Keio-Universität 慶應義塾大学

Juristische Fakultät 法学部

Studienjahr 2019 2019 年度

Die Cyber-Kriegstheorie in der realen Cyber-Sicherheitspolitik

— Unter besonderer Berücksichtigung der Bundesrepublik Deutschland —

「現実のサイバー安全保障政策におけるサイバー戦争論―特にドイツ連邦共和国を中心に―」

Abschlussarbeit

zur Erlangung eines Zertifikats des Nebenfachabschlusses

Fachbereich Geisteswissenschaft

副専攻（人文科学）認定申請のための修了論文

Geisteswissenschaftliches Seminar (Modernes Deutschland)

人文科学研究会（現代ドイツ研究）

vorgelegt von: Ayumi Chigusa 提出者：千草 歩実

Matrikelnummer: 31658073 学籍番号：31658073

eingereicht bei: Prof. Shin'ichi SAMBE 提出先：三瓶 愼一 教授

Abgabetermin: 4. Februar 2020 提出日：2020 年 2 月 4 日

Inhaltsverzeichnis

Einleitung

Gegenwärtig nimmt mit der rasanten Entwicklung der Informationstechnologie die internationale sozioökonomische Abhängigkeit vom Cyber-Raum zu[1]. Infolgedessen werden wichtige Computernetzwerke und Infrastrukturen in jedem Land zu immer attraktiveren Zielscheiben und Cyber-Technologie tendiert dazu missbraucht zu werden. Zum Beispiel wurde Sony Pictures Entertainment 2014 gehackt[2]. Der Angreifer hat zahlreiche vertrauliche Dokumente gestohlen und ins Internet gestellt. Dabei wurde eine Vielzahl von Daten – von Details zur neuesten Filmproduktion bis zu persönlichen Informationen über Mitarbeiter – veröffentlicht. 2019 hat Nordkorea Banken und Kryptowährungsbörsen angegriffen und illegal bis zu 17 Millionen Euro erbeutet[3].

In der Zwischenzeit beschäftigen sich Regierungen deutlich intensiver mit der Cyber-Politikgebung als jemals zuvor. Auf dem Treffen der sieben wichtigsten Außenminister im April 2019 war digitale Verteidigung ein zentrales Thema und „Die Dinard-Resolution zur Initiative für Cyber-Normen“ wurde verabschiedet[4]. Japan sucht nach öffentlich-private Kooperationen, um „eingebettete Typen“ von Spionage mit Halbleiterchips zu bekämpfen[5]. Angesichts der Situation, dass Cyber-Sicherheit für viele Staaten zu einem zentralen Politikfeld geworden ist, wird es immer wichtiger, die sich ständig weiterentwickelnde Cyber-Technologie und ihre Rolle in der staatlichen Sicherheitsstrategie zu betrachten.

Daher konzentriert sich diese Arbeit auf die Widerspiegelung der Cyber-Kriegstheorie in der realen Politik. Eine Studie Adam Liffs hat auf die übermäßig pessimistische Tendenz bisheriger Arbeiten durch eine Überprüfung der vier wichtigsten Aussagen zum Cyber-Krieg hingewiesen und argumentiert, dass der Cyber-Krieg nicht revolutionär sei. In der Arbeit von Liff fehlt es jedoch an politischen Implikationen.

Darauf aufbauend wird in dieser Arbeit folgende Forschungsfrage gestellt: „Wird die Cyber-Kriegstheorie Liffs von der deutschen Cyber-Sicherheitspolitik widergespiegelt?“ Und sie

vertritt die These, dass dies nicht der Fall ist.

In dieser Arbeit wird die These durch drei Fallstudien verifiziert. Die Beispiele hierfür sind die Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg, das Weißbuch 2016: Zur Sicherheitspolitik und zur Zukunft der Bundeswehr und die Cyber-Sicherheitsstrategie für Deutschland 2016. Die verwendenden Materialien und Daten basieren auf den drei oben genannten Regierungsdokumenten und auf Studien zum Cyber-Krieg.

Diese Arbeit gliedert sich in fünf Kapitel. Kapitel I erklärt die Übersicht zum Cyber-Krieg, kritisiert ein früheres Forschungsergebnis, wirft eine Frage auf und stellt die These und das Konzept dieser Arbeit vor. Darüber hinaus werden die Definitionen der Schlüsselbegriffe angeführt. Die Kapitel II bis IV bestätigen die These anhand von Fallstudien. Bei der Verifizierung der These konzentriert diese Arbeit sich auf die Frage, wie die vier wichtigsten Aussagen zum Thema Cyber-Krieg in der deutschen Cyber-Sicherheitspolitik berücksichtigt werden. Kapitel V beschreibt die Implikation der Schlussfolgerung dieser Arbeit.

I. Fragestellung und Ansatz

In diesem Kapitel wird eine Studie zur Cyber-Kriegstheorie kritisiert, die Forschungsfrage vorgelegt, und die These und der Entwurf für diese Arbeit aufgestellt. Abschnitt 1 fasst das Forschungsthema Cyber-Krieg zusammen. Abschnitt 2 betrachtet kritisch eine frühere Studie und stellt die Forschungsfrage auf. Abschnitt 3 beschreibt die These und Forschungsmethode dieser Arbeit.

1. Übersicht zum Cyber-Krieg

Bei der Untersuchung des revolutionären Charakters des Cyber-Kriegs muss man zuerst die Definition der Cyber-Technologie und ihre Auswirkungen auf Krieg erklären[6]. Cyber –

abgeleitet von dem Wort „Cybernetik“ – ist ein allgemeiner Begriff für Angelegenheiten, die mit Computer und dem Internet zusammenhängen[7]. Dies umfasst Hardware wie Computer und Netzwerke, die mit Cyber in Verbindung gebracht werden, und auch Themen wie Strategie- und Rechtsfragen. Ein Bestandteil dieser Verwendung des Begriffs ist die Cyber-Technologie. Unter Cyber-Technologie versteht man Computertechnologie und Netzwerktechnologie. Es hat sich in den vergangenen Jahrzehnten rasant weiterentwickelt und nicht nur die modernen sozioökonomischen Aktivitäten beeinflusst, sondern maßgeblich auch den militärischen Bereich.

Viele Truppen übernehmen aktiv Cyber-Technologie, weil sie den Krieg effizienter machen kann. Zum Beispiel verbindet ein Kommunikationssystem verschiedene Kommunikationsgeräte der Armee, so dass zerstreute Soldaten Informationen miteinander austauschen und sich in die Ziele angemessen zuweisen können. Wenn kämpfende Einheiten „früher als der Feind wissen, früher entscheiden, früher sagen und die Aktionen regulieren“ können, sind sie in die Lage, ihre Kräfte auf wichtige Orte zu konzentrieren und den Sieg zu erringen.

