Der Cyber- und Informationsraum: Ein Überblick zur Sicherheit

Dennis Gottfried Hennecken, Bonn*

Die Bedeutung von Informationen und deren ständiger Fluss und Verfügbarkeit haben die Rahmenbedingungen der Sicherheitslage in Deutschland verändert. Die zunehmende Verwendung von informationstechnischen Systemen und die im gleichen Zug zunehmende Abkehr von alten Medien zur Meinungsinformation bergen ein erhebliches Gefahrpotenzial für die innere Sicherheit und die außenpolitische Position Deutschlands. Wie ist der neue „Raum" der Informationen rechtlich, politisch und faktisch einzuordnen? Ein Versuch.

Am 05.04.2017 wurde der neue Organisationsbereich Cyber- und Informationsraum im Geschäftsbereich des Bundesministeriums der Verteidigung aufgestellt.[1] Um aus einer rechtswissenschaftlichen Perspektive auf die Frage der Auswirkungen des Cyber- und Informationsraums (CIR)[2] auf die Sicherheit, sei es äußere oder innere, zu antworten, muss ein grundlegender Befund getroffen werden: das Thema ist *interdisziplinär*, dadurch äußerst komplex und nur schwer in seiner Gesamtheit geordnet zu überblicken. Bereits diese offenkundige Feststellung greift ein Kernproblem des CIR auf. Alle von ihm betroffenen Beteiligten aus den verschiedenen Disziplinen, seien es Wissenschaftler oder Praktiker, arbeiten zum jetzigen Zeitpunkt multidisziplinar. Dies vorweggeschickt möchte und kann ich in diesem Aufsatz nur den vorsichtigen Versuch wagen dem interessierten Studierenden einen groben Überblick über die Materie zu verschaffen. Ich will aber versuchen, Vernetzungen aufzuzeigen und ein weitergehendes Verständnis für den interdisziplinären Charakter des CIR zu wecken, um schließlich den Appell an alle Beteiligten und Interessierten im CIR zu richten, weiterhin eine einheitliche konzeptionelle Rahmenstruktur aufzubauen und aus dieser heraus gemeinsame Lösungsstrategien zu erarbeiten. Der Schwerpunkt soll dabei, dem Thema angepasst, auf Gefahren liegen, die durch die Öffentliche Hand zu besorgen sind.

Dazu werde ich zunächst den Begriff des CIR untersuchen. Hiervon ausgehend den Begriff der Sicherheit aus einer rechtswissenschaftlichen Perspektive näher beleuchten und die mit ihm im CIR befassten Akteure, staatliche wie private, herausarbeiten und versuchen einzuordnen. Abschließend werde ich in einer Zusammenfassung die nach meiner Sicht größten offenen Fragestellungen (Herausforderungen) aufzeigen. Letztere können nur in aller Kürze angerissen werden, um Denkanstöße zu vermitteln.

A. Was ist der CIR?

Nach der Definition des Aufbaustabes ist der CIR: „ein komplexes System und vereint in sich den Cyber-Raum, das Elektromagnetische Spektrum und das Informationsumfeld."[3] Ausgangspunkt des CIR ist die Information. Im Informationsraum wird sie durch Menschen geteilt und aufgenommen, im Cyber-Raum durch Maschinen.[4] Für diesen Aufsatz werde ich das elektromagnetische Spektrum als eigenen Teil des CIR ausklammern, da es eine Spezialmaterie darstellt, deren Erläuterung mehr Raum, gerade auf technischer Seite, beansprucht.

Die deutsche Regierung definiert den Cyber-Raum als „virtueller Raum aller weltweit auf Datenebene vernetzten bzw. vernetzbaren informationstechnischen Systeme. Dem Cyber-Raum liegt als öffentlich zugängliches Verbindungsnetz das Internet zugrunde, welches durch beliebige andere Datennetze erweitert werden kann."[5] Eine wichtige Erkenntnis ist somit, dass der Cyber-Raum zwar physische Komponenten besitzt, selbst aber ein digitaler Raum ist, der keine eigene physische Sphäre hat.[6]

Der Informationsraum definiert sich durch das Informationsumfeld, „den Raum, in dem Informationen aufgenom-

---

* Der Autor ist Rechtsberater und externer Doktorand bei Prof. Dr. Dr. h.c. *Matthias Herdegen*, Bonn. Er gibt ausschließlich seine persönliche Meinung wieder.

1 https://www.bmvg.de/resource/blob/10780/c868d16eae69008e936b6da227518020/30-03-17-bundesministerin-der-verteidigung-stellt-neues-kommando-cyber--und-informationsraum-auf-data.pdf, Abruf v. 05.08.2018.

2 Aufgrund der angenehmen Weite des Begriffs CIR, wird dieser von mir verwendet, um nicht schon aufgrund einer zu engen Definition wertvolle Seitengedanken abzuschneiden.

3 *Bundesministerium der Verteidigung*, Abschlussbericht Aufbaustab Cyber- und Informationsraum – Empfehlungen zur Neuorganisation von Verantwortlichkeiten, Kompetenzen und Aufgaben im Cyber- und Informationsraum sowie ergänzende Maßnahmen zur Umsetzung der Strategischen Leitlinie Cyber-Verteidigung, http://cir.bundeswehr.de/resource/resource/RXdrN2tBYVgyYVh2QWtpYkZXTnl0VXZuclJFOWhIbVExT1A5TkhwYlNNZFlLcXNITzZhSWdWVnhRcitJQVhJVVdNcmlJSms3RDE0MFBpNU1CNkQ4QVVzb2hjL1pEejFZaXBBTUpWSkNtbzQ9/Abschlussbericht%20Aufbaustab%20CIR.pdf, Abruf v. 05.08.2018.

