Bundesakademie
für Sicherheitspolitik

Arbeitspapiere Sicherheitspolitik | Ausgabe 2/2014

Cyber-Security
Eine Frage der Begriffe

Die Arbeitspapiere Sicherheitspolitik

Die Bundesakademie für Sicherheitspolitik publiziert seit 2014 ihre „Arbeitspapiere Sicherheitspolitik“, die sie der interessierten Öffentlichkeit zur Verfügung stellt. Sie erscheinen unregelmäßig, weil wir auf diese Weise schnell auf aktuelles Geschehen und aktuellen Bedarf eingehen können. Dementsprechend veröffentlichen wir hier auch unterschiedliche Textformen: von Workshop-Arbeitsergebnissen über ausführliche Konferenzberichte bis hin zu detaillierten sicherheitspolitischen Analysen unserer Mitarbeiter sowie externer Autorinnen und Autoren.

Die Arbeitspapiere versenden wir in der Regel per E-Mail mit Hilfe unseres Newsletters „Infobrief Sicherheitspolitik“. Sämtliche Arbeitspapiere finden Sie auch auf unserer Website: www.baks.bund.de/de/service/arbeitspapiere-sicherheitspolitik.

Eine Frage der Begriffe

von Christine Hegenbart

Es wirkt wie ein Allgemeinplatz, aber der korrekte Umgang mit allem, was die Vorsilbe „Cyber-“ besitzt, ist dringend notwendig. Eine Einordnung

Schon länger diskutiert die sicherheitspolitische Community die Dimension der Bedrohungen aus dem Cyber-Raum intensiv. Konzeptionelle Unschärfe und Ungenauigkeiten stiften in dieser Debatte oft Verwirrung. Wie in allen Fachdebatten ist die verwendete Terminologie von zentraler Bedeutung, wenn es darum geht, die Bedrohung einzuschätzen. Denn unterschiedliche Begriffe haben unterschiedliche Bedeutungen und Konsequenzen.

Der Begriff „Cyber-Krieg“ verweist beispielsweise auf ein hohes Bedrohungspotential und schreibt die Zuständigkeit für Gegenmaßnahmen dem Militär zu. Demgegenüber vermittelt der Begriff „Cyber-Kriminalität“ eine niedrigere Bedrohungseinschätzung und legitimiert die Polizei, die Delikte zu verfolgen. Allein dieser Unterschied in der Wortwahl veranschaulicht, wie nützlich *und notwendig* angemessene Definitionen sind. Wo liegen also die begrifflichen Fallstricke der Cyber-Debatte?

Definitionen von Cyber-Konflikttypen

Gefahren aus dem Cyber-Raum können in unterschiedlichen Ausprägungen auftreten, die nicht immer leicht zu differenzieren sind. Absolute Trennschärfe in der Cyber-Terminologie wird kaum zu erreichen sein. Allerdings erscheint es zweckmäßiger auf nicht ganz präzise Definitionen zurückzugreifen, als ganz auf +

sie zu verzichten. Als Grundlage für zukünftige Diskussionen sind sechs Konflikttypen denkbar, die auf den amerikanischen Sicherheitsexperten James A. Lewis und die Schweizer Wissenschaftlerin Myriam Dunn Cavelty zurückgehen.

(1) Hacktivismus und Cyber-Vandalismus

Das Wort Hacktivismus setzt sich aus den Begriffen „Hacking" und „Aktivismus" zusammen. Es bezeichnet Aktivitäten von Privatpersonen oder staatlich unabhängigen Gruppen, die Computer oder Computernetzwerke für politischen Protest nutzen. Hacktivisten zielen darauf ab, mittels verschiedener Hacking-Methoden den Zugriff auf Informationen im Internet zu stören. Sie verändern beispielsweise den Inhalt von Internetseiten oder unterbinden den Zugriff auf Online-Dienste.

Demgegenüber stehen hinter Cyber-Vandalismus keine politischen Ziele. Die Motive sind im Bedürfnis des Hackers zu suchen, die Grenzen seines Könnens auszutesten und Selbstbestätigung zu erfahren.