Durch den Einsatz von Cyber-Technologie wird sich die Form des Kriegs mehr oder weniger ändern. Die Auswirkungen der Cyber-Technologie auf den Krieg lassen sich hauptsächlich in den folgenden drei Punkten zusammenfassen[8]. Erstens weitet Cyber-Technologie das Einsatzgebiet deutlich aus. Wenn man mit dem Internet verbunden ist, kann man Feinde auf der ganzen Welt angreifen. Zweitens bietet sie eine neue Methode für Kampfhandlungen. Man kann das eigene System schützen und gleichzeitig die Systeme des Gegners angreifen. Drittens fügt Cyber-Technologie ein neues Kampfgebiet hinzu. Die strategische Doktrin des amerikanischen Verteidigungsministeriums erkennt den Cyber-Raum als Kampfgebiet an und beschreibt, dass die Vereinigten Staaten in die vollständige und kontinuierliche Integration von Cyber-Verteidigung, Resilienz und Cyber-Fähigkeiten von militärischen Operationen investieren[9].

Auf diese Weise verändert die Cyber-Technologie den Krieg. Aber was genau kann man sich

dann unter einem Cyber-Krieg vorstellen? Die Definition des Cyber-Kriegs ist noch nicht klar, und es gibt verschiedene Ansichten dazu. Einerseits erklärt beispielsweise der amerikanische Ex-Sonderberater für Cyber-Sicherheit Richard Clarke, dass Cyber-Krieg „eine Handlung eines Staats ist, die in die Computer oder die Netzwerke eines anderen Staats eindringt, um Schaden oder Verwirrung zu verursachen“ [10] . Andererseits definiert der amerikanische Ex-Vizeverteidigungsminister Joseph Nye Cyber-Krieg als „Feindseligkeiten im Cyber-Raum, die die materielle Gewalt verstärkt oder vergleichbare Auswirkungen haben“[11]. Obwohl die Details unterschiedlich sind, haben die beiden Definitionen gemeinsam, dass der Angreifer Cyber-Technologie für einen strategischen Zweck gebraucht.

Im Vergleich zu früher werden internationale Konflikte häufiger, bei denen Cyber-Technologie eine wichtige Rolle spielt[12]. Beispielsweise hat 2006 die schiitische nichtstaatliche Militärorganisation Hisbollah während der Invasion im Libanon das Internet und andere Cyber-Technologien ausgenutzt, um das Informationsumfeld zu dominieren. In ähnlicher Weise wurden 2007 die Bank- und Verwaltungssysteme Estlands außer Funktion gesetzt, weil Millionen von Computern auf der ganzen Welt gehackt, als Botnets verwendet und gegen Estland eingesetzt wurden. Die Regierung und die Ministerien Georgiens erlitten im Kaukasuskrieg 2008 ebenfalls einen massiven Distributed-Denial-of-Service (DDoS) Angriff. Keiner dieser Fälle hat jedoch zu einem vollständigen Cyber-Krieg geführt. Eine mögliche militärische Aktion im Cyber-Raum ist ein Cyber-Angriff auf die iranische Nuklearanlagen im Jahr 2010 durch den von amerikanischen und israelischen Geheimdiensten gemeinsam organisierten Computerwurm „Stuxnet“.

2. Kritische Betrachtung der Forschungssituation

Aus den bisherigen Studien zur Cyber-Kriegstheorie soll zunächst eine wichtige Arbeit von Adam Liff herausgegriffen werden: „Cyber-Krieg: eine neue ‚absolute Waffe‘? Die Verbreitung

von Cyber-Kriegsfähigkeiten und zwischenstaatliche Kriege“ (2012)[13]. Im Gegensatz zu anderen Forschungen kommt Liff in dieser Studie zu dem Schluss, dass der Cyber-Krieg nicht revolutionär sei. Er stützt diese Behauptung auf die folgende Argumentation.

Zuerst definiert der Autor, was Cyberkrieg ist. Er betont dabei, dass der Cyber-Krieg den Charakter eines „Krieges als Teil eines politischen Verhandlungsprozesses zwischen zwei oder mehr Parteien“ trage und nicht auf den Cyber-Raum beschränkt sei. Zu den Mitteln dieser Auseinandersetzung gehörten Computernetzwerkoperationen (CNO), Computernetzwerkangriffe (CNA) und Computernetzwerkverteidigung (CNV).

Vor diesem Hintergrund diskutiert Liff die Auswirkungen der Cyber-Technologien auf die Art des Kriegs. Der Autor erklärt, dass die Verbreitung der Cyber-Technologien nur geringe Effekte habe, indem er die vier wichtigsten Aussagen zum Cyber-Krieg überprüft.

1. Asymmetrie: Bisherige Studien haben gezeigt, dass CNAs die Unterschiede zwischen konventionellen Streitkräften ausgleichen, weil sie nur niedrige Kosten für Entwicklung verursachen und die Distanz verkürzen können. Nach Liff verfügen jedoch nur die Großmächte über die Ressourcen, um CNAs zu entwickeln, und strategischen Überlegungen dieser Staaten haben eine Tendenz, Konflikte durch Verhandlungen zu lösen. Daher führe die Asymmetrie des Cyber-Kriegs nicht zu einer Zunahme des Kriegs.

2. Angriffsvorteil: Der herkömmlichen allgemeinen Ansicht zufolge behalte der Angreifer die Oberhand behalte, weil die Kosten für CNV hoch seien, und die für Angriff erforderliche Zeit im Cyber-Raum reduziert werde. Liff hält dem entgegen, dass dies nichts an der Kräftebalance bei den konventionellen Streitkräften ändere. Deshalb sei der Einfluss des Cyber-Kriegs auf zwischenstaatliche Kriege begrenzt.

3. Anonymität: In bisherigen Studien wurde darauf hingewiesen, dass im Cyber-Krieg der Angreifer keine Angst vor Vergeltungsmaßnahmen zu haben brauche, da es schwierig sei, die Quelle eines Angriffs aus dem Cyber-Raum zu identifizieren. Zusätzlich steige die Anzahl der Kriege aufgrund falscher Identifizierung der Angriffsquelle und die anschließende Eskalation

an. Auch in diesem Punkt widerspricht Liff. Für ihn müssen Kriege politische Zwecke haben, und ohne Selbstidentifikation der Angreifer könnten sie keinen Zwang ausüben. Deswegen seien die Auswirkungen der Cyber-Technologien auf die Stabilität des internationalen Systems gering.

4. Wirkungslosigkeit der Cyber-Abschreckung: Im Allgemein geht man davon aus, dass Abschreckung im Cyber-Krieg unwirksam sei, weil die Identifizierung der Angriffsquelle, die Entwicklung der CNV und der Abschluss von Rüstungskontrollabkommen schwierig seien. Aber laut Liff gibt es Unsicherheiten darüber, welche Effekte CNAs haben könne. Und ob Cyber-Abschreckung funktioniere, hänge nicht nur von den Cyber-Technologien der Akteure ab, sondern auch von den Vergeltungsfähigkeiten auf einer höheren Konfliktebene. Daher funktioniere Cyber-Abschreckung.