4 vgl. *Bundesministerium der Verteidigung*, (Fn. 3).

5 *Bundesministerium des Innern*, Cyber-Sicherheitsstrategie für Deutschland – 2016, http://www.bmi.bund.de/cybersicherheitsstrategie/BMI_CyberSicherheitsStrategie.pdf, Abruf v. 26.07.2018.

6 *Castel*, Canadian journal of law and technology 10 (2012), 89 (90).

men, verarbeitet und weitergegeben werden. Dabei kann die Information durch Sprache, Gestik, Mimik, Handlung, Schrift oder Bild, direkt von Mensch zu Mensch, oder durch mediale Mittel wie Handys, Emails, etc. erfolgen."[7]

I. Was sind Informationen im Sinne des CIR?

Ich definiere für den CIR wie folgt[8]:
Informationen (engl. data) sind eine ungeordnete Sammlung von Auskünften, Angaben, Aussagen, Meldungen, sonstigen Mitteilungen oder einzelnen Daten, welche in jeglicher Form vorliegen können. Informationen bedingen keine zeitliche, logische Ordnung oder irgendwie geartete Brauchbarkeit.
Nachrichten (engl. information) sind nach Zeit, Brauchbarkeit oder anderen Kriterien geordnete und in Relation gesetzte Gruppen von Informationen zu einem bestimmten Sachverhalt. Sie stellen die Umwandlung von Informationen und Fakten in einen bewerteten Sachverhalt dar (Auswertung).
Erkenntnisse (engl. intelligence) sind schließlich durch eine eingehende Analyse bewertete Nachrichten und Informationen über einen bestimmten oder mehrere zusammenhängende Sachverhalte, welche eine spezifische (grundsätzlich in die Zukunft gerichtete) Fragestellung eines Entscheidungsträgers beantworten.
Wie wir sehen erschließt sich ein Sachverhalt, indem zunächst einzelne Informationen gesammelt, dann zu Nachrichten verdichtet werden und schließlich prognostisch zur Vorhersage von Erkenntnissen über bestimmte Absichten verwendet werden. Informationen dienen damit grundsätzlich der Vorbereitung einer Entscheidung. Um welche Entscheidung es sich hierbei handelt, hängt vom jeweiligen entscheidenden Akteur ab. Damit haben Informationen und die aus ihnen gewonnenen Erkenntnisse eine erhebliche Bedeutung für Entscheidungsträger, da sie ihnen überhaupt erst die Möglichkeit zum Entschluss eröffnen.

II. Wo befinden sich die Informationen im CIR?

Aus einer stark vereinfachten, rein technischen, Perspektive besteht der Cyber-Raum aus verschiedenen Schichten (layer).[9] Es unterscheiden sich dabei die physical, transport und application layer. Die physical layer beinhaltet die zur Verbreitung der Informationen erforderliche Hardware, d.h. das local area network, Router, Switches, Unterseekabel etc.[10] Die transport layer ist verantwortlich für die Bereitstellung von Daten für den entsprechenden Anwendungsprozess auf den Host-Computern.[11] Auf dieser Ebene findet die Verzahnung von Information und Informationstechnik statt. Die application layer schließlich beinhaltet die Benutzerschnittstelle, die für die Anzeige empfangener Informationen für den Benutzer verantwortlich ist.
In Bezug auf den Informationsraum gibt es keine feste räumliche Umgrenzung. Daher verwendet das ZOpKom, Zentrum Operative Kommunikation (ZOpKom) auch den Begriff des Informationsumfeldes. Das Informationsumfeld ist durch die rezipierenden und in ihm agierenden Personen eingegrenzt. Eine Schnittstelle zwischen Cyber-Raum und Informationsraum bilden die Social Media. Der Cyber-Raum kennt ebenfalls keine örtlichen geographischen Grenzen.

B. Was ist Sicherheit?

Der Begriff der Sicherheit ist umstritten. Dies liegt namentlich daran, dass Sicherheit zeit-, technik-, kulturell und sozial geprägt ist.[12] Juristisch ist der Begriff nicht legal definiert. Aus sozialwissenschaftlicher Sicht wird der Begriff der „inneren" Sicherheit durch eine Ableitung aus den Strafgesetzen bestimmt.[13] Danach umfasst „innere" Sicherheit „alle strafrechtlich sanktionierten kriminellen Handlungen im Inneren der Bundesrepublik"[14]. Für den Begriff der „äußeren Sicherheit" verwendet das Grundgesetz, wohl aus historischen Gründen, die Begriffe Frieden und Freiheit gleichbedeutend und meint dabei Determinanten für „äußere", gemeint als außenpolitische, Sicherheit. Erwähnt wird Sicherheit daher auch im Zusammenhang mit der „Wahrung des Friedens [in] einem System gegenseitiger kollektiver Sicherheit"[15]. Für den Bereich der „inneren Sicherheit" wird im Grundgesetz auf den unbestimmten Rechtsbegriff der „öffentlichen Sicherheit" abgestellt.[16] Insgesamt muss allerdings konstatiert werden, dass die Diskussion zur Auftrennung des Begriffs der Sicherheit in „innere" und „äußere" ein rein deutsches Phänomen zu sein scheint, das in anderen Rechtsordnung nicht geteilt wird. Diese Unterscheidung erschwert allerdings erheblich einen Konsens mit anderen Nationen auf internationaler Ebene zu erreichen. In diesem Zusammenhang ist insbesondere die Frage problematisch geworden, wie sich Sicherheit im Kontext der internationalen Beziehun-

---

7 *Zentrum Operative Kommunikation der Bundeswehr*, Über uns, http://cir.bundeswehr.de/portal/a/cir/start/dienststellen/ksa/zopkombw/ueber_uns, Abruf v. 07.08.2018.

