Cyber-War heißt Krieg im Internet

Friedensthemen in verständlicher Sprache vermitteln

60% der Deutschen verstehen keine Fachsprache, 5% können nur mittels Leichter Sprache erreicht werden (Netzwerk Inklusion, 2020). In der Entwicklung des Projektes „Cyberwar verstehen – Cyberpeace mitgestalten" der Ev. Arbeitsgemeinschaft für Kriegsdienstverweigerung (KDV) und Frieden (EAK) wurde deutlich, dass die bislang als Grundlage für Friedensbildung vorliegenden Informationen zum Thema Cyberwar abstrakt und schwer verständlich sind, beispielsweise die Publikation: Werkner; Schörnig: Cyberwar- die Digitalisierung der Kriegsführung. Springer, 2019. An der Kundgebung der EKD-Synode von 2019 wurde sichtbar, dass selbst auf synodaler Ebene noch nicht ausreichend Wissen vorhanden ist, um eine auch in Fachkreisen anerkannte Stellungnahme mit Zielen zu verfassen.

Maike Rolf
ist Mediatorin, Friedens- und Konfliktforscherin und Referentin für Friedensarbeit in der Ev. AG für KDV und Frieden in Bonn.

Auch in der Friedensarbeit gibt es Wissenslücken: Viele Personen haben noch keinen Zugang zum Wissen über „neue Kriegsführung" gefunden. Fundiertes Wissen über Friedensthemen muss so vielen Menschen wie möglich zugänglich gemacht werden. Deswegen geht es der EAK in ihrem Projekt und diesem Artikel darum, die Mechanismen der Kriegsführung im virtuellen Raum so zu vermitteln, dass jede*r sie verstehen kann.

Das Projekt der EAK besteht aus Bausteinen, die bedarfsorientiert genutzt werden können. Das ist zum einen ein Spiel in Form einer App für mobile Endgeräte. Hier geht es um die Beschäftigung mit Gewissensfragen und Verstehen der Problematiken durch das Treffen von Entscheidungen („was tun, wenn") und punktuelle Wissensvermittlung. Ein weiterer Bestandteil sind Begleitmaterialien in digitaler und analoger Version: um Multiplikator*innen passende Bausteine anzubieten, werden die Informationen in den Begleitmaterialien in zwei Verständlichkeitsstufen zur Verfügung gestellt.

In diesem Artikel werden Grundlagen zum Thema Cyberwar erläutert. Anhand dessen soll verdeutlicht werden, welche Wirkung Texte in verschiedenen Verständlichkeitsstufen haben. Es werden beispielhaft einige Fachinhalte in Standardsprache, vereinfachter Standardsprache und Leichter Sprache erklärt und nebeneinandergestellt.

Um insgesamt möglichst viele Menschen zu erreichen, ist es wichtig, Informationen in verständlicher Sprache zur Verfügung zu stellen. Darum haben Initiativen wie Inclusion Europe und das Netzwerk für Leichte Sprache die Leichte Sprache als Instrument zur Vermeidung von Ausgrenzung entwickelt. Mittlerweile gibt es dafür einen Leitfaden, feste Kriterien, zahlreiche Online-Angebote sowie Testleser*innen, die testen ob ein Text tatsächlich verständlich geschrieben wurde. Das Leseniveau liegt bei A1. Grundsätze sind beispielsweise leserfreundliches Layout (linksbündig, große Schrift), Nebensätze vermeiden, Verben statt Substantive, Fachbegriffe unmittelbar erklären, Aktiv statt Passiv, kein Konjunktiv oder Genitiv und Beispiele geben. Neben der Leichten Sprache gibt es auch die vereinfachte Standardsprache, auch Einfache Sprache genannt; hier liegt das Sprachniveau bei A2/B1, es gibt jedoch bisher kein Regelwerk dafür. Sie macht einen normalsprachlichen Eindruck, vermeidet aber komplizierte Sprachelemente. Laut Netzwerk Inklusion können 60% der Deutschen Texte nicht verstehen, die komplexer als die vereinfachte Standardsprache sind. In Ansätzen gibt es mittlerweile Lexika für verständliche Sprache (www.hurraki.de; www.bpb.de/nachschlagen/lexika/lexikon-in-einfacher-sprache) und einen Leitfaden für Leichte Sprache (www.bmas.de). Auch gibt es Konzepte für sprachsensiblen Unterricht. Kernelement ist, inhaltliche und sprachliche Lernziele gemeinsam zu betrachten. In der Umsetzung gilt es, zwischen Darstellungsformen zu wechseln und Sprachhilfen anzubieten.