(2) Cyber-Kriminalität

Cyber-Kriminelle agieren als Einzeltäter oder in Gruppen, die mehr oder weniger gut organisiert und ausgerüstet sind. Ihre illegalen Aktivitäten im Cyber-Raum sind darauf aus, finanzielle Gewinne zu erzielen. Dabei können sowohl Einzelpersonen als auch Unternehmen geschädigt werden. Die Straftaten weisen eine große Bandbreite auf und umfassen Delikte wie zum Beispiel Kreditkarten- und Warenbetrug, Identitätsdiebstahl und Erpressung.

(3) Cyber-Spionage

Es gibt zwei Ausprägungen von Cyber-Spionage: zum einen Wirtschaftsspionage und zum anderen politisch-militärische Spionage. Im ersten Fall sind die Akteure Unternehmen, die hoch entwickelte IT-Methoden für Spionagezwecke nutzbar machen: Sie versuchen, an vertrauliche Geschäftsinformationen und intellektuelles Firmeneigentum von hohem ökonomischen Wert zu gelangen.

Im zweiten Fall sind die Akteure Staaten, insbesondere Nachrichtendienste oder hochprofessionelle private Hacker, die in staatlichem Auftrag Spionage über den Cyber-Raum betreiben. Im Zentrum ihrer Aktivitäten stehen die verdeckte und illegale Beschaffung von sensiblen und klassifizierten Informationen ausländischer Regierungsinstitutionen und deren Streitkräfte. Attraktiv sind beispielsweise Informationen über militärische Kapazitäten und Strategien sowie Verteidigungskonfigurationen von einzelnen Zielcomputern oder ganzen Systemen.

(4) Cyber-Sabotage

Auch mit Blick auf Cyber-Sabotage muss man zwischen wirtschaftlichen und politisch-militärischen Absichten unterscheiden. Die Grenzen zwischen Cyber-Spionage und Cyber-Sabotage sind indes nicht leicht festzumachen: Zum einen sind bei beiden Konflikttypen dieselben Akteure aktiv. Zum anderen dienen die Informationen, die durch Cyber-Spionage gewonnen werden, als Grundlage für Cyber-Sabotageaktionen. Letztere nutzen solche Erkenntnisse über Sicherheitslücken und Verteidigungskonfigurationen aus.

Bei Cyber-Sabotage muss man zwischen wirtschaftlicher und politisch-militärischer Absicht unterscheiden – doch die Grenze zwischen Sabotage und Spionage ist verwischt.

Somit richtet sich Cyber-Sabotage gegen die Integrität und Verfügbarkeit von wichtigen IT-Systemen und Prozessen. Dies führt zur Zerstörung oder massiven Schädigung von technischer Ausrüstung oder gespeicherten Informationen. Dahinter stehen zumeist politische Ziele. Cyber-Sabotage ist – im Unterschied zu Cyber-Vandalismus – relevant für die nationale Sicherheit. Die Schwelle zum Cyber-Krieg wird jedoch nicht überschritten.

(5) Cyber-Terrorismus

Terroristische Netzwerke und Gruppen sowie radikalisierte Individuen können über den Cyber-Raum ihre politischen und ideologischen Ziele verfolgen. Mittels systematisch geplanter Gewaltaktionen, die zu materieller Zerstörung führen, wollen Cyber-Terroristen Aufmerksamkeit auf ihre Ideale und Werte lenken. Potentielle Ziele, die sie über den Cyber-Raum angreifen können, sind vor allem kritische Infrastrukturen.

Terroristische Cyber-Anschläge können beispielsweise Trinkwasservorräte kontaminieren oder Flugzeugabstürze und massive Stromausfälle verursachen. Sie haben somit das Potential nicht nur kostspielige Störungen hervorzurufen, sondern vielmehr zu Personen- oder Sachschäden zu führen.

(6) Cyber-Krieg

Nationale Streitkräfte oder staatlich finanzierte militärische Einheiten und andere offiziell autorisierte Gruppen, wie zum Beispiel so genannte „Cyber-Milizen", können Cyber-Techniken einsetzen, um eine kriegerische Auseinandersetzung zu führen. Diese aggressiven Aktivitäten im Cyber-Raum haben massive physische Auswirkungen auf die reale Welt.

