Mail-Diensten oder internen Netzwerken. Zu den Opfern von APT28 zählt auch der Deutsche Bundestag. Bei dem Angriff im Mai 2015 erbeuteten die Hacker Daten in einer Größenordnung von 16 Gigabyte und es dauerte Monate bis das Bundestagsnetz durch das Bundesamt für Sicherheit in der Informationstechnik (BSI) gereinigt und wieder freigegeben werden konnte. APT28 wird auch hinter Aktivitäten vermutet, welche die Position Russlands im Konflikt in Syrien, in den Auseinandersetzungen mit der NATO und der Ukraine, in der Flüchtlingskrise in der Europäischen Union sowie im Dopingskandal rund um die russischen Delegationen bei den Olympischen und Paralympischen Spielen 2016 stärken sollten.



Russlands Geheimdienst-Architektur

Bei APT29 (auch „Cosy Bear“ oder Dukes), einer Gruppe die erstmalig im Jahr 2014 identifiziert wurde, handelt es sich vermutlich um eine hochentwickelte und äußerst fähige Cyber-Spionage-Gruppe mit einem vielfältigen, sich ständig weiterentwickelnden „Cyber-Werkzeugkasten“ und äußerst talentierten Betreibern. Bereits im Sommer 2015 soll diese Gruppe in die Rechner der Demokratischen Partei der USA eingedrungen sein und wurde nicht entdeckt, bis ihre vermutlich militärischen Kollegen von APT28 durch unvorsichtiges Verhalten in den gleichen Zielsystemen die Alarmglocken zum Schrillen brachten. Dieses Beispiel macht deutlich, dass die beiden Gruppen weder zusammenarbeiten noch sich über Operationen austauschen. Dies ist in Russland nichts ungewöhnliches, wie ein im Mai 2016 veröffentlichtes Papier des Europäischen Rates für Auswärtige Beziehungen mit dem Titel „Putins Hydra: Inside Russian’s Intelligence Services“ deutlich macht. In der Vergangenheit lag der Schwerpunkt der Operationen von APT29 beim Diebstahl von Informationen aus Unternehmen um die geopolitischen Interessen und Prioritäten Russlands zu unterstützen. In jüngster Zeit scheint sich die Gruppe mehr auf Ziele mit nachrichtendienstlichem Wert zu konzentrieren. Dazu gehören westliche Regierungen, internationale Sicherheits- und Rechtsinstitutionen, Denkfabriken und Bildungseinrichtungen.
Normalerweise kompromittiert APT 29 seine Ziele über Social-Engineering Spear-Phishing E-Mails – entweder mit bösartigen Mailanhängen oder über einen Link zum Herunterladen einer schädlichen Datei von einer kompromittierten Webseite um Anmeldeinformationen zu stehlen. Ist man mit diesen Informationen in ein System oder Netzwerk eingedrungen wird dieses mit Hilfe von sehr guten Steath-Techniken meist über einen langen Zeitraum ausgeforscht und ausgebeutet. Es ist bekannt, dass APT 29 erbeutete Dokumente und Informationen auch als Köder für weitere Angriffe wiederverwendet. Um die eigenen Operationen zu verschleiern und besser zu schützen, konfiguriert APT29 seine Malware häufig so, dass sie nur zu bestimmten Zeiten aktiviert wird. Die komplexe Malware und die für die Angriffe genutzte Infrastruktur erfordern erhebliche finanzielle Ressourcen und exzellentes Fachwissen.
Bei den russischen Cyberangriffen handelt es sich neben DDoS- und Hacking-Attacken in hohem Maße auch Desinformationskampagnen. Hauptziel der Angriffe sind ausländische Parteien und Regierungen, Rüstungsfirmen und Medienkonzerne.

Die Troll-Armee

Wer twittert zur Unterstützung der Politik? Wer postet auf Facebook Informationen über Militäroperationen oder über die Vergewaltigung einer Dreizehnjährigen durch Migranten in Berlin? Natürlich gibt es Millionen von echten Anhängern einer Regierung oder von Oppositionellen und ihrer Politik, aber besonders im Cyberraum fällt es sehr leicht, solche Unterstützung vorzutäuschen. Die sozialen Medien bieten große Möglichkeiten für staatliche und nichtstaatliche Akteure, gefälschte Identitäten oder automatisch generierte Konten (Social Bots) zu verwenden, um ihre Informationskampagnen massiv zu unterstützen. Über das Vorgehen staatlich gesteuerter russischer Spezialisten für Desinformationskampagnen, der sogenannten Web-Brigaden oder auch Trolle wurde bereits 2003 berichtet. Über die tatsächliche Existenz sowie über Strukturen war aufgrund des verdeckten Charakters lange Zeit nur wenig bekannt. Aus der im Mai 2014 gehackten und durchgesickerten E-Mail-Korrespondenz einer Firma namens „Internet Research Agency“ in St. Petersburg ließ sich die Existenz einer professionellen Troll-Gruppe und die enge Beziehung des Unternehmens zur russischen Regierung sehr deutlich ableiten. Wegen ihres Hauptsitzes in Olgino, einem Bezirk von Sankt Petersburg, spricht man im Englischen auch von den „Trolls from Olgino“. Inzwischen gilt es als gesichert, dass die Organisation im Frühjahr 2015 nach einem Umzug in der Uliza Sawuschkina 55 in Sankt Petersburg ansässig ist.
Dort arbeiten mehrere Hundert freie Mitarbeiter mit entsprechenden Fremdsprachenkenntnissen. In der Regel handelt es sich um junge Studenten denen es vollkommen egal ist was sie schreiben. Sie betreiben in den Kommentarbereichen und Diskussionsforen nationaler und internationaler Nachrichtenportale „Astroturfing“ mit Propaganda der russischen Regierung unter Beachtung und Verwendung vorgegebener Schlagwörter. Medienberichte deuten darauf hin, dass die Beschäftigten damit beauftragt sind, pro Tag 100 Internet-Posts zu schreiben. Nach verschiedenen Quellen ist der Restaurant-Unternehmer und Putin-Vertraute Jewgeni Prigoschin für die direkte Finanzierung zuständig.
Ein bemerkenswertes Beispiel für die erfolgreiche Arbeit der russischen Trolle ist „Jenna Abrams“. Das Profil dieser jungen, fiktiven Amerikanerin tauchte 2014 auf Twitter auf. Zunächst äußerte sie sich zu allen möglichen unverfänglichen Themen. Je näher aber die Präsidentschaftswahlen in den USA kamen umso politischer wurden ihre Kommentare. Sogar die "New York Times" und die BBC zitierten ihre Tweets und Geschichtsprofessoren, Journalisten und sogar Diplomaten antworteten darauf. Ihrem Account folgten mehr als 70.000 Twitter-Nutzer. Das Gleiche gilt für den Account von „Pamela Moore“. Tweets wie „Ich würde eher zehn obdachlose US-Veteranen aufnehmen als 50.000 Migranten / illegale Fremde. Wie sieht es bei euch

aus?“ wurden begeistert aufgenommen. Dadurch, dass sie von Trump-Mitarbeitern wie dem ehemaligen Sicherheitsberater Michael Flynn gelikt und geteilt wurden, erhielten sie eine zusätzliche Legitimität. Hinter diesen Accounts steckten aber keine jungen Amerikanerinnen, sondern wie auch hinter mehr als 2.750 weiteren falschen Inhabern von Twitter-Konten die Troll-Fabrik Internet Research Agency aus St. Petersburg. Mittlerweile sind diese Twitter-Accounts verschwunden, und wer versucht, ihnen eine E-Mail zu schreiben, erhält eine Fehlermeldung.

++ Quellen ++

Lage zur IT-Sicherheit in Deutschland
Bundesamt für Sicherheit in der Informationstechnik (BSI), Stand Oktober 2016

Putins Hydra: Inside Russian's Intelligence Services
http://www.ecfr.eu/publications/summary/putins_hydra_inside_russias_intelligence_services

Cyber War in Perspective – Russian Aggression against Ukraine
edited by Keneth Geers, CCDCoE

APT28: Mitten im Sturm – Russland entwickelt seine Cyber-Operationen strategisch weiter
FireEye, Sonderbericht/Januar 2017

Russlands Informationskrieg - So funktioniert eine Troll-Fabrik
David Nauer
https://www.srf.ch/news/international vom 20.02.2017

Die Trolle des Kremls
Friedrich Schmidt
http://www.faz.net/aktuell/politik/ausland/

Cyberübungen: NATO und EU wappnen sich gegen russischen Cy-Bären
https://de.rt.com/17w9

Der Cyberraum als Teil der russischen Strategie

Die russische Strategie geht davon aus, dass die Cyber-Fähigkeiten direkt zur Gestaltung politischer Zielsetzungen beitragen müssen. Die Besetzung der Krim und der Ukrainekonflikt zeigen auf beeindruckende Weise, wie gut es die Russen verstanden haben, die Möglichkeiten des Cyberraums in einem speziellen geopolitischen und militärischen Kontext einzusetzen. Mit begrenzten kinetischen Effekten und minimalen Opfern wurden vollendete Tatsachen geschaffen, stets begleitet durch umfangreiche Informationsoperationen, die in erster Linie als Mittel der politischen Nötigung, zur Meinungsbildung und zur Informationsbeschaffung eingesetzt wurden. Damit ist es ihnen gelungen, die Abschreckungsstrategie der NATO zu umgehen und die Entscheidung über eine mögliche Eskalation auf die NATO zu verlagern.
Die Besetzung der Krim war ein Musterbeispiel dafür, wie die Russen die Möglichkeiten des Cyberraums in militärischen Operationen nutzen, um einen Gegner technisch zu isolieren, schildert Nato-General Philipp Breedlove das russische Vorgehen: Telefonleitungen wurden durchgeschnitten, das Mobilfunknetz gestört, Internetverbindungen unterbrochen. „Sie haben die ukrainischen Einheiten der Krim von ihrem Kommando abgeschnitten“.
Und bei der Unterstützung der Separatisten in der Ukraine wurden ebenfalls massiv Cyberattacken eingesetzt. Praktisch jeder wichtige Bereich der Ukraine ist von Hackern systematisch erschüttert worden: Medien, Finanzsektor, Transport, Militär, Politik, Energie. Bei immer neuen Wellen von Angriffen wurden Daten gelöscht, Computer zerstört und in einigen Fällen die grundlegendsten Funktionen von Institutionen zumindest vorübergehend gelähmt. Ein relativ aktuelles Beispiel waren die Angriffe mit dem Erpressungs-Trojaner „Petya / NotPetya“ im Juni 2017. Bekanntlich missbrauchten die Täter die Steuersoftware MeDoc, die in der Ukraine bei Unternehmen eine große Verbreitung hat. Diese ganzen Cyberangriffe stiegen aber nie auf ein Niveau, welches mit einem kinetischen Angriff vergleichbar gewesen wäre und entsprechende Reaktionen gerechtfertigt hätte. Schwerpunkt waren vielmehr auch in der Ukraine Desinformationskampagnen und Informationsbeschaffung.
Im Vergleich zu Georgien, wo russische Panzereinheiten um die „friedensschaffende Durchsetzung“ kämpften und russische Flugzeuge Ziele bombardierten, war Russland im Ukrainekonflikt sehr vorsichtig, was den Einsatz der regulären russischen Streitkräfte anbelangt. Diese Vorsicht mag in den Erfahrungen aus dem Georgienkonflikt begründet sein oder aber dem Wunsch, nach einem gewissen Maß an Abstreitbarkeit von Verletzungen des Völkerrechts. In jedem Fall haben die Ereignisse auf der Krim und in der Ukraine gezeigt, dass Cyber-Fähigkeiten einer Nation neue Möglichkeiten verschaffen, offensive Aktionen mit geringerem politischem Risiko durchführen zu können. Für die NATO aber auch für die EU bedeutet dies, dass man die Bewertung des Einsatzes von Cyberangriffen durch einen Gegner neu durchdenken und möglicherweise anpassen muss. Dies schließt auch Überlegungen zur Schaffung eigener offensiver Cyberkräfte und die aktive Unterstützung der Schaffung von internationalen Rechtsnormen für den Cyberraum ein. Mit gemeinsamen Übungen wie EU CYBRID 2017 oder EU PACE 2017wollen NATO und EU deshalb die gemeinsame Verteidigungsfähigkeit gegenüber Cyberbedrohungen erhöhen.

Im nächsten und letzten Teil dieser Serie werden die Cyber-Fähigkeiten des IRAN und Nordkoreas behandelt.

Nachwuchsgewinnung im Informationstechnikbataillon 281

Oberstleutnant Torsten Täumer, StvBtlKdr ITBtl 281

Auf den sich in Bewegung setzenden Zug einer großangelegten Nachwuchskampagne sattelte auch das ITBtl 281 in der Erkenntnis auf, dass das Interesse von jungen Menschen und die Begeisterung für die Bundeswehr nur durch zwei große Pfeiler geweckt werden kann. Zum einen müssen Systeme, für deren Bedienung geworben wird, gezeigt und greifbar dargestellt werden, zum anderen muss Personal, welches diese Systeme bedient, vor Ort ansprechbar sein und die Begeisterung für den eigenen Beruf vermitteln können. Dieser Erkenntnis folgend war es der Anspruch des ITBtl 281 ein aktives Mitwirken zu etablieren, mit dem klaren Ziel in erster Linie Nachwuchs für die „eigenen Reihen“ zu gewinnen und dem deutlichen Mehrbedarf an IT-Fachpersonal durch geeignete Maßnahmen gerecht zu werden.

So entstand eine eigene „Zelle Nachwuchsgewinnung“ unter der Gesamt-Federführung des StvBtlKdr, für die Personal nicht zusätzlich bereitgestellt, sondern von bestehenden Aufgaben „abgezweigt“ werden muss. Bestehend aus zwei erfahrenen Unteroffizieren mit Portepee, die nicht nur die Fachexpertise bezüglich der IT- Systeme, sondern auch spürbare Begeisterung für den eigenen Beruf vermitteln können und zwei Mannschaftsdienstgraden wird die Idee, Begeisterung für den Beruf des Soldaten und im Besonderen des IT-Spezialisten mittels Präsentation greifbarer IT-Systeme aus dem Verband in die Tat umgesetzt. Schwerpunkt des Gerolsteiner Kommandeurs Oberstleutnant Christian Sohns ist es, für „sein Bataillon“ durch kreative Ansätze und neue Denkweisen den Fach-Bereich Informationstechnik für potentielle Interessenten attraktiv zu gestalten und so auf lange Sicht schlussendlich alle Dienstposten im eigenen Bereich mit geeigneten Bewerbern besetzen zu können. Hierzu wurden mehrere Projekte in Gerolstein ins Leben gerufen.

Suche
IT-Spezialisten –
biete
IT-Dienstposten in Gerolstein

. . . so oder ähnlich könnte eine Werbeanzeige in der lokalen Presse oder auf einschlägigen Social-Media Plattformen lauten, wenn es da nicht schon diverse Slogans der Bundeswehr zum Thema Nachwuchsgewinnung gäbe.

Unstrittig ist jedoch, dass bedingt durch die Komplexität der genutzten IT-Systeme eine hohe Anzahl an IT-Spezialisten für diverse Aufgabenbereiche benötigt werden, bzw. der Arbeitgeber Bundeswehr wieder deutlich in den Fokus von jungen Menschen gerückt und attraktiv gestaltet werden muss. Schließlich steht die Bundeswehr als Arbeitgeber im harten Wettbewerb zu der zivilen Arbeitswelt und buhlt ebenso um die besten „Azubis“. Die Aussetzung der Wehrpflicht 2011 und unterschiedliche Strukturreformen in den letzten Jahren hatten zur Folge, dass der danach entstandene überdurchschnittlich hohe Personalbedarf an IT-Spezialisten nicht mehr gedeckt werden konnte. Die Notwendigkeit die Abhängigkeit von Überbelastung des Personals, Abwesenheiten, Ausbildung, Einsatzgestellung und fehlenden Fachleuten bzw. einer grundlegenden Dienstpostenbesetzung zu begegnen, wurde mittlerweile auf allen Ebenen in der Bundeswehr erkannt.

Ein mittlerweile etabliertes und effektives Konzept verbirgt sich hinter dem vier Mal pro Jahr organisierten „IT-Info Tag“. Vor allem Schulklassen aus der Umgebung und Interessenten der Karrierecenter Düsseldorf und Mainz werden nicht nur der Auftrag und die Aufgaben des ITBtl 281 erläutert sowie gleichzeitig der Arbeitgeber Bundeswehr vorgestellt, sondern parallel mit einer Systemschau die unterschiedlichsten IT-Systeme von erfahrenen IT-Feldwebeln „zum Anfassen“ vorgestellt, Neugierde geweckt und zum Mitmachen angeregt. Die Kombination aus der Darstellung von „grünen“ und „gelben“ Anteilen, die authentische Vorstellung von Beruf und Technik, Präsentation von jungen IT-Charakteren sowie die unmittelbare Chance zur Informationsgewinnung über die beruflichen Möglichkeiten in der Bundeswehr werden bei Interesse direkt durch Reservierung eines Dienstpostens in Form einer Truppenwerbung umgesetzt.

Als Highlight der Gerolsteiner Nachwuchsgewinnung kann das seit 2015 ins Leben gerufene und zwei Mal jährlich angebotene, mit wachsender Nachfrage belegte, einwöchige „IT-Info Camp“ in Zusammenarbeit mit den örtlichen Karrierecentern bezeichnet werden. Dieses Jahr bündelte die Bundeswehr die Bemühungen der Nachwuchsgewinnung der einzelnen Bataillone erstmals in einem gemeinsa-

men Projekt unter dem Namen „Cyberdays“. Während einer erlebnisorientierten Woche im Bataillon werden den 30 - 40 Teilnehmerinnen und Teilnehmern in Gerolstein die verschiedenen IT-Systeme näher gebracht und gleichzeitig ein offener Einblick in das militärische Leben und die Anforderungen an den Beruf des Soldaten geboten. Die so dargestellte Kombination des Berufs „Soldat und IT-Spezialist“ können die Teilnehmer durch aktives Mitmachen z.B. durch Überwinden der Hindernisbahn, das Ablegen des Basis-Fitness-Tests und das Leben im Felde erfahren, aber auch durch Integration in Aufbau und Betrieb von Anteilen des IT-Systems Bundeswehr. Schlussendlich steht mit Hilfe einer „Funktionsüberprüfung“ in Form eines serverbasierten Netzwerkspiels der Abschluss des IT-Camps an, bei dessen Umsetzung letzte fachspezifische Fragen nochmals erörtert werden können. Das Engagement der Soldatinnen und Soldaten und ihr persönlicher Einsatz während der Vorstellung „ihrer IT-Systeme“ und ihres Berufs-Arbeitsalltags führt im Schnitt dazu, dass mehr als die Hälfte der Teilnehmerinnen und Teilnehmer als zukünftige Soldatinnen und Soldaten für den Standort Gerolstein gewonnen werden.

Mittlerweile üblich und nicht mehr aus dem Bereich der regionalen Job- und überregionalen Fachmessen wegzudenken ist das Bemühen der Nachwuchsgewinnung in der Fläche präsent zu sein, wie zuletzt am „Hessentag 2017“ mit einem Besuchervolumen von ca. 1,4 Millionen Interessenten. Entweder in Form eines eigenen, mittlerweile dem zivilen Standard angepassten Messestandes oder im Verbund mit anderen Einheiten bzw. öffentlichen Behörden präsentiert sich das in der Eifel beheimatete ITBtl 281 souverän. Besonders durch IT-Exponate, die die Aufmerksamkeit der Besucher auf sich lenken (SATCOM, VTC, DINGO, EAGLE), kreative Gewinnspiele und authentische Vermittlung der Tätigkeit, vermögen die Soldaten der Nachwuchsgewinnungszelle schnell den Kontakt zu den Besuchern herzustellen. Herausfordernd bleibt das Werben um die besten und ideenreichsten Köpfe dennoch auch weiterhin, da nicht nur die personelle Organisation der Nachwuchsgewinnung der Kreativität der Truppe überlassen ist, sondern finanzielle Ressourcen fehlen, um die auf hohe Qualität ausgerichtete Arbeit zu stützen. In Zusammenarbeit mit den Karrierecentern kann vor Ort der Informationsbedarf möglicher Bewerber sofort fundiert gedeckt und alle weiterführenden Fragen einer Bewerbung bei der Bundeswehr beantwortet werden.

Durch die zwischenzeitlich ins Leben gerufenen Partnerschaften und Kooperationen mit Schulen im Umkreis von Gerolstein wurde ein weiterer Baustein im Rahmen der Nachwuchsgewinnung gelegt. Durch das frühzeitige Erkennen der Bundeswehr als optionalen Arbeitgeber bei Schulleitern und Schülern sowie das Wecken von Interesse von Jugendlichen und Schulabgängern für den Beruf des IT-Spezialisten am Standort Gerolstein resultiert nicht nur das Knüpfen erster Kontakte, sondern stiegen stetig die Praktikumsanfragen im Jahr 2017. Die berufsbildende Schule Gerolstein oder die Realschule plus aus Niederzissen seien hier beispielhaft genannt.

Oberstabsfeldwebel Karlheinz Bolz, Leiter der Nachwuchsgewinnung, ist überzeugt, dass hiermit der richtige Schritt in Richtung einer nachhaltigen Regenation für die Zukunft eingeleitet wurde.

Resultierend aus allen angestoßenen und etablierten Maßnahmen vermochte die Nachwuchsgewinnung am Standort Gerolstein von September 2016 bis Juli 2017 ihre Truppenwerbungen auf mehr als 190 potentielle Bewerber zu steigern und ist damit ihrem Ziel, Nachwuchs „mit der Truppe für die Truppe“ zu generieren hinsichtlich der Besetzung offener Dienstposten im ITBtl 281 ein erhebliches Stück näher gekommen. Aufgrund der langen und intensiven Ausbildung ist es jedoch noch ein „langer und steiniger Weg“, bis ein Bewerber letzten Endes als IT-Spezialist zur Verfügung steht.

Die Methodik mit Hilfe von IT-Systemschau „zum Anfassen“, Präsentation der Systeme durch hochmotivierte IT-Feldwebel, dem Wecken von Neugierde und Anregung zum Mitmachen in Kombination aus der Darstellung von „grünen“ und „gelben“ Berufs-Anteilen, die authentische Vorstellung von Beruf und Technik, Präsentation von jungen IT-Charakteren sowie die unmittelbare Chance zur Informationsgewinnung und den regen Meinungsaustausch über die beruflichen Möglichkeiten in der Bundeswehr scheint in Gerolstein ein vielversprechender Weg zu sein, um dem stetig wachsenden Bedarf an IT-Profis vorausschauend begegnen zu können.

Partnerschaft mit der Realschule plus in Niederzissen

Murnauer Offiziere bei der historischen Weiterbildung

Oberleutnant Christopher Schüttler / Fotos: ITBtl 293

Vom 14. bis 15. November unternahmen die Offiziere des Informationstechnikbataillon 293 aus Murnau eine Offizierweiterbildung in Stetten am kalten Markt und Albstadt-Lautlingen. In unregelmäßigen Abständen finden solche Fortbildungen stand, bei denen die militärhistorischen Kenntnisse der Offiziere vertieft und der kameradschaftliche Zusammenhalt gefestigt werden soll.

Am ersten Tag besuchten die Offiziere die Militärgeschichtliche Sammlung der Bundeswehr in der Garnison Stetten a.k.M. Die Ausstellung ist im 1916 erbauten Gebäude im Lager Heuberg in der „ehemaligen kaiserlichen Offiziersspeiseanstalt“ zu finden. Die Sammlung ist für jedermann zu besichtigen und von außerhalb des Kasernenzauns zugänglich. Allein dies zeigt schon die Historizität des Standortes Stetten am kalten Markt und die tiefe Verflechtung zwischen ziviler und militärischer Welt. Die in liebevoller Handarbeit und oft aus privaten Mitteln heraus entstandene Sammlung präsentiert auf einer Fläche von mehr als 900 m² die über 100-jährige Militärgeschichte der Garnison von der Kaiserzeit bis zu Bundeswehr. Aber auch die unterschiedlichen Etappen der zivilen Nutzung, wie zum Beispiel die Zeit der Kindererholungsfürsorge e.V., finden ausreichend Beachtung.

Die Natter

Das Highlight der Sammlung ist wohl die lebensgroße Nachbildung der Bachem Ba 349 A Natter, samt Startrampe. Dieses senkrechtstartende Flugzeug, welches in der Endphase des Zweiten Weltkrieges entwickelt wurde, gehört zu den Pionierleistungen der Raketenentwicklung und ist im deutschen Geschichtsbild nur wenigen bekannt. Anschließend fuhren die Teilnehmer über den Truppenübungsplatz und besichtigten unter anderem die Startstelle der Natter.

