Sechstes Gebot

Digitalisierte Gewalt unterbrechen

Sechstes Gebot: „Du sollst nicht töten.“ (Ex 20,13)

Kapitel 2.6 aus „Freiheit digital. Die Zehn Gebote in Zeiten des digitalen Wandels, S. 124-144, Evangelische Kirche in Deutschland, Evangelische Verlagsanstalt GmbH, Leipzig, 2021.

2.6 Digitalisierte Gewalt unterbrechen

Sechstes Gebot: „Du sollst nicht töten." (Ex 20,13)

a) Einführung: „Slaughterbots"[27]

Der fiktive Kurzfilm ‚Slaughterbots' zeigt eine Verkaufsshow nach dem Muster populärer Produkteinführungen für elektronische Geräte. Ein Mann in grauem Anzug und T-Shirt präsentiert kleinste Flugdrohnen: Außer einer Zieleingabe bedürfen sie keiner Lenkung von außen. Neben ihrer Sensorik und Steuerung sind sie mit Explosivladungen bestückt. Sie treten im Schwarm auf. Sie töten gezielt Menschen: Man kann nach Aussage des Verkäufers ohne eigenes Risiko eine halbe Stadt töten – „aber natürlich nur die böse Hälfte". Im Film folgen auf die Schau Collagen fiktiver Nachrichtenclips. Darin geht es um gezielte Mordanschläge auf Menschen in der Politik oder Studierende – verübt von solchen Robotern, Urheberschaft nicht

27 Slaughterbots: Automatisierte Kampfroboter.

feststellbar. Der Film ist Teil einer ihrerseits hochumstrittenen Kampagne gegen hochautonome tödliche Waffensysteme und gibt Anlass zu Fragen: Wie gehen wir mit menschlicher Verantwortung um? Was bedeutet uns Sicherheit? Ist der Einsatz solcher Systeme realistisch?

b) Bibelauslegung: Das sechste Wort unterbricht Kreise der Gewalt

Das sechste Wort ist sehr knapp. Ursprünglich regelte es vorrangig das Verhalten innerhalb einer gegebenen Gemeinschaft. In diesem Kontext verbietet es, den Tod anderer Gemeinschaftsangehöriger absichtlich herbeizuführen. Es soll Mord vermeiden und so Gewalt begrenzen. Auch das Talionsrecht (Ex 21,24f.; Lev 24,20f.) soll Gewalt einhegen: Das „Auge um Auge, Zahn um Zahn" fordert Verhältnismäßigkeit der Reaktion und durchbricht so die Eskalationslogik der Blutrache (Gen 4,23). Ähnlich ist auch das sechste Wort im Sinne der Gewalteinhegung in einer Gesellschaft zu verstehen, der ein Rechtssystem mit staatlichem Gewaltmonopol und dem Ziel gewaltloser Konfliktbewältigung unbekannt ist. Allerdings wurde das Wort bald umfassender verstanden, sodass es die Tötung von Menschen überhaupt problematisiert. Ursprünglich galt der Schutz nur den Gemeinschaftsangehörigen. Ausgedehnt wird er nun auf die im Land lebenden Nichtisraelitinnen und -israeliten (Lev 24,22). Außerdem wird zunehmend jedes Töten von Menschen sanktioniert. So etwa im Noahbund: „Und das Leben des Menschen will ich einfordern von einem jeden anderen Menschen. Wer Menschenblut vergießt, dessen Blut soll um des Menschen willen vergossen werden; denn Gott hat den Menschen zu seinem Bilde gemacht" (Gen 9,6). Völlig auf kriegerische tödliche Gewalt verzichten zu können, bleibt aller-

dings zunächst eine messianische Verheißung (Sach 9,10). Die jesuanische Torainterpretation legte nahe, völlig auf Vergeltung zu verzichten (Mt 5,39) und die Feinde zu lieben (MT 5,44). Auf dieser Linie liegt die universale Ausweitung des Tötungsverbots. Deshalb lässt sich sagen: Die Texte der Bibel tendieren dazu, Gewalt zu unterbrechen. Der Zusammenhang von Gewalt und Gegengewalt führt nach der Logik von Sicherungsbedürfnis, Angst und wechselseitiger Verletzung zur Eskalation. Diese Eskalationslogik soll unterbrochen werden. Immer wieder erzählen die biblischen Texte solche Gewaltunterbrechungen: Sie skandalisieren etwa den Totschlag – es ist die Geschichte von Kain und Abel, in welcher hebräische Begriffe für das, was im Deutschen „Sünde" genannt wird, zum ersten Mal erscheinen (Gen 4,7.13); die Bergpredigt problematisiert Vergeltung und Feindschaft überhaupt.

