Kontakt:
Thomas Reinhold
cyber-peace.org
0176/62863067
@Cyberpeace1

Analyse der Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten der Fraktion DIE LINKE

zum Thema:

Rechtlich-organisatorischer Rahmen militärischer Cyber-Operationen

Quellen

- Kleine Anfrage, Drucksache 19/11330
  http://dip21.bundestag.de/dip21/btd/19/113/1911330.pdf
- Antwort der Bundesregierung, Drucksache 19/11920
  http://dip21.bundestag.de/dip21/btd/19/119/1911920.pdf

In der hiermit analysierten Antwort der Bundesregierung auf eine kleine Anfrage der Bundestagsfraktion DIE LINKE geht diese auf unterschiedliche Aspekte zu den militärischen Planung zum Aufklären und Wirken im Cyberspace ein, sowie auf internationale Kooperationen von Ministerien zu Cybersicherheit im Allgemeinen und Cyber-Rüstungskontrolle im Besonderen. Die einzelnen Antworten werden nachfolgend in Bezug auf die jeweilige Fragestellung sowie die bisherigen Informationen und Angaben der Bundesregierung und beteiligter Ministerien thematisch zusammengefasst analysiert und bewertet.

0. Wichtigste Erkenntnisse / Auskünfte

- Pläne für "Hackbacks" oder "aktive Cyberabwehr" und rechtliche Fragen sind weiterhin in Abstimmung
- Bundesregierung geht von Schadsoftware u.a. auch in IT-Systemen kritischer Infrastrukturen in Deutschland aus
- Kauf bzw. Entwicklung von Schadsoftware durch die Bundesregierung wird explizit nicht verneint, sondern nur deren Einsatz
- Abschreckung von Cyberattacken durch Verbesserung der Resilienz
- Antwort enthält Auflistung zu Beteiligung an internationalen Kooperationen zu Cybersicherheit sowie gesondert zu Cyber-Abrüstung und Rüstungskontrolle
- Keine öffentliche Angaben zu aktuellen und geplanten Ressourcen und Mittel für offensive Cyber-Operationen
- Keine öffentliche Angaben zum Personal beim Lagezentrum Cyber- und Informationsraum der Bundeswehr, Berichte weiterhin mindestens VS-NfD

1. Zur Vorbemerkung der Bundesregierung über Förderung der IT-Sicherheit

Die Bundesregierung stellt ihren Antworten folgendes Kommentar voran, mit dem auf die einleitenden Anmerkung der ursprüngliche kleinen Anfrage eingegangen wird:

Die Behauptung der Fragesteller, für den Schutz der Sicherheit und Vertraulichkeit von IT-Systemen seien nur mäßige Aufwüchse personeller und finanzieller Art zu erkennen, wird von der Bundesregierung zurückgewiesen. Allein der Stellenhaushalt des Bundesamtes für die Sicherheit in der Informationstechnik (BSI), das nach § 1 Satz 2 des Gesetzes über das Bundesamt für Sicherheit in der Informationstechnik (BSIG) für die Informationssicherheit

auf nationaler Ebene zuständig ist, wuchs mit den Haushalten 2018/2019 um mehr als 50 Prozent auf. Für das Haushaltsjahr 2020 setzt sich die Bundesregierung für einen weiteren Stellenaufwuchs ein.