8 Die folgenden Definitionen richten sich zum einen (für eine nationale Perspektive) nach § 2 Abs. 2 BND-Gesetz (BNDG) sowie (für eine internationale Perspektive) nach der *NATO Standardization Office,* AAP-06 – NATO Glossary of Terms and Definitions (English and French), Edition 2017, https://nso.nato.int/nso/zPublic/_BranchInfo/Terminology_Public/Non-Classified%20NATO%20Glossaries/AAP-6.pdf., Abruf v. 05.08.2018, präzisieren diese und sind für den CIR und das MilNW angepasst.

9 *Randel*, Internet Infrastructure and Organisation, 2018, S. 12.

10 *Randel*, (Fn. 9), S. 13 ff.

11 *Randel*, (Fn. 9), S. 19 ff.

12 *Gusy*, Freiheit und Sicherheit, http://www.bpb.de/politik/innenpolitik/innere-sicherheit/76651/freiheit-und-sicherheit, Abruf v. 05.08.2018.

13 *Bukow*, Deutschland – Mit Sicherheit weniger Freiheit über den Umweg Europas, in: Glaeßner/Lorenz (Hrsg.), Europäisierung der inneren Sicherheit – Eine vergleichende Untersuchung am Beispiel von organisierter Kriminalität und Terrorismus, 2005, S. 43 (43).

14 *Bukow*, (Fn. 13), S. 43.

15 Art. 24 Abs. 2 GG.

16 vgl. Art. 13 Abs. 4, Abs. 7; 35 Abs. 2 GG.

gen konkretisiert.[17] Hierbei erzeugen die widerstreitenden Meinungen ein Spannungsfeld, das nur schwer aufzulösen ist. Während die eine Seite einen „engen" Sicherheitsbegriff bevorzugt, der von Bedrohungen ausgeht, denen nur mit militärischen Mitteln zu begegnen ist, geht die andere Seite von einem „weiten" Sicherheitsbegriff aus, aufgrund dessen der Umfang der schützenswerten Güter erweitert wird und für den gewisse militärische Mittel zur Bestandssicherung als ungeeignet gehalten werden.[18]

Grundsätzlich wird Sicherheit aber negativ als „Abwesenheit von Gefährdung"[19] oder positiv als „Bestand von Werthaftem in der Zeit"[20] definiert werden dürfen.[21] Dabei entsteht ein Sicherheitsproblem immer dann, wenn das Sicherheitsgut durch Knappheit und/oder Widersprüchlichkeit eingeschränkt wird oder wenn Ungewissheit über dessen zukünftige Verfügbarkeit herrscht.[22]

Um für den CIR eine Definition von Sicherheit aufzustellen, muss vom schützenswerten Gut des CIR aus gedacht werden. Dieses Gut sind, wie schon gezeigt, Informationen. Die Bundesregierung definiert daher für den Teilbereich des Informationsbegriffes, der sich auf die zur Verarbeitung von Informationen notwendigen informationstechnischen Systeme bezieht, dass IT-Sicherheit „die Unversehrtheit der Authentizität, Vertraulichkeit, Integrität und Verfügbarkeit eines informationstechnischen Systems und der darin verarbeiteten und gespeicherten Daten"[23] ist. Diese Definition zeigt anschaulich die Gefahren auf, von denen Informationen betroffen sein können. Ich teile daher für den übergreifenden Begriff der Informationen im CIR drei Gruppen von Gefahren ein:

I. Informationsdiebstahl und -missbrauch

Informationsdiebstahl mit möglicherweise anschließendem Informationsmissbrauch ist das gezielte Ableiten von Informationen durch Unbefugte und in der Folge Verwenden der erlangten Informationen. Der Einbruch kann dabei durch das Ausnutzen von vorhandenen Sicherheitslücken (Exploit) oder durch das bewusste Schaffen solcher Lücken erfolgen. Dies kann zu Straftaten (Betrug, Diebstahl), Verrat von Geschäftsgeheimnissen (Spionage) oder zur illegitimen Ressourcennutzung führen.

Zur Veranschaulichung seien zwei Beispiele benannt. Erlangen Unbefugte Zugriff auf die Information über die Funktionsweise einer Maschine, die sich noch in der Konstruktionsphase befindet, können sie diese Informationen entweder selbst nutzen oder an andere verkaufen. Nutzen sie die Informationen selbst könnten sie Nachrichten über den Fortschritt des Projekts des Prototypen erlangen, die sie wiederum teurer verkaufen könnten, zum Beispiel an einen Konkurrenten. Schließlich könnten sie sogar Erkenntnisse erlangen über die voraussichtliche Markteinführung des Produkts. Ein anderes Beispiel ist das Erlangen von Kreditkartendaten und deren anschließende Verwendung im e-shopping. Eine besonders perfide Variante ist dabei auch personenbezogene Daten abzuleiten und somit die gesamte Identität anzunehmen.

II. Informationsmanipulation

Eine Informationsmanipulation liegt in der Veränderung des Inhalts einer Information, wobei der Inhaltsbegriff weit zu fassen ist und auch Metadaten umfasst. Zielsetzung einer Informationsmanipulation ist den eigentlichen Empfänger der Information aufgrund der Manipulation zu falschen Entscheidungen zu verleiten und ihn so zu beeinflussen bzw. zu lenken. Erhoffter Effekt ist dabei, dass für den Manipulierenden eine günstige Ausgangslage, sei es wirtschaftlich oder politisch, geschaffen wird.

Auch das neuere Phänomen der sog. „fake news" ist hiervon umfasst. Durch das bewusste Streuen von selbstgeschaffenen Informationen im Informationsumfeld werden die nachgeordneten Prozesse der Auswertung zu Nachrichten gestört und dadurch manipuliert. Zeitgleich erfolgt auch eine Manipulation des Informationsumfeldes und der in ihm agierenden Rezipienten selbst.