Der zweite Tag führte die Offiziere nach Albstadt-Lautlingen. Dort befindet sich das Stauffenberg-Schloss, welches der Sommersitz der Familie von Staufenberg war. Das Anwesen beherbergt eine Gedenkstätte, die dem Widerstandskämpfer Claus Schenk Graf von Stauffenberg gewidmet ist. Hier verbrachte der spätere Offizier und Widerstandskämpfer seine Ferienzeit. Der Besuch fand an einem besonderen Tag statt: es war der 110. Geburtstag Claus von Stauffenbergs. Die Ausstellung versucht, die Lebensgeschichte dieses Mannes nachzuzeichnen: seine Kindheit, seine Erziehung, seinen Gang ins Militär und seine anfängliche Begeisterung für den Nationalsozialismus und die militärischen Erfolge des Dritten Reichs. Schließlich wird sein Wandel vom Zweifler zum Gegner und letztendlich zum Kämpfer des Widerstands dargestellt. Die Ausstellung bietet genügend Raum für die Familie von Stauffenberg. Zahlreiche „stille Zeitzeugen“ in Form von Fotos, Briefen, Gedichten, Büchern und anderen Privatgegenständen lassen den Besucher wenigstens einen kleinen Einblick in das Leben der Familie nehmen.

Fazit

Die Offiziere des Informationstechnikbataillons 293 konnten mit vielen neu gewonnenen Eindrücken und der Erkenntnis, dass das militärgeschichtliche Wissen immer noch erweitert werden kann, die Heimreise nach Murnau antreten.

Einführung Dokumentenmanagementsystem Bundeswehr (DokMBw 1. AS)

EFO DokMBw SKB, KdoSKB Fü FüUstg
(OTL Andreas Koes, M Frank Schmeil, H Michael Kirsten, OSF Thomas Staab, SF Adrian Valette)

Mit der Einführung des Dokumentenmanagementsystems der Bundeswehr in der ersten Ausbaustufe (DokMBw 1. AS) will die Bundeswehr den aktuellen gesetzlichen Anforderungen Rechnung tragen und einen weiteren, gewaltigen Schritt in Richtung digitale Verwaltung gehen. Dies wird zu Veränderungen in der täglichen Stabs- und Verwaltungsarbeit aller Beschäftigten führen, denn insbesondere die Bereiche der revisionssicheren Vorgangsbearbeitung und Aktenhaltung, Archivierung und elektronischen Zusammenarbeit sind betroffen.

1. DokMBw 1. AS – Wo liegt der Ursprung?

Aufbauend auf den Konzepten „Dokumentenmanagement und elektronische Archivierung im IT-gestützten Geschäftsgang“ (DOMEA, 1996) sowie „Organisationskonzept elektronische Verwaltungsarbeit“ (OKeVA, 2012), wird das Ziel der Verwaltungsmodernisierung im Regierungsprogramm „Digitale Verwaltung 2020“ (DiV 2020) fortgesetzt und konkretisiert. Die entsprechenden Vorgaben zur Einführung der elektronischen Verwaltungsarbeit (eVA) sind im E-Government-Gesetz (EGovG) aus dem Jahr 2013 geregelt. Die Umsetzung dieser Vorgaben ab 2020 ist für alle Ressorts des Bundes und somit im GB BMVg für zivile als auch militärische Organisationsbereiche (OrgBer) bindend.

Gemäß Beschluss Staatssekretär-Ausschusstagung vom 03. März 2015 zur Programmumsetzung DiV 2020 befasst sich das Referat BMVg CIT I 4 (PG DiV) mit der Strategie und deren Umsetzungssteuerung und -kontrolle der Anforderungen eVA im GB BMVg Ablauforganisatorisch wurde zudem eine ministerielle Arbeitsgruppe „Elektronische Verwaltungsarbeit im Bereich Dokumentenmanagement im GB BMVg“ (AG eVA DokM) sowie die nachgeordnete UAG eVA DokM mit Vertretern der OrgBer/Ber eingerichtet. In letzterer werden Grundlagenthemen wie „Datenmigration“, „Workflows“, Wissensmanagement oder Ausbildung in einzelnen Facharbeitsgruppen betrachtet und Bw-gemeinsame Vorgaben erarbeitet. Für die konkrete Einführung des Systems wurden jeweils Einführungsorganisationen (EFO) in den OrgBer/Ber aufgestellt.

2. DokMBw 1. AS – Ziel und Zweck des Systems

Ziele der elektronischen Stabs- und Verwaltungsarbeit und somit gem. §6 EGovG sind es, Aufgaben in den Behörden effizienter und effektiver zu erfüllen. Kerngedanke ist dabei die nachvollziehbare, strukturierte Ablage der aktenrelevanten Dokumente, Vorgänge und Akten. Darüber hinaus soll dies medienbruchfrei und rein elektronische durch nachfolgender Elemente in DokMBw 1. AS umgesetzt werden:

- Die **elektronische Akte** (E-Akte) erlaubt dabei den orts- und zeitunabhängigen Zugriff auf das Schriftgut respektive die Dokumente. Verschiedene Funktionen erleichtern dem Bearbeiter das vollständige Ablegen von aktenrelevanten Informationen und Dokumenten, beispielsweise von E-Mails, und das Auffinden von Dokumenten in der Akte oder dem System. Die Anforderungen der Revisionssicherheit und Archivierbarkeit werden dabei mit erfüllt.
- Bei der **elektronischen Vorgangsbearbeitung** (E-Vorgangsbearbeitung) werden Vorgänge oder Untervorgänge papierlos abgewickelt. Daneben werden Erinnerungs- und Wiedervorlagefunktionen sowie eine Fristüberwachung angeboten. Der Status der Vorgangsbearbeitung ist jederzeit einsehbar – ein Vorteil gerade bei komplexen Verfahren.
- Die **elektronische Zusammenarbeit** (E-Zusammenarbeit) unterstützt Abstimmungen, besonders bei organisationsübergreifender Zusammenarbeit in Vorgängen, Projekten und Gremien. Darüber hinaus unterstützt sie die informelle Zusammenarbeit, das heißt den Austausch von Information und Wissen über Referats- oder Abteilungsgrenzen hinweg. Das sichert Effizienz und Qualität der Stabsarbeit und des Verwaltungshandelns. Eine leistungsfähige Suche in Kombination mit einer Metadaten-Systematik unterstützt den Nutzer bei der täglichen Arbeit.

Technisch gesehen ist DokMBw ein IT-Service, der als Web-Anwendung bereitgestellt wird. Die dahinterliegende Software auf Basis von Microsoft SharePoint 2016 und dem eGoverment-Framework der Fa. CGI führt ein Dokumentenmanagementsystem (DMS) mit einem Vorgangsbearbeitungssystem (VBS) mithilfe eines Berechtigungssystems zusammen. Über

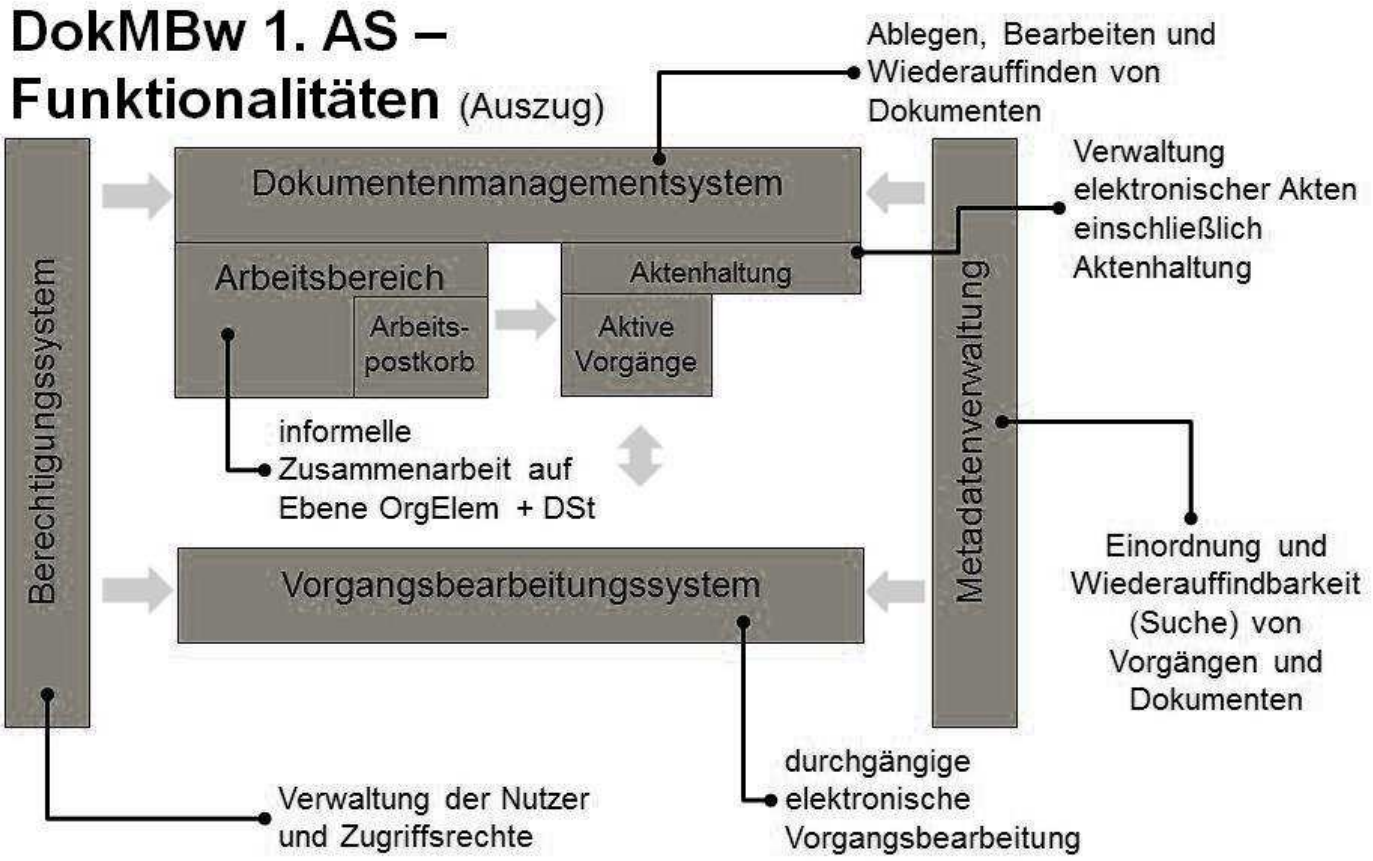


Abbildung 1:
Funktionalitäten DokMBw 1. AS
Quelle: in Anlehnung an CGI

eine integrierte Metadatenverwaltung wird der gesamte Lebenszyklus einer Information von der Erhebung bis hin zur Archivierung im Rahmen der Kaskade Dokument-Vorgang--Akten abgebildet und gesteuert. (vgl. Abb. 1). Durch diese Kombination beider Plattformen und den spezifischen Anpassungen für das BMVg und die Bundeswehr können circa 80 % der funktionalen Forderungen des OKeVA-Bausteins „E-Akte“ und circa 40% der OKeVA-Bausteine „E-Vorgangsbearbeitung“ und „E-Zusammenarbeit“ bereits abgedeckt werden.

3. DokMBw 1. AS – Einführung des Systems

Mit schrittweiser Einführung und weiterem Ausbau des Systems auf die beabsichtigte Nutzeranzahl von insges. 190.000 Nutzern wird DokMBw das „Hauptwaffensystem“ der Stabs- und Verwaltungsarbeit und schrittweise die Nutzung von Lotus Notes in Verbindung mit dem Fileservice der BWI deutlich minimieren. Mit anderen Worten: zukünftig wird der gesamte elektronische Geschäftsverkehr einer Dienststelle (DSt) im System DokMBw abgewickelt.

Dabei werden die bisherigen LoNo-Mails, mit denen Vorgänge und Aufträge gesteuert wurden durch Aufgaben und Vorgänge in DokMBw ersetzt. Das Aktenhaltungssystem des DokMBw übernimmt dabei künftig die bisherige Aufgabe des Fileservice. Auf diese Art und Weise wird nicht nur gleichzeitige Zusammenarbeit ermöglicht, sie wird darüber hinaus schneller, einfacher und transparenter.

Ein Pilotbetrieb DokMBw wurde bereits im Jahr 2013 im Streitkräfteamt (SKA) auf einer Weiterentwicklung des von der Firma CGI vertriebenen NATO Document Handling Systems (DHS) durchgeführt.

Die Einführung des Systems in der ersten Ausbaustufe folgt einem abgestimmten Rolloutplan, der unterteilt in insgesamt 12 Blöcke die Bereitstellung des Systems in 33 Dienststellen der Bundeswehr sowie dem BMVg bis Ende 2019 vorsieht.

Als erste DSt wurde im August 2017 das SKA mit dem System ausgestattet. Aktuell befindet sich das Projekt DokMBw 1. AS im Rollout des vierten (4.) Blocks. Dies umfasst den Stab KdoSKB auf der Bonner Hardthöhe, das Marinekommando (MarKdo) in Rostock sowie das Luftwaffentruppenkommando (LwTrKdo) in Köln-Wahn. In den Blöcken zwei (2) und drei (3) wurden bereits das Kommando Heer (Kdo H) in Strausberg, das Kommando Cyber-/Informationsraum (KdoCIR) in den Bonner Rheinauen, das Kommando Luftwaffe (Kdo Lw)

in Köln-Wahn, das Planungsamt der Bundeswehr (PlgABw) in Berlin, das Amt für Heeresentwicklung (AHEntwg) in Köln sowie das Einsatzführungskommando der Bundeswehr (EinsFüKdoBw) in Potsdam ausgerollt. Eine Gesamtübersicht aller auszustattenden DSt kann im Informationsportal DokMBw 1. AS unter dem Link: ***https://wiki.bundeswehr.org/display/DokMBwInfoP/Allgemeine+Informationen*** eingesehen werden. In diesem Zusammenhang sei dieses Portal grundsätzlich zur Informationsgewinnung empfohlen, da neben Grundlagendokumenten zum Projekt ebenso die jeweiligen Einführungsorganisationen der OrgBer dort über den jeweils aktuellen Sachstand informieren.

Leider konnte bisher weder das SKA, noch eine der anderen ausgerollten DSt den operativen Betrieb DokMBw 1. AS aufnehmen. Dies ist auf einige noch offene projektseitige Arbeitspakete zurückzuführen: Mit Blick auf derzeitigen Herausforderungen ist die Beschreibung auf zwei grundsätzliche Handlungsfelder beschränkt, nämlich einerseits die Maßnahmen, die gem. CPM (nov.) für den Übergang eines Projektes aus der Realisierungsphase in die Nutzungsphase erforderlich sind, und zum anderen die auf der betrieblichen Seite vorzusehenden Verfahren und Regelungen zum sicheren Betrieb des Systems.

Auf Seite des Bedarfsträgers steht die „Erklärung der Übernahmebereitschaft“ seitens der OrgBer der Bundeswehr aus, die aktuell an mehrere Bedingungen (HHM-Deckung IT-Erstausb 2018ff.; MZ HPR, ITSM, Freigabe IT-Sichh, ReleaseMgmt) geknüpft ist. Erst wenn die Bedingungen des Bedarfsträgers erfüllt, die Übernahmebereitschaft durch die OrgBer erklärt ist, wird der Bedarfsdecker (hier das BAAINBw) die „Genehmigung zur Nutzung“ (kurz: GeNu) des Systems erteilen. Diese GeNu liegt aktuell (noch) nicht vor. Derzeit wird in allen Bereich die vorhandene Installation zu Testzwecken und zur Inübunghaltung des ausgebildeten Personals genutzt.

Auf der betrieblichen Seite steht die Umsetzung des „Betriebskonzeptes DokMBw“ durch die BWI in entsprechende IT-Service-Prozesse aus, insbesondere die Anpassung des Ticketsystems der BWI (MAXIMO), als auch das IT-SPS-Verfahren für sog. „Standard Changes“ sind hier zu nennen. Ohne zugehörige Service-Management-Prozesse ist ein reines „Betriebskonzept“ wirkungslos und die Aufnahme eines „Wirkbetriebes“ in den DSt den Nutzern, vor allem jedoch den Nutzerbetreuern nicht zumutbar.

An diesen Herausforderungen wird intensiv gearbeitet. BMVg CIT I 4, als fachlich zuständiges Referat, ist unentwegt, mit dem Hersteller (CGI), dem Betreiber (BWI) sowie der Projektleitung (BAAINBw H2.3) in Kontakt, um die Einsatzreife des Produktes herzustellen und den Übergang in die Nutzung zu realisieren.

4. DokMBw 1. AS – Ausbildungssystematik

Ein wesentlicher Garant für das Gelingen des Projektes ist die zugehörige Qualifikation und Befähigung der Nutzer, der PowerUser und Fachadministratoren DokMBw. Hierzu ist ein mehrstufiger Ansatz vorgesehen:

Vertragsnehmer für die Durchführung der IT-Erstausbildung des Projektes ist die Firma ML Consulting, die den meisten Lesern wahrscheinlich aus dem Bereich der „KIT-Ausbildung“ bekannt sein dürfte, ist sie doch Rahmenvertragspartner der Bundeswehr. Auch für das System DokMBw hat ML Consulting im firmeneigenen Bereich „Training“ eine entsprechende Kompetenz aufgebaut und führt im Auftrag der Bundeswehr die eintägigen (1 Ausbildungstag = AT) Nutzerschulungen bei den betroffenen Dienststellen der Bundeswehr vor Ort durch. Die PowerUser-Schulungen (5 AT) sowie die Lehrgänge der Fachadministratoren (10 AT) werden dementgegen als Training an den Einrichtungen des Kompetenzzentrums IT-Ausbildung Bw (KIT) durchgeführt und sind entsprechend auch im System IAMS zu buchen.

Die Inhalte der Nutzerschulungen wurden mit dem Bedarfsträger abgestimmt und spiegeln in drei Grundbausteinen (Dateneingang – Vorgangsbearbeitung – Aufgabensteuerung) die wesentlichen Funktionalitäten des DokMBw 1. AS wieder. Ziel der Schulung ist die Grundbefähigung des Nutzers zur Wahrnehmung seiner Aufgaben mit Unterstützung des Systems DokMBw.

Ergänzt wird dieser Trainingsansatz durch die, ebenso durch ML Consulting erstellten, Web-based Trainings (WBT) im Lernmanagementsystem der Bundeswehr (LMSBw). In kurzen und verständlichen Video-casts werden einzelne Themen aufgegriffen und erklärt.

Nicht zuletzt können sich die Nutzerinnen und Nutzer über das oben genannte Informationsportal weitergehend informieren und austauschen sowie die ihnen zugeordneten PowerUser zu Rate ziehen.

5. DokMBw 1. AS – Zusammenfassung und Ausblick

DokMBw 1. AS legt den wesentlichen Grundstein der elektronischen Stabs- und Verwaltungsarbeit und wird damit das künftige Gesicht dieser in den Stäben der (höheren) Kommandobehörden und Ämtern zu verändern.

Es wird demnach also nicht nur ein reines Dokumentenmanagementsystems eingeführt: Nach dem Grundsatz „alles aus einer Hand“, kann der Dokumentenlebenszyklus

bruchfrei, d.h. ohne weitere IT-Services, wie Lotus Notes oder dem File Service, abgebildet werden. Darüber hinaus erleben die Grundsätze des Geschäftsverkehrs im GB BMVG ein „Revival“: das Aktenzeichen (Zentrale Dienstvorschrift A-500/11) wird als Teil des „Geschäftszeichens“ DokMBw als wesentliches Metadatum im System geführt Darüber hinaus finden Geschäftsgangvermerke und -verfügungen (Zentrale Dienstvorschrift A-500/0-0-10) ihr digitales Pendant.

In Abbildung 2 sind zu erwartende Mehrwerte aus der Nutzung DokMBw 1. AS zusammengestellt. DokMBw wird die Grundlagen für eine bessere eVA legen. Damit werden künftige Mitprüfung-/Mitzeichnungsgänge, Abstimmungs- und Beteiligungsverfahren, aber auch team- und projektbasierende Arbeiten deutlich einfacher und effektiver durchzuführen sein.

Abbildung 2:
Mehrwert DokMBw 1. AS
Quelle: KdoSKB EFO DokMBw SKB

Wesentlich für den Erfolg der Einführung und Nutzung sind die Nutzer und Nutzerinnen: Bearbeiter von Dokumenten oder Vorgängen werden sich an die zwingende Befüllung von Metadatenfeldern und die zentralisierte Ablage der Dokumente gewöhnen müssen.
Die theoretisch bereits bisher bestehenden Möglichkeiten, wie bspw. die Nutzung der Metadatenfelder in den Microsoft Office-Anwendungen oder der zentrale Dokumentenbereitstellung im WikiService-Bw, wurden meist aus Gründen der Bequemlichkeit oder aus Zeitgründen nicht genutzt.
Das Ergebnis war und ist zumeist eine Unzahl von gleichen, nicht registrierten Dokumenten desselben Inhaltes auf unseren Fileservern.

Im Rahmen von weiteren Ausbaustufen von DokMBw werden durch den Auftragnehmer weitere Anforderungen der OrgBer/Ber, wie bspw. die Workflow-Generierung, umgesetzt und Funktionalitäten ergänzt werden.

Im Zuge der Digitalisierung der Bundeswehr wird mit Blick auf das Projekt „GroupwareBw“ die Grundsteinlegung durch DokMBw manifestiert und durch weitere IT-Services (z.B. Videokonferenzsystem, Kollaborationssysteme) erweitert werden.
Hierzu ist die AWE (zwar unter Auflagen) gezeichnet und der Kurs des Projektes festgelegt und der Weg beschritten.

Die Aufgaben des Cyber Security Operations Centre der Bundeswehr (CSOCBw) im neuen Zentrum für Cyber-Sicherheit der Bundeswehr (ZCSBw)

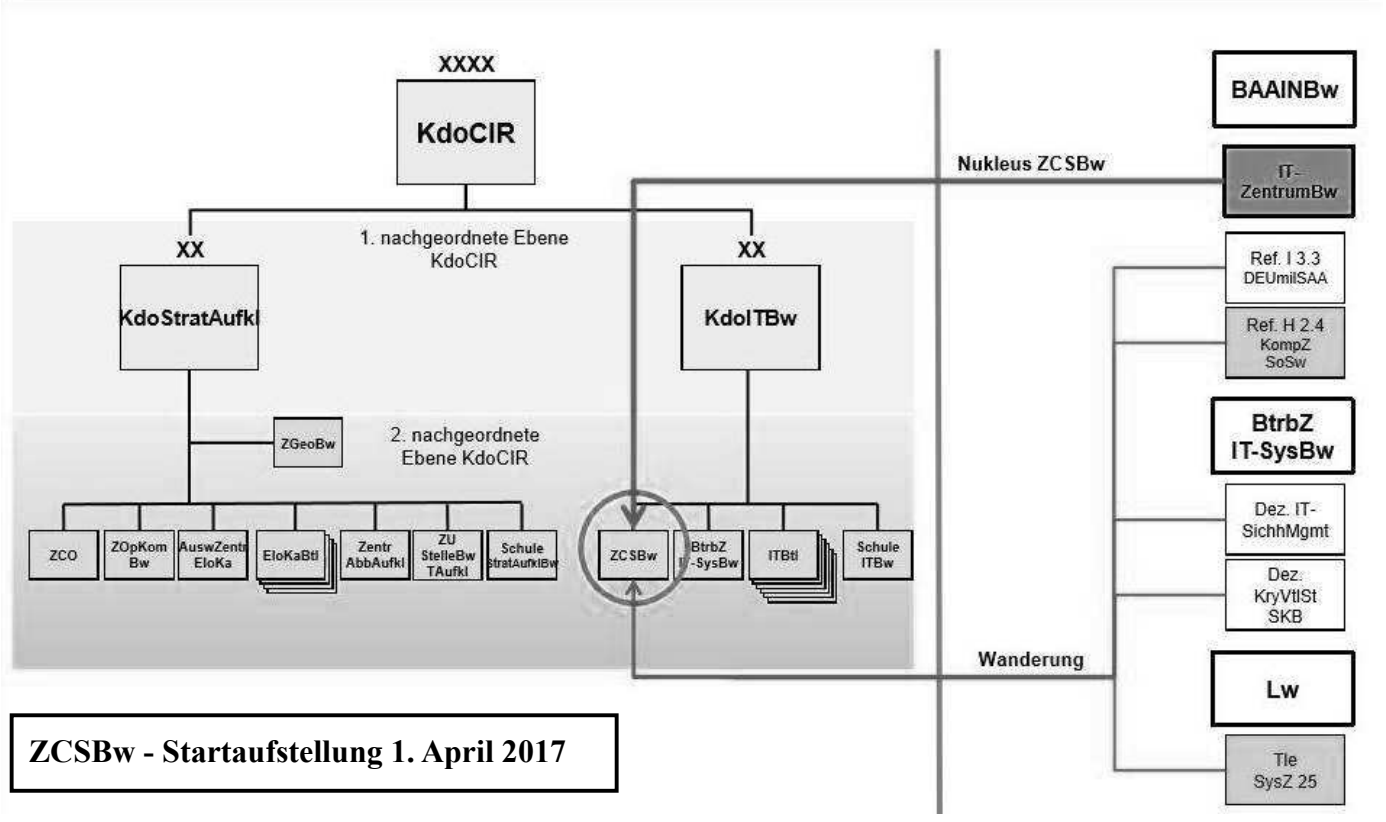
Oberstleutnant Marco Krempel

In den letzten Jahren sind die Bedrohung und die Gefährdungen von Angriffen aus dem Cyber-Raum weltweit und somit auch für die IT-Systeme der Bundeswehr, insbesondere durch die hohe Professionalität der Angreifer aber auch die hochgradige Vernetzung, deutlich gestiegen. Nicht zuletzt aus diesem Grund hat die Bundesministerin der Verteidigung im Herbst 2015 entschieden, dem Bereich Cyber und Informationstechnik in der Bundeswehr einen höheren Stellenwert beizumessen. In der Umsetzung zeigt sich dies u.a. in der Einrichtung der neuen Abteilung Cyber/IT im Bundesministerium der Verteidigung und in der Aufstellung des neuen Organisationsbereichs Cyber- und Informationsraum (OrgBer CIR). Eine wesentliche Aufgabe des OrgBer CIR ist der Schutz der IT-Systeme der Bundeswehr. Zur adäquaten Wahrnehmung dieser Aufgabe hat der Inspekteur der Streitkräftebasis am 6. Juni 2017 mit einem feierlichen Appell das Zentrum für Cyber-Sicherheit (ZCSBw) in Euskirchen neu aufgestellt.