Die Argumentation Liffs weist auf eine pessimistische Tendenz in den früheren Studien hin, indem deren wichtigsten Aussagen zum Cyber-Krieg hinterfragt werden. Liff vertritt die Meinung, dass die Verbreitung der Cyber-Technologien sich nur gering auswirke und Cyber-Krieg somit nicht revolutionär sei. Er untersucht die Entfaltung des Cyber-Kriegs von einem neutralen, emotional nicht aufgeladenen Standpunkt aus und ist sehr umfassend in der Erstellung seiner Cyber-Kriegstheorie.

Aber auch diese Studie hat zwei Fehler. Zum einen mangelt es ihr an Beweisen für die Theorie anhand konkreter Beispiele. Der Autor legt die Grundlage für seine Theorie nicht dar, weshalb die Glaubwürdigkeit leidet. Zum anderen mangelt es auch an einer Diskussion der politischen Folgen. Liff erklärt nicht, was seine Theorie zur politischen Gestaltung beiträgt. Die Entwicklung der Theorie verliert an Bedeutung, wenn die Ergebnisse nicht in tatsächlichen Situationen widergespiegelt werden.

Ausgehend von diesen zwei Schwächen konzentriert sich diese Studie auf die politischen Implikationen der Theorie, nach der Cyber-Krieg nicht als revolutionär gilt, und stellt die folgende Forschungsfrage: „Wird die Cyber-Kriegstheorie Liffs von der deutschen Cyber-

Sicherheitspolitik widergespiegelt?“

3. Themenstellung und Begriffsbestimmung

Die These dieser Arbeit ist, dass die Cyber-Kriegstheorie Liffs von der deutschen Cyber-Sicherheitspolitik nicht widergespiegelt wird. Dafür liegen zwei Gründe vor. Erstens wird die Theorie Liffs allgemein noch nicht berücksichtigt. Weder die Öffentlichkeit, noch die sich am politischen Entscheidungsprozess beteiligenden Politiker glauben, dass Cyber-Krieg revolutionäres Potenzial habe. Zweitens zeigt sich in Cyber-Sicherheitspolitik vieler Länder eine emotionale Reaktion auf Cyber-Technologie. Weil Cyber-Raum komplex und schwer zu verstehen ist, geht die Angst vor Unbekannten der nüchternen Analyse voraus.

In der vorliegenden Studie wird versucht, anhand von Fallstudien die obenstehende These zu verifizieren. Aufgrund der stürmischen Entwicklung der Informationstechnologie geraten viele Länder unter den Druck, in kurzer Zeit ihre Cyber-Sicherheitspolitik zu bestimmen, und Deutschland ist nicht eine Ausnahme. Daher nimmt diese Studie drei Regierungsdokumente, die die deutsche Cyber-Sicherheitspolitik zusammenfassen: „Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg“, „Weißbuch 2016: Zur Sicherheitspolitik und zur Zukunft der Bundeswehr“ und „Cyber-Sicherheitsstrategie für Deutschland 2016“.

In den Fallstudien werden die folgende Schlüsselbegriffe wichtig. Die erste vier Fachausdrücke beziehen sich auf die Natur des Cyber-Kriegs.

1. Asymmetrie: Asymmetrie ist ein Zustand, in dem ein konventionell schwaches Subjekt aufgrund von niedrigen Eintrittsbarrieren die Fähigkeit hat, einen stärkeren Staat effektiv zu bedrohen[14].

2. Angriffsvorteil: Das Gleichgewicht zwischen dem Angreifer und dem Verteidiger kann anhand des Verhältnisses der Kosten der Truppe, die der Angreifer benötigt, um das Ziel zu erreichen, und der Kosten der vom Verteidiger eingesetzten Truppe gemessen werden[15]. Unter

Angriffsvorteil versteht man einen Zustand, in dem es einfacher ist, den Gegner zu zerstören als sich selbst zu schützen[16].

3. Anonymität: Mit Anonymität bezeichnet man die Fähigkeit, das Ziel auf eine Weise anzugreifen, die es schwierig macht, die Verantwortlichkeit des Angreifers zu beweisen[17].

4. Wirkungslosigkeit der Cyber-Abschreckung: Abschreckung ist im Allgemeinen die Fähigkeit, das Ziel auf eine Weise anzugreifen, die es schwierig macht, die Verantwortlichkeit des Angreifers zu beweisen[18]. Vor diesem Hintergrund wird Cyber-Abschreckung als Abschreckung definiert, bei der sowohl der Angreifer als auch der Verteidiger identifiziert werden und eine Eskalation auf einer höheren Konfliktebene möglich ist[19]. Somit stellt die Wirkungslosigkeit der Cyber-Abschreckung einen Zustand dar, in dem die Verwendung dieser Bedrohung ungültig ist.

Der nächste Begriff, der in den Fallstudien zu einem entscheidenden Faktor wird, ist „widerspiegeln". Diese Studie beruht auf Überlegung, dass die Cyber-Kriegstheorie Liffs von der deutschen Cyber-Sicherheitspolitik nicht widergespiegelt wird, wenn alle Behauptungen Liffs gegen die vier Aussagen des Cyber-Kriegs in den analysierten Materialien nicht gefunden werden.

Zuletzt muss erwähnt werden, dass für die Fallstudie als primäre Quelle offizielle Dokumente der deutschen Bundesregierung besonders die drei oben genannte Sicherheitspolitik verwendet wurde und als sekundäre Quelle Aufsätze zu Cyber-Kriegstheorie.

II. Fallstudie 1: „Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg"

Dieses Kapitel stellt die „Strategischen Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg" als der Fall an. Im Abschnitt 1 wird die Hauptsachen des Dokuments zusammengefasst. Im Abschnitt 2 wird es analysiert, ob die Cyber-Kriegstheorie Liffs von diesem Weißbuch widergespiegelt wird.

1. Zusammenfassung des Dokuments

Zuerst werden die Hauptsachen der „Strategischen Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg“ erläutert[20]. Nach einer Erklärung über den Zweck dieses Weißbuchs werden die spezifischen Maßnahmen in den fünf Handlungsfeldern beschrieben.

Die „Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg“ ist ein Dokument, das vom Bundesministerium der Verteidigung (BMVg) im April 2015 veröffentlicht wurde. Sie verdeutlicht die Verantwortlichkeiten, Kompetenzen und Aufgaben des BMVg im Cyber-Raum. Die Bundeswehr müsse, so das Dokument, ihre Fähigkeiten im Cyber-Raum stärken, deshalb werden neue Ziele in diesen Domänen angesichts fünf Handlungsfeldern festgelegt.

