oder unbewusste Vermengung von „Verstehen" und „Verständnis". Die offensichtlich emotional-gewachsene Nähe der Autorin zum Sujet „Russland" erschwert es dem nicht mit ausreichender Sachkenntnis ausgestatteten Leser, sich ein differenziertes Bild zu machen. Krone-Schmalz trägt somit genau zu der von ihr so vehement kritisierten voreingenommenen Beschreibung des Konflikts bei.

So stellt sie bereits zu Anfang infrage, dass es sich beim russischen Vorgehen auf der Krim um eine „maskierte Annexion" handele. Krone-Schmalz zitiert den Rechtsphilosophen Reinhard Merkel und attestiert zu Recht, dass die Gemengelage deutlich komplizierter sei als oftmals angenommen (S. 29 ff.). Sie lässt dabei aber außer Acht, dass im Unterschied zum Kosovo, der Bevölkerung der Krim nicht genug Zeit gelassen wurde, sich über die wichtige Frage der weiteren territorialen Zugehörigkeit ausreichend ins Bild zu setzen. William Burke-White hat diesen signifikanten Fakt in einem deutlich ausdifferenzierten Artikel eingehend beleuchtet (siehe „Crimea and the International Legal Order", in: Survival, Bd. 56, Nr. 4, August-September 2014, S. 65-80).

Und es geht weiter. Dem Bruch des „Budapester Memorandums" setzt sie, unkommentiert, die russische Sicht entgegen, die EU und die USA hätten den Maidan-Umsturz akzeptiert und „damit ihre Garantiepflichten verletzt" (S. 33). Den Fall der entführten Militärinspektoren unter dem „Wiener Dokument" kommentiert sie mit der spitzen Frage: „Was soll man davon halten, wenn, bis auf eine Ausnahme, NATO-Offiziere unter der Führung eines deutschen Obersten, allesamt in Zivil unterwegs, an den Brennpunkten in der Ukraine herumfahren?" (S. 39). Hier und an anderen Stellen hätte man sich mehr journalistische Sorgfalt und weniger Polemik gewünscht.

Dabei bietet „Russland verstehen" durchaus viel Informatives. Akribisch arbeitet Krone-Schmalz die langjährige Evolution des Konflikts in drei Kapiteln auf. Von Gorbatschows Vision eines „gemeinsamen Haus Europas" über den Zusammenbruch der Sowjetunion, die Wirren der Jelzin-Jahre und das nationale Wiedererstarken unter Wladimir Putin – Krone-Schmalz' Kenntnisreichtum der jüngeren russischen Geschichte liest sich kurzweilig und verdeutlicht in ihrer konzisen Darstellung, welch fundamentalen Brüchen und Herausforderungen die russische Gesellschaft in den vergangenen 25 Jahren begegnet ist. Nicht nur an diesen Stellen hätten jedoch Endnoten, zur Unterstützung der zahllosen nicht zugeordneten Zitate, den Informationsgehalt des Buches noch verstärkt.

„Russland verstehen" hinterlässt beim kritischen Leser ein zwiespältiges Gefühl. Einerseits kann man sich in seinem Eindruck bestätigt fühlen, dass die deutschen Medien nicht umfassend, neutral und differenziert genug über den Krieg in der Ukraine berichten (aber bei welchem Krieg wäre dies jemals so gewesen?). Andererseits scheint es dieser Tage für die meisten Journalisten fast schon unmöglich, sich der gefühlten Parteinahme zu entziehen; und Krone-Schmalz' Herangehensweise wirkt hierbei beispielhaft. Der Malus ihres Buches ist nicht im Versuch, Russland „zu verstehen" zu suchen. Er liegt vielmehr im fragwürdigen Ansatz, unterschwellig Verständnis für die aktuelle Politik des Kremls einzufordern.

Ulrich Kühn

„Cyberwar: die digitale Front – ein Angriff auf Freiheit und Demokratie?", Ethik und Militär, Ausgabe 2014/2 (Zentrum für Ethische Bildung in den Streitkräften, Hamburg).

Noch ist wenig bekannt über den Cyber-„Angriff" auf den Deutschen Bundestag, der Mitte Mai dieses Jahres publik wurde. Weder die Anzahl der betroffenen Computer noch die abgegriffenen Daten oder gar die Urheber sind bekannt. Der Vorfall macht deutlich, dass dem Thema „Cybersicherheit" über Jahre nicht die Bedeutung beigemessen wurde, die es verdient. Umso erfreulicher ist es, dass die Zeitschrift „Ethik und Militär" dem Thema ein ganzes Heft gewidmet hat. Unter der Leitfrage „Cyberwar: die digitale Front – ein Angriff auf Freiheit und Demokratie?" bringen acht Beiträge und zwei lesenswerte Interviews, den Leserinnen und Lesern die wichtigsten Probleme nahe, die kritische Aktivitäten in der Cybersphäre aufwerfen.