Das ZCSBw ist die zentrale Dienststelle zur Gewährleistung eines umfassenden Schutzes der Interessen, IT-Services und IT-Systeme der Bundeswehr im Cyber- und Informationsraum und ist somit die konsequente Umsetzung der im Tagesbefehl der Bundesministerin der Verteidigung vom 26. April 2016 geforderten Bündelung der Zuständigkeiten und Fähigkeiten. Sehr deutlich wird dies, wenn man betrachtet, aus welchen zahlreichen Einheiten und Dienststellen sich das ZCSBw formiert.

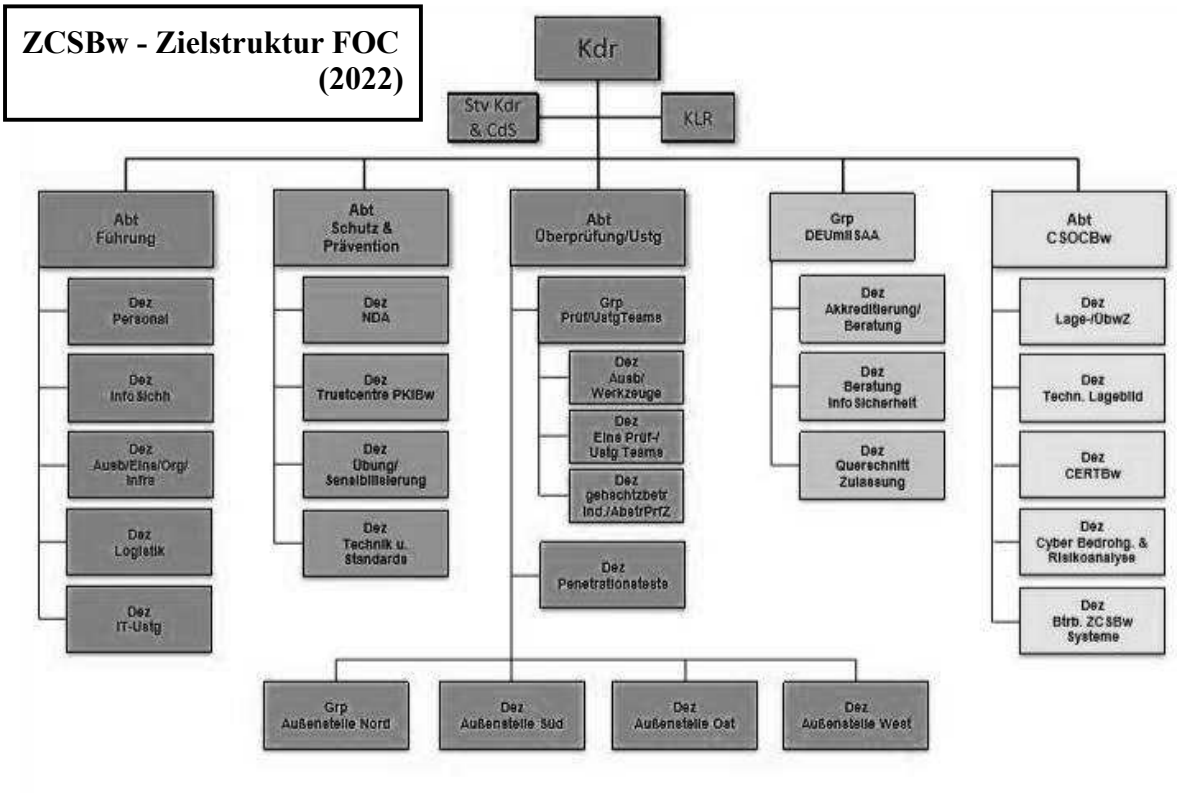
Den Nukleus des neuen ZCSBw bildet das ehemalige Zentrum für Informationstechnik der Bundeswehr (IT-ZentrumBw) in Euskirchen, welches vor seiner Auflösung zum 31. März 2017 dem Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) unterstellt war. Weiterhin wurden zum 1. April 2017 aus dem BAAINBw die Referate I3.3 – Deutsche militärische Security Accreditation Authority – und H2.4 – Kompetenzzentrum Sondersoftware der Bundeswehr – sowie aus dem Betriebszentrum IT-System der Bundeswehr die Dezernate IT-Sicherheitsmanagement und Kryptoverteilerstelle SKB und aus dem Organisationsbereich Luftwaffe Teile des Systemzentrums 25 in das ZCSBw eingegliedert.

Da die Neuaufstellung und die Integration der einzugliedernden Organisationselemente nicht von heute auf morgen zu realisieren sind, verläuft die Aufstellung des ZCSBw in mehreren Phasen. Zur Startaufstellung (Initial Operating Capability - IOC) gliedert sich das ZCSBw in die drei Abteilungen Zentrale Aufgaben, Cyber-Sicherheit und Softwarekompetenz. Die Abteilung Softwarekompetenz wird nach aktuellem Sachstand zum 1.



ZCSBw - Startaufstellung 1. April 2017

ZCSBw - Zielstruktur FOC (2022)



April 2019 aus dem ZCSBw ausgegliedert und als eigene Dienststelle „Zentrum für Softwarekompetenz der Bundeswehr (ZSwKBw)“ aufgestellt. In der Zielstruktur (Full Operating Capability - FOC) gliedert sich das ZCSBw in die vier Abteilungen Führung, Schutz und Prävention, Überprüfung/Unterstützung, Cyber Security Operations Centre Bundeswehr (CSOCBw) sowie in die Gruppe Deutsche militärische Security Accreditation Authority .

Das Computer Emergency Response Team der Bundeswehr (CERTBw), welches für viele bisher der Inbegriff für die Cyber-Sicherheit der Bundeswehr war, findet sich nun als Dezernat in der Abteilung CSOCBw wieder. Das CSOCBw ist im Wesentlichen die fachliche Weiterentwicklung des CERTBw, ergänzt um neue Fähigkeiten und Kapazitäten. Einzelne Elemente wurden zudem aufgrund der fachlichen und personellen Weiterentwicklung anderen Abteilungen des ZCSBw zugeordnet.

Die Aufgaben des neuen CSOCBw werden in der Folge näher vorgestellt.

Die durch den Aufbaustab CIR gewählte Organisation des CSOCBw orientiert sich an den CSOC – Modellen von MITRE[1] mit drei Stufen der Security Incident Response.

Das **Dezernat Lage- und Überwachungszentrum (LÜZ)** des CSOCBw ist die zentrale Ansprechstelle, bei der alle IT-Sicherheitsvorfälle und -verdachtsmomente (Security Incidents) von einem im 24/7 Schichtsystem arbeitenden Team aufgenommen, bewertet und in einem Ticketsystem aufgenommen werden. Die Security Incidents werden in der Regel durch die IT-Sicherheitsbeauftragten der Dienststellen bzw. der Einsätze gemeldet oder durch die eigenen Sensoren erkannt und im LÜZ zur Anzeige gebracht. Gleichzeitig erfolgt im LÜZ auch die Erstbearbeitung – Stufe 1 der Security Incident Response – und bei weniger komplexen Vorfällen sogar deren abschließende Bearbeitung. Zudem ist neu, dass das LÜZ zukünftig mit dem Network Operations Centre Basis Inland des Betriebszentrum IT-System der Bundeswehr kolloziert wird. Damit wird ein enger Schulterschluss zwischen der IT- und Cyber-Sicherheit und dem Verantwortlichen für den Betrieb des IT-Systems der Bundeswehr erreicht. Durch diese enge Zusammenarbeit können Anomalien oder gar Angriffe viel schneller erkannt, gemeinsam wirksame Maßnahmen zur Aufrechterhaltung oder Wiederherstellung der IT- und Cyber-Sicherheit erarbeitet und anschließend umgesetzt werden. Perspektivisch erfolgt an dieser Stelle auch eine engere Verzahnung mit dem CERT der BWI durch das Implementieren eines Verbindungselements.

Des Weiteren stellt das LÜZ die Teillagen „IT/Cyber-Sicherheit IT-SysBw“ und „Info-Sicherheitslage 24/7“ für den Chief Information Security Officer der Bundeswehr (CISOBw) im Kommando Cyber- und Informationsraum (KdoCIR) als Teil der Gesamtlage CIR bereit.

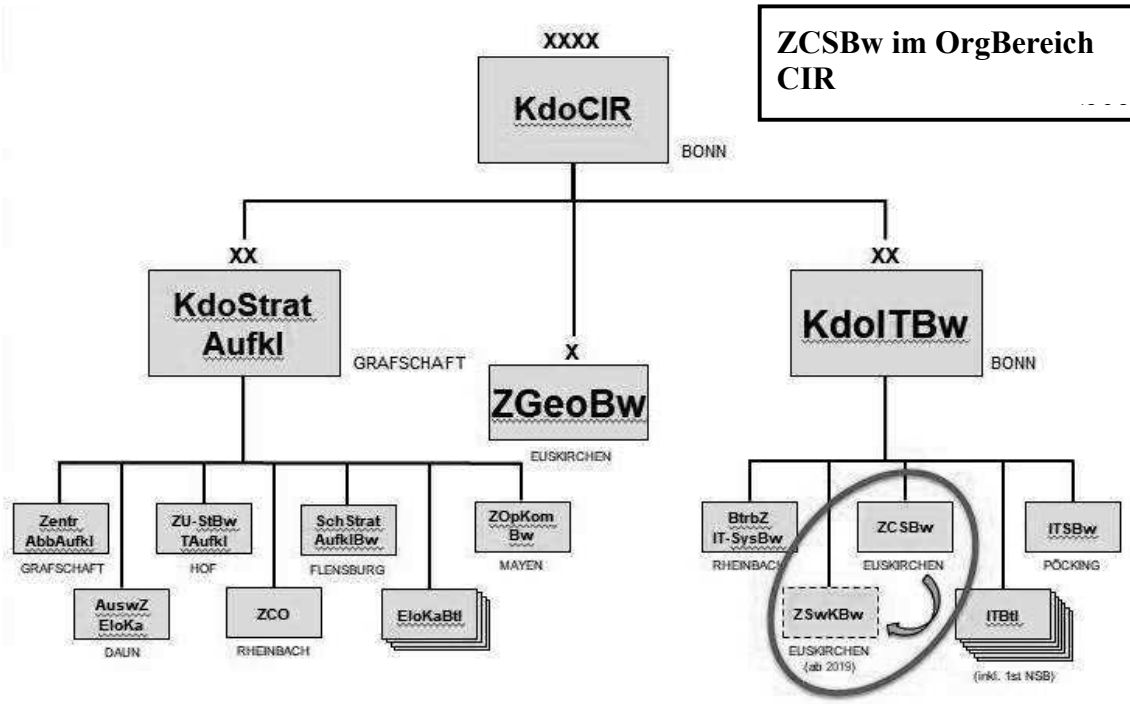
Auch wenn die Bundeswehr sich im Wesentlichen gegen Angriffe von außen schützen muss, so kommt es auch vor, dass die Security Incidents durch Fehlverhalten von Mitarbeitern und Mitarbeiterinnen der Bundeswehr verursacht werden. In solchen oder anderen Fällen, die eine disziplinar- oder strafrechtliche Untersuchung unter Einschluss von Informationstechnik erfordern, berät das LÜZ alle Disziplinarvorgesetzten und Wehrdis-

[1] MITRE is a not-for-profit organization that operates research and development centers sponsored by the federal government. (Quelle: https://www.mitre.org/about/corporate-overview)

ziplinaranwälte der Bundeswehr aber auch Strafverfolgungsbehörden im Rahmen der Amtshilfe.

Zur Erfüllung seiner umfangreichen Aufgaben steht das LÜZ im engen Kontakt zum CERT BWI sowie zu weiteren nationalen und internationalen Partnern, wie z.B. dem Nationalen Cyber-Abwehrzentrum (Cyber-AZ). Im Zuge der Weiterentwicklung des Cyber-AZ auf der Basis der aktuellen Cyber-Sicherheitsstrategie für Deutschland ist geplant, dass das LÜZ des CSOCBw mit einem Dienstposten dauerhaft im Cyber-AZ vertreten ist.

ZCSBw im OrgBereich CIR



Da die IT-Systeme der Bundeswehr immer umfangreicher und komplexer werden, ist der Einsatz von automatisierten Erkennungs- und Verteidigungssystemen unerlässlich. Nur so kann ein flächendeckenden Schutz sowie die Früherkennung von Angriffen gewährleistet werden. Das **Dezernat Technisches Lagebild** betreibt dazu ein zentrales informationssicherheitstechnisches Überwachungs-, Verteidigungs- und Auswertesystem. Durch den Einsatz von Intrusion Detection Systemen (IDS) und Intrusion Prevention Systemen (IPS), welche den Datenverkehr im Netzwerk aktiv überwachen, werden Angriffe automatisch erkannt bzw. abgewehrt. Die Filter der IDS/IPS-Sensoren werden nahezu täglich durch den Hersteller aktualisiert und anschließend, nach eingehender Analyse und Bewertung, auf die Sensoren ausgerollt. In Ergänzung zu den herstellerseitig bereitgestellten Filtern erstellt das Dezernat auch eigene Filterregeln. Die IDS/IPS werden mit weiteren Sensoren und Datenquellen der IT-Systeme der Bundeswehr in einem Security Information und Event Management (SIEM) zusammengeschaltet. Dieses ermöglicht die zentrale Speicherung, Aggregation sowie Korrelation der zielgerichtet gesammelten Daten und erlaubt eine Analyse nahezu in Echtzeit. Alle technischen Überwachungsmöglichkeiten sind dabei nicht nur auf das Bundesgebiet begrenzt, sondern finden sowohl in den Auslandsdienststellen als auch in den Einsatzgebieten der Bundeswehr Anwendung. Mit dem weiteren Rollout der sensorbasierten Überwachungs- und Verteidigungssysteme verfolgt das CSOCBw aber auch das Ziel, für alle Bedarfsträger eine speziell auf die jeweilige Dienststelle bzw. das System und die Bedürfnisse maßgeschneiderte „Sicht“ auf die Informationen des SIEM bereitzustellen, um zukünftig das Informationssicherheitsauditing zu unterstützen. Zusätzlich informiert das Dezernat Technisches Lagebild die Verantwortlichen für den IT-Betrieb und IT-Sicherheitsbeauftragten mit CSOCBw-Blacklists über IP-Adressen und URLs, die im Zusammenhang mit Cyber-Angriffen stehen und an den Übergängen zum Internet blockiert werden sollten.

Tritt ein IT-Sicherheitsvorfall, also ein Ereignis, das die Vertraulichkeit, Verfügbarkeit und Integrität der Informationen, Geschäftsprozesse, IT-Dienste, IT-Systeme oder IT-Anwendungen derart beeinträchtigt, dass ein Schaden für die Bundeswehr entstehen kann, ein und kann dieser nicht mehr durch das LÜZ eigenständig bearbeitet werden, übernimmt das Dezernat CERTBw den Vorfall. Typische Vorfälle sind das Einbringen von Schadsoftware wie Viren, Würmern und Trojanern in ein Netzwerk, unbefugte Veränderung von Software oder Hardware, Identitätsdiebstahl und Denial of Service (DoS) Angriffe.

Im Vergleich zum bisherigen CERTBw ist das neue Dezernat CERTBw des CSOCBw ausschließlich auf die Bereiche Security Incident Response, Computerforensik und Schadsoftwareanalyse fokussiert. Dabei stellt das CERTBw als ständige Eskalationsmöglichkeit für das LÜZ die Incident Response Fähigkeit 24/7 als Rufbereitschaft zur Verfügung. In diesem Zusammenspiel des LÜZ

mit dem CERTBw wird eine ständige Erreichbarkeit, informationssicherheitstechnische Überwachung der IT-Systeme der Bundeswehr und ständige Reaktionsfähigkeit auf IT-Sicherheitsvorfälle und Cyber-Angriffe gewährleistet. Die auch mobil einsetzbaren Incident Response Teams bilden dabei die zweite Stufe der Security Incident Response im CSOCBw ab.

Der primäre Auftrag der Incident Response Teams ist es, die Gefährdung für das IT-System der Bundeswehr einzudämmen, um einen größeren Schaden zu vermeiden. Dazu sind die Teams u.a. befähigt, Angriffswege und ausgenutzte Schwachstellen zu identifizieren, digitale Spuren auf Endgeräten und im Netzwerkverkehr zu erkennen, zu sichern und zu analysieren sowie zielgerichtete Maßnahmen zur Wiederherstellung der Cyber-Sicherheit der betroffenen Systeme zu entwickeln und gemeinsam mit dem Betriebspersonal umzusetzen. Um diesen Auftrag zu erfüllen, steht den Soldaten im mobilen Einsatz ein umfassendes technisches Equipment zur Verfügung. Dies sind u.a. zahlreiche, mit spezieller Software ausgestattete Laptops, Switches, Medienkonverter, Netzwerkkabel und Festplatten.

Neben den typischen Incident Response Aufgaben ist mittelfristig bis langfristig geplant, die Teams zum aktiven Suchen nach Angreifern in den eigenen IT-Systemen, dem sogenannten „Threat Hunting“, und zur Responsive Cyber Defence, also dem Einleiten aktiver Maßnahmen zur Abwehr erkannter Angreifer, zu befähigen. Letzteres bedarf jedoch noch der Klärung umfassender rechtlicher Aspekte.

Zur genauen und tiefergehenden Aufklärung eines Security Incidents, übergeben die Incident Response Teams die gerichtsverwertbar gesicherten Beweismittel an das Sachgebiet Forensik. Hier erfolgt in der dritten Stufe der Security Incident Response auch die technische und zeitlich aufwendige Analyse von Schadsoftware, zum Teil mit Unterstützung von Partnern aus der Industrie.

Die umfassende digitale Spurensuche der Forensikspezialisten beinhaltet sowohl die Analyse, Auswertung und Bewertung von Datenträgern und Speichermedien, wie z.B. Festplatten und Mobiltelefonen, als auch des Kommunikationsverhaltens innerhalb eines Netzwerkes, welches durch sogenannte Netzwerk-Captures erfasst wird. Die Analysen werden ausschließlich auf Kopien der Beweismittel durchgeführt, um eine Veränderung kategorisch auszuschließen. Dazu stehen den IT-Forensikern u.a. spezielle Analysewerkzeuge und –computer sowie zahlreiche Server mit mehreren Terrabyte an Speicherkapazität zur Verfügung.

Neben der computerforensischen Untersuchung im Zusammenhang mit Security Incidents führt das Sachgebiet Forensik des CERTBw auch Untersuchungen zur Unterstützung von Disziplinarvorgesetzten und Strafverfolgungsbehörden im Zuge der Amtshilfe durch. Dabei achten die IT-Forensiker besonders auf die lückenlose und umfassende Dokumentation der Beweismittel, um den strengen Anforderungen von Gerichten zu genügen.

Dass die IT-Forensiker des ZCSBw über eine ausgesprochen hohe fachliche Qualifikation verfügen, haben sie bereits mehrfach im Rahmen der multinationalen Cyber-Abwehr-Übung „Locked Shields“ bewiesen. In dieser Übung des NATO Cooperative Cyber Defence Centres of Excellence (CCDCOE) in Tallinn (EST), an der jedes Jahr ca. 20 Teams in 2017 aus 25 Nationen teilnehmen, konnte das deutsche Forensik-Team unter der Führung des ZCSBw in 2016 in der Kategorie Computer Forensik den 1. Platz erreichen und in diesem Jahr den Titel erfolgreich verteidigen. Damit sind die Forensiker des ZCSBw derzeit die Speerspitze der NATO.

Die Informationen für spezielle Filterregeln der Erkennungs- und Verteidigungssystem des CSOCBw und Blacklists werden im **Dezernat Cyber-Bedrohung und Risikoanalyse** anhand der Auswertung zahlreicher Daten aus überwiegend offenen Quellen recherchiert und durch eine anschließende Gefährdungsanalyse bewertet. Die gesammelten Informationen und spezifische Informationen aus der Bearbeitung von Security Incidents werden über die Fachanwendung Malware Information Sharing Plattform (MISP) mit anderen Organisationen und Nationen geteilt, um der Cyber-Bedrohung global zu begegnen. Darüber hinaus erstellt das Dezernat Advisories, die die IT-Sicherheitsbeauftragten der Dienststellen und im Einsatz sowie die Betriebsverantwortlichen der IT-Systeme der Bundeswehr über die gesammelten Erkenntnisse zu aktuellen Bedrohungen und Schwachstellen informiert. Bei der Informationsgewinnung wirkt sich die sehr starke Vernetzung des CSOCBw im nationalen und internationalen Bereich äußerst positiv aus. Zu den engsten Partnern zählen die Mitglieder des CERT-Verbundes, allen voran das CERT-Bund des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und im internationalen Umfeld die NATO, die USA sowie Österreich und die Schweiz. Der gegenseitige Austausch von Cyber Defence Informationen zwischen der NATO und der Bundesrepublik Deutschland sowie dem amerikanischen Department of Defense und dem Bundesverteidigungsministerium ist jeweils in einem Memorandum of Understanding (MoU) manifestiert und wird durch das CSOCBw aktiv gelebt.

Neben den aufgezeigten Aufgaben und Fähigkeiten des Dezernates werden mittelfristig Fähigkeiten zur ganzheitlichen Risikoanalyse ausgewählter kritischer IT-Serivces, Vorhaben und von IT-Anteilen in Waffensystemen aufgebaut.

Um seine vielfältigen fachlichen Aufgaben erfüllen zu können, benötigt das CSOCBw einen „querschnittlichen Dienstleister“. Dieser Dienstleister ist das **Dezernat Betrieb ZCSBw Systeme**. Zu dessen Aufgaben zählt die technische Realisierung und Bereitstellung von Fachdiensten für Projekt-IT, u.a. Infrastruktur, Plattformen und Anwendungen, sowie das Abstimmen, Bearbeiten und Verwalten von Projektabrufen, wie IT-Ausstattung, Software-Lizenzen, Ausbildung und Dienstleistungen. Dabei arbeitet das Dezernat eng mit dem S4 und S6 des ZCSBw zusammen.