Das erste Handlungsfeld ist der „Beitrag zur gesamtstaatlichen Sicherheitsvorsorge“. Eine landesweite Rolle der operativen militärischen Fähigkeiten im Cyber-Raum wurde noch nicht berücksichtigt. Es wird argumentiert, dass das BMVg sich mit diesem Problem auseinandersetzen müsse und eine mögliche Rolle für die Bundeswehr zu erstellen habe. Dabei sei zu prüfen, inwieweit andere Abteilungen und Betreiber kritischer Infrastrukturen einen wirksamen Beitrag zur allgemeinen Sicherheit leisten könnten. Dazu gehöre die Nutzung bestehender Personen mit Know-Hows zur Unterstützung staatlicher Strukturen und kritischer Infrastrukturen.

Das zweite Handlungsfeld ist „Internationale Rahmenbedingungen gestalten“. Um die IT-Sicherheit auf staatlicher Ebene zu gewährleisten, sei es unerlässlich, eine wirksame gegenseitige Abhängigkeit in Europa und der Welt aufzubauen. Die Bundeswehr setze sich für eine enge Zusammenarbeit mit seinen Partnern ein, beispielsweise im Rahmen der NATO, der EU und anderer internationalen Organisationen. Darüber hinaus sei die Ausarbeitung des Völkerrechts eine weitere Aufgabe, die besondere Aufmerksamkeit erfordere.

Als drittes Handlungsfeld wird der „Cyber-Raum als Operationsraum“ angeführt. Die organisatorischen, personellen und materiellen Anforderungen an die Betriebsführung im Cyber-Raum seien in einem gemeinsamen Bundeswehransatz zu erfüllen. Um die entsprechenden Truppen einzusetzen und Ressourcen in den Cyber-Raum zu investieren, plane die Bundeswehr, Strategien zur Verhinderung oder Eindämmung der CNAs zu entwickeln und Expertise zu CNOs sowie zu rechtlichen Aspekten zu erlangen.

Das vierte Handlungsfeld trägt den Titel „Chancen im Cyber-Raum nutzen“. Aufgrund der Vielfalt und Menge der verfügbaren Informationen sei Informationsmanagement notwendig. Die Eignung von Verfahren, die die Verwaltung von Informationen ermöglichen, müsse überprüft werden. Zusätzlich erhöhe die Fähigkeit, Netzwerkoperationen durchzuführen, einerseits die Effektivität militärischer Aktionen und andererseits die „digitale Verwundbarkeit“[21]. Es sei daher unentbehrlich, nicht nur über die Chancen, sondern auch über die Risiken der militärischen Nutzbarkeit des Cyber-Raums nachzudenken.

Das fünfte Handlungsfeld ist „Risiken im Cyber-Raum mindern“. Moderne Waffensysteme und militärische Kommunikationsmittel seien stark auf die IT angewiesen, weshalb schädliche Aktivitäten dagegen mit vorbeugenden Maßnahmen getroffen werden müssten. Zur Verbesserung der IT-Sicherheit werde eine homogene IT-Systemarchitektur aufgebaut und Risikomanagement eingerichtet, das die Konsequenzen eines Ausfalls oder einer Gefährdung minimiere. Zudem wird die Qualifizierung und Sensibilisierung der Mitarbeiter vorgeschlagen, um das Cyber-Bewusstsein zu verbessern.

Dieses Dokument bildet somit die Grundlage für die Stärkung der Bundeswehr im Cyber-Raum und die effektive Operationsführung im Informationsraum.

2. Bewertung

Als nächstes wird die „Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich

BMVg“ kritisch beurteilt. Es wird analysiert, ob die Cyber-Kriegstheorie Liffs von dieser Leitlinie angesichts der vier wichtige Aussagen zum Cyber-Krieg widergespiegelt wird.

1. Asymmetrie: Diese Leitlinie erkennt Asymmetrie an. Als strategischer Kontext im Cyber-Raum warnt dieses Dokument, dass die Häufigkeit der CNAs zunehme und „eine zunehmende Befähigung von Extremisten und Terroristen zu deren Ausübung nicht ausgeschlossen werden kann“[22]. Das BMVg schlägt also vor, dass selbst relativ schwache Akteure mit konventionellen Streitkräften in der Lage sein können, auf dem gleichen Niveau wie Staaten zu kämpfen, wenn sie Cyber-Technologien besitzen. Somit widerspricht diese Beschreibung die Behauptung Liffs.

2. Angriffsvorteil: Dieses Dokument trifft keine Aussage zum Angriffsvorteil. Stattdessen steht in der Leitlinie detailliert, dass „Strategien zur Verhinderung oder Eindämmung gegnerischer offensiver Cyber-Aktivitäten“ entwickelt werden sollen. Deswegen ist es schwierig zu beurteilen, ob die Behauptung Liffs hinsichtlich dieses Punkts widergespiegelt wird[23].

3. Anonymität: Die Leitlinie berücksichtigt Anonymität. Als ein Teil der CNVs in der Operationsführung wird dieser Aspekt wie folgt beschrieben: „Die Möglichkeit, reaktive Maßnahmen und Strategien einzusetzen, ist zu untersuchen. Als wichtige – wenn auch nicht hinreichende – Voraussetzung für eine politisch belastbare Zurechenbarkeit (Englisch: *attribution*) sind verbesserte Analysemethoden von Angriffen, u.a. in der Cyber-Forensik, anzustreben“[24]. Das heißt, die Bundeswehr der Ansicht hat, dass Anonymität nicht vollständig versichert wird, wenn bei forensischen Untersuchungen ausreichende Technologien eingesetzt werden. Insofern stimmt dieses Dokument mit der Argumentation Liffs überein.

4. Wirkungslosigkeit der Cyber-Abschreckung: In diesem Dokument gibt es keine direkte Erwähnung zur Wirkungslosigkeit der Cyber-Abschreckung. Die Bundeswehr berücksichtigt jedoch die Anwendung offensiver Cyber-Fähigkeiten in multinationalen Operationen. Wenn die Bundeswehr diese Fähigkeiten nicht nur als „unterstützendes, komplementäres oder substituierendes Wirkmittel“, sondern auch als Mittel zur Verhinderung von CNAs einsetzen

würde, würden diese Fähigkeiten zu einem Instrument der Cyber-Abschreckung[25].

Zusammenfassend lässt sich festhalten, dass die Cyber-Kriegstheorie Liffs von dieser Leitlinie in nur einem Punkt widergespiegelt wird. Grundsätzlich scheint es so zu sein, dass die Politik auf der allgemeinen Ansicht zum Cyber-Krieg basiert, nicht auf der Idee Liffs.

III. Fallstudie 2: „Weißbuch 2016: Zur Sicherheitspolitik und zur Zukunft der Bundeswehr“

Dieses Kapitel stellt das „Weißbuch 2016: Zur Sicherheitspolitik und zur Zukunft der Bundeswehr“ als einen weiteren Fall vor. Im Abschnitt 1 werden die Hauptargumente des Dokuments zusammengefasst. Im Abschnitt 2 wird analysiert, ob die Cyber-Kriegstheorie Liffs von diesem Weißbuch widergespiegelt wird.

