PFREUNDSCHUH
in Heidelberg

GERHARD PFREUNDSCHUH

Bausteine des Bürgerstaats

5.4 Dienst in der Cyberwehr

Inhalt

5.4 Dienst in der Cyberwehr……197

5.4.1 Die Lage……197

5.4.2 Die Strategie……199

5.4.3 Die operative Umsetzung……...…200

technischen Bereich, die einen betriebswirtschaftlichen Aufsetzer erwerben wollen, um ins höhere Management aufzusteigen.

Inzwischen sind die MBA aus weiteren Gründen in die Kritik geraten. Eine große Abhandlung im Handelsblatt über fünfeinhalb Seiten erklärte warum. Mehr als 60 % eines Jahrgangs gehen zu Finanzdienstleistern. Dort ist schneller und mehr Geld zu verdienen. Finanzdienstleister produzieren nicht Güter und Werte, sondern machen aus Geld neues und mehr Geld. „Viele Studenten haben kein Interesse daran, für große, komplexe Unternehmen zu arbeiten." Noch belegen es nicht die Zahlen, aber es ist die Hoffnung weitblickender Professoren:

> „Ich sehe eine neue Generation von Studenten", sagt er [= Dekan einer Managerschule]. Sie interessieren sich stärker für Unternehmensführung, fürs Gründen, für Ethik und Geisteswissenschaften oder Technologie. Für ihn steht fest, dass sich die Managementhochschulen ändern, weil sich ihr Publikum ändert."[391] – Hoffen wir das Beste!

5.4 Dienst in der Cyberwehr

5.4.1 Die Lage

*Wie ist die **sicherheitspolitische Lage**? Wir leben mitten in einem weltweiten, gnadenlosen Cyberkrieg. Dabei vermischen sich Militär- und Wirtschafts-Spionage sowie gezielte Angriffe auf Personen und Einrichtungen aller Art. Im Cyberkrieg wird heute abgehört und zerstört.*

Der Präsident des Bundesamts für Verfassungsschutz, Thomas Haldenwang, meinte, die Geheimdiensttätigkeit sei heute stärker und gewalttätiger als im Kalten Krieg. Er spricht von einer alarmierenden Brutalisierung der Spionage mit Gewalt und Morden. Und es arbeiteten heute in Deutschland mehr ausländische Geheimdienste als vor 1989.[392] Keine Spur von „friedlichem Eine-Welt-Dorf". Herkömmliche Spionage und Cyberkrieg sind verschmolzen.

Hacker und Spione, Saboteure und Terroristen greifen unsere Wirtschaft und staatlichen Einrichtungen an. Im Krisenfall können sie diese

[391] Handelsblatt, „Spezial: MBA", vom 18.10.2013, S. 14 ff (15)
[392] DIE ZEIT , 08. 10. 2020, „Es wurden gezielt Menschen getötet"

lahmlegen. Hinzu kommen EP (empfindliche Punkte) der Infrastruktur wie Strom- und Wasserversorgung, Fernmeldeeinrichtungen usw. Auch staatliche Hacker können wie Sagoteure und Terroristen große Schäden anrichten. Oft ist die Grenze unklar, der Angriff „asymmetrisch".

Die Verwundbarkeit zeigte kürzlich der großflächige Ausfall der Benzinversorgung in den USA. Hacker hatten eine 8.850 km lange Pipeline lahmgelegt. „Die Rohre von Colonial transportieren 45 Prozent der Treibstoffe für die Ostküste. Die Benzinpreise an den Tankstellen ziehen bereits an. Auch einzelne Flughäfen könnten im Laufe der Woche Versorgungsprobleme bekommen."[393] Die wohl „privaten" Hacker wollten „Lösegeld". Von meiner dort lebenden Tochter weiß ich, es gab einige Tage kein und dann kaum Benzin.

Wer spioniert? Wer agiert? Zu nennen sind China, Russland, die Türkei (z.B. wegen der Gülan-Bewegung), der Iran (wegen hier lebender Regimegegner) u.a. Hinzu kommen Hobby-Hacker und Internet-Dienste (Google u.a.), die im Netz und bei Programmen Daten abgreifen.