Aufstellungsappel am 6. April 2017: (v.l.) Kdr ZCSBw, Kdr SKB, Kdr ITKdo

Aus den dargestellten Aufgaben und Fähigkeiten leitet sich ein sehr hoher Grad an Spezialisierung jedes einzelnen Mitarbeiters des CSOCBw ab. Um den erforderlichen hohen Ausbildungsstand zu erreichen, durchlaufen alle Angehörigen des CSOCBw eine speziell auf den jeweiligen Dienstposten zugeschnittene Ausbildung. Für die Grundlagenausbildung wird in der Regel auf das umfangreiche Lehrgangsangebot der Kompetenzzentren Informationstechnologie (KIT), also Ausbildungseinrichtungen für die Bundeswehr mit externer Fachexpertise, zurückgegriffen. Das erweitere Fachwissen wird durch eine Qualifizierung an ausgewählten Ausbildungseinrichtungen außerhalb der Bundeswehr erreicht. Für das tiefgehende Spezialwissen werden u.a. auf die Bedürfnisse des CSOCBw zugeschnittene Lehrgänge als In-House-Schulungen durch Hersteller der eingesetzten Produkte (z.B. Prüfwerkzeuge und Software für computerforensische Untersuchungen) oder durch exklusiv akkreditierte Firmen durchgeführt. Weiterhin werden auch die fachspezifischen Ausbildungsangebote des SANS-Institutes und des NATO CCD COE intensiv genutzt. Mit der Einrichtung des neuen Master-Studiengangs „Cyber-Sicherheit“ an der Universität der Bundeswehr in München ab 2018 wird sich zudem das Niveau des fachspezifischen Eingangswissens des zukünftigen Personals im Bereich studierter Offiziere und Beamter weiter deutlich verbessern.

Neben der fachlichen Qualifikation des Personals gilt es auch die Fähigkeiten des CSOCBw weiterzuentwickeln und auf dem aktuellen Stand zu halten. Insbesondere in der Phase der Ausgestaltung des neuen ZCSBw gilt es bewährte aber auch neue Wege der Weiterentwicklung zu gehen. Dazu gehören u.a. das Durchführen technischer, nichttechnischer und rechtlicher Studien, z.B. mit dem Fraunhofer Forschungsinstitut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE), dem NATO CCDCOE aber auch durch Praktikanten-, Studien- sowie Bachelor- oder Masterarbeiten von Studenten der Universitäten der Bundeswehr und des Bildungszentrums der Bundeswehr in Mannheim. Hinzu kommen die vielfältigen neuen Möglichkeiten des gemeinsam mit Unternehmen der Wirtschaft entstehenden „Cyber Cluster“ in Anlehnung an das Forschungszentrum Cyber Defence CODE an der Universität der Bundeswehr München.

Ehemalige Fähigkeiten und Aufgaben des CERTBw in den Bereichen Schwachstellenanalyse und Erstellen von Härtungsmaßnahmen für Produkte, wie z.B. Windows Betriebssysteme, sind nicht im CSOCBw verortet. Beide Bereiche sind in ihren Fähigkeiten und Kapazitäten, u.a. für die Verbesserung der Cyber-Sicherheit von IT in Waffensystemen, aufgewertet und organisatorisch in anderen Abteilungen des ZCSBw verortet worden.

Mit der Einrichtung des ZCSBw mit dem CSOCBw ist es im Rahmen der Aufstellung des neuen OrgBer CIR gelungen, die überfällige Weiterentwicklung der Cyber Defence Fähigkeiten der Bundeswehr voranzubringen. Auch wenn einige Fähigkeiten schrittweise erst bis ins Jahr 2021 oder gar darüber hinaus bereitgestellt werden können, sind die richtigen und erforderlichen Schritte für eine deutliche Verbesserung der Cyber-Sicherheit der IT-Systeme der Bundeswehr eingeleitet worden. Zudem kann die Bundeswehr mit diesen Fähigkeiten zukünftig einen bedeutend besseren Beitrag im Rahmen der gesamtstaatlichen Sicherheitsvorsorge und der Bündnisverteidigung in diesem Bereich leisten.

Der Autor Oberstleutnant Marco Krempel ist Gruppenleiter CSOCBw im Zentrum für Cyber-Sicherheit der Bundeswehr und seit 13,5 Jahren im Bereich der IT-Sicherheit tätig.

AFCEA-Fachveranstaltung am 5.Dezember 2017 bei Fraunhofer FKIE in Wachtberg

Oberst a.D. Peter Warnicke

Bei der Abendveranstaltung der AFCEA Bonn e.V. am Fraunhofer FKIE in Wachtberg wurde zum Thema "Big Data 4.0 - Analyse und Schutz" eine wohl abgerundete Vortragsreihe von 4 gut aufeinander abgestimmten Vorträgen angeboten

Nach der Begrüßung durch den Vorsitzenden der AFCEA, Herrn Generalmajor a.D. Erich Staudacher, übernahm Herr Oberst a.D. Benz die Moderation. Er erläuterte, dass es schwer fiel, sich aus den sehr zahlreichen Vortragsvorschlägen auf die vier für den Abend möglichen Vorträge zu beschränken. Aus meiner Sicht kann ich feststellen - es ist ihm gut gelungen.

Als ersten Vortragenden stellte er mit Herrn Oberst i.G. Michael Hauschild (BMVg RefLtr CIT II 5) einen absoluten Kenner und Insider der SASPF[1] -Welt vor. Der befasste sich in seinem sehr kurzweiligen und lebendig vorgetragenen Einblick mit der Entstehung und Weiterentwicklung der bundeswehrspezifischen Anwendung der SAP-Welt. Dass es sich hier tatsächlich um Big Data - um Massendaten - handelt, belegen die vom Referenten genannten Zahlen eindrucksvoll: 60.000 Nutzer in der Bundeswehr, 1,2 Millionen Versorgungsartikel, 1,5 Millionen Materialbelege monatlich und insgesamt 1,2 Millionen Personendatensätze im System. Zu Beginn der Einführung des SASPF ging es darum, die vielfältigen eigenständigen Programme und Anwendungen der Bundeswehr abzulösen bzw. zu überführen in ein System mit einer konsistenten Datenhaltung, die schnell auswertbar für unterschiedlichste Anwendungen zur Verfügung stehen sollte. Mit seiner wiederholt aufgestellten Frage "Was wollen die eigentlich von mir" gelang es Hauschild, den Zuhörern einen Blick für die herausragenden Möglichkeiten, die im System SASPF verborgen sind, zu verdeutlichen. Sie bieten für die Zukunft noch ungenutzte Möglichkeiten, durch korrelative Auswertungen vieler verschiedenartiger Datenpunkte neue Zusammenhänge und Erkenntnisse zu gewinnen. Mit Hilfe von Data Science-Methoden [2] könnte die Analyse der SASPF-Daten zur Entscheidungsfindung in vielen Bereichen beitragen. Aus den verfügbaren hohen Datenmengen könnten z.B. Aussagen zur Einsatzbereitschaft, über IT-Sicherheitsverstöße oder verschiedensten Personalauswertungen rasch bundeswehrweit verfügbar machen.

Wer oder was ist Fraunhofer FKIE ?

Das Fraunhofer-Institut für Kommunikation, Informationsverarbeitung und Ergonomie (FKIE) entwickelt Technologien und Prozesse mit dem Ziel, existenzbedrohende Risiken frühzeitig zu erkennen, zu minimieren und beherrschbar zu machen. In enger Kooperation mit strategischen Partnern widmet sich das Institut hierbei der gesamten Verarbeitungskette von Daten und Informationen: vom Gewinn, der Übertragung und Verarbeitung bis hin zu ihrem zuverlässigen Schutz. Seinen Auftrag sieht das Fraunhofer FKIE hier sowohl im zivilen Sektor als auch bei Führungs- und Aufklärungsprozessen im wehrtechnischen Bereich

Quelle: Homepage Fraunhofer FKIE.

Auch wenn das System seinen Preis hat - insgesamt 2,12 Mrd. € von der Einführung bis 2016, im Jahr 2017 rund 245 Mio. €, und in den Jahren 2018 und 2019 sind 285 und 310 Mio. € geplant - gute Leistungen haben ihren guten Preis. Insofern sollte man die Fachleute wie den Referenten fragen, was das Anfangs durchaus auch gescholtene Projekt SASPF für die Zukunft noch an Wissen und Prognosen durch intelligente Datenanalysen bringen wird.

Der zweite Vortrag des Abends durch Herrn Frank Irnich (SAP Deutschland, Strategic Business Development Manager) fokussierte stärker auf die Herausforderungen in Sachen Cyber-Sicherheit.

Um die Ziele der IT-Sicherheit, Vertraulichkeit, Integrität und Verfügbarkeit zu erreichen, muss man sich in Zeiten der unaufhaltsam fortschreitenden Digitalisierung, in der sich auch die Angriffsflächen für Cyber-Angriffe vergrößern, stets mit neuen Techniken und Ideen anpassen. Die großen Datenmengen im eigenen System sind ständig in Echtzeit auf Anomalien zu untersuchen und auf Angriffsmuster und Alarme hin auszuwerten. Dabei war der der Aspekt seines Vortrages, zusätzlich proaktive IT-Sicherheit zu betreiben, ausgesprochen interessant. Proaktiv, das heißt heute Cyber Threat Intelligence[3] . Hier geht es darum, möglichst schon einen Angriff zu erken-

[1] SASPF = Standard-Anwendungs-Software-Produkt Familie; betriebswirtschaftliche Standardsoftware auf Basis von SAP-Lösungen

[2] Data Science (von englisch data „Daten“ und science „Wissenschaft“) bezeichnet generell die Extraktion von Wissen aus Daten (Quelle: Wikipedia).

[3] Threat = Bedrohung; Cyber Threat Intelligence (CTI), analysiert und verfeinert Informationen über potenzielle oder aktuelle Angriffe, die eine Organisation bedrohen; CTI bedient sich auch der gezielten Überwachung von bekannten Angreifergruppen.

nen, bevor er das eigene System erreicht. Die Idee besteht darin, konkrete Informationen über mögliche Angreifer sowie deren Methoden und Strategien zu sammeln und so aufzubereiten, dass Organisationen aufgrund dieser Expertise gezielt Härtungsmaßnahmen für ihre Systeme vornehmen können. Als Quellen werden hier das frei auswertbare Internet genutzt, aber auch Quellen aus dem Deep Net[4] und dem Darknet[5]. Weil zunehmend professionellere und zielgerichtete Attacken die Unternehmen Tag für Tag bedrohen, plädiert Irnich dafür, die Bedrohungslage auch durch das Auswerten von Hacker-Foren zu erfassen. Dabei stellt er fest, dass nur ca. 5% des Web-Inhalts von Suchmaschinen wie Google erfasst werden können, 95 % des Web seien so aber nicht erreichbar. Hier müsse man aktiv im Deep Net und im anonymen und verschlüsselten Dark Net "recherchieren", um Informationen über neue Angriffstechniken

Zufriedene Veranstalter: v.l.n.r., GenMaj a.D. Erich Staudacher (Vorsitzender von AFCEA Bonn e.V.) Herr Frank Irnich (SAP Deutschland), Moderator Oberst a.D. F.W. Benz, Oberst i.G. Michael Hausschild (BMVg), Herr Christian Zimmermann (Software AG) und Herr Marian Corbe (KPMG) Foto: AFCEA Bonn

und Malware zu erhalten und auszuwerten. SAP betreibt mit einem Dark Web Crawler (eine Art Suchmaschine) zum Schutz der eigenen Systeme ein Durchsuchen des Dark Net, um Anomalien und neue Angriffstools zu entdecken. Unterstützt wird dies durch einen Open Software Standard STIX (Structured Threat Integration Expression), der für den Informationsaustausch und zur Erfassung und Spezifizierung von Bedrohungen und Sicherheitslücken in IT-Systemen genutzt wird. Das SAP-System bedient sich beim maschinellen Auswerten der enormen Datenmengen eines flüchtigen Arbeitsspeichers von beeindruckenden 48 Terabyte.

Beim dritten Vortrag durch Herrn Christian Zimmermann von der Software AG ging es dann um die Streaming Analytics (Datenanalyse in Echtzeit), nach seiner Meinung die Schlüsseltechnologie auch auf dem digitalen Gefechtsfeld der Zukunft. Die Zahl der Nutzer im World Wide Web steigt Jahr für Jahr, die Zahl der vernetzten Geräte ebenfalls. Damit wird die Herausforderung, immer mehr neue Daten rasch auszuwerten, immer größer. Der langwierige Ansatz, erst Daten erfassen und speichern, dann analysieren, ist insbesondere beim Anfallen von Massendaten nicht mehr zielführend. Die Analyse von Daten aus unterschiedlichen Quellen in unterschiedlichen Formaten (Bild, Sprache, Daten) stellt dabei eine zusätzliche Schwierigkeit und Herausforderung auch für die Streitkräfte dar. Die Fähigkeit zur automatisierten Auswertung in Echtzeit ist unabdingbar geworden. Die Echtzeitanalyse von Daten aus unterschiedlichen Quellen, das Korrelieren dieser Daten und das Erkennen von Mustern und die vorausschauende Bewertung von Szenaren ist das Ziel für die Auswertetools der Streaming Analytics. Die Beispiele für entsprechende Softwaretools stammten allerdings allesamt aus nicht militärischen Anwendungsbereichen, z.B. Testzeitoptimierung durch Echtzeitauswertung in laufenden Produktionsprozessen oder Schiffsbewegungen weltweit zu steuern, um Liegezeiten in Häfen zu optimieren und Engpässe zu vermeiden. Vielleicht

---

4 Deep Web oder Deep Net (auch Hidden Web oder Invisible Web bzw. Verstecktes Web) bezeichnet den Teil des World Wide Webs, der bei einer Recherche über normale Suchmaschinen nicht auffindbar ist (Quelle: Wikipedia). Die Datenmenge des Deep Web soll einige hundertmal größer sein, als die des frei zugänglichen Internet. Andere Quellen sagen, es sei nur einige zehnmal größer.

5 Darknet oder Dark Web = Dunkles Netz; beschreibt in der Informatik ein Peer-to-Peer-Overlay-Netzwerk, dessen Teilnehmer ihre Verbindungen untereinander manuell herstellen (Quelle: Wikipedia). Im Ergebnis bietet das komplett verschlüsselte Darknet ein höheres Maß an Sicherheit. Wer im Darknet surfen möchten, braucht einen Zugang zum Tor-Netzwerk mit einem speziellen Tor-Browser. Das Darknet wird gern genutzt von Whistleblowern, Dissidenten und Tauschbörsen (Filesharer), aber auch von Kriminellen wie Geldwäschedienste, Killerdienste, Waffenhändler, Drogenhandel, Pornografie.

kann man in der Bundeswehr z.B. Fahrzeugleistungen, Erfahrungen aus der Instandsetzung und Lagerhaltungen derart korrelieren, das Ersatzteile zur Kostenminimierung bei kleinstmöglichen Beständen an allen Orten stets verfügbar sind?

Im vierten und letzten Vortrag des Abends rundete Herr Marian Corbe (Assistant Manager, KPMG Cyber Security Consulting) das Big Data-Thema mit einem Blick auf die Meldepflichten bei kritischen Infrastrukturen[6] ab. Bei den ständigen Bedrohungen durch immer professionellere Angriffe müssen die Betreiber von kritischen Infrastrukturen zwei Aufgaben erfüllen. Zum einen müssen sie pflichtgemäß technische und organisatorische Mindestmaßnahmen zum Schutz ihrer Systeme ergreifen, zum anderen müssen sie Cyberangriffe an das BSI (Bundesamt für die Sicherheit in der Informationstechnik) melden. Das Dilemma liegt auf der Hand. Wie unterscheidet man meldepflichtige Angriffe von den vielen kleinen Cyber-Vorfällen und wie erkennt man in der Flut der eigenen Daten die tatsächlich geschäftskritischen Angriffe? Die ersten Verordnungen zum IT-Sicherheitsgesetz in den Bereichen Gesundheit, Finanzen, Transport und Verkehr liegen vor, um die Vorgaben im Gesetzt zu präzisieren. Auch hier sind Big Data-Lösungen unentbehrlich, um aus der Vielzahl an Indikatoren frühzeitig Angriffe zu identifizieren und wirksame Gegenmaßnahmen zu ergreifen. Zum einen empfiehlt Corbe das Umsetzen der branchenspezifischen Vorgaben zum Schutz der IT-Infrastrukturen, die weniger umfangreich und kompliziert sind als die Vorgaben der IT-Grundschutz-Kataloge des BSI. Das betrifft insbesondere kleine und mittlere Betriebe, vor allem wenn sie nicht in der IT-Branche tätig sind, denn sie stehen oft vor großen Hürden wegen des nicht ausreichend ausgebildeten Personals. Zum anderen plädiert er für die Einrichtung eines effizienten Überwachungssystems. Er empfiehlt aber auch, das gemeinsamen Cyber-Lagebildes des BSI zu nutzen und mit eigenen Meldungen zu dessen Erkenntnissen beizutragen. Und schlussendlich ist das Gewinnen und Ausbilden von qualifiziertem Personal ein unverzichtbares Element für den Schutz der eigenen kritischen Infrastrukturen.

Als Fazit des Abends blieb die Erkenntnis, dass die fortschreitende Digitalisierung zwangsläufig zu mehr Daten (Big Data) und damit auch zu mehr Cyber-Attacken führt was wiederum mehr Anstrengungen und neue Ideen in der Cyber-Abwehr erforderlich macht. Ein Kreislauf, der wohl nie enden wird.

[6] Kritische Infrastrukturen = … sind Einrichtungen, Anlagen oder Teile davon, die den Sektoren Energie, Informationstechnik und Telekommunikation, Transport und Verkehr, Gesundheit, Wasser, Ernährung sowie Finanz- und Versicherungswesen angehören und von hoher Bedeutung für das Funktionieren des Gemeinwesens sind … (Quelle: Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme, §2 (10), abgekürzt IT-Sicherheitsgesetz). - Gemäß BMI gehören zwei weitere Sektoren zu den kritischen Infrastrukturen: Staat und Gesellschaft, Medien und Kultur

Wer kann helfen?

Ich suche einen Schaltplan und eine Anleitung für ein

Siemens Brustmikrofon,

zu dem auf dem Lagerkarton folgende Angaben zu finden sind :
5965-12-148-2421
Brustmikrofon
S30362-Z5046-X
1 Stck.
"C" -9/70
Fg l 4 e/01/35136/5654/9
Siemens AG, Betrieb Bocholt

Insbesondere suche ich die Information, was für (DIN) Stecker mit dem Gerät kompatibel sind (zweipolige Anschlußbuchse siehe Bild anbei) und Bezugsquellen, falls möglich.

Das Mikrofon wurde u.a. bei der Bundeswehr als Bestandteil der Sprechausstattung Fähre eingesetzt (Bild anbei), sowie meiner Information nach in Kettenfahrzeugen zur Bordkommunikation und Funk.

Viele freundliche Grüße,
Alexander Schuth
alexander_schuth@gmx.de

Offizierlehrgang 2017 / 2018 - Ein Rückblick

Oberleutnant Krischke

So wie das Jahr 2017 zu Ende ging, strebte auch der OL 3 seinem Abschluss entgegen. Vom sogenannten IT-Dreieck in Nordrhein-Westfalen, über Dresden, als den östlichen Ausläufer Deutschlands, von den Luftlandeeinheiten in Seedorf bis nach Feldafing, haben sich die Kameraden des OL 3 mittlerweile über Deutschland verteilt und ihre neuen Dienstposten angetreten. Es ist daher die Zeit gekommen, einen Rückblick auf die gemeinsam verbrachten 12 Monate zu wagen und ein Resümee zu ziehen.

Nach dem Abschluss des Studiums fanden sich die Teilnehmer des OL 3 für eine Woche am Maxhof zusammen, um sich kennenzulernen und auf die Begebenheiten des bevorstehenden Lehrgangs vorbereitet zu werden. In dieser Woche konnte auch gemeinsam der Gabrielstag, der dem Schutzpatron der Fernmelder gewidmet ist, begangen werden.

Die nächsten drei Monate bis Neujahr fand jedoch zuerst der OL 2 im über 400km entfernten Dresden statt. Dort schlüpften die Kameraden in die Rolle eines Bataillonskommandeurs, um ihre taktischen Kenntnisse und Führungsfertigkeiten, die nach dem langjährigen Studium aus dem OL 1 nur noch zum Teil vorhanden waren, aufzufrischen und zu erweitern.

Das neue Jahr begann in den eisigen Tälern und Höhen Hammelburgs. Dort fand der Lehrgang infanteristische Kompetenzerweiterung (LIKE) statt, bei dem auch Kameraden des alten OL 3 vertreten waren und ein reger Austausch zwischen diesen und den neuen OL 3 Teilnehmern stattfand. Neben Theorieunterricht standen unter anderem Märsche, Verhalten des Einzelschützen, Überwinden von Tiefen inklusive Abseilen und Gefechtsschießen auf dem Dienstplan. Zur Freude der meisten fiel die Gewässerüberquerung ins Wasser.

Nach einem Monat war der Lehrgang schließlich vorüber und die Lehrgangsteilnehmer packten ihre Sachen, um nach zwei Wochen Dienstzeitausgleich endlich in Feldafing zu beginnen. Doch hier erwartete diese kein warmer Hörsaal, sondern die Schießbahn, auf der sie zum Schießausbilder befähigt werden sollten. Mit P8 und G36 konnten die Kameraden nach dem neuen Schießausbildungskonzept im Nahbereich ihre Fertigkeiten in Schnelligkeit, Präzision und Technik nach und nach deutlich verbessern. Während das Wetter vom dichten Schneefall zu strahlender Sonne alle Variationen präsentierte, schossen die Soldaten was das Zeug hielt

und so einige mögen abends mit vom vielen Aufmunitionieren schmerzenden Fingern ins Bett gefallen sein. Zum Abschluss stand eine Lehrprobe an, bei dem jeder Teilnehmer die Ausbildung einer Schießübung übernehmen musste.

Nach dem physikalisch fordernden einmonatigen Schießen, widmete sich der IT-Manager den kognitiven Fähigkeiten. Schon zu Beginn wurden die Teilnehmer in die Prozesse der sowohl industriell als auch militärisch wichtigen ITIL eingeführt. Danach wurden die einzelnen Systeme und Komponenten der Bundeswehr zur Informationsübertragung und -verarbeitung vorgestellt. Während manch ein Elektrotechniker hier tiefere Einblicke in die IT gewann, konnten Informatiker umgekehrt mehr Verständnis über die Physik der Wellenausbreitung erlangen. Nicht zuletzt lernten die Lehrgangsteilnehmer realitätsnah die Rollen, Dokumente und Prozesse kennen, die von den Anforderungen eines Einsatzes über Fähigkeiten bis zu einem vollständigen Plan der einzusetzenden Systeme und deren Vernetzungen führen. Den Höhepunkt erreichte dies in einem über mehrere Tage stattfindenden Planspiels.

Anschließend fand der einwöchige Führerscheinlehrgang statt. Endlich konnte die Erlaubnis erlangt werden, auch Bundeswehrfahrzeuge der Klasse B zu fahren.

Es folgte der sehr praxisnahe BEFL. Hier wurde Wissen über die einzelnen Fernmeldesysteme der Bundeswehr vermittelt. In Theorie und Praxis lernten die Lehrgangsteilnehmer deren Grundlagen, den effektiven und effizienten Einsatz, sowie deren Zusammenspiel und Integration kennen. Ein Highlight der Ausbildung bildete der praktische Einsatz einer Fernmeldestaffel mit VHF-Trupps, bei denen die OL 3 Teilnehmer die Rolle der Truppbesatzungen, sowie des Marsch- und Staffelführers übernahmen. Auf der anderen Seite wurde auch nützliches Wissen und Erfahrungen über die Aufgaben in möglichen Folgeverwendungen mitgeteilt: Von den Aufgaben des Zugführers und Kompaniechefs bis zum Auslandseinsatz konnten die Themen von zum Teil externen Referenten lebhaft beschrieben werden.

Bevor in der großen dreiwöchigen Sommerpause Urlaubstage gegen Reisen eingelöst werden durften, erfuhren die OL 3 Teilnehmer welche Verwendung sie nach dem Lehrgang ereilen würde. Glücklicherweise konnten die meisten Wünsche der Kameraden erfüllt werden und niemand verließ die Personalgespräche vollends unglücklich.

Im anschließenden Gefechtsmodul wurden durch die einzelnen Lehrgangsteilnehmer ‚grüne' Ausbildungen gehalten, wobei diese ihre Organisations- und Ausbilderfähigkeiten unter Beweis stellten, während die Auszubildenden ihr Wissen erneuern und ergänzen konnten.

