Gerechter Frieden

Ines-Jacqueline Werkner
Niklas Schörnig *Hrsg.*

Cyberwar – die Digitalisierung der Kriegsführung

Fragen zur Gewalt • Band 6

Springer VS

Gerechter Frieden

Reihe herausgegeben von
Ines-Jacqueline Werkner, Heidelberg, Deutschland
Sarah Jäger, Heidelberg, Deutschland

„Si vis pacem para pacem“ (Wenn du den Frieden willst, bereite den Frieden vor.) – unter dieser Maxime steht das Leitbild des gerechten Friedens, das in Deutschland, aber auch in großen Teilen der ökumenischen Bewegung weltweit als friedensethischer Konsens gelten kann. Damit verbunden ist ein Perspektivenwechsel: Nicht mehr der Krieg, sondern der Frieden steht im Fokus des neuen Konzeptes. Dennoch bleibt die Frage nach der Anwendung von Waffengewalt auch für den gerechten Frieden virulent, gilt diese nach wie vor als Ultima Ratio. Das Paradigma des gerechten Friedens einschließlich der rechtserhaltenden Gewalt steht auch im Mittelpunkt der Friedensdenkschrift der Evangelischen Kirche in Deutschland (EKD) von 2007. Seitdem hat sich die politische Weltlage erheblich verändert; es stellen sich neue friedens- und sicherheitspolitische Anforderungen. Zudem fordern qualitativ neuartige Entwicklungen wie autonome Waffensysteme im Bereich der Rüstung oder auch der Cyberwar als eine neue Form der Kriegsführung die Friedensethik heraus. Damit ergibt sich die Notwendigkeit, Analysen fortzuführen, sie um neue Problemlagen zu erweitern sowie Konkretionen vorzunehmen. Im Rahmen eines dreijährigen Konsultationsprozesses, der vom Rat der EKD und der Evangelischen Friedensarbeit unterstützt und von der Evangelischen Seelsorge in der Bundeswehr gefördert wird, stellen sich vier interdisziplinär zusammengesetzte Arbeitsgruppen dieser Aufgabe. Die Reihe präsentiert die Ergebnisse dieses Prozesses. Sie behandelt Grundsatzfragen (I), Fragen zur Gewalt (II), Frieden und Recht (III) sowie politisch-ethische Herausforderungen (IV).

Weitere Bände in der Reihe http://www.springer.com/series/15668

Ines-Jacqueline Werkner ·
Niklas Schörnig
(Hrsg.)

Cyberwar – die Digitalisierung der Kriegsführung

Fragen zur Gewalt • Band 6

Springer VS

Hrsg.
Ines-Jacqueline Werkner
Forschungsstätte der Evangelischen Studiengemeinschaft
Heidelberg, Deutschland

Niklas Schörnig
Leibniz-Insitut Hessische Stiftung Friedens- und Konfliktforschung
Frankfurt am Main, Deutschland

ISSN 2662-2726 ISSN 2662-2734 (electronic)
Gerechter Frieden
ISBN 978-3-658-27712-3 ISBN 978-3-658-27713-0 (eBook)
https://doi.org/10.1007/978-3-658-27713-0

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Springer VS

Springer VS ist ein Imprint der eingetragenen Gesellschaft Springer Fachmedien Wiesbaden GmbH und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Abraham-Lincoln-Str. 46, 65189 Wiesbaden, Germany

Inhalt

Cyberwar – die Digitalisierung der Kriegsführung?
Eine Einführung

Ines-Jacqueline Werkner

1 Einleitung

> „Der Alptraum aller Militärs: Der Feind ist unsichtbar, blitzschnell und scheinbar überall, doch nicht zu fassen. Und er kann hart zuschlagen: Die Energieversorgung großer Städte bricht zusammen, die Verkehrsregelung ebenso wie der Währungskurs an den internationalen Börsen. Nationale und globale Infrastrukturen, Wirtschaft und Politik sind von Informationstechnik durchdrungen und Kriegsgeräte arbeiten auf informationstechnischer Grundlage, alles ist mit allem vernetzt" (Irrgang 2017, S. 101).

Mit dieser Beschreibung fasst der Philosoph und Theologe Bernhard Irrgang das Phänomen des Cyberwar. Dieser stellt – so die häufige Charakterisierung in der Literatur – neben Land, Wasser, Luft und Weltraum die „fünfte Dimension der Kriegsführung" dar. Mit ihm verlagert sich die Kriegsführung in einen vom Menschen selbst geschaffenen virtuellen Raum, in eine nicht-physische Domäne (vgl. Taddeo 2014, S. 42; Dickow und Bashir 2016). Das unterscheidet den Cyberwar von herkömmlichen Kriegsformen und macht ihn für ethische Anfragen virulent.