III. Informationsverlust und -ausfall

Unter Informationsverlust verstehe ich, die vollständige Zerstörung der Information, sei es durch physische Zerstörung oder durch die endgültige Verschlüsselung ohne Entschlüsselungsmöglichkeit. Es handelt sich somit um den endgültigen Verlust der Information. Davon zu unterscheiden ist der nur vorübergehende Informationsausfall. Dieser kann eintreten, wenn Informationen verschlüsselt werden und der Schlüssel gegen Lösegeld angeboten wird oder wenn die Informationen zwar im System gelöscht sind, aber durch ein vorhandenes Backup wieder aufgespielt werden können. Der Informationsausfall ist somit reversibel, zeitigt aber die gleichen Auswirkungen wie der Informationsverlust, in einer abgeschwächten Version würde man von Sabotage sprechen. Das hinter beiden Varianten verfolgte Ziel ist das vollständige Abschneiden der Information (black hole), verbunden mit der dadurch einhergehenden Handlungsunfähigkeit, insbesondere in der Planung und Entscheidungsfindung.

Alle drei oben benannten Gefahrengruppen haben gemeinsam, dass sie auf allen Ebenen, auf denen Informationen im CIR verfügbar sind, auftreten können. So kann der physische Ausfall von Hardware ebenso zu einem Informationsverlust führen, wie eine (unberechtigte) Verschlüsslung auf der application layer.

---

17 *Hellmann*, Sicherheitspolitik, in: Schmidt (Hrsg.), Handbuch zur deutschen Außenpolitik, 2013, S. 605 (606).

18 *Hellmann*, (Fn. 17), S. 606.

19 *Frei/Gaupp*, Das Konzept "Sicherheit" – Theoretische Aspekte, in: Schwarz (Hrsg.), Sicherheitspolitik – Analysen zur politischen und militärischen Sicherheit, 3. neu bearb. Aufl. 1978, S. 3 (5).

20 *Frei/Gaupp*, (Fn. 19), S. 5.

21 vgl. *Hellmann*, (Fn. 17), S. 606.

22 *Frei/Gaupp*, (Fn. 19), S. 7.

23 *Bundesministerium der Verteidigung*, (Fn. 3).

IV. Sicherheitsbegriff des CIR

Aus den oben aufgezeigten Szenarien lässt sich auf einen Sicherheitsbegriff des CIR schließen. Ich verstehe deshalb als Sicherheit im CIR: Die Freiheit der Informationen, die im nationalen Einflussbereich ausgetauscht oder bereitgehalten werden, von jedweder Form der Beeinflussung. Diese Definition gilt für äußere, wie innere Einflüsse gleichermaßen.

C. Welche Akteure nehmen im CIR Einfluss auf die Sicherheit?

Es gibt im Wesentlichen zwei Arten von Akteuren im CIR. Diejenigen, die versuchen Informationen, die ihnen nicht gehören oder die nicht für sie bestimmt sind, den oben benannten Gefahren auszusetzen (Sicherheitsgefährder) und diejenigen, die versuchen genau diese Informationen, vor den Versuchen der Erstgenannten zu schützen (Sicherheitsgaranten). Dabei können alle genannten Akteure sowohl auf staatlicher wie auch privater Seite stehen.

I. Sicherheitsgefährder

1. Script kiddies

Bei „Script kiddies" handelt es sich um Individuen, die über wenig geübte Fähigkeiten im Bereich der Informationstechnik verfügen, die aber durch die Nutzung von Skripts und vorgefertigten Programmen, welche durch Andere entwickelt wurden, Informationssysteme angreifen und Informationen auf diesen gefährden können.[24] Diese Gruppe handelt oft aus Nervenkitzel heraus und der vermeintlichen Anonymität der eigenen Handlungen. Dem Grunde nach können sie den Cyber-Raum selbst nicht direkt beeinflussen, aber aufgrund der Architektur des Internets besteht die Möglichkeit, dass ihre Handlungen (durch Ausnutzung von Vulnerabilities) in bestimmten Fällen größere Ausmaße annehmen können, welche sie selbst nicht (vollständig) übersehen können.[25] Informationsverluste erscheinen möglich, Informationsdiebstahl und deren anschließender Missbrauch aber unwahrscheinlich, da die Handelnden sich durchaus des (strafrechtlichen) Unrechts ihrer Handlungen bewusst sind und diese Schwelle erfahrungsgemäß nicht überschreiten wollen.[26]

2. Hacktivisten

Hacktivisten sind zumeist in dezentralisierten Gruppen organisiert, die auf einen bestimmten Sachverhalt fokussiert sind. Sie wählen ihre Ziele aufgrund von wahrgenommenen Missständen und bilden dabei eine Art Bürgerwehr. Meist ebbt die Flut der Angriffe relativ schnell ab, manche Hacktivisten erreichen aber auch eine dauernde Schädigung ihres Opfers.[27] Ziel ist zumeist die Informationsmanipulation der medialen Öffentlichkeit für Zwecke der jeweiligen Sache. In manchen Fällen auch durch Informationsverlust oder -ausfall die Position des Gegners in der Sache zu schwächen. Zu unterscheiden sind sie jedoch von Cyber-Kriminellen, die aus teilweise politischer Motivation handeln.

3. Cyber-Kriminelle

Bei Cyber-Kriminellen handelt es sich um Personen, die zur Verwirklichung von Straftaten, entweder auf informationstechnische Systeme angewiesen sind, weil diese ihr Ziel darstellen (Cybercrime) oder durch die Verwendung dieser Systeme den klassischen Kanon der Straftaten (einfacher) begehen können (cyber-enabled crime).[28] Cyber-Kriminelle verfolgen in erster Linie wirtschaftliche Interessen, so werden sie in der Regel aus eigenem Antrieb tätig. Sie können aber auch durch Dritte gegen Entgelt beauftragt werden, etwa um einen Konkurrenten zu schädigen, oder dessen Geschäftsgeheimnisse zu erlangen.