Diese Bemerkung der Bundesregierung geht an der ursprünglichen Kritik der Fragesteller vorbei. Das BSI ist auch mit der dargestellten Aufwertung ihrer Kompetenzen und Mittel primär für den Schutz der IT-Systeme der Regierungs- und in Teilen des Bundestages zuständig. Zivile Einrichtungen oder Unternehmen werden primär durch Aufklärungsmaßnahmen im Rahmen des Verbraucherschutz oder durch Sicherheitswarnungen unterstützt. Für besondere Sicherheitsvorfälle stehen auch sog. Mobile Incident Response Teams (MIRTs) bereit, die jedoch nur reaktiv agieren. Auch wenn diese Aktivitäten wichtig und begrüßenswert sind, reichen sie nicht aus um effektiv mittelfristig und gezielt eine sichere IT-Landschaft bei zivile Einrichtungen, Unternehmen und privaten Haushalten zu erreichen und aufrecht zu erhalten. Dafür wären weitaus stärkere, regulierend eingreifende Maßnahmen wie bspw. eine verpflichtende TÜV-Prüfung für IT-Endgeräte und Software oder die Einführung juristischer Haftungspflichten bei IT-Produkten notwendig. Neben diesen Aspekten ist anzumerken, dass in den vergangenen Monaten durch das BMI und das BMVg mehrere Agenturen gegründet, angekündigt oder mit Budgeterhöhungen ausgestattet worden sind, die sich im nachrichtendienstlichen oder militärischen Bereich dem Cyberspace widmen (bspw. die zentrale Stelle für Informationstechnik im Sicherheitsbereich ZITiS[1], der Cyber Innovation Hub der Bundeswehr[2], die Agentur für Innovationen in der Cybersicherheit[3]). Eine Verwertung der Ergebnisse oder Produkte aus diesen Aktivitäten für zivile Zwecke ist jedoch nicht vorgesehen und z.T. sogar explizit ausgeschlossen worden.

2. Zu dem Stand der Planung einer aktiven Cyberabwehr ("Hackbacks")

Hinsichtlich der regelmäßig durch unterschiedliche Ministerien geforderten Cyberabwehrmaßnahmen mit Hilfe von einem aktiven Eindringen in die IT-Systeme des (mutmaßlichen) Angreifers hält die Bundesregierung fest, dass sie den etablierten Begriff des "Hackback" formell nicht wendet:

Der von den Fragestellern verwendete Begriff „Hackback“ wird von der Bundesregierung konzeptionell grundsätzlich nicht verwendet, weder für Aktivitäten der Cyber-Abwehr noch der Cyber-Verteidigung. Der Beantwortung dieser Kleinen Anfrage legt die Bundesregierung die Begrifflichkeiten aus der Vorbemerkung der Bundesregierung in der Antwort auf die Kleine Anfrage der Fraktion der FDP auf Bundestagsdrucksache 19/2645 zugrunde.

In der bezeichneten Bundestagsdrucksache 19/2645[4] definiert die Bundesregierung den Begriff der "aktiven Cyberabwehr" wie folgt:

Cyber-Abwehr bezieht sich auf die zivile Abwehr aller Formen vorsätzlicher Handlungen, deren Ziel es ist, die Verfügbarkeit, Integrität und Vertraulichkeit von informationstechnischen Systemen mit informationstechnischen Mitteln zu manipulieren, zu beeinflussen oder zu stören und die keinen „bewaffneten Angriff“ im Sinne von Artikel 51 VN-Charta darstellen. Ein „Cyber-Gegenangriff“ ist insofern ebenfalls eine – aktive – Maßnahme der Cyber-Abwehr mit dem Ziel, die zum Angriff genutzten informationstechnischen Systeme mit informations- technischen Mitteln zu manipulieren oder zu stören. Maßnahmen in diesem Sinne bezeichnet die Bundesregierung als aktive Cyber-Abwehr.

1 https://cyber-peace.org/2018/10/30/kurz-notiert-steigendes-zitis-budget-fuer-2019-und-plaene-fuer-hochleistungsrechner/
2 https://cyber-peace.org/2017/04/04/cyber-fachkraefte-initiative-bei-der-bundeswehr/
3 https://cyber-peace.org/2018/10/17/weitere-details-und-unklarheiten-zur-agentur-fuer-innovationen-in-der-cybersicherheit/
4 https://dip21.bundestag.de/dip21/btd/19/026/1902645.pdf

Hinsichtlich der Frage, wie, unter welchen Bedingungen und gegen wen diese aktive Cyberabwehr eingesetzt werden könnten verweist die Bundesregierung leider nur wie bisher auf laufende Abstimmungen, konkretisiert aber, dass

Der Einsatz militärischer Fähigkeiten im Cyber-Raum erfolgt im Rechtsrahmen, der durch das Grundgesetz und das Völkerrecht gesteckt wird. Die gültigen Prozesse für Operationsplanung und -führung gewährleisten die politische Kontrolle des Einsatzes aller militärischer Fähigkeiten und beinhalten immer auch eine Risikoabschätzung.