Dieser Artikel fokussiert sich auf Beispiele für Leichte und vereinfache Standardsprache auf sprachlicher Ebene. Er soll anregen, ganzheitlich sprachsensible Lernsituationen zu schaffen. Die folgenden Textbausteine zeigen

Fachsprache	Leichte Sprache
Der Begriff Cyberwar beschreibt eine kriegerische Auseinandersetzung zwischen Staaten im virtuellen Raum, die mit Mitteln der Informationstechnologie geführt wird. Ein Cyberkrieg hat zum Ziel, Ländern, Institutionen oder der Gesellschaft auf elektronischem Weg Schaden zuzufügen und wichtige Infrastrukturen zu stören. **Dabei werden häufig drei Szenarien thematisiert:**	**Cyber-War ist Englisch und bedeutet Krieg im Internet. Das Ziel von Cyber-War ist: auf elektronischem Weg Ländern Schaden zufügen. Digitale Technologie wird immer wichtiger in unserem Leben. Diese digitale Technologie wird angegriffen, damit sie nicht mehr funktioniert. Davor haben viele Menschen Angst. Die Technologien sind neu. Darum wissen viele Menschen nicht, was passieren kann.** **Es gibt 3 Gefahren:**
1. unsichere Infrastruktur: **Sicherheitslücken in Software und punktuelles Ausnutzen derer geschieht sehr häufig. Sicherheitslücken sind die Munition für den Cyberwar.**	*1. Software sagt dem Computer, was er machen muss, wenn ein Mensch eine Taste drückt.* **Ein anderes Wort ist: Computerprogramm. Software hat eine virtuelle Mauer, um sich vor Angriffen zu schützen. Manchmal gibt es Löcher in der Mauer. Diese Löcher heißen Sicherheits-Lücken. Manche Menschen suchen die Sicherheitslücken. Diese Menschen heißen Hacker. Manche Hacker wollen etwas kaputt machen oder Informationen klauen. Oft arbeiten sie im Auftrag von einem Land oder sind Kriminelle. Das passiert sehr oft. Diese Sicherheits-Lücken machen Angriffe und Cyber-War möglich.** **Das nennt man: un-sichere Infra-Struktur.**

Fachsprache	Leichte Sprache
2. komplette Infiltration: Systeme sind gehackt und infiltriert. Dies wird teilweise als Verhandlungsmasse genutzt, denn die Bedrohung ist zu wissen, dass „die Anderen" dies technisch machen könnten.	*2. Hacker können durch die Sicherheits-Lücken in einer Software die ganze Software kaputt machen* oder alle Informationen klauen. Zum Beispiel: persönliche Konto-Daten. Oder Geheimnisse aus der Regierung. Oder die Strom-Versorgung in einem Krankenhaus. Das nennt man: komplette Infiltration. Das passiert selten. Aber es ist eine große Bedrohung. Denn wir wissen: das ist möglich. Manchmal droht ein Land einem anderen Land damit. Um seinen Willen zu bekommen.
3. aktiver Cyberkrieg: konkrete Angriffe im virtuellen Raum sowie mit konventionellen Waffen, Tote und Verletzte. De facto das meistbesprochene, aber am wenigsten relevante Szenario.	*3. Elektronische Angriffe, Tote und Verletzte.* Zum Beispiel: ein Land macht über das Internet die Strom-Versorgung in Deutschland kaputt. Dann funktioniert nichts mehr. Chaos entsteht. Die Krankenhäuser können nicht mehr richtig arbeiten. Deutschland wirft Bomben auf das andere Land, damit sie aufhören. Das nennt man: aktiver Cyber-Krieg. Viele Menschen reden darüber. Aber das passiert wahrscheinlich nicht.

eine von vielen Möglichkeiten, Wissensvermittlung sprachsensibel zu gestalten.