4. Nachrichtendienste

Staatliche Nachrichtendienste versuchen im Auftrag ihrer Regierung Informationen über andere Regierungen zu beschaffen, die sodann als Grundlage für Entscheidungen der eigenen Regierung dienen und tragen damit zur inneren und äußeren Stabilität ihres Landes bei.[29] Zu den Standardinstrumenten ausländischer Nachrichtendienste gehören dabei Informationsdiebstahl (u.a. in Form von Cyberspionage), Informationsverlust (u.a. Cybersabotage) und Informationsmanipulation (z.B. durch Desinformationskampagnen).[30] Ob Staaten dabei auch mit ihrer Privatwirtschaft zusammenarbeiten und erbeutete Informationen austauschen oder Ziele gemeinsam festlegen und angreifen, ist bisher nicht nachgewiesen worden, Vermutungen und Indikatoren legen dies aber nahe. [31]

5. Terroristen

Terroristen im CIR stellen eine Mischung aus den vorgenannten Gruppen dar. Zur Finanzierung ihrer Gruppe

---

[24] *HM Government*, National Cyber Security Strategy 2016-2021, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf, Abruf v. 12.08.2018.

[25] *Aigner/Gebeshuber/Hackner/Kania/Kloep/Kofler/Neugebauer/Widl/Zingsheim*, Hacking & Security – Das umfassende Handbuch, 2018, S. 35.

[26] *Aigner/Gebeshuber/Hackner/Kania/Kloep/Kofler/Neugebauer/Widl/Zingsheim*, (Fn. 25), S. 35.

[27] *HM Government*, (Fn. 24).

[28] *HM Government*, (Fn. 24).

[29] *Bundesministerium des Innern, für Bau und Heimat*, Verfassungsschutzbericht 2017, https://www.verfassungsschutz.de/download/vsbericht-2017.pdf, Abruf v. 14.08.2018.

[30] *Bundesministerium des Innern, für Bau und Heimat*, (Fn. 29).

[31] *Bundesministerium des Innern, für Bau und Heimat*, (Fn. 29).

arbeiten sie meist als Cyber-Kriminelle und versuchen durch Informationsdiebstahl und -missbrauch an Gelder zu kommen. Gerade in den Anfängen fehlte den Terroristen das notwendige Fachwissen, sodass sie meist wie Skript kiddies vorgingen und vorgefertigte Programme verwendeten. Mit dem Ziel ihre ideologische Position zu verbreiten und ihren eigenen Standpunkt zu verbessern, um unter anderem Nachwuchs zu rekrutieren, nutzen sie gezielte Informationsmanipulationen, ähnlich den Hacktivisten. Schließlich geht von ihnen auch die Gefahr eines Informationsverlustes aus, da auch sie erkannt haben, dass sie dadurch eine erhebliche Schwächung ihres Gegners, insbesondere bei hochtechnisierten Nationen, erreichen können.

II. Sicherheitsschützer/-garanten

Eine ausführliche Übersicht über die von staatlicher Seite handelnden Akteure und der gesamten Cyber-Sicherheitsarchitektur Deutschlands geben *Breternitz/Herpig*[32]. Ich will hier nur auf die meines Erachtens drei wichtigsten staatlichen Akteure eingehen, die auch in der „Cyber-Strategie für Deutschland 2011“[33] benannt werden.

1. Staatliche Behörden

Als Sicherheitsprovider sind die staatlichen Organe im Rahmen ihrer jeweiligen Zuständigkeiten verpflichtet die Sicherheit des CIR zu gewährleisten. Unter anderem dadurch entsteht die bereits angesprochene Interdisziplinarität.

a) Bundesministerium der Verteidigung (BMVg)

Das BMVg als „Herrin“ des von ihr definierten CIR zeichnet nach der Cyber-Sicherheitsstrategie[34] verantwortlich für den Bereich Cyber-Verteidigung. Dies umfasst nach der Definition der Bundesregierung „die in der Bundeswehr im Rahmen ihres verfassungsmäßigen Auftrages und dem völkerrechtlichen Rahmen vorhandenen defensiven und offensiven Fähigkeiten zum Wirken im Cyber-Raum, die zur Einsatz- und Operationsführung geeignet und erforderlich sind oder zur Abwehr von (militärischen) Cyber-Angriffen und damit dem Schutz eigener Informationen, IT, sowie Waffen- und Wirksysteme dienen.“[35]

b) Auswärtiges Amt

Das Auswärtige Amt setzt sich im Kern mit allen Fragen der Cyber-Außen- und internationalen Cyber-Sicherheitspolitik auseinander. Dabei liegt ein Fokus auch auf der Geltung von Menschenrechten im Cyber-Raum und der Nutzung wirtschaftlicher Chancen.[36] In Bezug auf die Sicherheitspolitik findet eine enge Verzahnung mit dem BMVg durch die gemeinsame Betreuung der Spitze der Bundesakademie für Sicherheitspolitik im Wechsel statt.