Drei zentrale Themen lassen sich nach der Lektüre identifizieren: Erstens die Frage, was unter „Cyberwar" zu verstehen ist und wie er von anderen Formen von „Cyberangriffen" und Störungen zu unterscheiden ist. Damit verbunden ist, zweitens, die rechtlich-ethische Dimension, und die Frage, inwieweit die Begriffe und Konzepte von „Krieg" und „Angriff" überhaupt angemessen sind. Und drittens, wie einem sich abzeichnenden staatlichen „Cyber-Wettrüsten" mit rüstungskontrollpolitischen Maßnahmen zu begegnen ist und welche Maßnahmen darüber hinaus zur Sicherung von Grund- und Freiheitsrechten nötig sind.

Obwohl der Titel des Sonderheftes zunächst nur den „Cyberwar" als Leitmotiv benennt, zeigen die Artikel schnell, dass „Cyberwar" nur eine von vielen Formen „potenziell zerstörerische[r] Handlungen" (PoKempner, S. 33) in der Cybersphäre ist. Umso wichtiger sind definitorische Abgrenzungen, was unter Cyberwar zu verstehen ist. Es ist verdienstvoll, dass sich die Autorinnen und Autoren durch Differenzierungsbemühungen und die Vermeidung eines undifferenzierten Kriegsbegriffs einer „Versicherheitlichung" der Cybersphäre entgegenstellen. Dass die Konzepte in den Texten nicht immer gleich oder konsistent genutzt werden, ist nicht den Autorinnen und Autoren anzulasten, sondern auch Ausdruck des aktuellen Standes der „Cyberdebatte".

Einen sehr guten Blick auf definitorische Fragen bieten die Beiträge von Robin Geiß und Dinah PoKempner, die jeweils das Völkerrecht als zentralen Maßstab nutzen: Beide führen überzeugend aus, dass von einem „(völker-)rechtlichem Vakuum" (Geiß, S. 13) oder einer hinsichtlich des Rechts „nebligen neuen Dimension" (PoKempner, S. 37) keine Rede sein kann. Das bestehende Völkerrecht ist abstrakt genug formuliert, um auch Definitionen und Regeln für „zukünftige Cyberkonflikte" (Geiß, S. 13) zu bieten. So gilt ein „Cyberangriff" nur dann als bewaffneter Angriff gemäß Artikel 51 UN-Charta, wenn er „Konsequenzen herbeiführt, die in ihrem Ausmaß und ihrer Schwere mit denen eines konventionellen bewaffneten Angriffs vergleichbar sind" (Geiß, S. 13-14, vgl. PoKempner S. 35, 37). Für beide Experten hat bislang noch keine Cyberaktivität diese Schwelle erreicht, weshalb sie es auch am konsequentesten vermeiden, von „Cyberangriffen" zu sprechen. Die Mehrzahl böswilliger Aktivitäten im Cyberraum, darunter „wirtschaftliche Schädigungshandlungen" (Geiß, S. 14),

stellt keinen Angriff in diesem Sinne dar. PoKempner sieht im inflationären Gebrauch der Begriffe „Krieg" und „Angriff" die Gefahr, dass (analog zum „war on terror") der Schutz von Grundrechten zugunsten der Sicherheit untergraben wird (S. 35-37). Andere Beiträge warnen ebenfalls vor einer Beschneidung von Freiheitsrechten etwa durch Massenüberwachung (Skierka S.49 f.; Geiß S.16). Laut Geiß wird die rechtliche Bewertung allerdings schwieriger, sollten in Zukunft militärische Angriffe auf die an sich zivile „Cyberinfrastruktur selbst" (S. 15) erfolgen. Er plädiert hierbei überzeugend für eine enge Auslegung des humanitären Völkerrechts, um militärische Handlungsspielräume einzugrenzen (S. 15).

Die Beiträge aus ethischer Perspektive von George Lucas und Mariarosaria Taddeo (in Teilen auch von Sandro Gaycken) fallen durch ein recht instrumentelles Verständnis des Völkerrechts auf: Laut Taddeo besteht die Aufgabe des Völkerrechts vor allem darin, ethische Grundsätze, allen voran die des Gerechten Krieges umzusetzen, während Lucas im Völkerrecht ohnehin keine „expliziten" Regelungen für den von ihm beschriebenen „Hacktivismus" unterhalb der Schwelle eines „Cyberwars" sieht. Taddeo leistet den umfassendsten Beitrag zur ethischen Diskussion: Für sie stößt der Ansatz, dass das bestehende Völkerrecht auch auf den „Cyberkrieg" ausdehnbar ist, „unvermeidlich an seine eigenen Grenzen" (S. 41). Taddeos Lösung liegt in der Überarbeitung der Lehre des Gerechten Krieges, um auch Angriffe auf nicht-physische sowie immaterielle Objekte ethisch erfassen und einordnen zu können. Darin sieht sie die Basis für Gesetze, die der „Neuartigkeit" des Cyberwarfare (S. 42) gerecht werden; ansonsten drohe ein „regulatorisches Vakuum" (S. 41). Insgesamt hat die Debatte um eine ethische Einordnung des „Cyberkriegs" noch Entwicklungspotenzial – vor allem eine kritischere Auseinandersetzung mit der Lehre des gerechten Krieges wäre wünschenswert.