3. Zur Frage der Abschreckung von Cyberattacken

Hinsichtlich den aktuellen Debatten zur Abschreckung von Cyberattacken, die vor allem in den USA mit einem Fokus auf das Konzept der "Abschreckung durch Vergeltung" geführt werden, verweist die Bundesregierung darauf, sich nicht an entsprechenden Plänen zu beteiligen. Im Gegensatz dazu wird auf die abschreckende Wirkung möglichst stabiler und resistenter IT-Systeme gesetzt: "*Die Erhöhung der eigenen Resilienz kann unter Umständen auch eine abschreckende Wirkung entfalten*"

4. Internationale Kooperation zum Thema Cybersicherheit

Die Antwort der Bundesregierung enthält die folgende Auflistung von Regierungsgremien und relevanten Ministerien, die sich an internationalen Kooperationen in Form von Gesprächsrunden, Verhandlungen etc. zu Themen der Cybersicherheit seit 2011 beteiligt haben.

Gremium	**Aktivität**
Bundeskanzleramt	Formate der unter deutscher Schirmherrschaft durchgeführten Münchner Sicherheitskonferenz
	Potsdamer Konferenz für Nationale Cybersicherheit
Auswärtiges Amt	NATO Cyber Defence Committee
	Gruppe der Regierungssachverständigen der Vereinten Nationen zum Thema internationale Cybersicherheit (GGE) 2012 – 2013, 2014 – 2015 sowie, unter deutschem Vorsitz, 2016 – 2017
	Horizontale Ratsarbeitsarbeitsgruppe der Europäischen Union zu „Fragen des Cyberraums“ sowie deren Vorgängerformation „Gruppe der Freunde der Ratspräsidentschaft zu Cyberfragen“
	Informelle Arbeitsgruppe Informations- und Kommunikationstechnologie der Organisation für Sicherheit und Zusammenarbeit in Europa (OSZE)
	„Freedom Online Coalition“, eine informelle Koalition von 30 Staaten aus fünf Kontinenten, die sich außenpolitisch für Menschenrechte im Internet einsetzt
	Wassenaar-Arrangement für die Exportkontrolle konventioneller Rüstungsgüter und Güter mit doppeltem Verwendungszweck (Dual-Use Güter) und von Technologie in Bezug auf Genehmigungspflichten für den Export bestimmter Schadsoftware (Wahrnehmung gemeinsam mit BMWi).

	Anlassbezogene multilaterale oder bilaterale Gespräche zum Thema Cybersicherheit
Bundesministerium des Innern, für Bau und Heimat	Horizontale Ratsarbeitsgruppe der Europäischen Union zu Cybersicherheits-angelegenheiten „Fragen des Cyberraums“ sowie deren Vorgängerformation „Gruppe der Freunde der Ratspräsidentschaft zu Cyberfragen“
	Kooperationsgruppe nach Artikel 11 der Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. Juli 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union
	GGE der Vereinten Nationen zum Thema internationale Cybersicherheit (unter Federführung des Auswärtigen Amts)
	Regelmäßiger Austausch mit strategisch wichtigen Partnern innerhalb und außerhalb der EU zu übergeordneten Fragen der Cybersicherheitspolitik
Bundesministerium der Verteidigung:	Capability Panel Information Assurance and Cyber Defense der Substruktur des Command and Control Consultation Board der NATO
	Steering Committee des NATO Cooperative Cyber Defence Centre of Excellence
	Bilaterale Dialoge im Rahmen des bilateralen Jahresprogramms des Bundesministeriums der Verteidigung sowie mit NATO- und EU-Partnern
	GGE der Vereinten Nationen zum Thema internationale Cybersicherheit (unter Federführung des Auswärtigen Amts)
	Informelle Arbeitsgruppe Informations- und Kommunikationstechnologie der Organisation für Sicherheit und Zusammenarbeit in Europa (unter Federführung des Auswärtigen Amts)
Bundesministerium der Finanzen:	Horizontale Ratsarbeitsgruppe der Europäischen Union zu Cybersicherheits-angelegenheiten „Fragen des Cyberraums“ sowie in deren Vorgängerformation „Gruppe der Freunde der Ratspräsidentschaft zu Cyberfragen“
	G7 Cyber Experts Group
	G7 Cross Border Coordination Exercise Working Group
	Financial Stability Board: Cyber Lexicon Working Group
	Regelmäßiger bilateraler Austausch zu Cyberthemen im Finanzsektor mit ein-zelnen EU-Staaten, USA und Israel