c) Ministerium des Innern, für Bau und Heimat

Das Innenministerium schließlich trägt die Federführung im Schwerpunkt in der IT-Sicherheit und ist dementsprechend federführend in den die IT-Sicherheit betreffenden Bereichen und Institutionen. Dies ändert sich an der Spitze im Nationalen Cyber-Abwehrzentrums (Cyber-AZ), das den Informationsaustausch zwischen den Bundesbehörden verbessert und in der Zukunft als zentralen Kooperations- und Koordinationsplattform dienen soll[37] oder bei der Gründung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich (ZITiS)[38].
(ISP) und ihre Cyber Emergency Response Teams (CERT) zu nennen (stellvertretend für den Bereich IT-Sicherheit), aber auch private Sicherheitsfirmen die sich sowohl mit der Erforschung von Vulnerabilities (etwa zur Entwicklung von Zero-Day-Exploits) als auch mit dem „härten“ von Systemen gegen Angriffe beschäftigen. Aufgrund der engen Anbindung an den Endnutzer, die jahrzehntelange Praxis durch die Begleitung des Internets seit seiner Entstehung und das dadurch bedingte flexible Handeln am Markt muss unterstellt werden, dass private Dienstleister stets einen gewissen Wissensvorsprung gegenüber staatlichen Institutionen haben werden. Dies ist in der Sache bedingt und hat sich in der Vergangenheit immer dann gezeigt, wenn staatliche Institutionen auf dem freien Markt Produkte von diesen Firmen erworben haben, um sich entweder selbst zu schützen oder das Produkt im Rahmen ihrer Zuständigkeit zu verwenden.

D. Fragestellungen und Herausforderungen für den Rechtsberater im CIR

Nach den oben festgestellten Befunden gilt es nun die juristischen Problemfelder im CIR zu identifizieren. Der Schwerpunkt soll, unter dem Gesichtspunkt des übergeordneten Themas der Sicherheit, bei den Juristen im CIR liegen, die in erster Linie für staatliche Sicherheitsschützer tätig sind. Ihre Perspektive ist diejenige der Sicherheit und der Stabilisierung dieser Sicherheit. Durch den strukturellen Aufbau und die in ihm wirkenden Akteure ist eine klare Grenzziehung zwischen „innerer“ und „äußerer“ Sicherheit, sowie zwischen kriminell und po-

[32] *Breternitz/Herpig*, Zuständigkeiten und Aufgaben in der deutschen Cyber-Sicherheitspolitik – Eine Übersicht, http://www.stiftung-nv.de/sites/default/files/cybersicherheitsarchitektur_papier.pdf, Abruf v. 04.08.2018.

[33] *Bundesministerium des Innern*, Cyber-Sicherheitsstrategie für Deutschland, http://www.cio.bund.de/SharedDocs/Publikationen/DE/Strategische-Themen/css_download.pdf, Abruf v. 05.08.2018.

[34] *Bundesministerium des Innern*, (Fn. 5).

[35] *Bundesministerium des Innern*, (Fn. 5).

[36] *Breternitz/Herpig*, (Fn. 32).

[37] *Bundesministerium des Innern*, (Fn. 5).

[38] *Bundesministerium des Innern*, (Fn. 5).

litisch motivierten Angriffen prima facie im CIR nicht möglich.[39] Dies erschwert die Rechtsberatung im CIR. Die folgende Aufstellung soll nur ein paar Fragestellungen aufzeigen, die ganze Tragweite wird sich dem geneigten Leser selbst schnell erschließen.

I. Auf nationaler Ebene

1. Zusammenarbeit der Sicherheitsschützer

Wie die bisherigen Ausführungen zeigen, hat der optimale Experte im CIR ein abgeschlossenes Studium der Informatik, der Rechts- und Politikwissenschaft und bestenfalls darüber hinaus noch Erfahrungen in der Intelligence Community gesammelt. In dieser erforderlichen Erfahrungsfülle liegt eine wesentliche Problemstellung. Um einen Sachverhalt des CIR in seinem multipolaren Ausmaß hinreichend erfassen zu können, ist eine enge Abstimmung und der Rückgriff auf Expertenwissen aus den jeweiligen Fachdisziplinen mit ihrer eigenen Entwicklungstradition und Fortentwicklung für das Recht des CIR erforderlich. Eine enge Abstimmung ist bisher zwischen BMVg und Innenministerium zu erkennen, das Auswärtige Amt hingegen scheint sich seit der letzten Cyber-Sicherheitsstrategie aus dem Jahre 2011 zurückgezogen zu haben. Hier gilt es Kooperationen zu verstärken und rechtliche Brücken zwischen den Ressorts zu bauen.

2. Herstellen von Sicherheit im Inneren zum Schutze der Bürger

Eine ganz wesentliche Fragestellung für Sicherheitsgaranten ist, wie sie Sicherheit für ihre Schutzbefohlenen (die Bürger) im CIR gewährleisten, ohne jedoch selbst zu Gefährdern dieser Sicherheit zu werden.

a) Grundrechte im CIR

aa) Meinungs- und Versammlungsfreiheit

So stellt sich beim Vorgehen gegen Hacktivisten die Frage, ab wann das Grundrecht aus Art. 5 Abs. 1 GG dieser Personengruppe eingeschränkt wird. Zu Bedenken ist dabei, dass jede herkömmliche Demonstration in Form einer Versammlung (insofern wäre Art. 8 GG spezieller anzuwenden) der Versuch einer Informationsmanipulation der öffentlichen Meinung ist. Dies ist aber völlig unstreitig durch das Grundgesetz gedeckt.

bb) Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme

Die Nachrichtendienste als Quell der Informationsgewinnung[40] haben ein erhebliches Eigeninteresse an Operationen im Cyber-Raum und Informationsumfeld. Erlaubt ist ihnen insofern die Brief-, Post- oder Fernmeldeüberwachung, wenn sich Cybercrimes (nach den §§ 202a , 202b, 303a , 303b StGB), gegen die innere oder äußere Sicherheit, insbesondere sicherheitsempfindliche Stellen oder lebenswichtiger Einrichtungen, Deutschlands richten.[41] Hierbei kommt es zu erheblichen Eingriffen in Grundrechte, die stets von Juristen mit der Befähigung zum Richteramt begleitet bzw. überwacht werden müssen, um die Rechtmäßigkeit des Handelns zu gewährleisten.