1. Zusammenfassung des Dokuments

Zuerst werden die Hauptpunkte des „Weißbuchs 2016: Zur Sicherheitspolitik und zur Zukunft der Bundeswehr“ erklärt[26].

Weißbücher sind vom BMVg erstellte Dokumente, die Abwehrmaßnahmen der Bundesrepublik Deutschland und ihrer Verbündeten in den nächsten Jahren beschreiben. Ihr Ziel ist es, die Handlungsrichtlinie Deutschlands im Bereich der Sicherheit und der Verteidigung aufzuzeigen. Im Gegensatz zu den früheren Weißbüchern, die die organisatorischen Aspekte eingehend beleuchtet haben, fokussiert das Weißbuch 2016 die Sicherheitspolitik und bezeichnet die Cyber-Sicherheit zum ersten Mal als eine der größten Aufgaben der Bundeswehr.

In diesem Weißbuch wird der Cyber- und Informationsraum (CIR) wie folgt definiert: Erstens sei Cyber-Raum „der virtuelle Raum aller weltweit auf Datenebene vernetzten bzw.

vernetzbaren informationstechnischen Systeme“ und basiere auf dem Internet[27]. Zweitens stelle der Informationsraum ein Umfeld dar, „in dem Informationen generiert, verarbeitet, verbreitet, diskutiert und gespeichert werden“[28].

Die sichere und freie Nutzung dieses CIR sei die Grundlage für das staatliche und private Handeln in einer globalisierten Welt. Aber die Digitalisierung mache den Staat, die Gesellschaft und die Wirtschaft angreifbar gegen CNAs und das erfordere direkte Verteidigung. In diesem Weißbuch wird die Gewährleistung der Cyber-Sicherheit als ein staatlicher Auftrag anerkannt und die Zusammenarbeit zwischen den betreffenden Ministerien eingefordert. Erstens fielen die Aufgabenverwaltung und die Beschlüsse zur Cyber-Sicherheitspolitik in die Zuständigkeit des Bundesministeriums des Innern (BMI). Zweitens sei der Verteidigungsaspekt der bundesweiten Cyber-Sicherheit eine Hauptmission des BMVg und der Bundeswehr. Zuletzt liege die gesamte Verantwortung für die Entwicklung der internationalen Cyber-Sicherheitspolitik beim Auswärtigen Amt.

Zusätzlich zu den Gefahren im CIR erwähnt dieses Weißbuch die hybriden Bedrohungen. Demokratische Gesellschaften seien besonders anfällig für hybride Aktivitäten, weil sie mehr Angriffsbereiche böten. Alle Gebiete des sozialen Lebens könnten durch CNAs und Informationsmanipulation reizende Scheibe werden. Effektive Zusammenarbeit in den relevanten Politikfeldern sei also wichtig. Dazu gehörten der verstärkte Schutz kritischer Infrastrukturen, eine schnell einsetzbare Armee und das Problem des Bürgerschutzes.

2. Bewertung

Im Folgenden wird das „Weißbuch 2016: Zur Sicherheitspolitik und zur Zukunft der Bundeswehr“ bewertet. Es wird analysiert, ob die Cyber-Kriegstheorie Liffs von diesem Weißbuch angesichts der vier wichtigen Aussagen zum Cyber-Krieg widergespiegelt wird.

1. Asymmetrie: Das Weißbuch berücksichtigt diesen Aspekt. In Bezug auf die

Herausforderungen aus dem CIR wird wie folgt argumentiert: „Auch terroristische Gruppierungen, kriminelle Organisationen und versierte Einzelpersonen können potenziell mit geringem Aufwand erheblichen Schaden anrichten“[29]. Das heißt, dass das BMVg den CIR als einen Bereich betrachtet, in dem konventionell schwache Akteure infolge niedriger Eintrittsbarrieren die Fähigkeit haben, stärkere Staaten zu bedrohen. Somit widerspricht das Weißbuch der Behauptung Liffs.

2. Angriffsvorteil: Dieses Dokument erwähnt den Angriffsvorteil nicht. Stattdessen erklärt es detailliert den Aufbau eines CNV-Systems, in dem sich die Bundesrepublik für die Zusammenarbeit zwischen den Ministerien und die Wahrung des Völkerrechts voll engagiere. Deswegen fällt es schwer zu beurteilen, ob die Behauptung Liffs hinsichtlich dieses Punkts widergespiegelt wird.

3. Anonymität: Die Erwähnungen zur Anonymität sind besonders zahlreich. Beispielsweise heißt es: „Angriffe aus dem Cyber- und Informationsraum sind leicht zu tarnen. Dies erschwert, verbunden mit der qualitativen und quantitativen Vielfalt an Akteuren, die eindeutige Zuordnung von Angriffen“[30]. Das Weißbuch stellt ebenfalls fest: „Angesichts der derzeit immer noch cyber-inhärenten Attributionsproblematik ist die Gefahr der unkontrollierten Eskalation aufgrund eines Cyber-Vorfalls besonders groß“[31]. Das heißt also, dass die in diesem Weißbuch vorgeschlagenen CNV-Politik von Anonymität ausgeht. Deshalb kann gesagt werden, dass dieses Dokument der Behauptung Liffs nicht entspricht.

4. Wirkungslosigkeit der Cyber-Abschreckung: Obwohl das Weißbuch nicht davon ausgeht, dass Cyber-Abschreckung wirkungslos sei, wird diese als schwierig angesehen. Das Weißbuch weist darauf hin, dass „die konventionellen Instrumente der Abschreckung vor besonderen Herausforderungen“ stehen[32]. Somit wird die Idee Liffs sehr deutlich nicht widergespiegelt.

Abschließend zu diesem Fall lässt sich festhalten, dass die Cyber-Kriegstheorie Liffs von diesem Weißbuch größtenteils nicht widergespiegelt wird. Grundsätzlich scheint es, dass die Politik auf der Annahme beruht, dass der Cyber-Krieg revolutionär sei.

IV. Fallstudie 3: „Cyber-Sicherheitsstrategie für Deutschland 2016“

Dieses Kapitel stellt die „Cyber-Sicherheitsstrategie für Deutschland 2016“ als dritten Fall dar. Im Abschnitt 1 werden die Kernpunkte der Strategie zusammengefasst. Im Abschnitt 2 wird es analysiert, ob die Cyber-Kriegstheorie Liffs von dieser Strategie widergespiegelt wird.

1. Zusammenfassung des Dokuments

Zuerst werden die Kernpunkte der „Cyber-Sicherheitsstrategie für Deutschland 2016“ erläutert[33]. Nach einer Erklärung über diese Strategie werden die spezifische Maßnahmen in den vier Handlungsfeldern beschrieben.