Ergänzend zu dieser Auflistung sei auf die Auswertung der Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der FDP – Drucksache 19/2032 verwiesen[5], zu den Cyberabteilungen im Zuständigkeitsbereich der Bundesministerien. Diese enthält eine Liste aller staatlichen deutschen Institutionen mit den jeweiligen Aufgabenbereichen die Cybersicherheit und Cyberabwehr umfassen sowie gesondert den Ressourcen für Cyber-Abwehr / direkt mir Cyber-Abwehr und Gegenangriffen befasstes Personal.

5. Internationale Kooperation zum Thema Cyber-Abrüstung und Rüstungskontrolle

Die Antwort der Bundesregierung enthält darüber hinaus die folgende Auflistung von Regierungsgremien und relevanten Ministerien, die sich an internationalen Kooperationen in Form von Gesprächsrunden, Verhandlungen etc. spezifisch zu Themen der "*Abrüstung und Rüstungskontrolle in der Cyber-Kriegsführung*" seit 2011 beteiligt haben.

Gremium	**Aktivität**
Auswärtiges Amt	Gruppe der Regierungssachverständigen der Vereinten Nationen zum Thema internationale Cybersicherheit (GGE) 2012 – 2013, 2014 – 2015 sowie, unter deutschem Vorsitz, 2016 – 2017
	Informelle Arbeitsgruppe Informations- und Kommunikationstechnologie der Organisation für Sicherheit und Zusammenarbeit in Europa
	Internationale Rüstungskontroll-Konferenz „2019. Capturing Technology. Rethinking Arms Control.“ am 15. März 2019 in Berlin
Bundesministerium der Verteidigung	GGE der Vereinten Nationen zum Thema internationale Cybersicherheit (unter Federführung des Auswärtigen Amts)
	Informelle Arbeitsgruppe Informations- und Kommunikationstechnologie der Organisation für Sicherheit und Zusammenarbeit in Europa (unter Federführung des Auswärtigen Amts)
	Internationale Rüstungskontroll-Konferenz „2019. Capturing Technology. Rethinking Arms Control.“ am 15. März 2019 in Berlin (unter Federführung des Auswärtigen Amts)

Ergänzend zu dieser Auflistung sei auf die Auswertung der Antwort der Bundesregierung auf die Kleine Anfrage der Fraktion der FDP – Drucksache 19/2032 verwiesen[6], zu den Cyberabteilungen im Zuständigkeitsbereich der Bundesministerien. Diese enthält eine Liste aller staatlichen deutschen Institutionen mit den jeweiligen Aufgabenbereichen die Cybersicherheit und Cyberabwehr umfassen sowie gesondert den Ressourcen für Cyber-Abwehr / direkt mir Cyber-Abwehr und Gegenangriffen befasstes Personal.

6. Zu fremden "Software-Implantaten" in KRITIS-Systemen Deutschlands

Auf Nachfrage zum "*Vorhandensein von Software-Implantaten anderer Staaten zum Monitoring von Computersystemen in kritischen Infrastrukturen in Deutschland*" antwortet die Bundesregierung, dass "*das Vorhandensein von Software-Implantaten in Computersystemen kann für jegliche IT-Infrastruktur durch die Bundesregierung nicht grundsätzlich ausgeschlossen werden*"

5 https://cyber-peace.org/2018/06/30/deutsche-cybersicherheit-und-abwehr-alle-staatlichen-institutionen-mit-kapazitaeten-sowie-perspektive-der-bundesregierung/

6 https://cyber-peace.org/2018/06/30/deutsche-cybersicherheit-und-abwehr-alle-staatlichen-institutionen-mit-kapazitaeten-sowie-perspektive-der-bundesregierung/

Diese Einschätzung ist vermutlich realistisch, bedeutet aber gleichzeitig auch, dass die Bundesregierung davon ausgehen muss, dass fremde Staaten in der Lage sein könnten IT-Systeme in Deutschland gezielt zu stören oder eventuell sogar zu zerstören. Aus technischer Sicht besteht kaum ein relevanter Unterschied zwischen Cyber-Spionage ("Monitoring") und Cyber-Sabotage, da in jedem Fall die gleichen Mittel für den Zugriff auf ein fremdes IT-System aufgewendet werden müssen um Schutzmaßnahmen zu umgehen und Hintertüren zu etablieren. Aus Sicht des Angreifers ist es lediglich eine Frage des Intention, welchen "Payload" auf infiltrierten Systemen ausgelöst wird. Etablierte Hintertüren und Zugriffsmöglichkeiten können demnach auch genutzt werden um IT-Systeme gezielt zu schädigen.