I.-J. Werkner und N. Schörnig (Hrsg.), *Cyberwar – die Digitalisierung der Kriegsführung*, Gerechter Frieden,
https://doi.org/10.1007/978-3-658-27713-0_1

Die Diskurse zum Cyberwar[1] sind divers (vgl. u. a. Linzen 2014, S. 3ff.; Heintschel von Heinegg 2015): Sie reichen vom Mythos bis zur real existierenden Bedrohung und virulenten Sicherheitsgefahr. Myriam Dunn Cavelty (2013, S. 106f.) vom *Center for Security Studies* in Zürich hält Cyberkriege – schon aufgrund der Ineffizienz und der Gefahr eines konventionellen Gegenschlages – für unwahrscheinlich. Für sie verbindet sich mit dem Mythos des Cyberwar vielmehr das Bestreben von Sicherheitsfirmen und Regierungen, Restriktionen von Freiheiten im Netz durchzusetzen. Auch für den Politikwissenschaftler Thomas Rid stellt dieser lediglich einen Mythos dar:

> „Es hat in der Vergangenheit keinen Cyberkrieg gegeben, es findet gegenwärtig keiner statt, und es ist überaus wahrscheinlich, dass auch in Zukunft keiner über uns hereinbrechen wird" (Rid 2018, S. 13).

Er sieht in Cyberangriffen gewöhnliche Formen von Sabotage und Spionage. „Bei näherer Betrachtung" seien sie sogar „eher ein Mittel zur Eindämmung als zur Eskalation politischer Gewalt". Zum einen seien damit „extrem präzise Angriffe auf die Funktionsfähigkeit technischer Systeme des Gegners" möglich, ohne die sie bedienenden Menschen unmittelbar zu schädigen. Zum anderen lassen sich durch Cyberangriffe „Daten herausschleusen, ohne zuvor Menschen einschleusen, also durch hochriskante Operationen in Gefahr bringen zu müssen" (Rid 2018, S. 15). Dahinter steht letztlich die Idee einer „sauberen und zivilisierten Form der Kriegsführung" (Linzen 2014, S. 5).

Dagegen halten Experten wie Sandro Gaycken den Cyberwar für eine real existierende Bedrohung:

---

1 Den Begriff des Cyberwar haben vor 25 Jahren John Arquila und David Ronfeldt (1993) geprägt.

> „Der Cyberkrieg wird kommen, nicht so sehr als heißer offener militärischer Konflikt, sondern mehr als eine elektronische Wiedergeburt des Kalten Krieges mit Spionage, Sabotage und zahlreichen kleinen Zwischenfällen" (Gaycken und Talbot 2010, S. 32; vgl. auch Irrgang 2017, S. 103).

Insbesondere ermögliche er schwächeren wie substaatlichen Akteuren, mit einem relativ geringen Ressourceneinsatz dem Gegner zu schaden (vgl. Gaycken 2010, S. 104f.). Weitaus dramatischer äußern sich US-amerikanische Politiker. Nach dem damaligen Antiterror-Berater des Weißen Hauses Richard A. Clark sei mit dem Cyberwar die Gefahr eines „electronic Pearl Harbor" verbunden (vgl. Linzen 2014, S. 5) und auch Leon Panetta, der ehemalige Verteidigungsminister der USA, warnte:

> "A cyber attack perpetrated by nation states [or] violent extremists groups could be as destructive as the terrorist attack on 9/11. Such a destructive cyber-terrorist attack could virtually paralyze the nation. […] The collective result of these kinds of attacks could be a cyber Pearl Harbor; an attack that would cause physical destruction and the loss of life. In fact, it would paralize and shock the nation and create a new, profound sense of vulnerability" (Panetta 2012, zit. nach Cook 2015, S. 23).

Unabhängig, welcher Denkschule man folgt, wird die zunehmende Digitalisierung die Kriegsführung wesentlich prägen. Zu klären bleibt, welcher Sphäre (zivil oder militärisch) sich Cyberangriffe zuordnen lassen, inwieweit sie konventionelle Vorstellungen von Gewalt, Krieg und Kriegsführung verändern und welche ethischen und völkerrechtlichen Infragestellungen mit ihnen einhergehen.