c) Gewaltunterbrechung ermöglicht Freiheit

Diese Tendenz legt nahe: Die biblischen Texte verstehen Gewalt und Tötung nicht als Ausübung, sondern als Bedrohung menschlicher Freiheit vor Gott. Der Noahbund verbietet das Blutvergießen. Die Verbindung dieses Verbots mit der Gottebenbildlichkeit der Menschen lässt einen Grund für das Tötungsverbot erkennen, der mit Freiheit zu tun hat: Gott betrachtet die Menschen als Gottes Ebenbilder und beauftragt sie mit Haushalterschaft. Ebenbildlichkeit und Auftrag weiten die menschlichen Verfügbarkeitsrechte aber nicht schrankenlos aus. In der ersten Schöpfungserzählung (Gen 1,29) enden die Verfügungsrechte am Leben der Tiere – Menschen dürfen sich nur vegetarisch ernähren. Der Noahbund erscheint als Zugeständnis an die Bosheit der Menschen (Gen 8,21–22). Darin wird das Vergießen des Blutes von Menschen und der Genuss

des Blutes von Tieren verboten (Gen 9,4–6), weil das Blut als Sitz des Lebens gilt, über das Gott allein verfügen kann. Damit ist die Tötung von Menschen durch Menschen immer auch als sündhafter Versuch zu deuten, sich der Freiheit Gottes zu bemächtigen und also absolute und totale Verfügungsmacht zu erlangen.

Dieser Versuch muss als vermessen gelten, schon, weil menschliche Erkenntnis endlich und begrenzt ist. Aber dieser Versuch hat historisch in der Regel zur Eskalation von Gewalt und zum Verlust von Freiheit geführt. Deswegen nimmt moderne Bibelauslegung zunehmend das Potenzial einer Sicht wahr, die auf Gewalteinhegung und -unterbrechung gerichtet ist. Angesichts der Faktizität von Gewalt zielt Gewalteinhegung auf ihre Begrenzung; begrenzt wird Gewalt vor allem dadurch, dass unerwartetes Verhalten oder alternative Konfliktlösungen die Kreisläufe der Gewalt und Eskalationsspiralen unterbrechen.

In reformatorischer Sicht kommen andere Menschen nicht vorrangig als Grenzen, sondern vor allem als Ermöglichung der Freiheit in den Blick. Insofern bedeutet der gewaltsame und vorzeitige Tod der Anderen auch eine Verarmung der individuellen Freiheit. Beide Aspekte, der Blick auf die Freiheit Gottes und die Berücksichtigung der Bedingungen der Freiheit der Menschen, haben nicht nur dazu geführt, dass Menschen die Todesstrafe problematisiert und vielerorts abgeschafft haben. In Verbindung mit Einsichten zur Dynamik des modernen Krieges und unter dem Eindruck der Entwicklung von Massenvernichtungswaffen haben besagte Aspekte Menschen christlichen Glaubens auch dazu gebracht, das Konzept des gerechten Krieges zugunsten eines Leitbilds des gerechten Friedens zu verlassen. Dieses Leitbild eines gerechten Friedens ist in einer

Reihe von kirchlichen Äußerungen vorbereitet, in der Friedensdenkschrift von 2007 dargelegt und in der Synodenerklärung von 2019 bekräftigt worden. Die besondere Pointe dieser Konzeption liegt darin, die Möglichkeit ernst zu nehmen, Kriege zu vermeiden. Daher genießen im Leitbild gerechten Friedens außer- wie innerstaatliche gewaltfreie, zivile Konfliktlösungen mit dem Ziel nachhaltiger Friedensentwicklung Priorität: Neben die theologischen Argumente der Gewaltunterbrechung treten dabei Einsichten, die Menschen auch unabhängig von ihrer weltanschaulichen Prägung einsehen können. Nachhaltig lässt sich tödliche Gewalt nämlich nur vermeiden, wenn gewaltlose Mittel der Konfliktbearbeitung institutionalisiert und gerechte Partizipations-, Teilhabe- und Anerkennungsverhältnisse ermöglicht werden. Die Androhung oder Ausübung von Gewalt kann so nur allerletzte Möglichkeit sein, noch Schlimmeres zu verhindern. Sie muss strikt darauf ausgerichtet sein, das Recht zu wahren oder zu etablieren, das zentraler gewaltfreier Konfliktlösungsmodus ist. Strenge Kriterien müssen Gewaltandrohung und -ausübung begrenzen.

d) Digitalisierung und tödliche Gewalt – zur Situation

Auch im Zusammenhang tödlicher Gewalt spielen die Informations- und Kommunikationstechnologien eine erhebliche Rolle, insbesondere die Vernetzung und Bearbeitung von ‚big data', die Beschleunigung, Diversifizierung und Ausdehnung der Datenmengen möglich gemacht haben. Selbstverständlich sollen an dieser Stelle nur Schlaglichter auf die verschiedenen Themenfelder im Kontext der Digitalisierung geworfen werden, um auf die nötigen weitergehenden Klärungen in der verzweigten friedensethischen Debatte hinzuweisen, wie sie etwa jüngst in einem kirchlich initiierten Konsultationsprozess angestoßen wurde.

Dies betrifft erstens den Themenkomplex der sogenannten „Cybersicherheit". Die zunehmend computergestützte Steuerung militärischer Instrumente und Prozesse, aber auch ziviler Großtechnologien hat diese anfälliger gemacht für elektronische Schädigungen etwa durch Schadsoftware. Nicht nur im militärischen Bereich, sondern auch etwa bei Angriffen auf die Computersysteme eines Krankenhauses oder Atomkraftwerks können diese Schädigungen tödliche Folgen haben.