cc) Recht auf informationelle Selbstbestimmung

Bei der Verarbeitung von Informationen durch öffentliche Stellen ist die Frage nach der Ermächtigungsgrundlage zur Verarbeitung[42] insbesondere personenbezogener Daten zu stellen. Das neue BDSG gibt auf Grundlage der Datenschutz-Grundverordnung (DSGVO) rechtliche Vorgaben auf.

b) Daseinsvorsorge

Durch Verordnung sind die Kritischen Infrastrukturen im Sinne des § 10 Abs. 1 BSI-Gesetz festgelegt worden.[43] Damit wurde ein wesentlicher Schritt zur Absicherung der informationstechnischen Daseinsvorsorge geleistet. Der Schutz dieser Anlagen ist nunmehr Staatsauftrag, auch wenn diese privat betrieben werden.

c) Vorenthalten von Sicherheitslücken

Insbesondere die Frage, wie mit einer aufgefunden Sicherheitslücke umzugehen ist, für die bisher kein Patch entwickelt wurde (Zero-Day-Exploit), ist umstritten. Unter dem oben genannten Gesichtspunkt der Daseinsvorsorge scheint es zwingend, dass einer breiten Öffentlichkeit die Sicherheitslücke mitgeteilt wird, damit dieser möglichst schnell geschlossen und damit die Gefahr gebannt wird. Indes argumentieren insbesondere Sicherheitsgaranten mit dem Vorteil einer unentdeckten Sicherheitslücke bzw. eines Exploits für die eigene Informationsgewinnung über weitere Sicherheitslücken und auch zur eigenen aktiven Nutzung der Sicherheitslücke. Eine erste Entscheidung des Gesetzgebers hat diese Frage offen gelassen, indem dem Bundesamt für Sicherheit in der Informationsrechnik (BSI) auf Grundlage von § 7 Abs. 1 Nr. 1 lit. a BSI-Gesetz ein weiter Ermessensspielraum eröffnet wurde.

3. Gegenmaßnahmen

Noch offen ist, wie gegen erkannte Angriffe auf Informationen vorgegangen werden darf. Unstrittig dürfte die Unterbindung weitere Attacken, etwa durch Abschaltung oder Abschottung der Systeme (passive Abwehr) sein. Fraglich ist jedoch, ob auch ein Gegenangriff (zum Beispiel in

---

39 vgl. *Bundesministerium der Verteidigung*, (Fn. 3).

40 Vgl. § 2 BND-Gesetz (BNDG).

41 *Schallbruch*, Computer und Recht 2018, 215 (217).

42 Art. 4 Nr. 2 DSGVO.

43 BSI-Kritisverordnung.

Form eines hackback) auf den jeweiligen Verursacher zulässig wäre (aktive Abwehr).

4. Falsche Schwerpunktsetzung

Lange Zeit wurde der CIR aus einer rein technischen Perspektive betrachtet. Dementsprechend lag der Fokus für Juristen lange Zeit in der Bewertung der Qualität der technischen Beweise, wobei sehr schnell klar war, dass aufgrund der im CIR vorherrschenden Anonymität diese niemals ausreichen konnten. Auch wurde zunächst mit Schwerpunkt DDoS-Attacken betrachtet, die zwar über einen gewissen Zeitraum eine erhebliche Zahl der Angriffe ausmachten und auch den größten „sichtbaren" Schaden anrichteten, die im verborgenen stattfindenden Informationsdiebstähle wurde hierüber jedoch im öffentlichen Rechtsdiskurs lange stiefmütterlich behandelt.[44]

5. Das Nomenklaturproblem

Zwar handelt es sich bei dem Begriff des CIR um ein rein durch das BMVg national festgelegtes Terrain. Jedoch sind in ihm die unterschiedlichsten Beteiligte verpflichtet, umso wichtiger ist ein gemeinsamer Zeichenvorrat im CIR. Auf nationaler Ebene haben sich bisher noch keine festen Definitionen als herrschend durchgesetzt. Begriffe wie Cyber Security, Cyber Defense und Cybercrime werden teils unreflektiert als Synonyme verwendet, obwohl sie völlig unterschiedliche Bedeutungen haben. Blickt man auf die internationale Ebene verschlechtert sich die Situation zudem. Ein häufiger Irrtum ist die direkte Übersetzung aus dem Englischen. Der Begriff der Information operation (engl.)[45] ist nur eine Teilmenge der Operationen die im CIR ablaufen können und hat mit dem Begriff der Informationsoperationen[46] zwar eine gemeinsame Schnittmenge, ist aber deutlich nuancierter. Auch die bereits aufgezeigte Schwierigkeit in Bezug auf den Sicherheitsbegriff erschwert den internationalen, wie nationalen Diskurs. Im Bereich des Cyber-warfare bzw. in Zeiten des Cyber Frieden ergeben sich schließlich Schwierigkeiten, wie die einzelnen Cyber Network Operationen bestehend aus Computer Network Attack (CNA), Computer Network Defense (CND) und Computer Network Exploitation (CNE) zu verstehen sind. Insbesondere welche Maßnahmen von den jeweiligen Begriffen gedeckt sind und welche rechtlich zu einem bestimmten Stadium zulässig sind.

6. Das Unterscheidungsproblem

Bei einem Angriff auf Informationen ist zunächst schwierig den Angreifer genau zu identifizieren.