Zum inhaltlichen Thema ist grundsätzlich zu sagen, dass militärische Operationen heute immer über eine Cyberdimension verfügen und die verschiedenen Dimensionen ineinander greifen: Waffen und Strategien im konventionellen sowie im virtuellen Raum, teilweise sogar automatisiert. So werden z.B. Drohnenangriffe durch die Ortung von Zielpersonen vorbereitet. An dieser Stelle wird die Abgrenzung zu automatisierten und autonomen Waffensystemen notwendig. Autonome und automatisierte Waffensysteme ermöglichen eine kriegerische Auseinandersetzung im konventionellen Raum mit Mitteln der Informationstechnik (sowie teilweise im virtuellen Raum). Automatisierte Waffensysteme wie eine bewaffnete Drohne, die ferngesteuert wird, aber eigenständig starten, landen und vorgegebene Strecken abfliegen kann, werden standardmäßig von der Bundeswehr genutzt. Doch der Übergang zu autonomen Waffensystemen ist fließend, insbesondere von hochgradig automatisierten, hin zu autonomen Waffensystemen. Autonome Waffensysteme Letztere können Tätigkeiten selbst und ohne menschliche Kontrolle ausführen. Im Falle von künstlicher Intelligenz kann ein System sich sogar neue, nicht programmierte Fähigkeiten aneignen und danach handeln (innerhalb des ihm von der Programmierung zugewiesenen Bereichs). Autonome Waffensysteme verstoßen gegen das Völkerrecht (Human Rights Watch; International Human Rights Clinic: heed the call- a moral and legal imperative to ban killer robots, 2018).

Aus diesen Zusammenhängen ergeben sich ethische Problematiken, auf die wir in den Bildungsmaterialien eingehen. Unklar ist, wann es sich im Cyberraum um einen Angriff nach völkerrechtlichem Verständnis handelt, der das Recht auf Selbstverteidigung nach sich zieht. Außerdem schließt sich die Frage an, wie herausgefunden und bewiesen werden kann, wer einen Angriff ausgeführt hat. Diese Attribution von Angriffen zu Staaten ist häufig problematisch: Nur wenn ein staatlicher Befehl an einen nichtstaatlichen Akteur, z.B. eine Hackergruppe nachweisbar ist, kann ein Staat verantwortlich gemacht und als Ziel für einen Selbstverteidigungsschlag identifiziert werden. Das ist schwierig, da Angriffe oft über Geräte von unbeteiligten Dritten laufen oder sogar explizite False-Flag-Operationen sind, die unter falscher Flagge durchgeführt werden. Eine weitere Herausforderung ist, dass im digitalen Raum die Grenze zwischen Angriff und Verteidigung verschwimmt. Selbstverteidigung ist nur erlaubt, wenn sie notwendig und verhältnismäßig ist, und so lange bis der Cyberangriff beendet ist. Jedoch lassen sich die konkreten Folgen von Angriff und Abwehr im Cyberraum schwer abschätzen. Die Bundeswehr will in Zukunft autonome Hackbacks – also offensive Verteidigungsschläge – durchführen, wobei Algorithmen autonom und ohne menschliche Bestätigung den Gegenschlag ausführen sollen. Der wissenschaftliche Dienst des Bundestags stuft dies als illegal ein.

Die Problematik, die mit Dual-Use-Technologien einhergeht, wird in den folgenden Textbausteinen nicht nur in zwei, sondern in drei Verständlichkeitsstufen erläutert. Dies eröffnet

Oft ist nicht so ganz leicht auszumachen, wer im Krieg der gute und wer der Böse ist. Darth Vader jedenfalls ist böse trotz oder gerade wegen seiner Sehnsucht nach Erlösung. Foto: Unsplash/Josh Howard