Es betrifft zweitens den Einsatz hochautomatisierter, autoregulativer tödlicher Waffensysteme, die nach Definition des Einsatzziels ohne unmittelbare menschliche Einwirkung operieren können. Autoregulative Systeme erreichen ein vorgegebenes Ziel unter wechselnden Umweltbedingungen ohne menschlichen Eingriff. Gefördert wurden solche Systeme etwa durch die 2004 und 2005 von der DARPA initiierten Rennen in der Mojave-Wüste („DARPA Grand Challenge"). Die Convention on Certain Conventional Weapons (CCW) verhandelt schon seit 2014 über die internationale Kontrolle entsprechender Waffensysteme, allerdings bisher weitgehend ergebnislos.

Ein dritter Bereich ist der Einsatz von Mustererkennungsverfahren im Zusammenhang präventiver Polizeiarbeit. Die Polizei nutzt dabei Algorithmen, um mögliche tatverdächtige Personen und Opfer von Gewaltverbrechen präventiv zu identifizieren – wie etwa im Kontext der „Strategic Subject List" der Polizei von Chicago.

Cybersicherheit

Die Gefahren durch Phänomene elektronischer Schädigung lassen sich nach der Schadensschwere, den Tatmotiven, der

Urheberschaft und den Begleitumständen klassifizieren (Niklas Schörnig 2019): Auf der untersten Stufe rangiert der belästigende, oft zivilgesellschaftlich motivierte „hacktivism“[28], den man im günstigen Fall als Form zivilen Ungehorsams, im ungünstigen als groben Unfug an der Grenze zur Kriminalität verstehen kann. Gravierender ist die illegale, vorwiegend finanzielle Schädigung anderer zur Erringung eigener finanzieller Vorteile, die als „cybercrime“ beschrieben werden kann. Noch problematischer ist der politisch motivierte Datendiebstahl („cyber espionage“) oder gar die politisch motivierte physische Schädigung anderer durch die Beeinträchtigung lebenswichtiger oder unfallträchtiger Infrastruktur, die „cyberterror“ genannt wird. Die höchste Schädigungs- und Gefährdungsstufe ist dem „cyberwar“ zuzuordnen. Niklas Schörnig schreibt diese Gefährdung staatlichen Akteuren zu, die die Verteidigungsfähigkeit eines anderen Staates herabsetzen wollen. Vom „cyberwar“ nimmt Schörnig an, dass er mit kinetischen Schädigungen einhergeht. Allerdings sind die Grenzen zwischen diesen Kategorien verschiebbar, weil sich auch staatliche oder parastaatliche Akteure kriminell oder terroristisch engagieren können und kriminelle oder terroristische nichtstaatliche Akteure sich entsprechender Mittel zu bedienen vermögen. Damit ist es alles andere als selbstverständlich, elektronische Schädigungen im Kriegsparadigma zu verstehen. Oft werden alle möglichen elektronischen Schädigungen unter dem Begriff des „cyberwar“ zusammengefasst – das ist irreführend und problematisch. Denn schließlich spielen die Probleme, die mit den Herausforderungen der elektronischen Schädigung verbunden sind, in allen Schädigungskontexten eine zentrale Rolle: Schädigungen

28 Hacktivism: Kombination der Begriffe „Hack“ und „Aktivismus“ ist ein Akt des Einbrechens in ein Computersystem zu politisch oder sozial motivierten Zwecken.

treffen überraschend und ohne Vorwarnung ein, sind kaum zu den Verursachern zurückzuverfolgen und können mit relativ schwachen Mitteln große Schäden anrichten, die Wirkasymmetrie ist maximal.

Für die Frage der Gewaltunterbrechung sind die Bedrohungen kritischer ziviler Infrastruktur besonders bedeutsam. Sowohl cyberterrorism als auch cyberwar können diese Infrastruktur bedrohen. Deshalb lassen sich diese Bedrohungen aufgrund der oben beschriebenen Mechanismen nicht einfach unter die Überschrift „Krieg" oder die Überschrift „Verbrechen" einordnen. Damit ist die Schutzzuständigkeit fraglich: Für den Zivilschutz im Verteidigungsfall ist bisher vorrangig das Bundesministerium des Inneren zuständig, für den Katastrophenschutz sind es die jeweiligen Bundesländer, und der „Organisationsbereich Cyber- und Informationsraum" der Bundeswehr sorgt hauptsächlich für den Schutz der militäreigenen IT sowie die Aufklärung im Cyberraum.

Zahlreiche Entwicklungen fordern gegenwärtig die Friedenssicherung heraus: Die internationalen Beziehungen der Gegenwart sind gekennzeichnet durch Multipolarität und eine Abkehr vom Internationalismus zugunsten nationaler Perspektiven. Hinzu kommen die Herausforderungen durch Klimawandel und politische Disruptionen. Das internationale Völkerrechtssystem zeigt sich geschwächt. Die digitale Technologie kann dabei Konflikte verschärfen: Früh industrialisierte Staaten können ihre Waffenarsenale, Konfliktszenarien, ihre politischen und militärischen Strategien Schritt für Schritt den neuen digitalen Möglichkeiten anpassen – anders als nichtstaatliche Akteure, die Konflikte unter den Bedingungen fragiler politischer Ordnungen austragen, wobei Armut und

Klimawandel diese Konflikte oft anfachen. Der digitale Wandel gewaltsamer Konfliktaustragung verschärft so die Asymmetrien: Auf der einen Seite treiben die starken Staaten mit forschungsintensiven und wissensbasierten Ökonomien den digitalen Wandel voran. Die relativ leicht zugänglichen digitalen Alltagstechnologien erreichen auch die andere Seite, die Konfliktparteien im globalen Süden und ihre weniger leistungsstarken Ökonomien.