Das Vorgehen eines Nachrichtendienstes, Skript kiddies oder Cyber-Kriminellen unterscheiden sich in der Anfangsphase der Aufdeckung zumeist nicht wesentlich. Alle nutzen zumeist ähnliche, teils dieselben, Programme und Hilfsmittel. Die Identität des Angreifers stellt jedoch wesentliche Weichenstellungen für die Bearbeitung des Vorfalls. Von ihr hängt wesentlich die Zuständigkeit des Sicherheitsgaranten und die damit verbundene Bandbreite der rechtlich mögliche Reaktionen und inklusive etwaiger Komplikationen ab. So kann ein Sicherheitsgefährder der Informationendiebstahl begeht sowohl als Cyber-Krimineller unter nationales Recht fallen, als auch als prisoner of war dem Völkerrecht.[47]

II. Auf internationaler Ebene

Diese Fragestellung zeigt zugleich die verschwimmende Grenze von nationalem und internationalem Recht auf und schlägt damit die Brücke zur internationalen Ebene.

1. Das Abwarteproblem

Ein grundsätzliches Problem, das im Völkerrecht bekannt und immanent ist, besteht in der langsamen Reaktion auf Veränderungen, da das Völkerrecht ein Konsensrecht ist. Diese Haupteigenschaft der Diplomatie steht dem Geist des Informationszeitalters diametral entgegen. Sie führt im CIR, auf internationaler wie auf nationaler Ebene, zum Dilemma des gegenseitigen Abwartens. Kein Staat möchte den ersten Schritt tun, dies kann dabei durchaus tragfähige Gründe haben. Durch die Preisgabe gewisser Rechtsansichten lässt ein Staat etwa Rückschlüsse auf seine Tactics, Techniques and Procedures (TTPs), sowie die ihm hierfür zur Verfügung stehenden Mittel zu. Ohne die Mitteilung seiner Rechtsansicht kann aber keine *opinio iuris* entstehen, die zur Rechtssetzung im Völkerrecht aber erforderlich wäre. Rechtsmeinungen sind in der Vergangenheit vielfach geäußert worden[48], doch bisher stellen sich Staaten nicht hinter diese Ansichten, um sich Handlungsspielräume zu erhalten. Hier kommt es daher weniger auf weitere dogmatische Herleitungen an, als vielmehr auf eine konkrete politische Entscheidung.

2. Cyber deterrence

Im Bereich der Cyber-Außen- und internationalen Cyber-Sicherheitspolitik stellt sich derzeit die Frage, ob die Aufrüstung von Fähigkeiten im CIR mit der seinerzeit (Wett-)Aufrüstung von Massenvernichtungswaffen vergleichbar ist. In diesem Zusammenhang wird nunmehr von einer Strategie der Cyber Deterrence gesprochen, um eine Proliferation von Cyber-Waffen zu verhindern.

---

44 *Fabian A. Scherschel*, DDoS-Untersuchung: Angriffe werden zum Problem für die Allgemeinheit, https://heise.de/-3631903, Abruf v. 15.08.2018.

45 *Chairman of the Joint Chiefs of Staff*, Joint Publication 3-13, Information Operations.

46 *Stein/Marauhn*, Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 60 (2000), 1 (1).

47 Longobardo, Zeitschrift für ausländisches öffentliches Recht und Völkerrecht 77 (2017), 809 (822).

48 Beispielhaft statt aller *Schmitt/Vihul*, Tallinn manual 2.0 on the international law applicable to cyber operations, 2. Aufl. 2017.

3. Das Schwellenproblem

Ein lang bemühtes und noch immer nicht vollständig geklärtes Problem bereitet die Skalierung von Angriffen und die Möglichkeiten der Reaktion z.B. in Form von Gegenmaßnahmen. Im Zentrum steht hierbei meist die Auslegung des Art. 51 der UN-Charta. Problematisch ist, dass Operationen im CIR auch als politische Operationen ohne Anwendung militärischer Gewalt gesehen werden.[49] Diese Ansicht höhlt den Gewaltbegriff der UN-Charta vollständig aus und hält eine Rückzugsposition für Persistent objector bereit. Hier stellt sich die Frage, welches Ausmaß der Angriff haben muss und gegen wen er gerichtet sein muss.

4. Grauzonen

Schließlich befinden sich im Völkerrecht derzeit zahlreiche ausfüllungsbedürftige Grauzonen. Schmitt identifiziert diese, von denen einigen bereits hier angesprochen wurden, in den Gebieten der *Sovereignty, Intervention, Attribution, Due Diligence* und *Use of Force and Self-Defense*.[50]

E. Ausblick

Eine stark treibende Kraft war die militärische Komponente der Sicherheitspolitik in Form der Nato mit der Aufstellung des Cooperative Cyber Defence Centre of Excellence (CCDCoE) und der Etablierung einer regelmäßigen jährlichen Konferenz (CyCon). Auch die neusten Entwicklungen mit der Schaffung einer Agentur für Innovation in der Cybersicherheit durch die Bundesregierung sind in diesem Kontext sehr zu begrüßen.[51] Zu warnen ist aber vor der selektiven Finanzierung nur eines Ressorts und nur einer Ressource im CIR. Cyber- und Informationsraum bedeutet nicht Cyber-Raum, der Schutz von Informationen, nicht von informationstechnischen Systemen, muss im Vordergrund stehen.

Für den Rechtsberater im CIR gilt daher zwingend die Interdisziplinarität zu suchen und mit seinen Kolleginnen und Kollegen der anderen Ressorts, insbesondere den politischen Beraterinnen und Beratern, und dem privaten Sektor zusammenzuarbeiten.

---

[49] *Castel*, (Fn. 6), S. 93.

[50] *Schmitt*, The Yale Journal of International Law Online 42 (2017), 1.

[51] *DLF24*, "Agentur für Cyber-Sicherheit" geplant, https://www.deutschlandfunk.de/bundesregierung-agentur-fuer-cyber-sicherheit-geplant.1939.de.html?drn:news_id=913063, Abruf v. 15.08.2018.