Während die OL 3 Teilnehmer mit ihren künftigen Einheiten Kontakt aufnahmen und ihren Brief an deren Kommandeur verfassten, begann an der Sportschule der Bundeswehr in Warendorf südlich an Niedersachsen grenzend der Lehrgang Übleiter Bw. Hier standen vier Wochen Sport in Theorie und Praxis auf dem Programm. Die Soldaten lernten wie eine Sportstunde aufzubauen und durchzuführen ist, wie Trainingspläne erstellt, Sportfeste organisiert werden und wie sich der menschliche Körper während des Sportes verhält. Gleichzeitig konnte die körperliche Leistungsfähigkeit verbessert werden,

was auch ein nahe gelegenes All-you-can-eat-Flammkuchen Restaurant nicht zu verhindern wusste. Den Abschluss bildete eine selbst organisiertes Sportfest mit Volley- und Völkerball, bei dem sich die Teilnehmer freudig beteiligten.

Den Abschluss des OL 3 bildete ein einwöchiger Übungsplatzaufenthalt in Heuberg. Hier mussten die Lehrgangsteilnehmer in Gruppen von halber Hörsaalstärke an einem Tag ein Gruppengefechtsschießen leiten und durchführen. Die Vorbereitungen dazu waren bereits im Gefechtsmodul weitgehend abgeschlossen worden und so konnte montags in aller früh mit dem Bus auf den nahe Stetten a.k.M. gelegenen Truppenübungsplatz Heuberg verlegt werden. Nach letzten Vorbereitungen begannen am Dienstag die Schießen. Die schießende Abteilung wurde einerseits durch die Hörsäle des OL 3 gestellt, andererseits auch durch Kameraden aus Murnau, die hierbei sehr gute Leistungen zeigten. Neben der Verwendung von Panzerfaust, MG und Granatpistole wurden auch Stellungswechsel und Munitionsnachführung durchgeführt, sowie Verwundetenlagen eingespielt. Der in Stetten nicht selten fallende Schnee blieb glücklicherweise aus, dafür regnete es zum Teil ununterbrochen, weswegen die vormals in Tarndruck angetretenen Soldaten mit einer Schlammschicht überzogen zurückkehrten. Auch der natürliche Nebel, der ein Schießen verhindert hätte, hielt sich zurück, dafür wurde mit dem künstlichen nicht gegeizt. Bis Donnerstag dauerten die Schießen an, während am Mittwochabend ein gemütliches Zusammensein in der UHG stattfand. Nach einem Freitagsputz konnte die Rückreise angetreten werden und alle in das verdiente Wochenende wegtreten.

Mit einem aufregenden Jahr mit Höhen und Tiefen, in dem die Bundeswehr durch das Aufstellen des Kommando CIR und der damit einhergehenden Umbenennungen der Führungsunterstützungsschule in IT-Schule ein neues Kapitel aufgeschlagen hat, endet der OL 3. Auch für dessen Teilnehmer beginnt ein neuer Abschnitt, denn mit dem Lehrgang endet auch die langjährige Offiziersausbildung und es erfolgt der Übertritt zur ‚richtigen' Arbeit in der Bundeswehr. Nicht alles Erlernte wird in Erinnerung bleiben, doch genauso wird jeder in seiner neuen Verwendung auf das für ihn relevante Wissen zurückgreifen können, um seine Aufgaben erfolgreich zu bewältigen.

So bleibt allen in ihrer Folgetätigkeit viel Glück zu wünschen, allen Beteiligten des OL 3 Dank auszusprechen und diesen Beitrag mit einem Hinweis von Goethe zu schließen: "Es ist nicht genug zu wissen – man muss es auch anwenden. Es ist nicht genug zu wollen – man muss es auch tun."

Der Fernmeldering hat den Offizierlehrgang Teil III (OL III) 2016-2017 über die gesamte Lehrgangsdauer hinweg begleitet. Wir wünschen allen Teilnehmern nun viel Soldatenglück in ihrer Erstverwendung in der Truppe und hoffen auf ein Wiedersehen im Rahmen einer FmR-Veranstaltung.

Der OL III 2016-2017 ist vorüber, der OL III 2017-2018 lebt... Gerne wird der Fernmeldering auch diese Kameradinnen und Kameraden wiederum bei ihrer Ausbildung zum IT-Offizier begleiten.

Ideen und Planungen für eine militärische Funkaufklärung in Westdeutschland nach Ende des 2. Weltkrieges - Teil 1

Oberst a.D. Rudolf Grabau

Einleitung des Autors

In den Jahren 1992 bis 1998 habe ich die Entwicklung der Fernmeldetruppe EloKa des Heeres in den Jahren 1956 bis 1990 in einer Dokumentation festgehalten. Wesentliche Teile der Ergebnisse dieser Arbeit wurden in vier Bänden vom Fernmeldering e.V., herausgegeben. Hierin sind allerdings die konzeptionellen Ideen und Planungen vor und während der Aufbauphase nur sehr lückenhaft und knapp dargestellt worden, weil mir kaum Quellenmaterial dafür zur Verfügung stand. Dann habe ich doch noch Zugang zu wenigen zusätzlichen Quellen gefunden und einige seinerzeit noch lebende Zeitzeugen befragt. Hierdurch konnten einige weiterführende Erkenntnisse zum Aufbau einer westdeutschen Funkaufklärung gewonnen werden, die das Gesamtbild für die Jahre 1948 bis 1957 vervollständigen.

Für diese Ergänzung meiner historischen Dokumentation hatte ich die Form einer wissenschaftlichen Arbeit gewählt. In dieser habe ich versucht, alle mir derzeit zu diesem Thema vorliegenden Informationen mit exakter Angabe ihrer Herkunft zu verarbeiten sowie einige Erläuterungen beizufügen. Insbesondere kam es mir natürlich darauf an, den auf diesem Thema lastenden Schleier des Geheimnisvollen noch ein wenig weiter zu lüften und bereits existente Legenden durch eine Darstellung von Fakten zu ersetzen.

Ursprünglich war nicht vorgesehen, die dabei entstandene Arbeit zu publizieren. Ich hatte mich statt dessen zunächst dazu entschieden, sie nach Fertigstellung (1999) an einen eng begrenzten Kreis mir bekannter Institutionen und Personen zu verteilen, von denen ich annahm, daß sie an historischer Erschließung dieser Thematik interessiert waren. Kürzlich habe ich dann doch noch den Originaltext unter weitgehendem Verzicht auf Quellenangaben und ergänzenden Erläuterungen für eine Veröffentlichung überarbeitet.

Der Anstoß, sich mit diesem Thema zu beschäftigen, ging aus vom Entwurf der Diplomarbeit von Dr. Bodo Wegmann, Berlin, in welcher auf zwei im Bundesarchiv verfügbare konzeptionelle Dokumente hingewiesen wurde, die in der "Handakte Heusinger" aus dem "Amt Blank" enthalten sind. Es handelt sich um zwei Studien aus dem Jahr 1950, die sich mit dem Neuaufbau einer militärischen Funkaufklärung in Westdeutschland befassen. Diese Studien gedachte der Verfasser der Diplomarbeit dem General Heusinger persönlich zuzuordnen. Seinerzeit konnte ich zwar auf meine Zweifel an dieser Annahme hinweisen, jedoch über die Herkunft der Dokumente und die weitere Entwicklung bis zur Aufstellung erster Fernmeldeaufklärungsverbände in der Bundeswehr keine verbindlichen Aussagen machen.

Ich nahm mir daraufhin vor, die Dokumente inhaltlich näher zu untersuchen, Veröffentlichungen jener Zeit daraufhin durchzusehen und die wenigen noch lebenden Zeitzeugen zu dieser Thematik zu befragen. Dabei wurde auch angestrebt, die bestehenden Lücken in der von mir zuvor erarbeiteten Dokumentation der Geschichte der Fernmeldetruppe EloKa der Bundeswehr zu schließen. Soweit möglich sind zur Darstellung des Themas Originalzitate verwendet worden; ich habe diese aus umfangreicheren Dokumenten danach ausgewählt, ob sie ihrem Inhalt nach bei weiterer Planung und beim Aufbau der Fernmeldetruppe EloKa verwertet oder wenigstens beachtet wurden. Die weitere konzeptionelle Entwicklung der FmTr EloKa (nach etwa 1960) wurde hier nicht noch einmal dargestellt, da sie mir bereits ausreichend dokumentiert erschien. Allerdings wurden an verschiedenen Stellen einzelne Perspektiven aufgezeigt, an denen sich das weitere Wachstum später ausgerichtet hat.

Ursprünglich hatte ich dem Text vielfältig Fußnoten mit Quellenangaben und Erläuterungen beigefügt; 130 davon wurden hier entfernt, um die Lesbarkeit nicht zu beeinträchtigen. Bei begründetem Interesse stelle ich gern den gesamten Text zur Verfügung.

Rudolf Grabau, Sommer 2017

Aufbau der Funkaufklärung der Organisation Gehlen

1946/47 baute der ehemalige Chef der Abteilung Fremde Heere Ost (FHO) des Oberkommandos des Heeres (OKH), Generalmajor Reinhard Gehlen, im Auftrag der US-Geheimdienste mit ehemaligen Mitarbeitern der verschiedenen Aufklärungs- und Abwehrdienste des 3.Reiches eine deutsche nachrichtendienstliche Organisation auf. Im Rahmen dieser "Organisation Gehlen" (OG) wurden auch Kapazitäten zur Funkaufklärung wieder aktiviert, und zwar durch Anwerbung ehemaliger Nachrichtenaufklärer, vorwiegend aus dem Heer der früheren Wehrmacht. Die erste Horchstelle ist ab 1948 von dem ehemaligen Major Bödigheimer (unter Mitarbeit von Hauptmann Alf Rump als Leiter der Telegraphie-Erfassung) auf Schloß Kransberg bei Usingen im Taunus eingerichtet worden. Erster Dienststellenleiter ab etwa 1949 war der ehemalige General der Nachrichtenaufklärung, Oberst a.D. Boetzel, dessen Auswerteleiter und Stellvertreter wurde der 1950 neu eingestellte ehemalige Hauptmann Ernst Bode.

Diese erste Kapazität der OG zur Funkaufklärung wurde von Pullach aus geführt, erster Leiter dort war der ehemalige Oberst i.G. Leo Hepp, in der Wehrmacht zuletzt Chef des Stabes beim General der Nachrichtentruppe (Chef HNW/WNV). 1952 wechselte die "Nachrichtenbearbeitung" von Kransberg nach Pullach in die "Zentrale".

Konzeptionelle Planungen für den Aufbau einer Funkaufklärung der Bundeswehr durch die Organisation Gehlen

Aus zwei in der Handakte Heusinger aus dem "Amt Blank" enthaltenen Dokumenten ergibt sich, daß bereits 1950 über den Aufbau einer militärischen Funkaufklärungskapazität für Westdeutschland nachgedacht wurde. Die umfangreichere Studie "Gedanken über die Einrichtung eines atlantischen Horchdienstes" ist von Wilhelm Flicke verfaßt. Das weniger umfangreiche Dokument "Gedanken über eine zukünftige deutsche Funkaufklärung" geht mit an Sicherheit grenzender Wahrscheinlichkeit auf Hepp zurück.

Vor Beginn des 2.Weltkrieges war bei OKW/Chi ein Regierungsrat Wilhelm Flicke tätig. Flicke war nach Schilderungen ein etwas seltsamer Kauz, ein sich selbst überschätzender Querulant, mit dem niemand in seiner Umgebung etwas zu tun haben wollte. Später wurde Flicke nach Lauf/Pegnitz versetzt. Nach dem Kriege wurde er vorübergehend stellvertretender Landrat im Landkreis Lauf. Während dieser Zeit schrieb er den Roman "Die Rote Kapelle".

Flicke nahm Kontakt zu der amerikanischen Besatzungsmacht auf und bot dieser seine Unterstützung beim Aufbau einer Funkaufklärung gegen die sowjetischen und osteuropäischen Funkdienste an. Die DIA (Defense Intelligence Agency) erklärte sich bereit, das Vorhaben zu sponsorn. Daraufhin begann Flicke, ehemalige Nachrichtenaufklärer anzuwerben und in Lauf Horchdienst zu betreiben. Gehlen, der inzwischen in Zusammenarbeit mit der CIA (Central Intelligence Agency) eine Funkaufklärungsorganisation aufgebaut hatte (s.o.), protestierte gegen die Aktivitäten von Flicke bei seinem Auftraggeber. Er erreichte, daß die Horchstelle Lauf (unter Leitung von Flicke) fachlich der Organisation Gehlen unterstellt und bis zur Gründung eines eigenen deutschen Nachrichtendienstes weiterhin von den USA finanziert wurde.

Flicke stellte zur Wahrnehmung seiner Außenbeziehungen, insbesondere für Kontakte zur Organisation Gehlen, den ehemaligen Nachrichtenaufklärungs-Oberst Kettler ein; dieser führte nun in Flickes Auftrag die notwendigen Gespräche zur Fortsetzung der Arbeit der Horchstelle und zur Überführung in die OG (z.B. mit den ehemaligen Obristen Hepp und Boetzel). Arbeitsmäßig übernommen von der OG wurde die Horchstelle Lauf im Herbst 1952, endgültig 1956. Flicke und Kettler sind nicht von der OG übernommen worden und beendeten daher 1956 ihre Tätigkeit in der Funkaufklärung.

Die Studienarbeiten von Wilhelm Flicke im Zeitraum 1945 bis 1952

Von Flicke stammt die wohl ausführlichste schriftliche Auseinandersetzung mit der Nachrichtenaufklärung der Wehrmacht. Er hatte 1945 eine (noch umfangreichere) historische Darstellung der Entwicklung der Funkaufklärung und Funkabwehr, vorzugsweise in Deutschland, fertiggestellt, die in die Hände von USA-Dienststellen kam. Diese wurde in wesentlich erscheinenden Teilen ins Englische übersetzt und später ins Deutsche rückübersetzt. Flicke beschrieb darin auf Grundlage einer 29jährigen Tätigkeit (vorwiegend als Auswerter) u.a. auch die Betriebsverfahren und setzte sich sehr kritisch mit bestimmten Erscheinungsformen der militärischen Funkaufklärung auseinander. Aber dieses Dokument enthält auch viele Hinweise auf Einsatzerfahrungen sowie Empfehlungen konzeptioneller Art, insbesondere:

- Zusammenwirken aller Auswertezweige.
- Wichtigkeit der Funkpeilung.
- Manöverbeobachtung des Gegners als wichtigste Ausbildung für das Fachpersonal und zur Grundlagengewinnung.
- Aufklärungseinsätze gegen eigene Truppe hingegen bringen wenig Ausbildungseffekt.
- Entscheidend ist die Qualität des Fachpersonals.
- Erfasser und Auswerter lassen sich nicht auf dem Kasernenhof ausbilden. Die äußere Form darf nicht - wie oft in der Wehrmacht - Vorrang haben.
- Geheimhaltung ist notwendig, sie darf aber innerhalb der eigenen Organisationen nicht übertrieben werden.
- Eine Aufsplitterung der Aufklärungsdienste ist schädlich; Konkurrenz ist unnötig, Zusammenarbeit unverzichtbar.

Ob diese Arbeit Flickes die konzeptionellen Planungen der Funkaufklärung der Bundeswehr und vor allem deren Realisierung mitbestimmt hat, konnte der Verfasser nicht eindeutig klären, weil nicht zu ermitteln war, wann deren Rückübersetzung angefertigt wurde bzw. verfügbar war. Jahre später jedenfalls war ihr Inhalt vielen "EloKa-Offizieren" der Anfangsjahre bekannt. Auch wurde daraus bisweilen bei der Ausbildung und bei Informationsveranstaltungen über die Elektronische Kampfführung zitiert.

Weitgehend unbekannt blieb auf jeden Fall diejenige Denkschrift von Flicke, die in der "Handakte Heusinger" aufgefunden wurde, nämlich die über einen "atlantischen Horchdienst". Deren Grundgedanken waren:

- Bruch mit der Tradition der nationalen Funkaufklärung.
- Horchdienst der "Westblockstaaten" auf überstaatlicher Basis.

Dabei unterstellte er, daß die Arbeit der "5. Kolonnen" der Sowjetunion in Zukunft "gigantische Formen" annehmen würde. Flicke unterschied zwischen strategischem, operativem und taktischem Horchdienst, wobei er feststellte, daß "die Hauptrichtung der Beobachtungsarbeit des Horchdienstes sich gegen alle strategisch wichtigen Funkverkehre des Gegners orientieren sollte." Aber auch in einem "Funk-Krieg" ("als Gesamtheit aller erzielbaren störenden Einflußmöglichkeiten auf Maßnahmen des Gegners, die entweder ganz oder teilweise durch Funkausstrahlungen betätigt, gesteuert oder verbreitet werden") sah er "in einem kommenden Kriege ein wichtiges militärisches Aufgabengebiet", das nach seiner Auffassung allerdings "in keiner direkten Beziehung zum Horchdienst steht." Ein "diplomatischer Horchdienst" war für ihn das "Kernstück des strategischen Horchdienstes, daneben sah er eine "Funkabwehr", die militärisch orientierten Horchdienste "der strategischen Luftwaffe", des Heeres und der Marine sowie einen "Rundfunk-Horchdienst". Dabei hielt er es für sinnvoll, die Beobachtung "der Bodenfunkstellen der fremden Luftwaffe" dem strategischen oder Heeres-Horchdienst zuzuordnen, den Funkverkehr fliegender Verbände der "Arbeitsgruppe 'Funk-Krieg'". Zum Aufbau eines Heeresanteils im Rahmen des atlantischen Horchdienstes entwickelte er u.a. folgende Gedanken:

Der Heeresfunk der Sowjetunion ist gegen die Beobachtung seitens eines fremden Horchdienstes durch eine ununterbrochene Kette isolierender Faktoren abgeschirmt. Entweder handelt es sich um Seengebiete oder um Satellitenstaaten, verbündete oder streng neutrale Staaten.(...) Bei der Tiefe des russischen Raumes ergeben sich Entfernungen, die sich auf Tausende von Kilometern belaufen. Man könnte daraus den Schluß ziehen, daß die Situation hoffnungslos erscheint, es also keinen Sinn hat, Kräfte für die Beobachtung russischer Heeresfunkstellen zu verschwenden. Eine solche Schlußfolgerung wäre falsch und würde viele Chancen ungenutzt lassen.

Die vollständige Beobachtung ist auch jetzt und in Zukunft nicht möglich. Man wird sich daher mit Teilergebnissen begnügen müssen. Dabei erhebt sich die Frage, welches Ziel einem atlantischen Horchdienst gegenüber der Sowjetunion gesetzt werden kann. Die Absicht, einen klaren Einblick in den Gesamtaufbau des sowjetischen Heeres durch Horchbeobachtung zu gewinnen, muß von vornherein aufgegeben werden. Man wird sich darauf beschränken müssen, durch planmäßiges Absuchen des Äthers diejenigen Garnisonfunkstellen zu beobachten, die nach Lage der Dinge beobachtet werden können.

Das eigentliche Ziel der Beobachtung des russischen Heeresfunks scheint mir aber in anderer Richtung zu liegen. Es gilt, genauen Einblick in die Betriebs- und Verkehrssysteme des feldmäßigen russischen Heeresfunks zu gewinnen, d.h. des Manöver- und Übungsfunks, der ja dem Funksystem im Kriegsfall gleichkommt. Hierfür ergeben sich Möglichkeiten: Zunächst einmal besteht die Möglichkeit, den gesamten Funkverkehr der in Ostdeutschland stationierten russischen Heeresverbänden zu beobachten.(...) Dies kann von Westdeutschland, West-Österreich, Italien und Griechenland aus geschehen.(...) Gegenüber der Sowjetunion ergeben sich - horch-technisch gesehen - zwei weitere Ansatzmöglichkeiten: von der nördlichen Türkei und von Schweden aus. Es müßte daher mit allen Mitteln angestrebt werden, sobald wie möglich in diesen beiden Ländern eine Anzahl Horchstellen zu etablieren, bzw. die dort schon vorhandenen in den Gesamtkomplex des atlantischen Horchdienstes einzube-

ziehen. Die Gesamtheit der auf diesem Wege zu erzielenden Horchergebnisse würde ausreichen, sich einen genügend guten Einblick in die Heeresfunksysteme der Sowjetunion zu verschaffen. Der westeuropäische Horchdienst muß in die Lage versetzt werden, bei Ausbruch der Feindseligkeiten den "Kontakt im Äther" mit dem Gegner zu haben. Er muß so gestaltet werden, daß er vom ersten Kriegstage an die eigene Führung mit Informationen versorgen kann. Diese Aufgabe wäre auf folgende Weise zu lösen:

- *Eine Kette von Horchstellen, die sich von Nordschweden und Nordnorwegen über Dänemark, Westdeutschland, Italien, Griechenland, Türkei bis zur Persischen Grenze erstreckt, sorgt durch laufende Beobachtung für die Erstellung der Arbeitsgrundlagen, die der operative Horchdienst benötigt.*
- *Eine Anzahl motorisierter Horchkompanien bekommt ständig diese gewonnenen Unterlagen und bildet das eigene Personal damit aus.*

Es muß damit gerechnet werden, daß die russischen Armeen Westdeutschland überrennen. Um den eingearbeiteten Horchdienst zu sichern, müßten deswegen auch die festen Horchstellen motorisiert werden, um schnell hinter die 2. Verteidigungslinie zurückgenommen zu werden. Sollte die Gefahr drohen, daß ganz Westeuropa von den russischen Armeen besetzt wird, so müßte die obenerwähnte Kette der Horchstellen sozusagen "auseinanderklappen": die nördliche Hälfte der Stationen wäre dann auf der Linie Süd-England-Norwegen-Süd-Schweden neu zu errichten, während die südliche Hälfte entlang der nordafrikanischen Küste Stellung zu beziehen hätte. Auch mit den Horchkompanien wäre in gleicher Weise zu verfahren. Der Aufbau eines Horchdienstes im Nahen Osten erscheint mir als besonders wichtig.(...) Das rechtzeitige Erkennen von militärischen Vorbereitungen der Russen im Raume zwischen dem Schwarzen und Kaspischen Meer und ostwärts des Kaspischen Meeres könnte durch einen gutausgebauten Horchdienst ermöglicht werden.

Die Errichtung eines taktischen Nah-Horchdienstes halte ich gegenwärtig für überflüssig; ob sich im Kriegsfalle eine solche Einrichtung als notwendig erweisen würde, hängt ganz von der sich ergebenden Situation ab.

In jedem Falle ist eine zentrale Lenkung des gesamten Heeres-Horchdienstes unerläßlich. Die zentrale Auswertung des Materials.(...) ist von größter Wichtigkeit. Andererseits muß sichergestellt sein, daß auch die nächstgelegenen militärischen Befehlsstellen auf dem schnellsten Wege die anfallenden Informationen bekommen. Die russischen (und andere) Heeresgeheimschriften müßten bei der Entschlüsselungsstelle der Zentralen Horchleitstelle bearbeitet werden; schwierige Verfahren wären vorher in Washington zu lösen, einfachere könnten hier bearbeitet werden. Den Horchstellen und Horchkompanien müßten je nach Bedarf Entschlüssler beigegeben werde, die mit den gelösten Geheimschriften das Spruchmaterial zu entschlüsseln hätten.

Während des 2. Weltkrieges sind auf deutscher Seite die Horchkompanien des Heeres zu Abteilungen und Regimentern zusammengefaßt worden. Dies war nach meiner Überzeugung ein Fehler; der gesamte Apparat des Heeres-Horchdienstes muß beweglich sein; je einfacher die Organisation, desto schneller ihre Arbeit. Es darf auf der Basis der Horchkompanien keine hohe Pyramide von vorgesetzten Stellen sich aufbauen; sonst wird das praktische Ergebnis der Arbeit erdrückt.

Wenn der Aufbau eines atlantischen Horchdienstes erörtert wird, entsteht unvermeidlich die Frage nach der benötigten Personalmenge, der Zahl der Horchstellen und dem Zeitraum, innerhalb dessen die Errichtung dieses Dienstes möglich wäre. Es würde kein Zeichen großer Intelligenz sein, wollte man diese Fragen sofort mit präzisen Angaben beantworten. Nichts wäre falscher, als eine fixierte Zahl von Leuten und Horchstellen bereitzustellen, deren Einsatz sich vielleicht sehr bald als falsch erweisen würde. Dieser Dienst muß organisch wachsen. Man muß schon jetzt die Wahrscheinlichkeit als gegeben hinnehmen, daß der Anfang enttäuschend sein wird und man nur durch viele Versuche, Rückschläge und Umwege an das Ziel herankommen kann. Gewisse Erfahrungen der vorhandenen Stellen wird man als Grundlage der weiteren Arbeit nehmen müssen.