7. Zur Beschaffung, Entwicklung und den Einsatz von "Software-Implantaten" durch Deutschland

Die Nachfrage ob die Bundesregierung "*die Entwicklung oder Beschaffung vergleichbarer Software-Artefakte zur Verwendung in kritischen Infrastrukturen anderer Staaten ausschließt*" wird wie folgt beantwortet:

Die Bundesregierung schließt aus, Software-Artefakte im Sinne der Fragesteller ohne die entsprechenden, insbesondere völkerrechtlichen, Rechtsgrundlagen einzusetzen

Damit wird weder die Beschaffung, noch die Entwicklung entsprechender Mittel verneint, sondern nur der Einsatz derartiger Mittel. Dies untermauert Mutmaßungen, dass insbesondere mit der neuen Agentur für Innovation in der Cybersicherheit Mittel zum offensiven militärischen und nachrichtendienstlichen Wirken im Cyberspace geschaffen werden soll[7], unabhängig ob und unter welchen Bedingungen diese eingesetzt werden können (siehe Punkt 2).

8. Zu Ressourcen zum offensiven Wirken der Bundeswehr im Cyberspace & Kooperationen

Im Zuge der Einrichtung des Kommandos Cyber und Informationsraum (KdoCIR) wurde die seit 2005 bestehende Einheit für "Computer Netzwerk Operationen" (CNO) zum Zentrum für Cyberoperationen (ZCO) aufgewertet. Dazu wurde die Bundesregierung gefragt, welche personellen Ressourcen und Mittel sie für offensive Cyber-Operationen einzusetzen erwägt und welche Einrichtungen und Kapazitäten zum jetzigen Zeitpunkt bestehen.

Leider wird diese Frage durch die Bundesregierung nicht beantwortet bzw. auf bereits bestehende Auskünfte zur organisatorischen Aufteilung der Dienste und Ministerien verwiesen[8]. Eine darüber hinausgehende Antwort erfolgt in einer, als „VS – Nur für den Dienstgebrauch“ eingestufte Anlage.

Hinsichtlich Kooperation des KdoCIR bzw. des ZCO mit privaten Unternehmen sowie weiteren Training mit "Red-Teaming"[9], also dem Üben von Cyberattacken als simulierter Angreifer in einem Testszenario, erklärt die Bundesregierung, dass es "neben der einmaligen Kooperation des ZCO mit der Firma CGI (..) keine weiteren Kooperationen des ZCO mit privaten Firmen" gegeben hat. Darüber hinausgehend waren ZCO-Soldaten bei der diesjährigen NATO-Cyberübung "Locked Shields" in der Rolle des "Red Teams" beteiligt.

Eng verbunden mit dem Training zum offensiven Einwirkungen auf fremde IT-Systeme wurde danach gefragt, ob der in Verhandlung befindliche "EU-Rahmen zur Beantwortung böswilliger Cyberaktivitäten"[10] "*nach Auslegung der Bundesregierung auch Bestimmungen enthält, die – nach Vorliegen rechtlicher Voraussetzungen – ein Eindringen der Bundeswehr*

7 https://cyber-peace.org/2019/07/04/updates-zur-cyberagentur-von-bmvg-bmi-zu-standort-rechtsform-und-offizieller-kritik/
8 https://cyber-peace.org/2018/06/30/deutsche-cybersicherheit-und-abwehr-alle-staatlichen-institutionen-mit-kapazitaeten-sowie-perspektive-der-bundesregierung/
9 https://de.wikipedia.org/wiki/Red_Team
10 Dies bezieht sich auf den „Cyberdiplomatischer Reaktionsrahmen“ der Verordnung (EU) 2019/796 des EU-Rates vom 17. Mai 2019 und Beschluss (GASP) 2019/797 des EU-Rates

in ausländische staatliche Informationssysteme und das Stören oder Abschalten derselben diplomatisch unterstützen kann?". Laut Antwort der Bundesregierung enthält der „Cyberdiplomatische Reaktionsrahmen“ und die Umsetzungsleitlinien jedoch keine Bestimmungen, "*die in die Prärogative der Mitgliedstaaten für ihre nationale Sicherheit eingreifen*".