Die „Cyber-Sicherheitsstrategie für Deutschland 2016“ ist eine Maßnahme der Cyber-Sicherheitspolitik, die im November 2016 beschlossen wurde, um die „Cyber-Sicherheitsstrategie für Deutschland 2011“ zu aktualisieren. In Deutschland, so konstatiert das Dokument, steige die technologische Komplexität an und damit verändere sich die Cyber-Bedrohungslage ständig. Gleichzeitig nähmen die Verwundbarkeit und die Möglichkeit des Missbrauchs im Cyber-Raum zu. Vor diesem Hintergrund werde Cyber-Sicherheit wichtiger. Der Staat und die Wirtschaft müssten das Fundament für Vertrauen bauen und auch im Zeitalter der Digitalisierung die Handlungsfähigkeit und die Souveränität bewahren. Und mit dieser Strategie werde ein ressortübergreifender strategischer Rahmen für die Aktivitäten der Bundesregierung im Bereich der Cyber-Sicherheit geschaffen.

Die Strategie setzt vier Handlungsfelder fest. Das erste Handlungsfeld heißt „Sicheres und selbstbestimmtes Handeln in einer digitalisierten Umgebung“. Die Fähigkeit, in einer digitalisierten Umgebung sicher und autonom zu handeln, sei eine bedeutende Grundlage für die Cyber-Sicherheit. Dazu müssten nicht nur die Bürger, sondern auch der Staat und die

Unternehmen die mit der Anwendung der Informationstechnologie verbundenen Risiken verstehen und ihr Handeln entsprechend anpassen. Zu diesem Zweck sieht diese Strategie vor, dass Maßnahmen wie die Förderung der digitalen Bildung, der Schutz der Kommunikation durch Verschlüsselung sowie die Zertifizierung kritischer IT-Geräte ergriffen werden müssen.

Das zweite Handlungsfeld trägt den Titel „Gemeinsamer Auftrag von Staat und Wirtschaft". Um die deutsche Cyber-Sicherheit auf einer hohen Ebene dauerhaft zu gewährleisten, seien eine verlässliche Zusammenarbeit und ein enger Austausch zwischen dem Staat und der Wirtschaft entscheidend. Deutsche Unternehmen müssten sich und ihre Kunden effektiv vor CNAs schützen. Insbesondere einheimische Provider und IT-Sicherheitsdienstleister spielten wichtige Rollen bei der Erkennung von CNAs. In dieser Sektion werden Maßnahmen zur Stärkung der nationalen IT-Wirtschaft und zur engen Zusammenarbeit mit Providern zum Schutz kritischer Infrastrukturen erklärt, um die Basis für einen zuverlässigen Informationsaustausch zu legen.

Das dritte Handlungsfeld ist „Leistungsfähige und nachhaltige gesamtstaatliche Cyber-Sicherheitsarchitektur". Auch im Cyber-Raum müssen die nationale Sicherheit, Gerechtigkeit und Freiheit garantiert sein. Dies setze eine hochmoderne Cyber-Sicherheitsarchitektur voraus, die verschiedene Akteure auf Bundesebene miteinander verbinde und jedes Bundesland, jede Gemeinde und die Wirtschaft einrechne. Dabei bereite der Staat ein breites Spektrum von Maßnahmen vor, von der Weiterentwicklung des Nationalen Cyber-Abwehrzentrums über die Stärkung der Strafverfolgung im Cyber-Raum bis hin zum Aufbau eines Frühwarnsystems für CNAs aus dem Ausland.

Das vierte Handlungsfeld ist „Aktive Positionierung Deutschlands in der europäischen und internationalen Cyber-Sicherheitspolitik". Um ein hohes Niveau an Cyber-Sicherheit zu erreichen, müsse Deutschland eine aktive Rolle bei der Ausarbeitung internationaler Cyber-Sicherheitspolitik spielen. Ein klarer rechtlicher Rahmen, der Vertrauensaufbau und die Erhöhung der weltweiten Resilienz stärkten den Schutz in Deutschland. Zu den spezifischen

Maßnahmen gehörten die Weiterentwicklung der Cyber-Verteidigungspolitik der NATO, die Initiierung eines auf internationale Cyber-Sicherheit spezialisierten Instituts sowie die regionale Unterstützung und Kooperation zum Aufbau von Cyber-Fähigkeiten.

Auf diese Weise deklariert die „Cyber-Sicherheitsstrategie für Deutschland 2016“ eine Fülle von Gegenmaßnahmen und bildet die Grundlage der aktuellen deutschen Cyber-Sicherheitspolitik.

2. Bewertung

Im Folgenden wird die „Cyber-Sicherheitsstrategie für Deutschland 2016“ bewertet. Es wird analysiert, ob die Cyber-Kriegstheorie Liffs von dieser Strategie angesichts der vier wichtigen Aussagen zum Cyber-Krieg widergespiegelt wird.

1. Asymmetrie: In der „Cyber-Sicherheitsstrategie für Deutschland 2016“ gibt es keine Erwähnung zur Asymmetrie. Vielmehr besteht die Richtlinie darin, deutsche Ressourcen für verschiedene Formen der CNV-Entwicklung bereitzustellen, zum Beispiel für die Förderung der digitalen Bildung, die Anlage eines Frühwarnsystems und die Gründung einer auf internationale Cyber-Sicherheit spezialisierten Forschungsanstalt[34]. In Bezug auf Asymmetrie kann daher gesagt werden, dass diese Strategie die Cyber-Kriegstheorie Liffs nicht widerspiegelt.

2. Angriffsvorteil: Das Dokument beschreibt nichts bezüglich des Angriffsvorteils. Deutschland scheint sich mehr auf die CNV-Entwicklung zu konzentrieren und die Seiten zur Erklärung des noch zu entfaltenden CNV-Systems zu nutzen. Deshalb ist es schwierig zu beurteilen, ob die Strategie hinsichtlich des Angriffsvorteils der Behauptung Liffs entspricht.

3. Anonymität: Die Strategie berücksichtigt den Aspekt der Anonymität. Zum Beispiel finden sich in Bezug auf die Cyber-Bedrohungslage die folgenden Aussagen: „Die Angreifer sind dabei technisch in der Lage, Cyber-Angriffe zu verbergen oder ihre Täterschaft zu

verschleiern. Daher sind Cyber-Angriffe und deren Ursprung immer häufiger nicht oder nur mit großem Aufwand und erheblicher Zeitverzögerung festzustellen“[35]. Das heißt also, dass nach der Strategie ein Angreifer im Cyber-Raum seine Verantwortlichkeit verstecken kann und aus dieser Fähigkeit die Schwierigkeit der Ermittlung folgt. Dies steht jedoch nicht mit der Behauptung Liffs im Einklang, weil die Strategie sich darauf konzentriert, wie Deutschland sich im Cyber-Krieg vor CNAs schützen können.