Auch digitale Technologien selbst bedrohen die Friedenssicherung: Im Bereich des Militärs erlauben sie eine immense Beschleunigung und erhöhen so die Gefahr nicht-intendierter Konflikte. Die sogenannte „Kill-Chain", die Kette von Zielerkennung, Zielfokussierung und Waffeneinsatz (detecting, targeting, strike) kann automatisiert immer schneller ablaufen. Ging es bislang vorrangig um kinetische Angriffe auf gegnerische „Hardware", stehen heute „Cyberattacken" auf die militärische „Software" und gesellschaftliche Steuerungskapazitäten (kritische Infrastruktur) im Fokus der Kriegführung.

Mit diesen Entwicklungen sind strategische Fragen verbunden, die noch weitgehend ungeklärt sind, auch wenn das sogenannte „Tallinn-Manual" von 2013 Cyberangriffe nach Artikel 51 der UN-Charta als kriegerische Akte wertet, die Selbstverteidigung ermöglichen. Seit 2016 erfasst die Beistandsverpflichtung des NATO-Vertrages auch Cyberangriffe. Die herkömmliche Doktrin (atomarer und konventioneller) Abschreckung beruht auf Transparenz und Zurechenbarkeit von Angriff und Reaktion. Die Logik von Cyberattacken ist eine andere: Nichtzurechenbarkeit und Intransparenz. Das stellt vor die problematische Alternative von reaktivem, präventivem oder präemptivem Umgang.

Diese Entwicklungen sind auch in den früh industrialisierten Staaten nicht unproblematisch. Denn im Zuge dieser Entwicklung kehren sich diese Staaten von der Idee ziviler Sicherung ab und tendieren dazu, die Gewährleistung von Sicherheit und den Schutz vor Gewalt vorrangig von den Agenturen des Gewaltumgangs, Militär und Polizei, zu erwarten, zumal militärische und polizeiliche Tätigkeiten in Zeiten von Friedensmissionen und Terrorabwehr immer mehr verschwimmen.

In der scheinbar binären Alternative zwischen „Sicherheit" und „Freiheit" stehen die freiheitlichen Gesellschaften unter dem Druck eines Grundgefühls rasant wachsender Verunsicherung. Dieses Gefühl ist politisch hochwirksam. Die Wege der „entwickelten" und der im globalen Maßstab „abgehängten" Gesellschaften erweisen sich als eng miteinander verbunden und wechselweise voneinander abhängig, sodass hier auch Fragen kosmopolitisch wirksamer Gerechtigkeit berührt sind.

Innerstaatlich entspricht dem die Debatte um polizeiliche Instrumente der Prävention durch Datenerhebung und digitalen Mustererkennung. Behörden nutzen diese Möglichkeiten auch jenseits ihrer legitimen Befugnisse, wie die Enthüllungen des ehemaligen NSA-Mitarbeiters und Whistleblowers Edward Snowden 2013 mit Wucht ins öffentliche Bewusstsein brachten.

Hochautomatisierte autoregulative Waffensysteme

Digitale Technologien können Probleme verschärfen. Das zeigt sich auch im Kontext autoregulativer Waffen. Mit diesen Systemen sind hier solche gemeint, die landläufig als „autonom" bezeichnet werden (Nicole Kunkel 2020). Der verbreiteten Definition des US-Verteidigungsministeriums zufolge sind dies

Waffensysteme, die „einmal aktiviert, Ziele ohne weiteres menschlichen Eingreifen auswählen und angreifen können" („once activated, can select and engage targets without further intervention by a human operator")[29]. Sowohl der Autonomiebegriff als auch die Verben „auswählen" (select) und „angreifen" (engage) legen jedoch schwerwiegende anthropomorphe Missverständnisse nahe, weil sie komplexe menschliche Entscheidungs- und Auswahlprozesse unterstellen, in denen regelmäßig nach Gründen gefragt und das „Auch-anders-Können" vorausgesetzt werden kann. Maschinen aber sind durch die zugrundeliegende algorithmische Struktur determiniert, sodass hier der Begriff des „autoregulativen Systems" vorgezogen wird.