9. Angaben zum gemeinsame Lagezentrum Cyber- und Informationsraum der Bundeswehr

In ähnlicher Weise wie die Antwort zum ZCO lehnt die Bundesregierung öffentliche Angaben zum Personal des gemeinsamen Lagezentrum Cyber- und Informationsraum (GLZ CIR) der Bundeswehr ab. "Im GLZ werden fusionierte Lagebilder erstellt und Zusammenhänge in bisher nicht zusammengeführten Daten erkannt sowie analysiert"[11]. Weitere Antworten erfolgen in der, als „VS – Nur für den Dienstgebrauch“ eingestuften Anlage.

Die im GLZ erstellten Lagebilder sind "*je nach Schutzbedürftigkeit, in einem Spektrum von „VS – Nur für den Dienstgebrauch“ bis „Geheim“ eingestuft*"

Die Lagebildaufklärung im Cyberspace ist, im Gegensatz zu klassischer Aufklärung bspw. mit Hilfe von Satelliten, deutlich sensibler zu handhaben. Relevante Informationen die über öffentlich verfügbare Quellen hinausgehen sind oft nur durch Analysen von fremden IT-Systemen zu erzielen. Dies trifft umso mehr zu, je stärker Informationen über relevante Ziel zusammengetragen werden müssen, die innerhalb komplexer IT-Netzwerke verknüpft und nicht direkt ans Internet angeschlossen sind. In solchen Fällen müssten Mitarbeiter der Bundeswehr oder kooperierender Dienste in diese fremden IT-Systeme eindringen um sich Zugang zu relevanten Informationen verschaffen. Diese Aktivitäten sind jedoch, selbst wenn sie nur der Aufklärung dienen sowohl völkerrechtlich als auch technisch problematisch da mit dem Eindringen die fremden Systeme gefährdet werden und potentiell versehentlich schadhafte Effekte ausgelöst werden könnten. Die Bundesregierung hat sich bislang nicht explizit geäußert wie derartige Effekte vermieden werden sollen bzw. wo die "rote Linie" für Aktivitäten der Bundeswehr bzw. kooperierender Nachrichtendienste in Friedenszeiten gezogen wird.

10. Weitere Themen

Die kleine Anfrage enthält darüber hinaus noch weitere Fragen, die über die hier analysierten militärische Nutzung des Cyberspace hinausgehen. Dazu zählen

- Stand zu deutsch-französischen Kooperationen zur Cybersicherheit und Cyberabwehr insbesondere im Rahmen des Aachener Vertrages sowie zu Planungen für gemeinsame Projekte
- Stand des Projektes des Auswärtigen Amtes zur Krisenfrüherkennung anhand der Analyse von Big-Data und Social Media-Informationen
- Stand zur Einrichtung eines „Kompetenzzentrums Krisenfrüherkennung“ bei der Bundeswehr
- Stand zur bilateralen Zusammenarbeitsvereinbarung zwischen dem Allied Command for Transformation (ACT) und der Universität der Bundeswehr München (UniBw M)
- Zum Umfang der Datensammlungen durch Bundesbehörden zur Analyse der Urheberschaft von Cyber-Angriffen
- Zur Unabhängigkeit des CertBW von ZCO-Aktivitäten trotzdem erfolgter gemeinsamer Verortung innerhalb des KdoCIR
- Zum Stand und der möglichen Verlängerung des Pilotprojekt „Metis“
- Zum Beitrag Deutschlands zu einem EU-weit gemeinsamen Verständnis der hybriden Bedrohungen und den daran beteiligten deutschen Institutionen

Für Rückfragen oder weiterführende Einschätzungen stehe ich gern zur Verfügung.

11 https://www.behoerden-spiegel.de/2019/04/09/bsi-praesident-zu-gast-im-kommando-cir/