Wie soll es in der Cybersphäre nun konkret weitergehen? Einig sind sich die meisten Autorinnen und Autoren darin, dass sich ein gefährliches staatliches „Cyberwettrüsten" abzeichnet (z.B. Neuneck S. 30, Skierka S. 51), weshalb Rüstungskontrollmaßnahmen geboten sind. Am konkretesten wird Götz Neuneck, der eine kurze Übersicht der bisherigen Diskussion gibt (S. 28ff.) und auch weitere mögliche Maßnahmen vorschlägt (S. 30). Aktuell stehen seiner Einschätzung nach vor allem definitorische Fragen und gemeinsame Interpretationen des Völkerrechts im Vordergrund, während zusätzlich rudimentäre Vertrauensbildende Maßnahmen (VBM) (weiter)entwickelt werden (S. 29). Gleichwohl sieht er das Potenzial für umfassendere und „im militärischen Bereich vielfach erprobt[e]" Maßnahmen, z.B. „vertrauensbildende Kontrollmechanismen der Verifikation" (S. 30; ähnlich PoKempner S. 39 und Skierka, S. 51). Mit Blick auf autokratische Systeme findet sich im Heft außerdem die Forderung nach stärkerer Exportkontrolle von Überwachungstechnologie (PoKempner, S.39f.; Bendiek, S. 5). PoKempner bemängelt allerdings, dass die Zivilgesellschaft von den bisherigen Debatten weitgehend ausgeschlossen ist (S. 40). Für die „weicheren" Cyberaktivitäten unterhalb der Schwelle eines Cyberkriegs sieht Lucas die Notwendigkeit einer „informellen normativen Regelung" zwischen Staaten (S. 24), um „kinetisch[e]" Eskalationen zu vermeiden (S. 24). Annegret Bendiek gibt aber zu bedenken, dass sich auch innerhalb des westlichen Lagers, speziell zwischen den USA und Europa, die jeweils präferierte Cybersicherheitspolitik deutlich unterscheidet (S. 5), die bis auf die Privatsphäre der einzelnen Bürger durchschlägt. Hier plädiert sie für eine „sehr viel höher[e] Bereitschaft, auf den anderen zuzugehen" (S. 4). Als Ausgangspunkt könnten hier die geteilten Interessen aller Staaten an der „zuverlässige[n] Funktionsweise des Internets und die Kontrolle von Cyberkriminalität" (Skierka, S. 51) dienen.

Abschließend ist anzumerken, dass die „Ethik und Militär" die Lesbarkeit ihrer Beiträge durch die Beschränkung auf wenige Literaturverweise fördern will. So kommen die Beiträge mit Fußnoten im einstelligen Bereich und sogar ganz ohne Verweise aus. Zumindest an Stellen, an denen explizit auf andere Experten, Regierungsdokumente oder Ereignisse verwiesen wird, wären weitere Angaben aber wünschenswert. Auch hätte ein stärkerer redaktioneller Eingriff bei dem einen oder anderen Artikel die Lesbarkeit sicherlich verbessern können.

In der Summe ist die Lektüre des besprochenen Heftes lohnenswert, denn es gelingt, die aktuelle Debatte aus unterschiedlichen Disziplinen und interessanten Problemperspektiven aufzugreifen. Die Beiträge ergänzen sich und enthalten ausnahmslos konkrete Handlungsempfehlungen und Diskussionsanregungen für Wissenschaft und Politik.

Annabel Schmitz
Niklas Schörnig

Nark Maguire, Catarina Frois and Nils Zurawski (eds). The Anthropology of Security: Perspectives of Policing, Counter-terrorism and Border Control. London (Pluto Press) 2014.

As many anthologies, *The Anthropology of Security* proposes a wide contribution to its field, including new conceptual backgrounds, methodologies and a new range of empirical data.

The publication of the book follows scholarly events that took place in Ireland and Paris, as well as the worldwide collaboration through the Anthropology of Security Network. The authors share the focus on recent security developments in Europe and criticize how these have been taken for granted. In contraposition to that, the eight chapters intend to "see security and insecurity from different vantage points and thereby de-familiarize it; and to critically explore the styles of reasoning, calculations and operations in very powerful domains" (p. 10). The general aim of the book is to "provide critical evaluations of policing and policymaking, to show up the fissures in security-scapes, and to open space for future projects" (ibid). Therefore, the book aims at other publics than anthropologists and has as higher ambition to impact on European security policymaking.

Those aims are achieved by some chapters, but not by all of them. The quality of the contributions vary depending on the objectivity of each chapter in offering new evidence or perspectives to a specific problem, and on the authors' long expositions on a very specific anthropological debate. Some chapters effectively shed light on national and transnational security problems of European countries, but others lose sight and spend most of their pages on arguing in favor or against a scholarly issue.

On the former, Marion Demossier's "Sarkozy and Roma" expands the conventional and superficial understanding of French policy to Roma and Sinti populations. It tracks