Mit der Durchsetzung der 5G-Technologie und des „Internet der Dinge" werden Sensoren allgegenwärtig. Daten sind damit im Übermaß vorhanden. Kein menschlicher Akteur kann all diese Daten noch angemessen verarbeiten. Verarbeitet werden die Daten algorithmenbasiert. Diese algorithmenbasierte Auswertung bildet die Grundlage für Entscheidungen, die entsprechend vorformatiert sind und tendenziell immer weiter in hochautomatisierte Systeme ausgelagert werden. Wird die sogenannte automatisierte Intelligenz durch „deep learning" optimiert, verschärft dies einerseits die Kontrollproblematik. Das Postulat einer „meaningful human control" für jeden Waffeneinsatz wird zusehends obsolet. Andererseits werden die spezialisierten Algorithmen mit der Verheißung propagiert, viel genauer unterscheiden zu können als Menschen. Das wäre auch rechtlich relevant, weil diese Unterscheidungsfähigkeit verspricht, die Kollateralschäden zu minimieren.

29 United States of America Department of Defense (2012). Directive No 3000.09 (November 21, 2012) on Autonomy in Weapon Systems, URL: https://cryptome.org/dodi/dodd-3000–09.pdf (Zugriff v. 20.01.2020), 13.

Die Frage nach der Anwendung autoregulativer Waffensysteme wird angesichts der fortschreitenden Entwicklung kontrovers diskutiert. Die einen lehnen deren Anwendung ab und fordern mit unterschiedlichen Argumenten eine komplette Ächtung – analog zu derjenigen von Landminen. Die anderen befürworten sie, indem sie zwischen rein reaktiven, etwa zur Raketenabwehr dienenden und letalen Systemen unterscheiden oder mit menschenrechtlichen Vorteilen argumentieren.

So behauptet etwa der Robotik-Experte Ronald C. Arkin, dass autoregulative Waffensysteme in höherem Maße kriegsvölkerrechts- und menschenrechtskonformes Handeln ermöglichten als menschliche Akteure (Ronald C. Arkin 2014). Unter der Voraussetzung, dass entsprechende normative Verhaltensmaßregeln algorithmisch implementierbar seien, plädiert er für den Ausbau der Erforschung solcher Systeme, weil sie sich gegenüber Mitgliedern der Streitkräfte dadurch auszeichneten, dass ihnen Selbstschutzimperative und Angst fehlen. Während bei menschlichen Agierenden nie auszuschließen sei, dass sie Informationen zu langsam verarbeiteten, dass sie aus Rache für getötete Teamkameraden oder aus Angst vor eigener Verletzlichkeit überreagieren oder sogar schwere Menschenrechtsverletzungen begehen, sei dies bei autoregulativen Systemen nicht der Fall: Eine Maschine auf Wachdienst könne ein Fahrzeug, das aus der Ferne nicht eindeutig zu klassifizieren ist, auf kürzeste Distanz herankommen lassen, um zu klären, ob es eine Bedrohung darstellt. Im ungünstigsten Fall sei nur eine Maschine zerstört. Ein menschlicher Wachtposten feuere im Zweifelsfall auch ohne genaue Identifikation, um sich selbst zu schützen.

Gegner bezweifeln allerdings, dass solche normativen Abwägungen synthetisch implementierbar sind. Sie kritisieren Arkin da-

für, bisher nicht entwickelte Technologien vorauszusetzen und argumentieren mit dem Problem der Verantwortungsdiffusion: Wie sich autoregulative Systeme verhalten, sei nicht vollständig vorhersehbar. So entstehe eine Verantwortungslücke, in der weder die Programmierenden noch die Einsetzenden vollständig verantwortlich seien, während den Systemen selbst als Maschinen keine Verantwortung zugeschrieben werden kann. Damit aber sei jede Zurechenbarkeit und folglich die Basis des Rechts im Krieg aufgegeben. Die Behauptung einer Verantwortungslücke überzeugt zwar nicht vollständig. Denn Verantwortungszuschreibung muss nicht zwingend mit unmittelbarer Zuständigkeit einhergehen – ein Minister wird für Fehlverhalten unterer Ebenen auch dann verantwortlich gemacht, wenn er davon gar nicht wusste; es wird ihm aber vorgehalten, dass er sich darüber hätte kundig machen müssen. Trotzdem ist zu fragen, ob solch strenge Maßstäbe der Verantwortungszuschreibung im militärischen Kontext Anwendungschancen haben. Zudem gilt, dass der menschenrechtlich unverzichtbare Grundsatz einer menschlichen Beherrschbarkeit der Technologie, einer „meaningful human control", angesichts der Reaktionszeiten solcher Systeme kaum umsetzbar erscheint. Zwar können menschliche Akteure vielleicht äußerlich von ihrer Verantwortung entlastet werden. Damit ist aber auf der Ebene der Gewissen die Schuldproblematik noch nicht einfach abgeblendet: Selbst wenn scheinbar „die Maschine schießt", sind Menschen aktiv involviert.