4. Wirkungslosigkeit der Cyber-Abschreckung: Die Strategie beinhaltet eine Erklärung zur Cyber-Abschreckung. Nach der Strategie besteht das Ziel Deutschlands bei der Formulierung der internationalen Cyber-Sicherheitspolitik darin, „die Resilienz der Alliierten und der Allianz insgesamt kontinuierlich zu erhöhen und nicht zuletzt im Kontext hybrider Bedrohungen die Abschreckungs- und Verteidigungsfähigkeiten zu steigern“[36]. Dies weist darauf hin, dass diese Strategie auf der Wirksamkeit der Cyber-Abschreckung beruht. Daher wird die Argumentation Liffs von diesem Dokument nicht widergespiegelt.

Als Schlussfolgerung lässt sich festhalten, dass sich die Cyber-Kriegstheorie Liffs nur in einem Punkt in der „Cyber-Sicherheitsstrategie für Deutschland 2016“ widergespiegelt. Die Strategie basiert insgesamt nicht auf wissenschaftlich-fachlichen Forschungsergebnissen.

V. Beurteilung der Forschungsfrage

In diesem Kapitel wird anhand der oben beschriebenen Fallstudien und der Überprüfung der These die Forschungsfrage beurteilt.

Abschließend wurde die These, dass die Cyber-Kriegstheorie Liffs nicht von der deutschen Cyber-Politik widergespiegelt wird, bewiesen. Erstens wurde weiter oben festgestellt, dassdie „Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg“ die Idee Liffs nur in einem der vier wichtigsten Aussagen zum Cyber-Krieg, der Anonymität, widergespiegelt. In Bezug auf die Asymmetrie nimmt sie im Vergleich zur Behauptung Liffs einen vollkommen

gegensätzlichen Blickpunkt ein, und sie erwähnt weder den Angriffsvorteil und noch die Wirkungslosigkeit der Cyber-Abschreckung. Daher wurde die Cyber-Kriegstheorie Liffs kaum reflektiert.

Zweitens spiegelt auch das „Weißbuch 2016: Zur Sicherheitspolitik und zur Zukunft der Bundeswehr“ die Behauptung Liffs in keinem der Hauptaussagen zum Cyber-Krieg wider. Hinsichtlich der Asymmetrie und der Anonymität widerspricht es die Idee Liffs, und es gibt keine ausdrückliche Erwähnung des Angriffsvorteils oder der Wirkungslosigkeit der Cyber-Abschreckung. Somit wird die Cyber-Kriegstheorie Liffs kaum widergespiegelt.

Drittens spiegelt die „Cyber-Sicherheitsstrategie für Deutschland 2016“ die Argumentation Liffs in nur einer der vier wichtigsten Aussagen zum Cyber-Krieg, der Wirkungslosigkeit der Cyber-Abschreckung, wider. Bezüglich der Asymmetrie und der Anonymität steht sie im Gegensatz zu Liff. Was den Angriffsvorteil angeht, findet sich keine entsprechende Aussage. Somit wird die Cyber-Kriegstheorie Liffs kaum reflektiert.

Es lässt sich resümieren, dass keine der drei untersuchten Dokumente über die Cyber-Sicherheitspolitik die Cyber-Kriegstheorie Liffs widergespiegelt. Vielmehr scheinen sie im Großen und Ganzen auf der allgemeinen Ansicht zuberuhen, dass der Cyber-Krieg revolutionär sei.

Schluss

Zusammenfassend lässt sich feststellen, dass sich die Cyber-Kriegstheorie Liffs nicht in der deutschen Cyber-Sicherheitspolitik widergespiegelt und daher die These dieser Arbeit bewiesen wurde. In der „Strategischen Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg“ wird von den Gedanken Liffs nur die Anonymität reflektiert. Im „Weißbuch 2016: Zur Sicherheitspolitik und zur Zukunft der Bundeswehr“ findet sich kein Widerhall der Ideen von Liff. Und in der „Cyber-Sicherheitsstrategie für Deutschland 2016“ wird die Behauptung Liffs

nur in Bezug auf die Wirkungslosigkeit der Cyber-Abschreckung reflektiert. Die deutsche Cyber-Sicherheitspolitik basiert somit auf der Überzeugung, dass der Cyber-Krieg revolutionär sei.

Deutschland ist nicht für eine vorbildliche Cyber-Sicherheitspolitik bekannt. Laut des Globalen Cyber-Sicherheitsindexes (Englisch: *Global Cybersecurity Index*) 2018 der Internationalen Fernmeldeunion, der das Engagement für Cyber-Sicherheit auf der Grundlage von fünf Säulen – rechtliche-, technische-, organisatorische-, Kapazitätsaufbau- und Kooperationsmaßnahmen – einschätzt, steht Deutschland an der 13. Stelle in Europa und an der 22. Stelle in der Welt[37]. Zum Vergleich: Großbritannien, Frankreich und Spanien, die alle wichtige staatliche Akteure in Europa sind, rangieren unter den Top 10 der engagiertesten Länder weltweit. Sandro Gaycken, ein IT-Sicherheitsexperte und Direktor des Projekt Wissenschaft für Frieden und Sicherheit Cyber-Verteidigung der Nato (Englisch: *NATO Science for Peace and Security Project Cyberdefense*), urteilte in einem Interview mit der Tagesschau: „Was in den vergangen Jahren an Sicherheitsmaßnahmen eingebaut wurde, steht auf einem sehr wackeligen Fundament. Deutschland realisiert erst jetzt, dass es selbst Sicherheitskonzepte entwickeln muss“[38]. Es scheint also, dass Deutschland seine Cyber-Sicherheitspolitik noch einmal überdenken muss.

Was bedeutet dieses Resultat? Es zeigt, dass die deutsche Cyber-Sicherheitspolitik gegenüber dem Cyber-Krieg sehr pessimistisch ist. Cyber-Kriege sind technologisch neu und komplex. Sie gehen teilweise über das menschliche Verständnis hinaus. Deshalb geht bei der Politikgestaltung die Angst oft einer emotional nicht aufgeladenen Analyse voraus. Es ist jedoch sinnlos, neue Strategien verängstigt zu planen, wenn sie weit von der Realität entfernt sind. Gegenwärtig ist die Cyber-Sicherheitspolitik vieler Länder äußerst ängstlich, aber es ist notwendig, die Politik auf der Grundlage wissenschaftlicher Ergebnisse zu überdenken.