Es wäre auch falsch, wollte man heute schon bestimmte Punkte auswählen und Horchstellen nach der Art der früheren deutschen als feste Bauten errichten. Man wird sich zweckmäßigerweise auf das System der amerikanischen zerlegbaren Bauten stützen, die innerhalb einer Woche montiert werden können. Erweist sich der Platz als nicht ganz geeignet, so ist eine Verlegung leicht durchführbar. Also: Beweglichkeit auch der festen Horchstellen!

Das erfahrenste Personal wird in Deutschland zu finden sein. Aber gerade hier darf man nicht ohne weiteres jeden Mann, der früher im Horchdienst tätig war, nehmen.(...) Die bisherige militärische Entwicklung im Westen hat seinen Glauben an dessen Widerstandskraft und Widerstandsbereitschaft untergraben. Erst wenn er den Ernst des westlichen Verteidigungswillens erkennt, wird sich seine Einstellung wieder ändern.(...) Warnen möchte ich ferner vor der Aufstellung "gemischter" Formationen, d.h. vor Formationen aus Angehörigen verschiedener Länder. Die Einheiten müssen homogen sein. Lediglich bei der Zentralleitung müssen Angehörige aller beteiligten Nationen vertreten sein. Zusammenfassend möchte ich feststellen, daß bei Vorhandensein genügender Mengen an technischen Gerät und Behelfsbauten innerhalb eines halben Jahres ein Horchdienst aufgestellt werden kann, der eine solide Grundlage für den weiteren Ausbau darstellen würde.

Es ist wahrscheinlich, daß Flicke diese Studie 1950 im Hinblick auf einen Kontakt mit der amerikanischen Funkaufklärung verfaßt hat. Entkleidet man seinen Vorschlag einmal der rein organisatorischen Strukturen, so ist vieles, bezogen auf die europäisch-atlantische Hemisphäre, später so gekommen, wie seinerzeit erdacht (vor allem wenn man es aus SIGINT-Sicht der Führungsnation der NATO, nämlich der USA betrachtet), was allerdings bei europaweiter Beurteilung der Lage auch wieder nicht so besonders bemerkenswert ist. Da aber diese Ausarbeitung Flickes sicherlich weder den Intentionen der OG noch der späteren Bundeswehrplaner entsprochen haben dürfte, außerdem nicht allgemein bekannt war, hat sie wohl auf die konzeptionelle Entwicklung der Funkaufklärung der Bundeswehr keinen Einfluß gewonnen, obwohl sie viele Gesichtspunkte enthält, die später so realisiert wurden. Auf welchem Wege Heusinger in den Besitz dieser Studie kam, konnte noch nicht geklärt werden.

Bei aller Skepsis bezüglich der Person Flickes und der Subjektivität seiner Darstellung ist doch aus seinen beiden Arbeiten zu erkennen, daß in der Nachrichtenaufklärung der Wehrmacht eine Fülle wertvoller Erfahrungen angesammelt wurden. Diese brachten aber naturgemäß auch die anderen Offiziere und Unteroffiziere mit, die sich nach 1956 am Aufbau der FmTr EloKa beteiligten.

In der nächsten F-Flagge lesen Sie:
Beiträge von Leo Hepp zur Aufstellung einer militärischen Funkaufklärung

In Memoriam

Wir betrauern den Heimgang
unserer Kameraden, Freunde und Wegbegleiter

Oberstleutnant a.D.
Jürgen von dem Borne
* 4. August 1940 † 26. Januar 2018

Hauptmann a.D.
Bernd Ulrich
* 18. Dezember 1942 † 19. Januar 2018

Herr
Hans-Eberhard Sense
* 24. Juni 1936 † 7. Januar 2018

Hauptmann a.D.
Rudolf Bölecke
* 9. Juni 1921 † 29. Dezember 2017

Oberst a.D.
Joachim-Ernst Hennig
* 12. Mai 1932 † 29. Dezember 2017

Herr
Heribert Schwanitz
* 12. Mai 1932 † 27. Dezember 2017

Hauptmann a.D.
Eberhard Eichhorn
* 10. Februar 1943 † 8. November 2017

Herr
Rüdiger Praun
* 14. September 1939 † 7. November 2017

Oberstleutnant a.D.
Dieter Goebel
* 14. Dezember 1933 † 2. Dezember 2017

Brigadegeneral a.D.
Henning Brümmer
* 27. April 1941 † Sommer 2017

Unsere Gedanken sind bei ihren Hinterbliebenen.

Im Namen aller Mitglieder
der Vorstand des Fernmeldering e.V.

V e r a n s t a l t u n g s h i n w e i s e

Stand: 31. Januar 2018

Fernmeldering

Frau Hella Schoepe-Praun, geschaeftsstelle@fernmeldering.de

20. - 22. April 2018 - Jahrestreffen 2018 in Potsdam

Gelber Kreis Rheinbach

KdoITBw, Frau Brauer, Telefon 0228 / 55 04 - 7001

24.04.2018 - Gelber Kreis

23.10.2018 - Gelber Kreis

Gelber Kreis Feldafing

ITSBw, Vorzimmer Schulkommandeur, Telefon 08157 / 273 - 2002

voraussichtl. 2. Quartal 2018 - 1. Gelber Kreis 2018

Die Teilnehmer am Gelben Kreis im 4. Quartal 2017, als ein Besuch der Lehrmittelsammlung auf dem Programm stand

Freundeskreis der Fernmeldetruppe und Führungsunterstützungskräfte an der Uni BW

Lt Sascha Klement, eMail : sascha.klement@hsu-hh.de, Tel: 0151 / 43200188
Lt Martin Hallmann, eMail: martinhallmann@hsu-hh.de; Tel.: 0152 / 51 33 34 44

Bei Redaktionsschluss lagen keine Veranstaltungstermine vor

Fernmeldebataillon 2

OStFw a.D. Bernd Niesel, Tel.: (0561) 820 24 42 - OStFw a.D. Wolfgang Prang, Tel.: (05607) 71 11,
Oberst a.D. Peter Kilian, Tel.: (06694) 9 11 98 26

jeden 1. Mittwoch in ungeraden Monaten, 19 Uhr (Januar, März, Mai, Juli, September, November): **Stammtisch** in der Kombinatsgaststätte, dem ehemaligen Unteroffizierheim der Lüttichkaserne in Kassel, Eugen-Richter-Straße.

Vorankündigung

15. und 16. Juni 2019 - Treffen auf Bataillonsebene in Fuldatal-Rothwesten

Fernmeldekameradschaft Hannover Ehemalige FmBtl 1/NA 6/19

Hauptmann a.D. Adalbert Mark, Tel.: (0511) 602 218, Fax: (0511) 606 1000, E-Mail: Adalbert.Mark@gmx.de

jeweils am 1. Mittwoch im Monat, 15.oo Uhr (im November am Sonntag vor dem Volkstrauertag / im Dezember kein Stammtisch!)**: Stammtisch** (Herren wie Damen) im Offiziersheim, Hannover-Bothfeld, General-Wever-Straße 12

25. März 2018, 12 Uhr - Gemeinsames Mittagessen im Offiziersheim Hannover-Bothfeld, General-Wever-Str. 120 und anschließendem Beisammensein. (Nähere Einzelheiten erhalten die Mitglieder mit gesonderter Einladung.)

11. November 2018 (Sonntag vor dem Volkstrauertag): **Kranzniederlegung** in der Nordring-Kaserne anläßlich des 30jährigen Vereinsbestehens

Kameradschaft der Fernmelder Koblenz /Lahnstein e.V.

Oberst a.D. Hans-Jürgen Siegel, Tel.: (0261) 5 46 68
E-Mail: 1vors@diefernmelder.de oder Juergen.Siegel@t-online.de + www.diefernmelder.de

10. März 2018, 13 bis 20 Uhr - Besuch der militärgeschichtlichen Sammlung "Wiege der Bundeswehr Andernach" und des Klosters Maria Laach mit anschliendem Abendessen im Restaurant Waldfrieden

26./27. Mai 2018, ganztägig - Wehrgeschichtliche Weiterbildung "Schlacht um Verdun" mit OTL a.D. Dr. Achim Kloppert *(ausgebucht)*

22. Juni 2018, 19 Uhr - Mitgliederversammlung mit Vorstandswahlen im Traditionsraum mit anschließenden Abendessen im Soldatenheim

15. September 2018, 13 bis 20 Uhr - Schießen am Schießsimulator AGSHP in Mayen mit anschließenden Abendessen in der OHG

9. November 2018, 19 Uhr - Kegeln mit anschließendem Abendessen im Soldatenheim

Freundeskreis Fernmelderegiment 120 in Rotenburg/Wümme

Hauptmann a.D. Sven von Ehrenkrook, Tel.: (04261) 54 57, Internet: www.fmrgt120.de

Bei Redaktionsschluss lagen keine Veranstaltungstermine vor

Traditionsverband FmBtl 890

StFw a.D. Heinz Nickel + Oberstlt a.D. Friedrich W. Koopmann, Tel.: 0621/303216

Bei Redaktionsschluss lagen keine Veranstaltungstermine vor

Traditionsverband Fernmeldebataillon 620, Flensburg

OTL a.D. Alfred Ott ; Tel.: 04638 / 89 90 89: E-mail: alfred-ott@versanet.de

8. und 9. September 2018 - Jahrestreffren zum 25 jährigen Bestehen des Traditionsverbandes

Traditionsverband Fernmeldebataillon 11 Oldenburg

Vorsitzender Stabsfeldwebel a.D. Claus-Jürgen Musial, Tel.: (0441) 44019
Herr Hans-Jürgen Schonhoff, eMail: hans-juergen.schonhoff@ewetel.net

Bei Redaktionsschluss lagen keine Veranstaltungstermine vor

Hinweis auf die Chronik des FmBtl 11

Nach der Auflösung des Fernmeldebataillons 11 im Jahr 1994 haben Angehörige des Bataillons eine Chronik der Hindenburg-Kaserne und seines Fernmeldebataillons 11 verfasst und herausgegeben. Die Chronik ist kartoniert, reich bebildert und umfasst 192 Seiten. - Bei Interesse am Erwerb dieser Chronik wenden Sie sich bitte an Herrn StFw a.D. Musial oder Herrn Hptm a.D. Voges.

Traditionsverein FmBtl 860, FmKp 880, FmAusbKp 861 Bad Bergzabern e.V.

StFw a.D. Günter Schüler, Tel.: (06343) 73 40, E-Mail: guenterschueler@t-online.de

Samstag, 10. März 2018, um 15,00 Uhr in der Kaserne - Mitgliederversammlung 2018 und anschließendem Eintopfessen. *(Anmeldungen bitte bis zum 01.03.)*

Dienstag, 10. April 2018, 19,00 Uhr in der Kaserne - „Babbel Owend“ und Nachbereitung der Mitgliederversammlung

Traditionsverband Luftlandefernmelder

Oberstleutnant a.D. Hartmut Schenk, Tel.: 0521 / 5 57 41 21 , E-mail: HartmutSchenk@web.de

Bei Redaktionsschluss lagen keine Veranstaltungstermine vor

Jahreshauptversammlung der FmKameradschaft Hannover / Ehemalige FmBtl 1 / NA 6/19

Hauptmann a.D. Adalbert Mark, Vorsitzender der Kameradschaft

Zum Auftakt bat ich darum, sich im Gedenken an unsere im Berichtszeitraum Verstorbenen vom Platz zu erheben. Am 10. März 2017 verstarb Oberstabsfeldwebel Otto Fricke mit 81 Jahren in Starnberg, er diente auch als KpFw der 3. Kp und am 25.03.2017 Brigadegeneral Heinrich Stoffregen mit 97 Jahren.

Grüße durfte ich ausrichten von General Boehr, General Berk, Oberst Siegfried Becker, Oberst Peter Kilian, den Oberstleutnanten Heinz Schweda, Günter Peters, Jürgen Holz, weiter von Werner Wienecke, Hans-Jürgen Kausche, Atze Gorr wie auch von Wilfried Müller, ehemals Rechnungsführer in der 3./Kp.

Die Stammtische 2018 finden, wie gewohnt, jeweils am 1. Mittwoch im Monat statt. Am Sonntag, 25. März, treffen wir uns aus Anlass des 30jährigen Bestehens unserer Kameradschaft zu einem Beisammensein und am Sonntag vor dem Volkstrauertag (11. November) holen wir die Kranzniederlegung nach.

Wie in den Vorjahren hatte Manfred Stüwe am 30. September zum Kartoffelfeuer in seinen Kleingartenverein eingeladen. Es war offenes, angenehmen Wetter und der kleine Kreis unserer Kameradschaft fühlte sich bei Kartoffelpuffer nach Elfriedes Geheimrezept sehr wohl. Auch an dieser Stelle vielen Dank an das Ehepaar Stüwe.

Zu besonderen Geburtstagen haben wir im Jahr 2017 gratuliert:

96 Jahre Heinz Stoffregen
94 Jahre Irmgard Nevermann
92 Jahre Sigrid Themann
88 Jahre Wilfried Bohmann
87 Jahre Adalbert Mark
86 Jahre Wolfgang Kühl
85 Jahre Horst Neumann
83 Jahre Günter Peters und Werner Rieger
82 Jahre Helmut Tröger, Bernhard Fritsch und Lothar Schramm
81 Jahre Dietmar Potempa, Hartmut Skupin und Siegfried Sprunk
80 Jahre Peter Damm und Ulrich Klippel
76 Jahren Hans-Jürgen Siegel und Siegfried Peters
75 Jahre Siegfried Becker, Jürgen Holz und Erhard Lange

Die letzte Überlebende der alten Kameradschaft NA 6/19 ist Sigrid Themann, der wir in diesem Jahr zum 92. Geburtstag gratulieren und weiterhin Gesundheit wünschen konnten. Zur Erinnerung: Ihr Mann hatte zu seinen Lebzeiten den Vorsitz der Kameradschaft.

Unser Kassenprüfer Peter Damm berichtete zur Kassenlage der FmKameradschaft, bedankte sich für die gute Kassenführung und entlastete Bernhard Fritsch zur Kassenführung. Er bat um Zustimmung hierfür durch die Hauptversammlung, die einstimmig erfolgte. Da Bernhard Fritsch gesundheitliche Probleme hat, bat er um Abgabe seines Amtes als Kassenverwalter. Rainer Gottschalk erklärte sich zur Übernahme des Amtes des Schatzmeisters der Kameradschaft bereit und wurde von der Hauptversammlung zum Schatzmeister bei einer Stimmenthaltung gewählt. Bernhard Fritsch wurde von der Hauptversammlung für seine Arbeit entlastet und bedankt. Als Kassenprüfer für die nächste Wahlperiode wurden Peter Damm und Joachim Wedemeyer von der Hauptversammlung einstimmig gewählt, sie nahmen ihr Amt an. Dem Vorstand wurde durch die Versammlung ebenfalls einstimmig Entlastung erteilt und für die neue Amtsperiode wieder gewählt, seine Mitglieder nahmen die Wahl an.

Kamerad Willi Eligehausen durfte ich zum Verdienstabzeichen in Gold des Verbandes der Reservisten der Bundeswehr für seine Arbeit in Bad Harzburg herzlich gratulieren.

Gedanken zum Jahreswechsel

von Hauptmann a.D. Adalbert Mark

Seit dem Jahresende 2015 haben wir nun keinen Patenverband mehr. Unser FmRgt wurde nach dem Abschiedsappell Ende Juni 2015 zum 31. Dezember 2015 aufgelöst und damit hat der norddeutsche Raum keinen intakten FmVerband des Heeres mehr. Lediglich in Prenzlau ist noch das FmBtl 610 stationiert, dass die Verbindung zum polnischen NATO-Partner aufrecht erhält und Multi-National eingesetzt ist. In den Divisionen und Brigaden gibt es nun nur noch FmStaffeln, die den inneren Betrieb aufrechterhalten wie z.B. den Anschluss der HQ's. Daneben gibt es im Bundesgebiet noch Informationstechnik-

Bataillone (IT-Btl abgekürzt, früher Führungsunterstützungs-Bataillone).

***W**ir mussten zu unserem Leidwesen aus Versicherungs-Gründen im vergangenem Jahr am Sonntag vor dem Volkstrauertag auf unsere Kranzniederlegung an unserem Nachrichten-Denkmal und dem Gedenkstein des FmBtl 1 verzichten. Die heutigen Nutzer der alten Nordring-Kaserne, heute Behördenpark Möckernstraße 30, die Bundesanstalt für Immobilienaufgaben und die Bundespolizei haben aus versicherungstechnischen Gründen den Zugang zu den Denkmälern abgelehnt. Das alte Wirtschaftsgebäude hinter dem Nachrichten-Denkmal von 1924 wird zur Zeit renoviert und der gesamte Raum bis zum Außenraum wurde der Baufirma übergeben und abgesperrt. Wegen Verzögerung der Baumaßnahme konnte daher aus Versicherungsgründen der Zugang nicht freigegeben werden. Wir mussten unsere Kranzniederlegung verschieben und werden diese am 11. März 2018 nachholen.*

***D**as 1924 von Generalfeldmarschall von Hindenburg eingeweihte Nachrichtendenkmal zur Erinnerung an die gefallenen und vermissten Nachrichtensoldaten der Telegraphenbataillone 3 und 6 erhielt 1924 zum 25. Jahrestrag der Aufstellung der Nachrichtentruppe in der kaiserlichen Armee in der Nordring-Kaserne seinen Standort und steht dort nun bereits 94 Jahre. Hierzu Anekdote: Unser am 25. März 2017 verstorbener General Stoffregen hat als fast vierjähriger Knabe an der Denkmal-Einweihung teilgenommen. Sein Vater führte zur damaligen Zeit die angetretenen Kriegsteilnehmer des ersten Weltkrieges, es war der Verein der Nachrichtentruppler in Hannover und Umgebung, und nach der Einweihungsfeier erfolgte dann der Vorbeimarsch an Generalfeldmarschall von Hindenburg.*

***I**nzwischen ist es das älteste Denkmal dieser Art in der Bundesrepublik. Ein Vorgänger des Denkmals stand in Potsdam in der Delius-Kaserne und ging nach dem Ende des II. Weltkrieges während der russischen Besetzung verloren. Laut Auskunft des Brandenburgischen Landesamts für Denkmalspflege und Archäologischen Landesmuseums in Zossen vom 3.11.2017 ist der Verbleib nicht bekannt. Neben dem alten Denkmal steht bei uns seit 2015 der Gedenkstein der hannoverschen Fernmelder und erinnert an das 59 ½ Jahre bestandene FmBtl 1 bzw. FmRgt 1, das in der Nordring-Kaserne am 1. Juli 1956 aufgestellt wurde. Ein kleines Hinweisschild auf der Rückseite des Steins weist auf diesen Vorgang hin.*

***2017** waren 72 Jahre seit dem Ende des II. Weltkrieges vergangen. Inzwischen haben wir wieder seit 28 Jahren ein geeintes Deutschland (allerdings ohne die 1945 verlorenen Gebiete im Osten unseres Vaterlandes) und unsere Bundeswehr feierte ihr 62jähriges Bestehen: Am 12. November 1955 wurde sie in der Ermekeil-Kaserne in Bonn in einer Feierstunde offiziell aus der Taufe gehoben. Als markantes Datum wurde hierfür der Geburtstag des preußischen Heeresreformers General Gerhard von Scharnhorst, vor 203 Jahren hier bei uns in der Nähe in Bordenau geboren, festgelegt. In der festlich geschmückten Fahrzeughalle unter dem Eisernen Kreuz erhielten seinerzeit 101 ehemalige Soldaten (95 Offz und 6 Uffz) ihre Urkunden. Allerdings war der damalige Bundeskanzler Dr. Adenauer mit dem Festakt nicht zufrieden, denn es trugen nur wenige neue Soldaten eine Uniform, der größte Teil von ihnen war noch nicht eingekleidet und in Zivil angetreten. Übrigens hatte das Jahre 1955 noch zwei weitere wesentliche Ereignisse im Zusammenhang mit den Streitkräften. Am 9. Mai wird die Bundesrepublik in die NATO aufgenommen und ab dem 7. Juli wurde das BMVg mit Theodor Blank als ersten Verteidigungsminister der Bundesrepublik Deutschland aufgebaut.*

***E**ine Übersicht über die aktuellen Einsätze unserer Bundeswehr (Stärke der deutschen Einsatzkontingente) ergibt auch der Blick auf die Personalstärke der Streitkräfte und deren Möglichkeiten. Hierbei muss man auch den Anteil der Reservisten sehen, die z.Zt. mit knapp 200 Angehörigen die aktiven Soldaten unterstützen. Von den 3360 Soldaten mit Beginn des III. Quartals 2017 war auch der weibliche Anteil von 257 Soldatinnen erstaunlich hoch. Unter Berücksichtigung der gesamten Einsatzstärke war 1/3 davon in Afghanistan eingesetzt, ein*

doch sehr hoher Anteil, obwohl man von diesem Schauplatz schon länger Abschied nehmen wollte.