Überwachung und Predictive Policing[30]

Wie bereits erwähnt, bringt die Veränderung internationaler Beziehungen neue Sicherheitsfragen mit sich. Angesichts der

30 Predictive Policing, dt.: vorhersagende Polizeiarbeit.

Zunahme digitaler Optionen führt das auch innerstaatlich zu Konsequenzen: Strafverfolgungsbehörden und Geheimdienste machen geltend, dass sie mehr Probleme beim Zugang zu relevanten Informationen über Verdächtige haben, weil digitale Kommunikation oft besser verschlüsselt ist. Gleichzeitig ist das Ausmaß der Überwachung heute unbestritten größer als je zuvor: Smartphones und andere Computer ermöglichen anders als analoge Kommunikationstechnologie nicht nur einzelne, abgeschlossene Kommunikationsvorgänge, sondern enthalten detaillierte Spuren des gesamten Lebens ihrer besitzenden Personen und können mehr Auskunft über diese geben, als es jede verdeckte Ermittlung erfassen könnte. Staatsorgane können Kommunikationsgeräte infiltrieren und so Individuen und Gruppen gezielt überwachen (sogenannte Quellentelekommunikationsüberwachung, im Volksmund „Staatstrojaner"). Dazu gibt es unterschiedliche Systeme der Massenüberwachung, etwa das Mitschneiden des gesamten Internetverkehrs an Knotenpunkten, der Zugriff auf alle E-Mails eines bestimmten Anbieters oder auch auf Direktnachrichten eines Social-Media-Unternehmens. Eine Variante dieser Form stellt die Vorratsdatenspeicherung dar, die in Europa für Kommunikations- und Flugreisedaten gilt. Denn längst rüsten Strafverfolgungsbehörden und Geheimdienste technologisch nicht nur digital auf. Entsprechend gibt es in Deutschland Stimmen, die eine Videoüberwachung des öffentlichen Raums fordern. Die flächendeckende Verknüpfung mit automatischen Systemen zur Gesichtserkennung wird diskutiert: Staatliche Stellen sollen jederzeit die Möglichkeit haben, nachzuvollziehen, welche Person sich zu welchem Zeitpunkt wo befindet.

Digitalisierung verändert nicht nur, wie Menschen Waffensysteme gestalten. Sie bringt nicht nur die Herausforderung

mit sich, die Sicherheit von vernetzten Computersystemen selbst zu gewährleisten. Digitale Möglichkeiten sehr weitgehender datenbasierter Mustererkennung versprechen auch Fortschritte in der Verbrechensprävention, die sich auch auf Gewaltverbrechen und Tötungsdelikte bezieht. In Deutschland sind bisher fünf Systeme präventiver digitaler Polizeiarbeit, des sogenannten Predictive Policing, im Einsatz, die vor allem auf Einbruchs- und Eigentumsdelikte angewandt werden.

Davon ist der Einsatz von mustererkennender Software zur Terrorismusprävention zu unterscheiden, der auf soziale Medien zielt, wie etwa das BKA-Programm RADARite, dessen Resultate bisher noch ambivalent ausfallen: Denn noch kann nicht auf die menschliche Risikobewertung und Dateninterpretation verzichtet werden.

Die erstgenannten Verfahren sollen allerdings nicht zuletzt Geld einsparen. Im Wesentlichen werden dabei Täterprofile, geographische Gegebenheiten sowie zeit- und raumbezogene Daten bisheriger Delikte ausgewertet, um besonders betroffene Zeiten und Gebiete zu identifizieren, in denen dann die Patrouillenhäufigkeit erhöht werden kann, um Verbrechen vorzubeugen. Personenbasierte Profile sind bisher ausgeschlossen. Allerdings ist die Bedeutung und Wirkung stark umstritten. Das liegt einerseits daran, dass die Wirksamkeit kaum klar nachgewiesen werden kann: Selbst, wenn die Deliktrate in einem bestimmten Raum sinkt, ist nicht zu bestimmen, ob dies auf die entsprechende Maßnahme zurückgeht. Andererseits liegt dies daran, dass die entsprechenden Maßnahmen stark im politischen Diskurs genutzt werden, um Problembereiche zu definieren, die dann politisch bewirtschaftet werden können.

Besondere Gefahren ergeben sich dann, wenn hier personenbezogen gearbeitet wird. In den USA ist besonders die „strategic subject list" bekannt geworden, die aus Chicago stammt. Auf der Basis verschiedener Merkmale identifiziert sie konkrete Risikopersonen. Weil der Algorithmus von der Annahme ausgeht, dass die personale Nähe zu Gewalt ausübenden Personen die Wahrscheinlichkeit erhöht, Tatbegehende oder Opfer von Gewalttaten zu werden, werden sowohl Opfer wie Tatbegehende erfasst. Merkmale sind etwa die Häufigkeit von Schussverletzungen, das Alter während der letzten Verhaftung, die Häufigkeit, in der jemand Opfer von Körperverletzung wurde, und andere. Problematisch ist allerdings, dass schon die Erhebung dieser Daten in der Regel nicht unparteiisch ist, sondern durch Vorurteile gesteuert wird. Zudem gehen in entsprechende Algorithmen Annahmen ein, wie sie etwa die strategic subject list macht, deren Korrektur nicht sichergestellt ist, weil der Hersteller des Programms ein exklusives Recht darauf hat. Überdies schließen solche Vorhersageprogramme aus der bekannten Vergangenheit auf die unbekannte Zukunft: Damit ist stets auch eine Schließung der Zukunft und im ungünstigen Fall eine sich selbst erfüllende Prophezeiung verbunden. Schließlich stellt Mustererkennung natürlich niemals Kausalität, sondern immer nur Korrelation fest: Wer in einer Gegend wohnt, in der kriminelle Gewalt sich häuft, kann in den Sucher geraten, auch wenn er oder sie selbst keinerlei Affinität dazu hat, also nicht Ursache krimineller Gewalt ist.