Ohne materielle Schäden oder Verletzte ist ein Cyber-Konflikt nicht als Cyber-Krieg zu klassifizieren. Auch ist diese Zuschreibung nicht korrekt, wenn der Aggressor *kein* staatlicher Akteur ist. Eine Kriegshandlung (act of war) umfasst die zwischenstaatliche Anwendung von Gewalt (use of force), die politischen Zwecken dient. Dieses Prinzip ist auch auf den Cyber-Raum anzuwenden.

Eigenschaften und Mittel des Cyber-Kriegs

Cyber-Krieg beziehungsweise „cyber war" ist ein mehrdeutiger und kontrovers diskutierter Begriff. Vor allem die Medien überstrapazieren ihn, indem sie ihn geradezu inflationär verwenden. Eine genauere Betrachtung ist daher notwendig.

Das so genannte Attributionsproblem bezeichnet die Schwierigkeit einen Cyber-Angriff zurückzuverfolgen. Mit Blick auf Cyber-Kriege ist diese Problematik nur eingeschränkt relevant. Digitale Kampfhandlungen stehen normalerweise in Zusammenhang mit einem zwischenstaatlichen Konflikt und dienen dazu, konventionelle militärische Aktionen zu unterstützen.

» Es besteht die Gefahr, dass Entscheidungsträger die Wirkung von Cyber-Waffen einerseits und die Reaktionen des Kontrahenten andererseits falsch einschätzen.

In diesem Fall wäre es präziser, den Konflikttyp mit Cyber-Kriegsführung zu umschreiben. Dabei zielen militärische Cyber-Einheiten darauf ab, die Dominanz im Kampfgeschehen über Kommunikations- und Informationssysteme zu erreichen: Taktisch verwendete Cyber-Mittel ermöglichen oder erleichtern konventionelle Offensivmaßnahmen. So ist es beispielsweise möglich, die Daten von Waffen- und Radarsysteme zu manipulieren oder ganze Anlagen auszuschalten, um damit die Waffenwirkung des Gegners zu reduzieren. Darüber hinaus können Cyber-Angriffe die Funktionsfähigkeit von kritischen Infrastrukturen einschränken oder ganz zum Erliegen bringen. Diese Formen der Cyber-Kriegsführung werden eine bedeutende Rolle in allen zukünftigen bewaffneten Konflikten spielen.

Im Gegensatz dazu erscheint ein militärischer Konflikt, der sich ausschließlich Cyber-Mittel bedient und nicht im Zusammenhang mit einer kriegerischen Auseinandersetzung steht, wenig wahrscheinlich. Es ist zwar technisch möglich, schwerwiegende und lähmende Cyber-Angriffe auszuführen, ohne einen politischen und militärischen Konflikt als Kontext ist dies aber kaum vorstellbar. Gegenwärtig haben nur China, Russland, Israel, Frankreich, Großbritannien und die USA entsprechend hochentwickelte technologische Fähigkeiten. Auch können die Risiken einer Cyber-Attacke für den Angreifer schwerer wiegen als seine Vorteile. Zudem teilen potentielle Angreifer die Unfähigkeit, sich gegen einen hoch entwickelten Cyber-Gegenschlag zu verteidigen.

Solche Abwägungen berücksichtigen die spezifischen Eigenschaften von Cyber-Waffen. Zu ihren Vorteilen zählen unter anderem vergleichsweise geringe Anschaffungskosten, schnelle Wirksamkeit und Heimlichkeit, mit der sie eingesetzt werden können, sowie der daraus resultierende Überraschungseffekt.

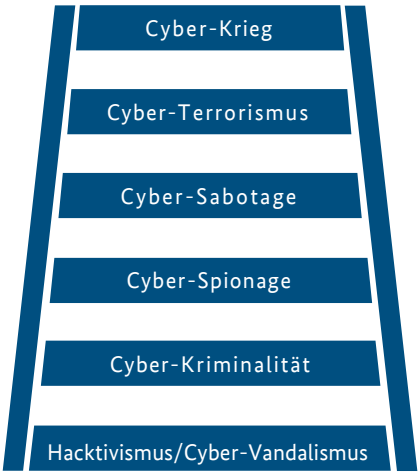
Dennoch haben Cyber-Waffen einige nicht zu vernachlässigende Nachteile. Sie sind nicht kontrollierbar im militärischen Sinn: Cyber-Waffen sind nicht zuverlässig und können Auswirkungen haben, die nicht beabsichtigt oder sogar kontraproduktiv sind. Darüber hinaus müssen sie speziell auf ein bestimmtes Ziel zugeschnitten sein und sind daher oft nur einmal verwendbar (single use). Vor allem aber stellen viele – von Medien bis zur Sicherheitsindustrie und -beratern – ihr Zerstörungspotential oft übertrieben dar.