***H**inzu kommt, dass man seit der Wiedervereinigung und der Auflösung des „Warschauer Paktes“ einen erheblichen Rückgang der Personalstärke wie der materiellen Ausstattung feststellen muss. Seit nun 28 Jahren ist die Bundeswehr „Stabil auf wirklich niedrigem Niveau“! Als sie noch eine Wehrpflichtarmee war, hatte man immer junge Rekruten, von denen sich viele auch für eine längere Dienstzeit verpflichteten. Heute boomt unsere Industrie und Wirtschaft, die Arbeitslosigkeit ist gering und es ist schwer, den Nachwuchsbedarf abzudecken. Die nach einer Pressemitteilung gegenwärtig dienenden 178.433 aktiven Soldaten verteilen sich auf die Streitkräfte wie folgt: Bereich Infrastruktur, Dienstleistungen, Umweltschutz 977, Bereich Ausrüstung 1544, BMVg und nachgeordnete Dienststellen 3310, Bereich Personal 7127 (davon 4810 Studenten an Bw-Universitäten und in Ausbildung), Bereich Kdo CIR einschl. der IT-Soldaten 12248, Marine 16053, Zentraler Sanitätsdienst 19703, Luftwaffe 28002, SKB 28104 und Heer 61365.*

***D**ie seit 1989 geltende Friedensinitiative nach der Maueröffnung hat unsere Streitkräfte den politischen Forderungen entsprechend zum Sparen und Umstrukturieren gezwungen. Ihre Einsatzaufträge konnte sie nur noch mit erheblichen Schwierigkeiten erfüllen. Größere Aufgaben, wie sie z.Zt. des „Kalten Krieges“ geübt wurden, konnten nicht mehr erledigt werden. Personal und Ausrüstung reichen für die Landes- und Bündnisverteidigung nicht mehr aus, das Geld fehlt! Wir sind nicht mehr in der Lage, eine vollausgerüstete Brigade in den Einsatz zu schicken. Unsere Verteidigungsministerin hat bereits festgestellt, dass der Finanzbedarf für die nächsten Jahre zur Beschaffung von Material und Munition 140 Milliarden Euro beträgt. Ob und wer nun den Auftrag hierfür erhält, wird die Zusammensetzung der neuen Bundesregierung zeigen.*

***N**euer General der Fernmeldetruppe ist Oberst i.G. Kai Heß, Unterabteilungsleiter Führungsunterstützung im Kommando Heer. In seiner Laufbahn führte er u.a. auch drei Jahre lang das FüUstBtl 393 in Murnau.*

***D**ie Bundeswehr ist wie auch andere Behörden und Unternehmen ständig das Ziel von Hackern. Allein in den ersten neun Wochen des Jahres 2017 wurden Bundeswehrnetze 284.000 Mal attackiert. Ein Schaden ist bisher nicht entstanden, aber täglich werden neue Angriffe festgestellt, gegen die sich die Bundeswehr wappnen und Abwehrmechanismen kontinuierlich entwickeln muss. Durch die Digitalisierung in der Welt sind wir nicht nur effektiver und leistungsfähiger, sondern auch verwundbarer im Cyber- und Informationsraum geworden und sie wird auch in Zukunft zunehmen. Dem Schutz eigener Systeme kommt daher eine hohe Bedeutung zu. Hierzu wurde zum 1. Juli 2017 dem Kommando CIR unterstellt das Kommando Strategische Aufklärung, das Kommando Informationstechnik der Bundeswehr (bisher Führungsunterstützungskommando der Bundeswehr), das Zentrum Operative Kommunikation der Bundeswehr und das Zentrum für Geoinformationswesen der Bundeswehr. Das Kommando CIR hat als Personal 13.500 Stellen verfügbar und bis 2021 sollen es 15.000 werden. Zurück geblickt auf die letzten 27 Jahre sind es 20.000 Fernmeldesoldaten weniger.*

***D**as Rückgrat bilden weiterhin die bisherigen Führungsunterstützungsbataillone, ab sofort als Informationstechnische Bataillone (IT Btl), die über die Bundesrepublik verteilt sind und vom Kommando Informationstechnik der Bundeswehr, Generalmajor Steiner, geführt werden. Um die volle Einsatzbereitschaft zu erreichen, sucht die Bundeswehr im IT-Bereich verstärkt IT-Fachkräfte und ist hierfür ein attraktiver Arbeitgeber. Die Aufgaben des neuen Organisationsbereichs werden in Zusammenarbeit mit nationalen und internationalen Einrichtungen zur gesamtstaatlichen Sicherheitsvorsorge beitragen. Ein gemeinsames Lagebild im Kommando CIR wird hierzu einen wesentlichen Beitrag liefern. Große Bedeutung für die Sicherheit und Einsatzbereitschaft der Bundeswehr und dem Schutz der eigenen und verbündeten Soldaten wie auch im digitalen Bereich obliegt dem Militärischen Nachrichtenwesen und wird im Kommando Strategische Aufklärung für CIR zusammen gefasst. An der Bundeswehr-Universität in München ist im Januar ein Master-Studiengang für Information/ Cyber-Sicherheit mit 13 Professuren eingerichtet worden. Alle Angehörigen des Organisationsbereichs CIR, ohne Berücksichtigung der TSK, werden in Zukunft ein blaues Barett mit zugehörigem Barettabzeichen CIR als Erkennungszeichen tragen. Ja, so geht es weiter. Bisher sprach man von Nachrichtlern, dann Fernmeldern, Führungsunterstützern und jetzt sind es Informationstechniker, kurz IT'ler. Wie sich die Zeiten doch ändern!*

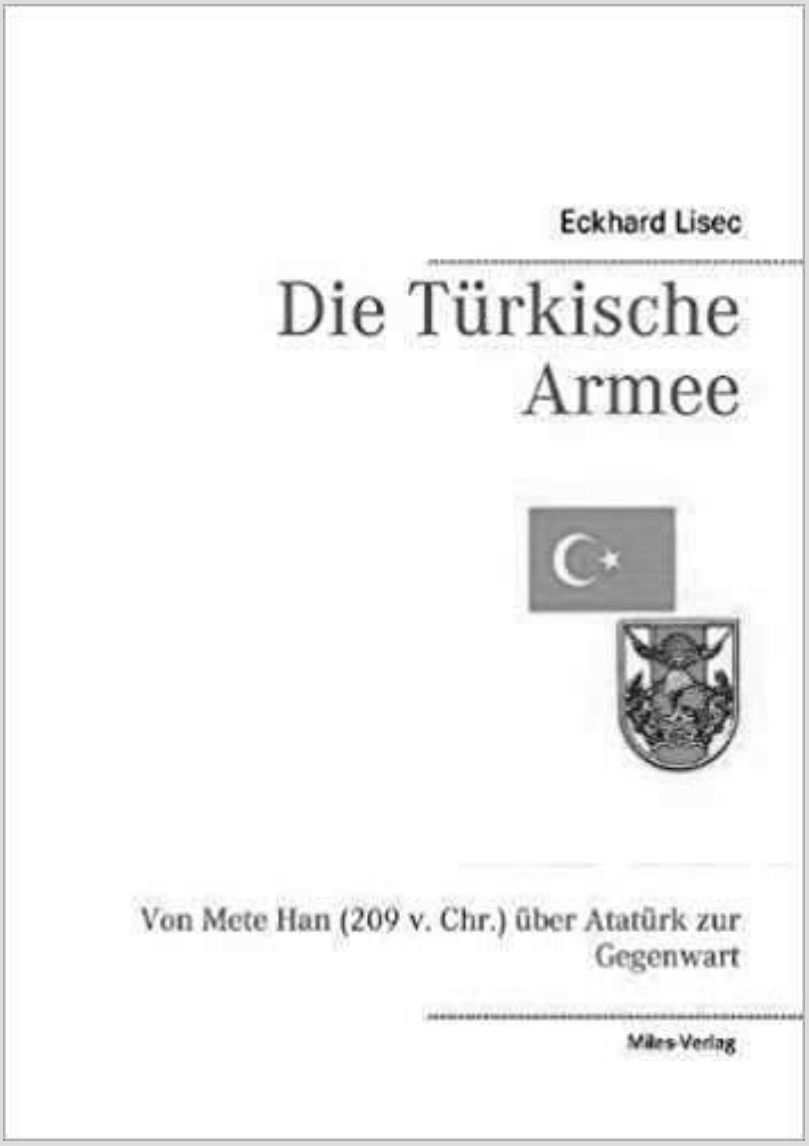
Eckard Lisec:
Die Türkische Armee.
Von Mete Han (209 v. Chr.) über Atatürk zur Gegenwart

Die jüngsten Ereignisse in der Türkei haben nicht nur für die Türkei, sondern auch für die türkische Armee die Frage aufgeworfen „Quo Vadis?“. Wer die Tradition dieser Armee, das Denken und die Absichten ihres bisher kemalistisch geprägten Generalstabes verstehen will, muss weit in die Geschichte eintauchen – in die vorosmanische, die osmanische und die türkische.

Es ist anrührend, dass ein Offizier der Bundeswehr mit jahrelanger militärischer Erfahrung in der Türkei über die türkische Armee schreibt. In gewisser Weise steht er damit in der Tradition zahlreicher Offiziere, die insbesondere nach dem Ersten Weltkrieg ihre Eindrücke und Erfahrungen zu Papier gebracht haben. Der bekannteste unter ihnen ist Liman von Sanders Pascha. Eckhard Lisec schreibt nicht seine Memoiren nieder, sondern stellt dem Leser die türkische Armee in ihrer ganzen langen Tradition vor. Wie seine schreibenden Vorgänger-Kameraden aber tut er es in positivem Geist.“

Aus dem Geleitwort von Professor Dr. Udo Steinbach

Zum Autor:
Eckhard Lisec, Jahrgang 1944, Brigadegeneral a.D. und Mitglied im Fernmeldering seit 2000, diente von 2002 bis 2005 in einem NATO-Stab in Istanbul. Er war damit der erste Bundeswehrgeneral, der nach dem 2. Weltkrieg, außerhalb eines Einsatzes, in der Türkei friedensstationiert war.



Eckard Lisec
Die Türkische Armee.
Von Mete Han (209 v. Chr.) über Atatürk zur Gegenwart

Carola Hartmann Miles-Verlag
Berlin 2018

288 Seiten, Paperback

ISBN 978-3-945861-68-4

Preis: 24,80 Euro

Armin Müller:
Wellenkrieg

Besprechung durch Oberst a.D. Rudolf Grabau

Bundesnachrichtendienst und Bundeskanzleramt haben im Jahr 2011 eine Historikerkommission zur Erforschung der „Geschichte des Bundesnachrichtendienstes in den Jahren 1945 bis 1968“ berufen und dazu die verfügbaren Akten dieses Untersuchungszeitraums freigegeben. Armin Müller, Schiffsoffizier der Handelsmarine und Reserveoffizier der Bundeswehr, bearbeitete dabei nach Studium der Sozial- und Wirtschaftsgeschichte die Thematik Agentenfunk und Funkaufklärung. Er promovierte mit dem vorliegenden Band.

Das Buch beschreibt anhand umfangreichen Aktenmaterials die Weiterentwicklung der Funkaufklärung und des Agentenfunks des „Dienstes“ aus seinen militärischen Wurzeln, welche auch im Zeitraum nach Kriegsende bis zur „Tschechenkrise“ und darüber hinaus weit überwiegend durch die Konfrontation in Mitteleuropa bestimmt war. Besonders ausführlich werden die Ausbildung und der Einsatz der Funkagenten des BND sowie die unterschiedlichen Auffassungen zur Fernmeldeelektronischen Aufklärung von Bundeswehr und Abteilung Technik des BND (Konkurrenzsituation/Zusammenarbeit/Koordinierung) geschildert.

In einigen Fällen hat offenbar die Fülle des vorliegenden Materials den Verfasser zur Überschreitung der selbstgesteckten Thematik veranlasst (z. B. Absetzen von Agenten des BND mit U-Booten an der Ostseeküste) und ebenso des Betrachtungszeitraums (wie der organisatorischen Zusammenfassung des Militärischen Nachrichtenwesens der Bundeswehr ab Anfang der 80er Jahre). Aber gerade auch diese Überschreitungen dienen der Darstellung von Zusammenhängen/historischen Abläufen und verleihen teilweise den geschilderten Sachverhalten sogar eine gewisse zusätzliche Spannung.

Armin Müller
Wellenkrieg
Agentenfunk und Funkaufklärung des Bundesnachrichtendienstes 1945-1968,
Band 5 der Unabhängigen Historikerkommission

Ch.Links Verlag Berlin 2017

416 Seiten, Hardcover

ISBN 978-3-86153-947-6

Preis: 45,-- Euro

Zwangsläufig wird vieles aufgrund der Quellenlage (relevante Dokumente aufseiten des BMVg Führungsstab Bundeswehr und der Fernmeldedienststelle der Bundeswehr sind ja leider vollständig vernichtet worden) zumeist aus der Sichtweise des BND dargestellt. Dies wird besonders deutlich z.B. an der Darstellung der Entwicklung der grenznahen Aufklärung der Bundeswehr, der Tätigkeit des EloKa-Instituts in Werthhoven und in Zusammenhang mit der Aufstellung des Amtes für Nachrichtenwesen der Bundeswehr.

Auch bei dieser Veröffentlichung fehlen leider wie in anderen Publikationen die Aufklärungsergebnisse (Inhalt von Lagemeldungen sowie von zusammenfassenden Original-Berichten). Abgesehen nur von einer Zusammenfassung der Lageentwicklung während des Einmarsches der WP-Streitkräfte in die Tschechoslowakei 1968 – aber auch hierbei fehlen Angaben darüber, woher die Situationsschilderungen des BND ursächlich stammten, denn nicht alles kam damals aufgrund der Erfassung und Nachrichtenbearbeitung des BND zustande - wurde aber natürlich vom „Dienst“ gegenüber der Bundesregierung so „verkauft“. Enge Grenzen setzt naturgemäß auch das Enddatum der Verfügbarkeit von Quellen über den Zeitraum nach 1968 hinaus.

Obwohl ich ja mit dem BND in diesem Fachgebiet aufseiten der Bundeswehr jahrelang und teilweise recht intensiv kooperiert habe, war vieles in dem Buch neu für mich und hat etliche meiner noch vorhandene Wissenslücken aufgefüllt. Das liegt natürlich auch daran, dass meine Kontakte mit dem BND vor allem in den 70er bis 80er Jahren datieren. Zudem hatte ich in „meinen“ Bänden über die Historie der FmTruppeEloKa, die ab 1992 mithilfe des Fernmelderings herausgegeben wurden, der dienstlichen Anweisung Folge zu leisten, Querbeziehungen zum BND nicht erkennen zu lassen – was dem Autor den Zugang zu meinen Publikationen eingeschränkt haben könnte.

Es ist ein wichtiges Buch, vor allem eine als zuverlässig einzustufende Quelle für die historische Erschließung der Fachgebiete Funkaufklärung und Agentenfunk in der Aufbauphase des westdeutschen Nachrichtendienstes nach Kriegsende 1945.

Insgesamt ist es eine umfängliche und mit großer Sorgfalt zusammengestellte Darstellung der Aktivitäten der Abteilung Technik in der Organisation Gehlen im gewählten (also dem bislang der Öffentlichkeit zugänglichen) Zeitraum. Der Inhalt ist verständlich formuliert, allerdings erschließt er sich vollständig wohl nur demjenigen, dem die Organisation und die Arbeitsweise des BND und dessen Vorbehalte gegenüber Aktivitäten der Bundeswehr nicht unbekannt sind. Dies betrifft vor allem auch die gedankliche Einordnung der über 1000 präzise in Fußnoten aufgelisteten Quellen, in denen im Einzelfall auch noch ergänzende Informationen aufgefunden werden können.

Es ist ein wichtiges Buch, vor allem eine als zuverlässig einzustufende Quelle für die historische Erschließung der Fachgebiete Funkaufklärung und Agentenfunk in der Aufbauphase des westdeutschen Nachrichtendienstes nach Kriegsende 1945 – und zwar in deutlicher Fortführung der zuvor von Wehrmacht und Reichssicherheitshauptamt betriebenen aufklärerischen Aktivitäten. Aber natürlich unterstützt es auch die Erinnerung der späteren (jetzt ehemaligen) „Insider“ dieses Fachgebiets, ergänzt und spiegelt deren eigenes Erleben. Einschränkungen hinsichtlich Vollzähligkeit und Objektivität der Darstellung waren durch Verfügbarkeit, Einseitigkeit und zeitliche Beschränkung des freigegebenen Quellenmaterials unvermeidbar; weitere Ergänzung um den anschließenden Zeitraum, wenigstens bis zur Wiedervereinigung, ist wünschenswert.

In eigener (Redaktions-)Sache

Die F-Flagge möchte die Zeitschrift von Mitgliedern über Mitglieder für Mitglieder sein.

Da versteht es sich von selbst, dass die Redaktion sich natürlich über jeden Buchtipp freut (insbesondere wenn er aus der Feder eines FmR-Mitglieds stammt) und diesem entsprechend gerne an dieser Stelle veröffentlicht. - Aber: Leider fehlt es an Zeit, Manpower und auch Fachwissen, alle uns vorgeschlagenen (und zugeschickten) Bücher zu rezensieren.

Daher die Bitte: Für die Veröffentlichung von Buch-Tipps/-Besprechungen wird ein vorbereiteter Text erbeten, der unter dem Namen des Einsenders veröffentlicht werden darf. - Wenn der (elektronischen) Zusendung dann noch ein Foto vom Cover beiliegt, ist das Redaktionsglück komplett!

V o r s t a n d

Vorsitzender

Brigadegeneral a. D. Helmut Schoepe
Waldschmidtstraße 16 + 82327 Tutzing + Tel. 08158 / 90 44 100
vorstand@fernmeldering.de ++ h.schoepe@t-online.de

1. Stv. Vorsitzender

Oberst i.G. Peter Uffelmann
Tulpenweg 3 + 35066 Frankenberg/E.
Tel: 03341/ 58 - 4810 (dienst.)
vorstand@fernmeldering.de
peteruffelmann@bundeswehr.org

2. Stv. Vorsitzender

Oberstabsfeldwebel Wilhelm Fischer
Seeleite 15 + 82386 Huglfing
Tel.: 0176 / 22 15 57 70
vorstand@fernmeldering.de
wilhelm1fischer@bundeswehr.org

Beisitzer

Oberst i.G. Jürgen Schick
Ravensberger Straße 34
53474 Bad Neuenahr-Ahrweiler
Tel.: 01515 / 8 78 46 19
vorstand@fernmeldering.de
juergen.schick@t-online.de

Kassenwart

Oberst a.D. Peter Warnicke
Westerwaldstraße13
56244 Ötzingen
Tel.: 02602 / 77 46
vorstand@fernmeldering.de
peter.warnicke@rz-online.de

Schriftführer

Hauptmann André Frank
Rolandsweg 105
33102 Paderborn
Tel.: 0174 / 3 19 56 01
vorstand@fernmeldering.de
frank.andre@gmx.net

Geschäftsführer / Geschäftsstelle

Frau Hella Schoepe-Praun
geschaeftsstelle@fernmeldering.de ++ h.schoepe-praun@arcor.de
Waldschmidtstraße 16 + 82327 Tutzing +
Telefon 08158 / 90 44 100

Redaktionsbüro F-Flagge

Frau Hella Schoepe-Praun
redaktion@fernmeldering.de
h.schoepe-praun@arcor.de

Personalia / Mitgliederverwaltung
Meldungen gerne an jedes Vorstandsmitglied

Web-Master

Oberstleutnant Ulrich Graf von Brühl-Störlein (*)
webmaster@fernmeldering.de

R e g i o n a l b e a u f t r a g t e

Süd

OLt Joachim Dey (*)
joachim.dey@online.de

Nord

Lt Martin Hallmann (*)
martinhallmann@hsu-hh.de

Ost

N.N.

West

Oberstlt i.G. Roland Kaiser (*)
otlrokai@aol.com

S t a n d o r t - B e a u f t r a g t e

UniBw Hamburg

Lt Martin Hallmann (*)
Tel.: 0152 / 51 33 34 44
martinhallmann@hsu-hh.de

FüUstgSBw

Oberstlt Alexander Gerber (*)
Tel.: 08157 / 273 - 48 80 (dstl.)
Mobil.: 0173 / 9 50 88 66
alexander2gerber@bundeswehr.org

FüAkBw

N.N.

UniBw München

N.N.

Standort Storkow

Hptm Martin Heusler (*)
Tel.: 0160 / 94 93 09 64
fernmeldering@martin-heusler.de

Standort Hamburg

Lt Martin Hallmann (*)
Tel.: 0152 / 51 33 34 44
martinhallmann@hsu-hh.de

Standort Bonn/Köln/Rheinbach

Oberstlt Roland Kaiser (*)
Tel.: 0228 / 5 36 83 - 62 40 (dstl.)
Tel.: 0171 / 2 10 29 46
otlrokai@aol.com

Standort Lechfeld

Oberstlt Andreas Hadersdorfer (*)
Tel.: 0176 / 62 02 40 83
Andreas.Hadersdorfer@gmx.de

Standort Veitshöchheim

Maj Björn M. Scherer (*)
Tel.: 0151 / 24 00 55 81
Bjoern.scherer@web.de

**** nicht Mitglied des Vorstandes***

Angehörige Fm/EloAufkl

Hptm d.R. Uwe Lünsmann (*) + Uferstraße 2d, 26409 Wittmund + Tel.: (04464) 8 68 99 48 + uwe@luensmann.it

Personalia

- abgeschlossen für diese Ausgabe am 31. Januar 2018 -

Jubilare im 1. Quartal 2018

30 Jahre
Oberleutnant Eddie Kropfgans (4.3.)

40 Jahre
Major Stephan Bader (17.3.)
Hauptmann Christian Frechen (22.3.)
Major Michael Sahlmüller (26.2.)
Hauptmann d.R. Stephan Zerling (20.2.)
Major Matthias Bober (7.1.)
Oberstleutnant i.G. Jan Mosel (4.1.)
Hauptgefreiter d.R. Michael Woyscheszik (18.1.)

50 Jahre
Oberstleutnant d.R. Jens C. Becker (23.2.)
Hauptmann Hans Freisler (15.2.)
Hauptmann d.R. Jürgen Hofmann (6.2.)
Oberst i.G. Sönke Marahrens (21.2.)
Oberstleutnant i.G. Dirk Hunke (11.1.)
Oberstleutnant Karl-Heinz Kerber (29.1.)
60 Jahre
Unteroffizier d.R. Norbert Engesser (30.3.)
Brigadegeneral Jens-Olaf Koltermann (20.3.)
Oberst Manfred Warnebold (23.2.)
Oberst i.G. Reinholf Janke (12.1.)
Oberstleutnant Dietmar Poplawski (17.1.)
Oberst i.G. Peter Uffelmann (5.1.)

65 Jahre
Herr Robert Robin (27.2.)
Oberst a.D. Udo Galle (31.1.)

70 Jahre
Oberstleutnant a.D. Herbert Memmer (1.3.)
Oberst a.D. Olaf Bendrat (17.2.)

75 Jahre
Frau Helga Balazs (21.2.)
Frau Lieselotte Mey (17.2.)
Oberstleutnant d.R. Josef Pütz (3.2.)
Oberstleutnant a.D. Detlef Ende (20.1.)

80 Jahre
Oberstleutnant a.D. Günter Marquardt (25.3.)
Oberstleutnant a.D. Horst H. Schweighöfer (20.3.)
Stabsunteroffizier d.R. Peter-Michael Wolter (19.2.)
Oberstleutnant a.D. Reiner W. Möller (27.1.)
Oberstleutnant a.D. Reiner Schraff (29.1.)
Oberst a.D. Arnd Winkelmann (18.1.)

81 Jahre
Oberstleutnant a.D. Jürgen Hauser (17.3.)
Frau Renate Bergener (7.1.)
Oberstleutnant a.D. H.-Joachim Schrader (9.1.)

82 Jahre
Hauptmann a.D. Gerhard Pfeifer (27.1.)

83 Jahre
Oberstleutnant a.D. Dirk Heye (28.3.)

84 Jahre
Oberstleutnant a.D. Günter Jaschke (25.2.)
Oberst a.D. Kurt Rauchmann (14.1.)

85 Jahre
Oberstleutnant a.D. Peter Freude (4.2.)
Oberstleutnant a.D. Klaus Franke (22.1.)

87 Jahre
Oberstleutnant a.D. Manfred Bahr (1.1.)
Oberst a.D. Adolf Göller (28.1.)

88 Jahre
Hauptmann a.D. Adolf Tröster (22.1.)

89 Jahre
Capitaine Cue Max Mury (19.1.)

91 Jahre
Hauptmann a.D. Hans Motejus (28.3.)

Neue Dienstposten

Oberst Dr. Volker Pötzsch wurde am 8. Dezember als Kommandeur der Abteilung Süd des Technischen Ausbildungszentrums der Luftwaffe in Kaufbeuren verabschiedet. Seine Folgeverwendung führt ihn als Chef des Stabes zum IT-Kommando nach Bonn.

Beförderungen

zum Oberst d.R.
Oberstleutnant d.R. Rainer Sieber

zum Oberstleutnant d.R.
Major d.R. Dr. Matthias Witt-Brummermann

zum Stabsfeldwebel
Hauptfeldwebel Thomas Hehnle

Personalia

- abgeschlossen für diese Ausgabe am 31. Oktober 2017 -

Willkommen im Fernmeldering

Leutnant Matthias Carstensen
Kolonie 1, 24983 Handewitt
Tel.: 0160 / 93 23 35 57

Oberstleutnant Maurizio Klug
Goethestraße 32, 63857 Waldaschaff
Tel.: 0179 / 12 12 070

Herrn Marc Rawer
Fichtenweg 3, 73760 Ostfildern
Tel.: 0711 / 46 05 87 30

Oberstleutnant Sven Schatz
Jakob-Katzfey-Straße 23, 53902 Bad Münstereifel
Tel.: 0172 / 35 99 877

Oberfeldwebel d.R. Klaus Wagner
Julius-Schmuck-Straße 7, 91781 Weissenburg
Tel.: 0171 / 63 08 962

Neue Adressen

Ein aktuelles Mitgliederverzeichnis
(Stand Februar 2018)
steht in der Cloud (*)

(*) für Cloud-Zugang bitte
geschaeftsstelle@fernmeldering.de
kontaktieren!

Herzlichen Dank für Ihre Treue

40 Jahre
Oberstleutnant a.D. Wolfgang Goetze

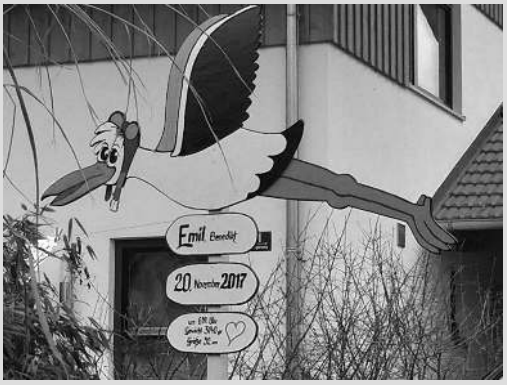
25 Jahre
Oberst a.D. Werner Bermbach
Oberstleutnant a.D. Detlef Ende
Oberst a.D. Kurt Grooz
Oberst a.D. Hans-Peter Grünebach
Oberstleutnant a.D. Udo Hergesell
Oberst a.D. Hubert Küpper
Oberstleutnant a.D. Herbert K.A. Kulbarsch
Oberst a.D. Adrian Maier
Oberst a.D. Siegfried Peters
Oberst a.D. Kurt Rauchmann
Stabsfeldwebel a.D. Heribert Rossmeisl
Oberst a.D. Armin Saal
Oberstleutnant a.D. Klaus Tappe

Wir gratulieren

Alina &
Oberstleutnant Alexander Gerber

zur Geburt ihres Sohnes

Emil Benedikt



Unser Hinweis zum Datenschutz

Das Bundesdatenschutzgesetz (BDSG) verlangt von jedermann die Einhaltung strenger Dokumentationspflichten. Es drohen erhebliche Bußgelder und Strafen bei Verstößen. Der Vorstand des Fernmeldering e.V. möchte auch in der Zukunft über den Werdegang seiner Mitglieder mit Anschriftenänderungen, Beförderungen und Zuruhesetzungen informieren. Dies können wir aber nur mit Einwilligung unserer Mitglieder. Mit der Beitrittserklärung haben die Mitglieder dazu ihre Erlaubnis erteilt bzw. Auflagen gemacht. Mitglieder, die der Veröffentlichung ihrer Daten in der Mitgliederliste bzw. im Veränderungsdienst der F-Flagge nicht mehr zustimmen wollen, bitten wir um eine kurze formlose Information an den Geschäftsführer, den Vorsitzenden oder an jedes andere Vorstandsmitglied. Bereits verfügte Einschränkungen der Veröffentlichungserlaubnis in den Beitrittserklärungen gelten weiter und müssen nicht erneuert werden. Für die unter Personalia veröffentlichten Angaben zum Werdegang unserer Mitglieder gibt es aus Datenschutzgründen auch keine andere Informationsquellen als die Mitteilungen unserer Mitglieder selbst. Bitte denken Sie daran, den Vorstand des Fernmeldering e.V. zu informieren, wenn Sie Ihre Kameraden auf diesem Wege über dienstliche oder private Veränderungen in Kenntnis setzen wollen.