e) Gewaltunterbrechung und Digitalisierung

Digitalisierung wird in ihrem Bezug zur tödlichen Gewalt vor allem dann diskutiert, wenn es um Kriegsführung geht. Angesichts dessen ist die Frage drängend, welchen Beitrag digitale

Technologie auch dazu leisten kann, Gewalt zu unterbrechen. Denn in der Unterbrechung von Gewalt realisieren Menschen ihre Freiheit zum Verzicht auf Gewalt. Gleichwohl muss die Gesellschaft aus christlicher Perspektive auch andere Fragen bearbeiten: Wie wird digitale Sicherheit möglich? Wie ist mit hochautomatisierter Waffentechnologie oder Möglichkeiten gezielteren Gewalteinsatzes umzugehen, die digitale Mustererkennung verspricht? Aus der Perspektive des Tötungsverbots, das darauf verpflichtet, Kreise der Gewalt zu unterbrechen, und der Vorstellung einer freiheitsfördernden Digitalisierung ergeben sich drei Erwägungen.

Cybersicherheit

Elektronische Schädigungen finden mehrheitlich im zivilen Zusammenhang statt. Das stellt einerseits infrage, ob das militärische Paradigma eigentlich das zentrale und zielführende ist, um die Abwehr und Bekämpfung solcher Schädigungen zu reflektieren. Es stellt andererseits infrage, ob militärisch ausgerichtete Organisationen und Institutionen die angemessenen Akteurinnen und Akteure zur Abwehr und Bekämpfung darstellen. Geht man nämlich davon aus, dass hacktivism, cybercrime und cyberterror als Phänomene ziviler Kriminalität auch schon rein empirisch von höherer Bedeutung sind als der cyberwar, dass die Kooperation der Bürgerinnen und Bürger zur Stärkung des individuellen Schutzes zentral ist, dass die Sicherung elektronisch sensibler Infrastrukturen auch im zivilen Kontext von organisierter Kriminalität oder politischem Terrorismus hohe Priorität genießen sollte und dass Forschung und Entwicklung vorrangig im privaten Sektor und auf Massenmärkten loziert sind, auf die sich auch militärische Forschungsagenturen wie DARPA stützen, zumal

das Militär im Digitalbereich zunehmend auf kommerziell erhältliche Anwendungen zurückgreift (components off the shelf, COTS), wird die Frage militärischer Anwendung entsprechender Instrumente nicht unerheblich, aber sekundär. Für eine zivile digitale Sicherungsstrategie, die von menschenrechtlichen Vorgaben auszugehen hätte, spricht also zunächst das Übermaß an Phänomenen, die nicht als cyberwar zu klassifizieren sind – ein Problemschwerpunktargument also. Für eine zivile digitale Sicherungsstrategie spricht auch ein technologisches Kompetenzargument: Entsprechende Verfahren und Technologien werden stärker im zivilen als im militärischen Bereich beforscht, selbst wenn dazu – wie im Falle der amerikanischen Militärforschungsbehörde (Defense Advanced Research Projects Agency, DARPA) – staatliche Mittel eingesetzt werden. Zudem stehen die Effizienz und Effektivität militärischer, hierarchischer Organisation nicht außer Zweifel, wie die jüngsten Einsatzbereitschaftsberichte etwa der Bundeswehr zeigen. Dazu kommt ein soziales Kompetenzargument: Es steht nämlich friedensethisch zu befürchten, dass eine Strategie der Friedenssicherung durch Hochrüstung, die die Frage der digitalen Sicherheit vorrangig militärisch organisiert, diese Sicherheit letztlich nicht erhöhen, sondern vermindern könnte, etwa, weil im Bereich der sogenannten „Cyberabwehr" nicht eindeutig zwischen defensiven und offensiven Strategien unterschieden werden kann und so die strikte Konzentration auf Verteidigung ausgehöhlt wird. Soweit militärische Organisationen nicht verpolizeilicht sind, vorfolgen sie ein Feindabwehrparadigma. Insofern lässt sich zudem fragen, ob solche Organisationen tatsächlich die beste Wahl zur Bearbeitung entsprechender Sicherheitsprobleme darstellen – zugleich ist der unterschiedslosen Rede vom „Cyberkrieg" entgegenzutreten.