Cyber-Waffen können lediglich indirekten Schaden verursachen, da sie allein die Kraft und Energie ihres Ziels nutzen. Die Auswirkungen von Cyber-Angriffen sind so nur schwer mit konventionellen militärischen Operationen und unter keinen Umständen mit Nuklearangriffen zu vergleichen.

Aufgrund dieser Eigenschaften von Cyber-Waffen und der Unsicherheit darüber, was überhaupt einen *act of war* im Cyber-Raum konstituiert, werden die zuständigen Entscheidungsträger die Anordnung von Cyber-Angriffen mit großer Sorgfalt abwägen müssen: Es besteht die Gefahr, die Wirkung dieser Waffen einerseits und die Reaktionen des Kontrahenten andererseits falsch einzuschätzen. Hierdurch können Konflikte eskalieren und letztendlich einen Vergeltungsschlag außerhalb des Cyber-Raums mit konventionellen Waffen provozieren.

Die Cyber-Konflikt-Eskalationsleiter

Die Bedrohung aus dem Cyber-Raum hält unvermindert an. Insbesondere ist zu beobachten, dass die Angreifer sich zunehmend professionalisieren und folglich die technische Qualität der Cyber-Vorfälle insgesamt zunimmt. Dennoch ist die sprachliche Darstellung dieser Entwicklungen, unter anderem in den Medien, häufig übertrieben und undifferenziert. Dabei dominieren Begriffe wie „Cyber-Angriff“ und „Cyber-Krieg“, auch wenn es um nicht- +



militärische Vorfälle geht, die keine Bedeutung für nationale Sicherheit haben.

Um die aktuelle Bedrohungslage möglichst objektiv einschätzen zu können, muss man die eben beschriebenen Konfliktdefinitionen so präzise wie möglich anwenden. Es hilft, hierfür das Bild einer „Cyber-Konflikt-Eskalationsleiter" heranzuziehen. Sich dieses Modell zu vergegenwärtigen, erlaubt militärischen und politischen Entscheidungsträgern, ein Verständnis für die Bedrohung zu entwickeln, Prioritäten zu setzen und über die angemessensten Gegenmaßnahmen zu entscheiden.

Die Leiter visualisiert zwei zentrale Eigenschaften der eben vorgestellten Konflikt-Typen: Sie lenkt die Aufmerksamkeit sowohl auf die Häufigkeit von Angriffen, als auch auf das Ausmaß der Schadenswirkung. Die Eskalationsleiter führt von der Konfliktart, die am häufigsten vorkommt, zu der, die am seltensten zu beobachten ist. Auch reicht sie von der Angriffsart, die am wenigsten, zu der, die am meisten Schaden verursacht.

Gemäß dem Leitermodell sind die vorherrschenden Konfliktformen Hacktivismus beziehungsweise Cyber-Vandalismus, Cyber-Kriminalität und Cyber-Spionage. Die ersten beiden sind nicht von direkter militärischer Bedeutung – sie betreffen ausschließlich die allgemeine Einsatzbereitschaft von Streitkräften – und haben nur geringen Einfluss auf nationale Sicherheit. Ihnen kann durch die gängigen IT-Sicherheitsmaßnahmen begegnet werden. Die strafrechtliche Verfolgung der Taten fällt in den Zuständigkeitsbereich von zivilen Behörden.