2 Was bedeutet Cyberwar?

Dass neueste Technologien zugleich die Kriegsführung prägen, zieht sich durch die gesamte Geschichte. Teilweise sind sie eigens dafür entwickelt worden (vgl. Mey 2017). Auch das Internet ist ursprünglich für den militärischen Daten- und Informationsaustausch geschaffen worden (vgl. Heintschel von Heinegg 2015). Für den Friedensforscher Götz Neuneck (2017, S. 806) könnte die Informationstechnik mit ihrer globalen Nutzung und Vernetzung digitaler Medien sogar „die mächtigste technologische Revolution in der Geschichte der Menschheit" werden. Im Cyberwar wird diese sowohl zum Ziel als auch zum Mittel der Kriegsführung und damit zugleich zur Waffe (vgl. Gaycken 2012, S. 91).

Was lässt sich nun aber unter dem Cyberwar konkret verstehen und was unterscheidet ihn von kriminellen Formen im digitalen Netz? Eine verbindliche Definition des Cyberwar existiert nicht; in der Literatur finden sich verschieden enge beziehungsweise weite Verständnisse. Einigkeit besteht allerdings darin, den Cyberwar als eine „Zustandsbeschreibung eines Krieges mit Cybermitteln" zu verstehen (Linzen 2014, S. 2), ganz im Sinne von Peter W. Singer und Allan Friedman (2014, S. 121): „The key elements of war in cyberspace all have their parallels and connections to warfare in other domains."

Das viel zitierte *Tallinn Manual on the International Law Applicable to Cyber Warfare,* eine Studie über die Anwendbarkeit des Völkerrechts auf Cyberkonflikte und Cyberkrieg, versteht unter einem Cyberangriff (im Sinne eines Cyberwar)

> "a cyber operation, whether offensive or defensive, that is reasonably expected to cause injury or death to persons or damage or destruction to objects" (Schmitt 2013, Rule 30; identisch in der Fassung 2.0 von 2017, Rule 92).

Zentral ist bei dieser Begriffsbestimmung der Aspekt der Gewaltanwendung („the use of violence against a target"), die einen Cyberangriff beispielsweise von Cyberspionage unterscheidet. Dabei versteht das *Tallinn Manual* unter Gewalt nicht nur den gewaltsamen Akt selbst, sondern auch seine Konsequenzen: „‚[V]iolence' must be considered in the sense of violent consequences and is not limited to violent acts" (Schmitt 2013, Rule 30; 2017, Rule 92). Diese Definition lässt ein weiteres wie auch engeres Verständnis zu, je nach Interpretation des Begriffs „objects" (vgl. Taddeo 2014, S. 44).

Kontroversen um seine Reichweite durchziehen die gesamte Debatte um den Cyberwar. Insbesondere erweist es sich als strittig, wann von einem bewaffneten Angriff gesprochen werden kann, das heißt, inwieweit und ab welchem Zeitpunkt ein Cyberangriff auf die Infrastruktur eines Landes als „digitale Kriegserklärung" (Linzen 2014, S. 2f.) aufzufassen ist.

In Anlehnung an das *Tallinn Manual* differenziert Götz Neuneck (2017, S. 809) drei Typen des Cyberwar: erstens umfassende Angriffe gegen den Cyberraum, zweitens begrenzte Angriffe auf die (vitale) Infrastruktur eines Landes mit dem Ziel, wichtige Funktionen zu unterbrechen, und drittens „Angriffe mit regulären Streitkräften gegen zentrale Knotenpunkte des Cyberraums". Was ihn von Cyberkriminalität unterscheide, seien – so Sandro Gaycken (2012, S. 93) – die Qualität der Angriffe:

> „[T]raditionelle Angreifer auf die IT waren bislang wenig koordinierte Kleinkriminelle und Teenager. Jetzt kommen Militärs mit ihren typischen Vorgehensweisen und Mitteln. Sie nutzen Nachrichtendienste zur Vorbereitung, zum Transport und zur Nachbereitung, sie arbeiten in großen, gut organisierten Teams mit mehrstufigen Taktiken, sie nutzen hochrangige Experten verschiedenster Disziplinen, sie bauen Testgelände auf, sie werden professionell geführt, und sie können das Tausendfache in das Design eines Angriffs investieren, ohne das als teuer zu empfinden."