Es ist ein Problem, in hochautomatisierten autoregulativen Waffensystemen menschliche Autorisierung so zu integrieren, dass sie diesen Namen verdient („meaningful human control"). Außerdem ist kaum zwischen Offensiv- und Defensivwaffen zu unterscheiden. Angesichts dessen stehen die moralischen Problemlagen solcher Waffensysteme deutlich vor Augen. Zudem wird kritisch gegen autoregulative letale Waffen eingewandt, dass sie die menschliche Würde verletzten, weil ihnen an menschlicher Urteilskraft und menschlichem Mitgefühl fehlt: Eine Maschine kann nicht gnadenweise vom Tötungsprogramm abweichen; es handelt sich um einen „death by algorithm" (Christoph Heyns). Auch bei der Folgenabschätzung ist Vorsicht geboten: Letale autoregulative Systeme könnten „gehackt" werden und sich dann gegen ihre ursprünglichen Verwender kehren oder in asymmetrischer Kriegführung von Agierenden eingesetzt werden, die sich an das Kriegsvölkerrecht nicht gebunden fühlen. Diese Gefahr ist genauso real wie die, dass in der Interaktion solcher Automaten unerwartete und unerwünschte Konsequenzen auftreten, wenn etwa Sonnenspiegelungen als Raketenflammen interpretiert werden und dadurch einen präemptiven Schlag auslösen, der aufgrund der kurzen maschinellen Reaktionszeiten jeden menschlichen Eingriff ausschließt („spoofing"[31]), oder dass die Beschädigung einzelner Module eine Kaskade weiterer Fehlfunktionen auslöst. In der Perspektive einer vom Tötungsverbot inspirierten christlichen Ethik der Gewaltunterbrechung und Friedensorientierung liegt die Gefahr solcher Waffensysteme auch darin, wie sie sich in größerem Rahmen und langfristig auf

31 Spoofing: Täuschungs- und Manipulationsmethoden zur Verschleierung der eigenen Identität im digitalen Raum.

Konfliktzusammenhänge auswirken könnten: Ähnlich wie ferngesteuerte Technologien schonen autoregulative Systeme zwar die je eigenen militärischen Kräfte weitgehend. Weil menschliche Steuerung fehlt, tragen sie aber zu einer Bedrohungskulisse bei, die jeder Art des peace-building abträglich ist. Sie untergraben die Notwendigkeit vertrauensbildender Maßnahmen am Konfliktort. Insofern ist die Bemühung um eine Ächtung letaler autoregulativer Systeme nicht unplausibel, auch wenn die Debatte noch keinesfalls als abgeschlossen gelten kann.

Überwachung und Predictive Policing

Die Bilanz des Predictive Policing fällt ambivalent aus. Dies gilt noch mehr für generelle Überwachungsinstrumente im digitalen Kontext: Bislang fehlen empirische Belege dafür, dass Überwachungsmaßnahmen die Sicherheit verbessern. Der Breitscheidplatz-Attentäter Anis Amri beispielsweise war Polizei und Verfassungsschutzämtern nicht nur bekannt, es gab sogar diverse V-Personen in seinem Umfeld. Zudem kann Überwachung neue Risiken schaffen: Der Preis für den ‚Staatstrojaner' ist eine Schwächung der allgemeinen IT-Sicherheit. Damit Sicherheitsbehörden in die IT-Systeme von Verdächtigen eindringen und Überwachungssoftware installieren können, müssen sie schließlich technische Schwachstellen ausnutzen. Das bedeutet, dass erkannte Schwachstellen von Staats wegen bewusst erhalten werden. Natürlich können auch Kriminelle diese Schwachstellen nutzen. Das zeigt unter anderem eine Cyberattacke, die 2017 die Öffentlichkeit in Atem hielt: Der Krypto-Trojaner „WannaCry" griff die Systeme von Krankenhäusern und von Firmen wie der Deutschen Bahn an – nur durch Glück kam niemand ernsthaft zu Schaden. Die Sicherheitslücke, die Einfallstor für den Angriff darstellte, war der US-amerikanischen NSA bekannt. Durch ei-

nen Hackerangriff auf die eigenen Systeme gelangte das Wissen um die Schwachstelle ins Internet.

Insgesamt scheint bei der Anwendung von mustererkennenden Verfahren in der Sicherheits- und Polizeiarbeit besonders zentral, dass Freiheitsrechte nicht beschnitten werden, die ökonomische Rationalisierungslogik nicht leitend und der Einbezug einer kritischen Öffentlichkeit gewährleistet wird. Dabei gilt es in der Perspektive des gerechten Friedens zu bedenken, dass totale Sicherheit nicht möglich ist und weder Polizeimaßnahmen noch das Justizsystem allein die Ursachen krimineller Gewalt nachhaltig bearbeiten können.

f) Beschäftigung in Kirche und Theologie

Die Frage nach dem gerechten Frieden und der Gewaltunterbrechung hat die Evangelische Kirche seit der Ostermarschbewegung nach dem Zweiten Weltkrieg immer wieder beschäftigt, in Akademiearbeit, Kirchentagen, akademischer Ethik sowie Militär-, Polizei- und Wehrdienstverweigererseelsorge. Zu den jüngsten Herausforderungen zählen auch diejenigen der Digitalisierung in Bezug auf Gewaltunterbrechung und Tötungsverbot. Diesen Herausforderungen hat sich die Evangelische Kirche nicht zuletzt in einem dreijährigen interdisziplinären Konsultationsprozess gewidmet, dessen Ergebnisse die EKD-Herbstsynode 2019 erörtert hat und die Basis weiterer Beratungen sind. Die Perspektive des gerechten Friedens mit ihrem Fokus auf die Konfliktursachen und der Priorisierung gewaltfreier und nachhaltiger Konfliktlösungen macht darauf aufmerksam, dass auch die digitale polizeilich-militärische Sicherheitsarchitektur eine zwar unersetzliche, aber eben nur komplementäre Funktion haben kann.