Fachsprache	Vereinfachte Standardsprache/Einfache Sprache	Leichte Sprache
Dual Use-Technologien sind doppelverwendungsfähige Technologien oder Produkte, die für zivile und militärische Zwecke genutzt werden können. Im Fall der europäischen Firma FinFisher wurden Produkte von deutschen Sicherheitsbehörden gekauft, aber während des arabischen Frühlings auch an das autoritäre Regime in Bahrain exportiert, um dort gegen Oppositionelle vorzugehen. Als Versuch, damit umzugehen, gibt es die Dual-Use-Verordnung der EU, seit 2015 wird darin auch Überwachungstechnologie erfasst. Solche Exporte werden jedoch meistens genehmigt. Friedensorganisationen fordern daher strenge Prüfungen anhand von moralischen Gesichtspunkten. Ein weiterer Versuch, mit umzugehen ist das Hackertoolverbot in der BRD. Seit 2008 ist es strafbar, Sicherheitslücken durch Testprogramme ausfindig zu machen, weil diese Programme auch für das Eindringen in fremde Systeme genutzt werden können. Dadurch ist es allerdings auch illegal, Sicherheitslücken durch Tests zu suchen um sie zu reparieren.	Oft können Technologien für militärische und nicht-militärische Zwecke verwendet werden, das sind sogenannte Dual-Use-Technologien. Ein Beispiel ist die Firma FinFisher, deren Produkte von deutschen Sicherheitsbehörden gekauft werden. Gleichzeitig werden diese Produkte auch von der autoritären Regierung in Bahrain genutzt, um gegen Menschen vorzugehen, die die Regierung kritisieren. Als Versuch, mit diesem Dual-Use-Problem umzugehen, gibt es die Dual-Use-Verordnung der EU. Wenn ein Unternehmen bestimmte Güter und Technologien exportieren will, muss es das jeweils beim Zoll beantragen. Wie in dem Beispiel zu sehen ist, trifft der Zoll oft leider falsche Entscheidungen. Das kann aus Unwissenheit, wirtschaftlichen Interessen oder sogar Korruption passieren. Friedensorganisationen fordern, dass der Zoll die Anträge strenger prüft und gewissenhaft entscheidet.	Digitale Technologie wird immer wichtiger in unserem Leben. Oft kann die gleiche Technologie für militärische und nicht-militärische Zwecke benutzt werden. Das sind Dual-Use-Technologien. Zum Beispiel: Die Firma FinFisher verkauft Software an Deutschland. Die Software kann manchmal Terroristen über das Internet finden. Die Firma FinFisher verkauft die gleiche Software auch an andere Länder. In dem Land Bahrain bestraft die Regierung Menschen, die eine andere Meinung haben. Dafür hat die Regierung die Software von FinFisher gekauft. Dann wird die Software benutzt, um Menschen zu bestrafen. Eigentlich hatte die Software einen guten Zweck. Darum prüft der Zoll jedes Mal, ob eine Dual-Use-Technologie an andere Länder verkauft werden darf oder nicht. Leider entscheidet der Zoll oft falsch. Dann kann die Technologie trotzdem für schlechte Dinge benutzt werden. Friedens-Organisationen fordern: der Zoll muss die Exporte strenger prüfen. Ein Export darf nur erlaubt werden, wenn er keine Menschen-Rechte gefährdet. Wenn der Export erlaubt wird, nur damit Deutschland mehr Geld verdient, dann ist das schlecht.

eine Möglichkeit, verständliche Sprache in diesem Artikel differenzierter kennen zu lernen.

Abschließend lässt sich sagen, dass verständliche Sprache den*die Autor*in zwingt, präzise zu formulieren. Verständliche Sprache nimmt der Sprache zahlreiche Facetten und Schönheit, kann aber auch neue Schönheiten eröffnen. Details gehen zum Teil verloren, denn um auch die Textlänge angemessen zu gestalten, müssen zwangsläufig Informationen weggelassen werden. Und es ist eine Herausforderung, einen Text in verständlicher Sprache zu schreiben: selbst die Beispiele im vorliegenden Artikel können sicher noch einfacher formuliert werden. Weitere Schritte sind graphische und symbolische Darstellungen als Ergänzung zum Text. Doch es lohnt sich: Bereits der Versuch befähigt eine große Zahl von Kindern und Erwachsenen dazu, eigenständig Informationen einzuholen, sich fortzubilden und damit auch sich eine Meinung zu bilden. Friedensethische Bildung an alle Menschen heranzutragen, ist unerlässlich für Inklusion, gesellschaftlichen Zusammenhalt und eine breite zivilgesellschaftliche Beteiligung an politischen Prozessen. Nur wer von friedensethischen Themen weiß, kann sich für den Frieden einsetzen.

Interessierte können sich über Neuigkeiten zum EAK-Projekt „Cyberwar verstehen- Cyberpeace mitgestalten“ ab 2021 informieren unter: www.eak-online.de.

rolf@eak-online.de