Haldenwang wählt dann eine geschickte Umschreibung, die keine Länder wie die USA nennt. Er sagt es so: „Wir mussten in der Vergangenheit lernen, dass auch Länder Angriffe gegen Deutschland vornehmen, mit denen wir eigentlich partnerschaftlich verbunden sind und intensiv zusammenarbeiten." Wir ermitteln heute in alle Richtungen. Im Handelsblatt steht es deutlicher:

> „In den sensibelsten Bereichen der Mobilfunknetze in Deutschland stecken neben europäischen Anbietern schließlich nicht nur Komponenten von Huawei, sondern auch Geräte des US-Anbieters Cisco. Wenn es die Bundesregierung mit der Sorge um die Sicherheit unserer Netze wirklich ernst meint, dann sollte sie sich auch Komponenten dieses amerikanischen Herstellers vorknöpfen."[394]

Was wird ausgespäht?

- das Militär und die Politik,
- unsere Wirtschaft und Technik (Werk- und Wirtschaftsspionage),
- einzelne Personen (Dissidenten, angebliche Staatsfeinde im Exil),
- Bürger in ihrem Privatleben.

[393] Handelsblatt, 10.05.2021; https://archiv.handelsblatt.com/document?id=HBON__HB+27177356&src=hitlist
[394] HB 06.02.2019, Scheinheilige Debatte

Die Schwerpunkte sind unterschiedlich. Russen treiben mehr klassisch-militärische Spionage. Dazu kommen Falschmeldungen, Desinformation. Haldenwang meint, wenn wir letzteres aufdecken und veröffentlichen, stellen die Russen diese Tätigkeit oft ein. Chinesen wollen vor allem Wissen, unsere Technologie; aktuell sind der Corona-Impfstoff und unser Gesundheitssystem betroffen. Ähnliches gilt auch für andere Staaten, „die Neuentwicklungen planen und nicht über die notwendigen Forschungskapazitäten verfügen". Die Türkei und der Iran interessieren sich für ihre hier lebenden Landsleute und bedrohen sie gegebenenfalls.

> „Ausländische Dienste sind daher sehr an deutscher Politik interessiert, an unserer Außenpolitik, unserer Rüstungspolitik, aber auch an Forschungspolitik und aktuell Gesundheitspolitik."[395]

5.4.2 Die Strategie

Es ist Aufgabe der Politik, eine Strategie zu entwickeln, die unser Land, seine Bürger und sein Einrichtungen vor Cyberangriffen schützt. Denn immer, wenn der Einzelne oder einzelne Institutionen zu schwach für ihre Verteidigung sind, ist die höhere Gemeinschaft, hier der Staat, zur Schutzgewährung verpflichtet. Deshalb haben wir u.a. den Staat.[396]

Dabei darf sich eine Cyberwehr nicht verzetteln. Sie muss sich auf das Wesentliche und Wichtige beschränken. Das sind die Militär- und die Wirtschaftsspionage. Gerade das Rückgrat unserer Wirtschaft, die KMU, sind mit einer Cyberabwehr überfordert. Der Staat, und zwar das Militär ist damit gefordert. Die gefährlichsten Angreifer sind staatlich-militärische Einrichtungen. Chinesen, Russen, aber auch Amerikaner unterscheiden nicht zwischen Militär-, Rüstungs- und Wirtschaftsspionage.

Bei uns fällt – wie so oft in der Bundespolitik – die Aufteilung der Zuständigkeit auf die verschiedensten Ministerien unangenehm auf:

> „Die Cyber-Abwehr unterliegt der Verantwortung des ***Bundesministeriums des Inneren***, während das ***Auswärtige Amt*** für die Cyber-Außen- und internationale Cybersicherheitspolitik verantwortlich ist. Verteidigungsaspekte der gesamtstaatlichen Cyber-Sicherheitsarchitektur werden gemäß Weißbuch

[395] Thomas Haldenwang in: Die ZEIT, 08.10.2020

[396] Die Schutzpflicht nach innen und außen ist uralt. Schon im Schwabenspiegel (1275/76) heißt es: „Wir sollen den Herren dienen, damit sie uns beschirmen. Und beschirmen sie uns nicht, sind wir ihnen keinen Dienst schuldig nach dem Recht."