Mit dem Cyberwar verbinden sich vier zentrale Herausforderungen: Erstens kommt es zu einer *Verschmelzung militärischer und ziviler Räume*, sowohl bezüglich der Ziele – angesichts der zunehmenden Digitalisierung können prinzipiell alle Bereiche des Lebens zum Ziel von Cyberangriffen werden – als auch der Mittel des Cyberwarfare. Die Kriegsführung wird mit zivilen Mitteln geführt; sie erweist sich als „vollkommen blutlos" (Gaycken 2014, S. 6). Ihre – zumeist zeitlich verzögerten – Wirkungen beispielsweise auf vitale Teile der Infrastruktur eines Landes können dagegen dramatisch sein. Und je nachdem, ob Cyberangriffe als zivile oder militärische Bedrohung gefasst werden, werden auch Verantwortlichkeiten und Maßnahmen zur Abwehr dieser virtuellen Angriffe unterschiedlich ausfallen (vgl. Kriesel und Kriesel 2012, S. 128f.; Theiler 2012, S. 145; PoKemptner 2014, S. 39).

Zweitens sind Cyberangriffe durch eine *hohe Wirkasymmetrie* gekennzeichnet (vgl. Gaycken 2012, S. 98ff.). So können schon kleine Angriffe mit wenig technischem Aufwand und geringen Kosten dramatische Wirkungen zeitigen, insbesondere wenn diese kritische Bereiche der Infrastruktur treffen. Man denke nur an den Ausfall von Wasser- oder Stromversorgungen in Großstädten oder Angriffe auf Chemiefabriken und Atomkraftwerke. Innerhalb weniger Tage könnten Zwischenfälle dieser Art – ganz unblutig – zu hohen Opferzahlen führen. Zugleich besteht eine „Asymmetrie der Fehlertoleranz" (Gaycken 2012, S. 99). Während der Angreifer etliche Versuche unternehmen kann, von denen nur einer seine Wirkung entfalten muss, hat der Verteidiger zur Abwehr dieses Angriffs in der Regel nur einen Versuch und dieser müsse dann „immer erfolgreich sein" (Gaycken 2012, S. 99). Dabei scheint ein passiver Schutz gegenwärtig durchaus begrenzt, wenn nicht gar unmöglich zu sein.

Die dritte Herausforderung besteht in der Attribution. Angreifer können im Cyberwar häufig nicht – und wenn überhaupt, dann

nur mit großer zeitlicher Verzögerung – identifiziert werden. Dies ist allerdings zentral, wenn potenzielle Angreifer durch Strafen abgeschreckt werden sollen. Die fehlende Täteridentifikation lässt sich auf verschiedene Gründe zurückführen: (1) auf „die Flüchtigkeit der physischen Spuren" im Internet, (2) auf den „apologetische[n] Charakter der Datenspuren", ist der informatorische Gehalt bei Cyberangriffen grundsätzlich manipulierbar, (3) auf den „Mensch-Maschine-Gap", denn selbst wenn die Maschine identifiziert werden könne, sei weiterhin ungeklärt, welche Person zum entscheidenden Zeitpunkt einen Zugriff gehabt habe, und (4) „die Alltäglichkeit der Waffe", handelt es sich im Cyberwar um „handelsübliche Alltagstechnologien" wie alltägliche PCs, USB-Sticks oder Standardprogramme (Gaycken 2012, S. 101ff.).

Schließlich weisen Cyberangriffe gegenüber allen konventionellen Formen der Kriegsführung einen zentralen Vorteil auf: Sie benötigen *keine Vorwarnzeiten*. Digitale Erstschläge erfolgen in Bruchteilen von Sekunden. Entsprechend gering ist die Zeit, sich gegenüber diesen Angriffen zu verteidigen (vgl. Theiler 2012, S. 138).

3 Cyberangriffe und Reaktionen

Wie sieht nun der empirische Befund aus? Hat es bislang schon Angriffe im Sinne einer Kriegshandlung gegeben oder handelt es sich beim Cyberwar eher um einen Mythos? In den vergangenen Jahren lassen sich durchaus Beispiele aufzeigen, die auf die außenpolitische Dimension von Cyberangriffen verweisen (vgl. u. a. Heintschel von Heinegg 2015; Reinhold 2016; Neuneck 2017, S. 808f.): So hat 2007 ein DDOS-Angriff[2] auf Estland (durch kremlnahe Aktivisten aus

2 Sogenannte „Distributed Denial of Service"-Angriffe (DDOS) auf IT-Systeme können die Funktionsfähigkeit und Verfügbarkeit von