Cyber-Spionage nimmt eine Sonderstellung ein: Einerseits sind die Übergänge von Cyber-Spionage zu Cyber-Sabotage fließend; andererseits können die gewonnenen Erkenntnisse auch für Cyber-Terrorismus oder Cyber-Kriegsführung genutzt werden. Cyber-Spionage kann also indirekt massiven Schaden verursachen, so dass man der Abwehr dieses häufigen Konflikttyps besondere Aufmerksamkeit schenken muss. Die Umsetzung anspruchsvoller Sicherheitsmaßnahmen, etwa um militärische Netzwerke der Bundeswehr zu schützen, ist folglich zwingend notwendig.

Cyber-Spionage wird auch mit Blick auf das Völkerrecht nicht sanktioniert. Ebenso wie konventionelle Spionage ist sie gemäß der meisten nationalen Rechtsprechungen eine nach dem Gesetz strafbare Handlung und kann von zivilen Behörden verfolgt werden.

Die anderen drei Konflikttypen – Cyber-Sabotage, Cyber-Terrorismus und Cyber-Krieg – sind, wie die Eskalationsleiter veranschaulicht, am seltensten. Sie sind dennoch von Bedeutung, da sie potentiell hohe Schadenswirkung und damit auch Auswirkungen auf nationale und internationale Sicherheit haben.

Bisher wurden nur wenige Cyber-Angriffe beobachtet, die Eigentum beschädigt oder zu ernsthaftet und langanhaltenden Störungen geführt haben. Allein der gegen das iranische Atomprogramm gerichtete Computerwurm Stuxnet hat

eine zerstörerische Wirkung entfaltet und gilt als physischer Cyber-Angriff im zwischenstaatlichen Bereich .

Es gibt keine Beispiele dafür, dass tatsächlich Menschenleben gefährdet wurden. Einen eigenständigen kriegerischen Akt im Cyber-Raum, der als Cyber-Krieg zu bezeichnen wäre, hat es bisher nicht gegeben. Allerdings bauen viele Staaten ihre Fähigkeiten zur Cyber-Kriegsführung weiter aus, was das Problem langfristig verschärfen kann.

Konsequenzen für Deutschland

Die Bundesregierung sollte einer verbalen Militarisierung des Cyber-Raums entgegenwirken und Cyber-Konflikte gezielt sprachlich realistisch darstellen.

Die Gefahren aus dem Cyber-Raum sind nicht primär militärisch. Ist jedoch die nationale Sicherheit betroffen – wie bei Cyber-Sabotage, Cyber-Terrorismus und Cyber-Krieg – sind die Streitkräfte, also die Bundeswehr, wichtige verantwortliche Akteure.

Allerdings sollte die Bundesregierung, beispielsweise durch die Presse- und Öffentlichkeitsarbeitsabteilungen von Ministerien und Behörden, einer verbalen Militarisierung des Cyber-Raums entgegenwirken und Cyber-Konflikte gezielt sprachlich realistisch darstellen. Reine Cyber-Kriege sind, wie beschrieben, kein absehbares Zukunftsszenario. Wird der Begriff „Krieg“ überstrapaziert, kann dies zu Fehleinschätzungen oder gar Überreaktionen führen und in letzter Konsequenz zur Eskalation von Konflikten beitragen.

Klare, allgemein anerkannte Definitionen, wie die eben vorgestellten, sind für den rhetorischen Umgang mit Cyber-Konflikten grundlegend. Je konkreter die Bedrohungen definiert sind, desto einfacher können die verantwortlichen Akteure sie durch angemessene Cyber-Sicherheitsstrategien angehen. ■

Autorin:
Christine Hegenbart ist Wissenschaftliche Mitarbeiterin der Akademie für Politik und Zeitgeschehen der Hanns-Seidel-Stiftung

mehr zum Thema:
www.baks.bund.de/de/aktuelles/neustart-gewuenscht

Bildnachweise
Cover (von links oben nach rechts unten): Eneas De Troya/CC BY 2.0, Crown Copyright/MoDUK, BAKS/Mario Gabler

Herausgeber
Bundesakademie für Sicherheitspolitik
Schlossanlage Schönhausen
Ossietzkystraße 44/45 | 13187 Berlin

Redaktionsleitung
Martin Lammert

Redaktion
Marcus Mohr

Druck
BAKS

Gestaltung
Marcus Mohr

Kontakt
Telefon 030 40046-230
Telefax 030 40046-421
E-Mail info@baks.bund.de

www.baks.bund.de