> 2016 als originäre Aufgaben des ***Bundesministeriums der Verteidigung*** und als verfassungsgemäßer Auftrag der Bundeswehr zugewiesen.“[397]

So hat das Bundesinnenministerium 2016 die „Cybersicherheitsstrategie“ entworfen.[398] Doch die Trennung von äußerer und innerer Sicherheit ist bei der heutigen „hybrider und asymmetrischen Kriegführung“ nicht mehr möglich.[399] Denn man muss das Ganze vor den Teilen sehen.

Es bedarf einer generalstabsmäßigen Gesamtstrategie. Daher ist nach unserer Vorstellung die Cyberwehr der richtige Auftragnehmer. Die ernsten Angriffe kommen auch von außen (fremde Staaten, Konzerne).

5.4.3 Die operative Umsetzung

Hier können wir ein gutes mit einem schlechten Beispiel vergleichen. Das schlechte betrifft Deutschland, das gute Israel.

In Erkenntnis der Lage hat 2017 die Verteidigungsministerin Ursula von der Leyen das ***Kommando Cyber- und Informationsraum (CIR)*** zur Verteidigung Deutschlands im Cyberkrieg eingerichtet.[400] Doch es ist nur *„Bedingt abwehrbereit 4.0“* (2019), wie die WirtschaftsWoche zeigt.[401]

In der Cyberstrategie der Bundeswehr heißt es:

> „Ähnlich wie Heer, Luftwaffe und Marine für die Dimensionen Land, Luft, Weltraum und See zuständig sind, sind die Angehörigen des neuen Organisationsbereiches ganzheitlich für die Dimension Cyber- und Informationsraum[402] verantwortlich.“

Das spricht für eine eigene ***Teilstreitkraft „Cyberwehr“;*** bisher ist es nur ein eigener Organisationsbereich, der keiner Teilstreitkraft angehört.

---

[397] https://www.bundeswehr.de/de/organisation/cyber-und-informationsraum/auftrag

[398] Herunterladen als PDF-Datei (46 Seiten) unter: https://www.bundeswehr.de/resource/blob/89756/6b2dcb8af248db01ea3e338d8a54e8bb/cybersicherheitsstrategie-data.pdf

[399] ***Hybride Kriegsführung*** (***verdeckte Kriegführung***) ist die Kombination von konventionellen und irregulären Kampfweisen in Verbindung mit terroristischen Aktionen und kriminellem Verhalten (Terror, Sabotage). Sie kennen keine „Kriegserklärung“ und kein Kriegsvölkerrecht; keine offenen Kriege!
Asymmetrische Kriege (ungleiche Kriege) sind solche, bei denen sich eine militärische starke und eine schwache Partei gegenüberstehen. Der Schwache verwendet i.d.R. die „hybride Kriegführung“.

[400] Stärke: Aktive Soldaten: 13.439 (Juli 2020); davon Frauen: 1.305

[401] WirtschaftsWoche, 15.11.2019: „Bedingt abwehrbereit 4.0“

[402] Informationsraum sind alle Medien, die Nachrichten erzeugen und verbreiten (z.B. Presse, TV, Internet).

Dabei ist bei uns die größte Schwierigkeit, geeignetes Personal zu gewinnen. Das gilt für Friedenszeiten, aber erst recht für Krisen oder den Ernstfall. So will die Verteidigungsministerin eine „Reserve“ aufbauen. Doch ohne Wehrpflicht wird das scheitern. Etwas Erfolg hatte man mit ehemaligen Wehrpflichtigen, die noch dem Reservistenverband angehören. Sie werden aber weniger und älter. So sagt ein Oberst d.R., der beim Cyberkommando mitmacht:

> „Deutlich schwerer ist es, Neulinge aus der Wirtschaft [als aus dem Reservistenverband] für die Bundeswehr zu begeistern. ‚Die Bundeswehr ist lange nicht mehr so präsent in der öffentlichen Wahrnehmung, seit die Wehrpflicht ausgesetzt ist‘, sagt Mario Hempel, langjähriger IT-Berater beim deutschen Softwarekonzern SAP und zugleich Oberst der Reserve. ‚Viele junge Leute, und damit auch die Top-IT-Experten, die wir suchen, kommen nicht auf die Idee, dass sie auch in der Cyberreserve eine spannende Aufgabe finden könnten.‘“[403]

Auch die wichtige Kooperation mit Wirtschaftsverbänden, die Ursula von der Leyen vorhatte, sei oft zäh und frustrierend, erzählt Hempel, „weil die Bundeswehr häufig als Fremdkörper wahrgenommen wird“. Deshalb wollen Unternehmen auch keine IT-Leute für Reserveübungen freistellen. Dabei wäre der Wissensaustausch von Cyberwehr und Unternehmen für beide Seiten sehr wichtig. Doch wie es aussieht, ist unter den gegenwärtigen Bedingungen keine Besserung, keine ernst zu nehmende Abwehrbereitschaft im Cyberkrieg zu erwarten.