Zum Schluss muss ein zukünftiges Forschungsthema erwähnt werden. Heute gibt es keine internationalen Rechtsnormen, die auf den Cyber-Raum anwendbar sind. Die liberal-

demokratischen westlichen Länder und die autoritären Staaten wie China und Russland stehen sich bei der Frage, wie das Internet und der Cyber-Raum geregelt werden sollen, in Opposition entgegen. Zum Beispiel haben Russland und China 2015 ein Cyber-Sicherheitsgeschäft unterschrieben, in dem sie sich verpflichten, keine Cyber-Angriffe gegeneinander durchzuführen und sich darauf einigen, gemeinsam gegen Technologien vorzugehen, die „die interne politische und sozioökonomische Atmosphäre destabilisieren“ oder „in die inneren Angelegenheiten des Staates eingreifen“ können[39]. Andererseits haben 27 Länder 2019 ein Cyber-Sicherheitsversprechen darüber unterzeichnet, was faire- oder unfaire Spiele im Cyber-Raum ausmacht – mit dem Hinweis, China und Russland zu verurteilen[40]. Wenn die internationale sozioökonomische Abhängigkeit vom Cyber-Raum zunimmt, wird dieser Mangel an Rechtsnormen ein schwereres Problem. Daher kann gesagt werden, dass der Aufbau von internationalen Rechtsnormen im Cyber-Raum ein repräsentatives Forschungsthema darstellt.

---

[1] 千草歩実「サイバー戦争の革命性―「スタックスネット」を事例に―」2020 年、1-2 頁（未公刊）。Die Einleitung ist eine deutschsprachige Fassung der entsprechenden Stelle in der Abschlussarbeit der Autorin.
[2] “The Sony Pictures Hack, Explained,” The Washington Post, 19. Dezember 2014.
[3] AP News, UN Probing 35 North Korean Cyberattacks in 17 Countries, 13. August 2019, https://apnews.com/ece1c6b122224bd9ac5e4cbd0c1e1d80 (zugegriffen 14. Dezember 2019).
[4] 「デジタル防衛へ G7 主導　外相宣言を採択、中ロ念頭に」『日本経済新聞』2019 年 4 月 6 日。
[5] 「「スパイ部品」官民で排除　車や防衛、業種ごとに指針・検証」『日本経済新聞』2019 年 4 月 7 日。
[6] 千草　「サイバー戦争論の革命性」2–3 頁。Dieser Abschnitt ist eine deutschsprachige Fassung der entsprechenden Stelle in der Abschlussarbeit der Autorin.
[7] 伊東寛『サイバー戦争論―ナショナルセキュリティの現在』原書房、2016 年、21 頁。
[8] 伊東　『サイバー戦争論』27–33 頁。
[9] United States Department of Defense, Summary of the 2018 National Defense Strategy, Januar 2019, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf (zugegriffen 21. September 2019).
[10] Richard A. Clarke and Robert K. Knake, Cyber War: The Next Threat to National Security and What to Do about It (New York: Harper-Collins Publishers, 2010), 6.
[11] 伊東『サイバー戦争論』41 頁。
[12] Ronald Deibert, “Cyber-Security,” The Routledge Handbook of Security Studies, 2nd ed., ed. Myriam D. Cavelty and Victor Mauer, (Milton: Routledge, 2017), 178.
[13] Adam P. Liff, “Cyberwar: A New ‘Absolute Weapon’? The Proliferation of Cyberwarfare Capabilities and Interstate War,” *Journal of Strategic Studies* 35, no. 3 (Juni 2012): 401-428.
[14] Liff, “Cyberwar,” 409.
[15] Charles L. Glaser and Chaim Kaufmann, “What Is the Offense-Defense Balance and Can We Measure It?” *International Security* 22, no. 4 (Frühlings 1998): 49-50.
[16] Robert Jervis, “Cooperation Under the Security Dilemma,” World Politics 30, no. 2 (Januar 1978): 187.
[17] Liff, “Cyberwar,” 412-413.
[18] Lawrence Freedman and Srinath Raghavan, “Coercion,” *Security Studies: An Introduction*, 3rd ed., ed. Paul D. Williams and Matt McDonald, (Milton: Routledge, 2018), 193, 196-197.
[19] Liff, “Cyberwar,” 417-422.
[20] Das Bundesministerium der Verteidigung, *Strategische Leitlinie Cyber-Verteidigung im Geschäftsbereich BMVg*, 16. April 2015, https://netzpolitik.org/2015/geheime-cyber-leitlinie-verteidigungsministerium-erlaubt-bundeswehr-cyberwar-und-

offensive-digitale-angriffe/ (zugegriffen 20. Januar 2020).
[21] BMVg, *Strategische Leitlinie Cyber-Verteidigung* (zugegriffen 20. Januar 2020).
[22] Ibid.
[23] Ibid.
[24] Ibid.
[25] Ibid.
[26] Das Bundesministerium der Verteidigung, *Weißbuch 2016: Zur Sicherheitspolitik und zur Zukunft der Bundeswehr*, Juli 2016, https://www.bundesregierung.de/resource/blob/975292/736102/64781348c12e4a80948ab1bdf25cf057/weissbuch-zur-sicherheitspolitik-2016-download-bmvg-data.pdf?download=1 (zugegriffen 20. Januar 2020).
[27] BMVg, *Weißbuch 2016*, 36 (zugegriffen 20. Januar 2020).
[28] BMVg, *Weißbuch 2016*, 37 (zugegriffen 20. Januar 2020).
[29] BMVg, *Weißbuch 2016*, 36 (zugegriffen 20. Januar 2020).
[30] BMVg, *Weißbuch 2016*, 37 (zugegriffen 20. Januar 2020).
[31] BMVg, *Weißbuch 2016*, 38 (zugegriffen 20. Januar 2020).
[32] BMVg, *Weißbuch 2016*, 37 (zugegriffen 20. Januar 2020).
[33] Das Bundesministerium des Innern, *Cyber-Sicherheitsstrategie für Deutschland 2016*, November 2016, https://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf (zugegriffen 20. Januar 2020).
[34] BMI, *Cyber-Sicherheitsstrategie*, 12-19 (zugegriffen 20. Januar 2020).
[35] BMI, *Cyber-Sicherheitsstrategie*, 7 (zugegriffen 20. Januar 2020).
[36] BMI, *Cyber-Sicherheitsstrategie*, 40 (zugegriffen 20. Januar 2020).
[37] Die Internationale Fernmeldeunion, *Global Cybersecurity Index (GCI) 2018,* 2019, 16, 60, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (zugegriffen 30. Januar 2020).
[38] Die Tagesschau, *Interview mit IT-Experten: "Die Gefahr eines Cyberkriegs ist real"*, 14. Februar 2019, https://www.tagesschau.de/inland/cybersicherheit-109.html (zugegriffen 30. Januar 2020).
[39] "Russia and China Pledge Not to Hack Each Other," The Washington Post, 8. Mai 2015.
[40] CNN, *27 Countries Sign Cybersecurity Pledge with Digs at China and Russia*, 23. September 2019, https://edition.cnn.com/2019/09/23/politics/united-nations-cyber-condemns-russia-china/index.html (zugegriffen 30. Januar 2020).