Bitte melden!

Nachfolgenden Mitgliedern konnte diese Ausgabe der F-Flagge leider nicht zugestellt werden, da uns ihre aktuelle Adresse nicht vorliegt:

Major Stefan Bader ++ Leutnant David Christ ++ Hauptmann Christian Frechen ++ Oberleutnant d.R. Andy Großmann ++ Hauptmann Ansgar Henn ++ Major d.R. Arnd Kaufmann ++ Fahnenjunker Kevin Mahlmann ++ Hauptmann Andreas Merz ++ Major d.R. Stefan Miebach ++ Oberstleutnant Wolfgang Schäfer ++ Leutnant Duncan Seitz ++ Hauptmann Katharina Tibbetts ++ Oberstleutnant Sven Voigtmann ++ Fahnenjunker Heinrich Wertmann

! ! ! Alles Gute zum Geburtstag ! ! !

März

Baumgartner, Werner – OTL (10.)
Czada, Thomas – M i.G. (10.)
Schmidt, Norbert – O i.G. (10.)
Tanneberger, Andreas – OL (10.)
Brosowski, Frank – OTL (11.)
Geisen, Jörg – SU d.R. (11.)
Welter, Julia – Frau (11.)
Bröcker, Felix – M (12.)
Müller, Heinz Konrad – OTL (13.)
Jansen, Stephan – OTL i.G. (15.)
Scherer, Björn Markus – M (15.)
Brandes, Peter-Michael – O (16.)
Conradi, Jens Roman – H d.R. (16.)
Jodl, Dr. Herbert – M d.R. (16.)
Kesselheim, Jürgen – OSF (16.)
Konkol, Philipp – M (16.)
Pauland, Hartmut – BG a.D. (16.)
Bader, Stephan – M (17.)
Hauser, Jürgen – OTL a.D. (17.)
Benz, Friedrich W. – O a.D. (19.)
Messner, Stefan – OTL a.D. (19.)
Asl, Igor – OTL (20.)
Koltermann, Jens-Olaf – BG (20.)
Schweighöfer, Horst H. – OTL a.D. (20.)
Thieme, Immo – OTL a.D. (20.)
Christ, David – L (21.)
Koberg, Guido – OTL (21.)
Lips, Dieter – OTL a.D. (21.)
Frechen, Christian – H (22.)
Völkl, Norbert – OTL (24.)
Braun, Werner – O (25.)
Marquardt, Günter – OTL a.D. (25.)
Mosmann, Dietmar – BG (25.)
Hartmann, Rainald – OTL (26.)
Liemen, Alexander – OL (26.)
Lingauer, Andreas – H (26.)
Görlich, Jürgen – OSF (27.)
Kilchmann, Ruedi – Adj. UO (27.)
Napiwotzki, Ole – M (27.)
Scherz, Reimar – BG a.D. (27.)
Weber, Jens – OTL (27.)
Heye, Dirk – OTL a.D. (28.)
Motejus, Hans – H a.D. (28.)
Ojda, Michael – H (28.)
Schönberger, Stefan – OTL (28.)
Harbig, Markus – M (29.)
Ossenkop, Björn – H (29.)
Engesser, Norbert – U d.R. (30.)
Jarosch, Otto – O i.G. (30.)
Vogt, Holger – SF (30.)

April

Harings, Herbert – O a.D. (1.)
Klöffel, Peter – OTL (1.)
Plank, Michael – OTL (1.)
Klug, Maurizio - OTL (2.)
Bludau, Klaus – O a.D. (2.)
Hillermann, Peter – OTL i.G. (2.)
Mader, Johann – OTL (2.)
Barth, Annerose – Frau (3.)
Klein, Stefan – OTL d.R. (3.)
Becht, Alexander – OF d.R. (4.)
Kemmer, Stefan – OG d.R. (4.)
Barth, Volker – BG a.D. (5.)
Wierowski, Klaus – OTL a.D. (5.)
Giese, Horst – H a.D. (7.)
Werz, Steffen – H (7.)
Karow, Heinz – O a.D. (8.)
Klier, Marco – OL (8.)
David, Rainer H. – M d.R. (9.)
Jama, Bernd – OTL (9.)
Lorenz, Reinhard – OTL (9.)
Knab, Hans-E. – O d.R. (10.)
Schöneberg, Benjamin – M (10.)
Sutter, Thomas – Fachof M (10.)
Dreher, Martin W. – O (11.)
Kuc, Matthias – H (11.)
Lisec, Eckhard – BG a.D. (11.)
Siegel, Hans-Jürgen – O a.D. (11.)
Valentin, Hans-Joachim – OTL a.D. (11.)
Czok, Bernd – OL d.R. (12.)
Lünsmann, Uwe – H d.R. (12.)
Mett, Detlef – L d.R. (12.)
Recke, Hans-Joachim – O a.D. (12.)
Rönsch, Dennis – SF (12.)
Roßbach, Karl Dieter – O a.D. (12.)
Buhrmeister, Horst-Dieter – O a.D. (14.)
Haag, Alfred – OTL a.D. (14.)
Baumert, Uwe D. – OTL a.D. (15.)
Lippold – Dr. Heiko – O d.R. (15.)
Lobin, Gordon – SU d.R. (15.)
Geissbauer, Ludwig – OTL a.D. (16.)
Zwingmann, Ike – OL (16.)
Bock, Hartmut – O (17.)
Dworski-Eichhorn, Michaela – Frau (18.)
Hübel, Dietmar – OTL (18.)
Rambach, Ralf – OTL a.D. (18.)
Bermbach, Werner – O a.D. (19.)
Böttger, Thomas – OTL i.G. (20.)
Schwendler, Rainer – OTL (20.)
Schoepe-Praun, Hella – Frau (21.)
Blümel, Marco – OTL (22.)
Büttner, Ralf – M (22.)
Glotz, Hans-Jürgen – O a.D. (22.)
Hommer, Eleonore – Frau (22.)
Keul, Jan – H (22.)
Sage, Ludwig – OL d.R. (22.)
Witt-Brummermann, Dr. Matthias – M d.R. (22.)
Zimmermann, Thomas – O i.G. (22.)
Decker, Lars-Thorsten – M i.G. (23.)
Jost, Silvio – OF (23.)
Schwarzenberger, Klaus – OTL a.D. (23.)
Weinrich, Gunter – OTL a.D. (23.)
Wuttke, Lars – SF (23.)
Ziebert, Julia – OL (23.)
Heckenthaler, Falko – M i.G. (24.)
Krick, Meinhard – OTL i.G. (24.)
Dietze, Wolfgang – OTL a.D. (25.)
Hoffmann, Lutz – OTL (25.)
Trawiel, Philipp – L (25.)
Wallenhauer, Torsten – OTL (25.)

Walter, Martin – OTL i.G. (25.)
Wurmb, Wolfgang – H d.R. (25.)
Voltmer, Kai – OTL (26.)
August, Joachim – O (27.)
Perchtold, Guido – OTL i.G. (27.)
Wollschläger, Stefan – H d.R. (27.)
Kaufmann, Arnd – M d.R. (28.)
Kaufmann, Patrick – H (28.)
Müller, Jürgen – H a.D. (28.)
Munker, Dirk – OTL (28.)
Larsen, L. Uwe – O a.D. (29.)
Schuhmeier, Siegfried – H d.R. (29.)
Schulz, Christian – Herr (29.)

Mai

Schmid, Ralph – OG d.R. (1.)
Würth, Andreas – OL (1.)
Brettschneider, Ekkehard – O a.D. (2.)
Grabau, Rudolf – O a.D. (2.)
Larsen, Uwe – O (2.)
Stütz, Josef – H a.D. (2.)
Riegger, Horst – HF d.R. (3.)
Ruff, Rainer – O d.R. (3.)
Vorländer, Jens – Fhj (3.)
Bender, Rolf – (5.)
Böhn, Hilmar – OTL a.D. (5.)
Görtz, Alfred – O (5.)
Ritz, Michael – OTL a.D. (5.)
Müller, Burckhardt-Uwe – G d.R. (6.)
Renkwitz, Toralf – SU d.R. (6.)
Scharfenberger, Ralf – OTL (6.)
Huber, Ralph – M d.R. (7.)
Hager, Helmut – O (8.)
Kulbarsch, Herbert K.A. – OTL a.D. (8.)
Blessmann, Carl-Heinz – LPD a.D. (9.)
Diederich, Horst – O a.D. (9.)
von Rom, Constantin – OTL a.D. (9.)
Wertmann, Heinrich – Fhj (9.)
Lömker, Wilhelm – O i.G. (10.)
Mayer, Andreas – (10.)
Mertens, Dr. Peter – OTL d.R. (10.)
Schäfer, Wolfgang – OTL (10.)
Tappe, Klaus – OTL a.D. (10.)
Will, Hannelore – Frau (10.)

Dubrau, Danila – H (w) (11.)
Fischer, Wilhelm – OSF (11.)
Spanagel, Eckhard – O d.R. (11.)
Müller, Ingo – OTL a.D. (12.)
Widinger, Rolf – OTL a.D. (12.)
Armbruster, Günther – OTL a.D. (13.)
Jahn, Tobias – OTL i.G. (13.)
Martwich, Dietmar – OTL (13.)
Paulowicz, Wolfgang – O a.D. (13.)
Achterkamp, Klaus – OTL (14.)
Grooz, Kurt – O a.D. (14.)
Krüger, Max – OL (14.)
Winzen, Günther – O i.G. (14.)
Balzer, Thomas – OTL (15.)
Kilian, Peter – O a.D. (15.)
Mack, Karl-Wolfgang – OTL a.D. (15.)
Schulze, Werner – H a.D. (15.)
Reiske, Edwin-Walther – OTL a.D. (16.)
Peelen, Hans-Jürgen – OTL i.G. (17.)
Wrobel, Paul – OTL a.D. (17.)
Geihsler, Hedwig – Frau (18.)
Barth, Winfried – OG d.R. (19.)
Geyer, Klaus – OTL a.D. (19.)
Mattick, Manfred – O a.D. (19.)
Praun, Dieter – (20.)
Rammin, Detlef – OSF a.D. (21.)
Wilde, Gert – OTL a.D. (22.)
Buchin, Dr. Boyd – H d.R. (23.)
Liedtke, Wolfgang – O a.D. (23.)
Scheckenbach, Ralf – OTL d.R. (24.)
Lange, Jörg – OTL a.D. (25.)
Otting, Klaus – M d.R. (25.)
Pinkenburg, Henrike – Frau (25.)
Schenk, Hartmut – OTL a.D. (26.)
Hake, Thorsten – H d.R. (27.)
Renkwitz, Rudolf – G d.R. (27.)
Wilhelm, Reinhard – OTL a.D. (27.)
Messner, Horst – O a.D. (28.)
Quenstedt, Walter – (28.)
Klein, Sascha – OTL (30.)
Löbens, Manfred – OTL (30.)
Wolfram, Dominik – OF (30.)
Ahrens, Bernd – OTL (31.)
Beisicht, Georg – OTL (31.)

Juni

Bäurle, Benedikt – OL (1.)
Fertl, Dietmar – SF (1.)
Beckmann, Andreas – OTL (2.)
Kempf, Peter – H (2.)
Willer, Theo – H a.D. (2.)
Baierl, Peter – O (3.)
Erler, Bodo – M (3.)
Hahn, Immo – HG d.R. (3.)
Straub, Wilhelm – OTL a.D. (4.)
Weiland-Dubois, Peter H. – OTL a.D. (4.)
Zander, Reinhard – (4.)
Brückner, Jochen – (5.)
Freytag, Klaus-Günter – OTL a.D. (5.)
Peters, Jessy – OL (6.)
von Ehrenkrook, Annette – Frau (6.)
Färber, Ewald – O a.D. (7.)
Gaube, Lothar – OTL a.D. (8.)
Haase, Thomas – OL (8.)
Kostorz, Alexander – OTL (8.)
Walisch, Reinhold – O a.D. (8.)
Botz, Manfred – OTL a.D. (9.)
Gallmeier, Gerfried – OTL a.D. (9.)
Kuhnigk, Alexander – OTL d.R. (9.)
Kühn, Michael – OTL a.D. (10.)
Patz, Ralf – OTL d.R. (10.)
Schamfuß, Axel – (10.)
Willers, Peter – OTL a.D. (10.)
Hempel, Mario – OTL d.R. (11.)

Leitsätze für die Führungsunterstützung
Aushang im Lehrsaal 3-30 der ITSBw

1.
Wir sind die **Berater** in Fragen der Führungsunterstützung. - Dies verlangt von uns das aktive Mitwirken bei Planungs- und Entscheidungs-Prozessen und Fachkompetenz!

2.
Wir meistern die **Herausforderungen der Gegenwart**! - Dies verlangt übergreifend und vorausschauend zu denken und zu handeln sowie Einfühlungsvermögen!

3.
Unser Denken und Handeln orientiert sich an den **Forderungen an die Führungsunterstützung**! - Operatives und taktisches Wissen zur Bewältigung der Herausforderungen der Einsätze ist eine Selbstverständlichkeit.

4.
Wir entwickeln die Führungsunterstützungstruppe der Zukunft vor dem Hintergrund der **Einsatzerfordernisse**! Dies verlangt die Fähigkeit, in TSK-gemeinsamen (joint) und multinationalen (combined) Zusammenhängen planen und handeln zu können.

5.
Als **militärischer Führer** von Verbänden, Einheiten und Teileinheiten **führen wir Menschen im Friedensdienst und Einsatz**. Dies verlangt Identifikation mit den Aufgaben, Vertrauen in das Können unserer Untergebenen und soziale Kompetenz!

6.
Wir sind uns unserer **dienenden Funktion** bewusst, wissen aber auch, dass unsere **Leistung unverzichtbar** ist, um in Frieden, Einsatz und Krieg bestehen zu können. Dies verlangt Selbstbewusstsein, Einsatzbereitschaft und Beherrschung unseres Handwerks.

7.
Wir wissen, dass **ohne Information erfolgreiche Führungsprozesse nicht ablaufen** können. Wir stellen die dafür notwendigen Mittel bereit und setzen Sie ein.

8.
Wir sind uns bewusst, dass wir zu den **Ersten gehören**, die im Operationsgebiet sind und zu **den Letzten, die es verlassen.** Dies erfordert Einsatzbereitschaft und Vorbildcharakter für uns und unsere Soldaten.

9.
Wie gehören zu den ersten, die mit **Streitkräften** und den **Menschen anderer Staaten** zusammentreffen. Das bedeutet, wir sind so ausgebildet, dass wir uns mit ihrem Kulturkreis auseinandersetzen können, interkulturelle Kompetenz haben und die Grundsätze und Mittel zum Sicherstellen der Interoperabilität beherrschen.

10.
Wir pflegen den **Zusammenhalt**, denn Führungsunterstützung kennt **keine Grenzen** zwischen den Führungsunterstützern in Heer, Luftwaffe, Marine, Streitkräftebasis, zentraler Sanitätsdienst!
Dies bedeutet selbstverständlich Zusammenarbeit in der Auftragserfüllung, Bescheidenheit im Zusammenwirken und Unterstützung unserer Kameraden.

11.
Wir pflegen unsere **Tradition** und sind **stolz** auf sie!

12.
Wir kennen die **Geschichte** unserer Fernmelde-, Nachrichten- und Telegrafentruppen und können sie in die **Zeitenumstände einordnen**.

13.
Leben, **Werk** und **Sterben** des Generals der Nachrichtentruppe Erich Fellgiebel sind für uns **Verpflichtung** und **Herausforderung**.

14.
Unsere **Identität** begründet sich in unseren **übergreifenden Aufgaben**, dem Wissen um die **Unverzichtbarkeit von Informationen** für erfolgreiche militärische Führung und nicht zuletzt dem Willen, **die moderne Informationstechnik** für unsere Aufgaben **zu nutzen**.

Vorname / Name	Telefon / E-Mail
Adresse	

Anmeldungen mit Hotelreservierung bitte unbedingt bis zum 5. März an geschaeftsstelle@fernmeldering.de

Frau
Hella Schoepe-Praun
Waldschmidtstraße 16

82327 Tutzing

Verbindliche Anmeldung

zum Jahrestreffen 2018 vom 20. bis 22. April 2018 in Potsdam

Ich/wir nehme(n)
am Jahrestreffen 2018 des Fernmeldering e.V. in Potsdam
an folgenden Programmpunkten teil:

Kameradschaftsabend am 20.04.2018 ab 19 Uhr
o ..... Person(en)

Mitgliederversammlung des Fernmeldering e.V. /
Vorträge zu aktuellen Themen am 21.04.2018 vormittags
o ..... Person(en)

Damenprogramm am 21.04.2018 vormittags
o ..... Person(en) zur Potsdam-Besichtigung

Besuch des Walds der Erinnerung am 21.04.2018
o ..... Person(en)

Festliches Abendessen am 21.04.2018 abends
o ..... Person(en)

Besichtigung der Friedenskirche in Sanssouci /
Teilnahme am Gottesdienst am 22.04.2018 ab 9 Uhr
o ..... Person(en)

Imbiss am 22.04.2018 um 11.30 Uhr
o ..... Person(en)

Potsdam-Besichtigung am 22.04.2018 nachmittags
o ..... Person(en)

Ich bitten um Reservierung eines Hotelzimmers
o für ..... Person(en) vom 20. bis 22. April zum Preis von 80 Euro (EZ) bzw. 108 Euro (DZ) p.N.
o für .....Person(en) zusätzlich vom ..... bis ..... April zum Preis von 98 Euro (EZ) bzw. 126 Euro (DZ) p.N.

Ich komme in Begleitung von (Vorname, Name) .....

Besondere Wünsche (z.B. zur Unterbringung, zum vegetarischen Essen, etc.):

.....

Datum Unterschrift

Fernmeldering e.V.
Schatzmeister
Oberst a.D. Peter Warnicke
Westerwaldstraße13

56244 Ötzingen

Beitrittserklärung

Ich erkläre meinen Beitritt zum Fernmeldering e.V. und zahle einen Jahresbeitrag in Höhe von EURO ..... ab..... einschließlich Abonnement für das Mitteilungsblatt „F-Flagge“. Der Mindestbeitrag beträgt EURO 15,00 jährlich. (Ausnahmen: Für Ehefrauen/-männer, Lebenspartnerinnen/-partner von Mitgliedern, die keine zusätzliche F-Flagge zugestellt haben wollen, beträgt der Mindestbeitrag EURO 10,00 jährlich.)

Name, Vorname .....

.....
geb. am Dienstgrad/Amtsbezeichnung

.....
Straße PLZ, Wohnort

.....
Telefon E-Mail

Ich bin einverstanden mit - Nichtzutreffendes bitte streichen:
* der Veröffentlichung meiner persönlichen Daten in der jährlichen Mitgliederliste: ja/nein
* der Veröffentlichung bei Änderungen meiner Anschrift, des Dienstgrades und des Dienstverhältnisses: ja/nein

.....
Datum Unterschrift

Freiwillige zusätzliche Angabe(n) zur jetzigen bzw. letzter Dienststelle bzw. Arbeitgeber

.....

Freiwillige zusätzliche Angaben: Wer hat Sie auf den Fernmeldering e.V. aufmerksam gemacht?

.....

SEPA-Lastschriftmandat
Gläubiger Identifikationsnummer: DE88ZZZ00000080641
Hiermit ermächtige ich den Fernmeldering e.V., meinen Jahresbeitrag in Höhe von EURO ..... ab ..... bis auf meinen Widerruf mittels Lastschrift einzuziehen. Zugleich weise ich mein Kreditinstitut an, die vom Fernmeldering e.V. gezogenen Lastschriften von meinem Konto einzulösen.
Hinweis: Ich kann innerhalb von 8 Wochen, beginnenden mit dem Belastungsdatum, die Erstattung des belasteten Betrages verlangen. Es gelten hierbei die mit meinem Kreditinstitut vereinbarten Bedingungen.

..... **.....**
Bezeichnung des Geldinstitutes Kontoinhaber mit Anschrift, wenn Kontoinhaber und Mitglied nicht identisch ist

DE_ _/ _ _ _ _ / _ _ _ _/ _ _ _ _ / _ _ _ _/ _ _ **.....**
IBAN **BIC**

.....
Ort Datum Unterschrift

Änderungs-Mitteilung

Frau
Hella Schoepe-Praun
Fernmeldering
Waldschmidtstraße 16

82327 Tutzing

Änderungs-Mitteilungen per eMail an
geschaeftsstelle@fernmeldering.de
kommen schneller an - und können so früher berücksichtigt werden!

Benützen Sie daher bitte das Formular
Änderungsmitteilung - online
Danke!

O **Meine Adresse hat sich geändert - NEUE ADRESSE:**

..... (Name)
..... (Straße)
..... (PLZ / Stadt)
..... (Telefon)
..... (E-Mail)

O **Mein Dienstgrad hat sich geändert - NEUER DIENSTGRAD:**

.....

O **Meine Dienststelle hat sich geändert - NEUE DIENSTSTELLE:**

..... (Dienststelle)
..... (Dienstposten)

O **Meine Bankverbindung hat sich geändert - NEUE KONTODATEN:**

DE_ _/ _ _ _ _ / _ _ _ _/ _ _ _ _ / _ _ _ _/ _ _ .....
IBAN **BIC** (entfällt wenn IBAN mit DE beginnt)

..... **Kontoinhaber** (mit Anschrift, wenn Kontoinhaber und Mitglied nicht identisch)

O **Mein Familienstand hat sich geändert - NEUER NAME:**

.....

Datum Unterschrift

Leitbild Fernmeldering

Wir ...

1) bieten die geistige Heimat für alle aktiven und ehemaligen Angehörigen des Führungsdienstes und damit der Führungsunterstützung, der Fernmeldetruppe, der Informationstechnik, der Elektronischen Kampfführung, der Operativen Information, des Radarführungsdienstes und der Stabsunterstützung, dabei für alle Dienstgrade und deren Angehörigen.

2) stehen zu den im Grundgesetz verankerten Grundsätzen einer wehrhaften und streitbaren Demokratie als Voraussetzung für Frieden, Freiheit und Sicherheit der Bundesrepublik Deutschland.

3) bieten geistige Orientierung und vermitteln Truppengattungsidentität für junge Offiziere und Unteroffiziere.

4) fördern den Erfahrungsaustausch zwischen ehemaligen und aktiven Angehörigen unserer Truppengattung sowie mit vergleichbaren ausländischen Organisationen.

5) leisten einen Beitrag zur Pflege der Kameradschaft unserer Mitglieder, im Sinne des Zusammenhaltes und der Tradition der Führungsunterstützung und der Fernmeldetruppe.

6) unterstützen im Einsatz verwundete Kameraden bzw. die Familien gefallener Kameraden unserer Truppengattung.

7) bewahren ein ehrendes Gedenken an unsere verstorbenen Mitglieder und bieten deren Hinterbliebenen auch weiterhin eine geistige Heimat.

8) fördern den fachlich / technischen Austausch mit der Industrie.

9) dokumentieren den Werdegang und unterstützen die historische Aufarbeitung der Geschichte unserer Truppengattung.

10) kennen unsere Wurzeln, bewältigen die Aufgaben der Gegenwart und stellen uns zukünftigen Herausforderungen.

Postvertriebsstück G 13839 Nr. 1, I. Quartal 2018
ISSN 1314-1334