Wie es geht, zeigt **Israel.** Dort ist es sogar umgekehrt; ein Großteil des Wissens fließt von der Armee zur Wirtschaft.

> „Ein großer Teil der CybersecurityExpertise entsteht in der Armee-Einheit 8200, in der junge Menschen zu Cyberspionen ausgebildet werden. Die größte Einheit der israelischen Armee ist für die Fernmelde- und elektronische Aufklärung sowie für die Entschlüsselung von Codes zuständig. Sowohl männliche als auch weibliche Soldaten arbeiten mit Big Data, analysieren Algorithmen und lernen, im Team und unter Zeitdruck Probleme zu lösen. Die Frauen werden nach zwei Jahren aus der Armee entlassen, die Männer nach knapp drei Jahren. Danach reißen sich die Cyberfirmen um sie. ‚Die Armee ist das größte Start-up Israels und vielleicht der Welt‘, sagte kürzlich der Generalstabschef Aviv Kochavi.“[404]

[403] WirtschaftsWoche, 15.11.2019

[404] Handelsblatt, 05.08.2019, „Warum Israel so wichtig für das autonome Fahren ist“

Mit KI, Sensoren und Cybersicherheit wird in und um Tel Aviv an der Zukunft des autonomen Fahrens gearbeitet. Fast alle großen Autounternehmen wie BMW, Daimler, VW mit Porsche, Skoda und Audi, aber auch Ford, Renault und Nissan sind im israelischen „Silicon Wadi“. Sie lassen Israelis forschen und entwickeln.

Und nur in Israel setzen Volkswagen, Audi, Porsche und Daimler bei der Forschung auf Frauen, die den Ton angeben und die Teams führen. „Bei der Cyberfirma Cymotive, die zu 40 Prozent Volkswagen gehört, leitet die 27-jährige Urit Lanzet die Forschungsabteilung.“

> „Die starke Präsenz der Frauen hat viel damit zu tun, dass Frauen, die im Alter von 18 Jahren rekrutiert werden, in der israelischen Armee gleiche Startchancen und Möglichkeiten haben wie Männer – auch auf technischen Gebieten.“[405]

Wir kommen zu einem ***Ergebnis***. Nicht nur wegen Abwehr und Angriff im Cyberkrieg, sondern auch wegen Forschung und Entwicklung in diesen Zukunftstechnologien braucht die Bundeswehr eine mit Israel vergleichbare Cyberwehr. – Und wir brauchen eine allgemeine Dienstpflicht, die die Nachwuchs- und Personalprobleme für das Militär und (!) die Wirtschaft löst. Um die Besonderheit als technische Truppe herauszustreichen, könnte die Cyberwehr die beliebten Uniformen der Marine bekommen. Das schafft Gemeinschaftsgefühl, Stolz, Erfolgslust.

In der Teilstreitkraft Cyberwehr können unsere jungen Internet- und KI-Freunde eine zivilberuflich nutzbare Grund-, Fach- und Vollausbildung durchlaufen. Heute lassen sich viele halbprofessionelle IT-„Spezialisten“ als Freiberufler nieder und bieten ihre Dienstleistungen an. In der Cyberwehr muss es aufeinander aufbauende, praxisbezogene Lehrgänge mit Abschlüssen geben. Die Wirtschaft und die Kunden wissen dann, was sie erwartet, worauf sie sich verlassen können.

Dazu kann die Cyberwehr in Abstimmung mit der DUA und der Wirtschaft ggf. gezielte, für Zivilisten offene Schulungen und Lehrgänge anbieten. Sie müssen straffer und praxisnäher als herkömmliche universitäre Fort- und Weiterbildungen sein. Das zeigt auch der Vergleich des dreijährigen Bundeswehr-Studiums mit den deutlich längeren Studienzeiten an den öffentlichen Hochschulen.

[405] Handelsblatt, 05.08.2019