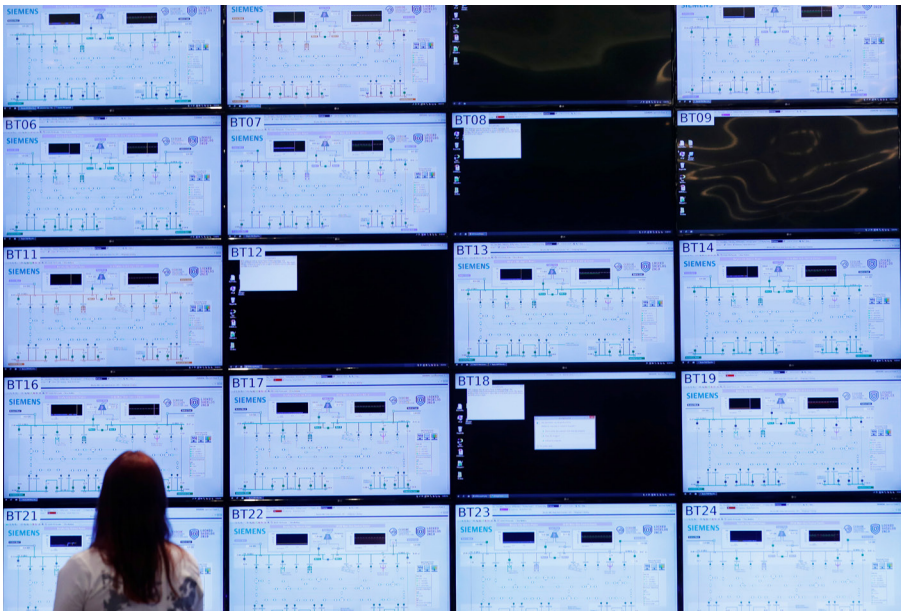
Die NATO und Artikel 5 im Cyberraum

Die NATO hat den Cyberraum als einen Bereich der Kriegsführung definiert und anerkannt, dass ein Cyberangriff den kollektiven Verteidigungsmechanismus des Bündnisses nach Artikel 5 auslösen könnte. Gegenwärtig ist nicht bekannt, ob und welche Art von Cyberangriff(en) eine Verteidigungsreaktion der NATO auslösen könnte.

Von Sarah Wiedemar

Auf dem NATO-Gipfel in Wales vor fast einem Jahrzehnt hat das Bündniss anerkannt, dass die Cyberverteidigung ein untrennbarer Bestandteil der kollektiven Verteidigung ist. Daher kann ein Cyberangriff gegen einen oder mehrere Mitgliedstaaten die Klausel zur kollektiven Verteidigung auslösen, die in Artikel 5 des Washingtoner Vertrags, dem Grundpfeiler des Militärbündnisses, verankert ist. Artikel 5 beruht auf dem Grundsatz, dass ein Angriff gegen einen Mitgliedstaat als Angriff gegen alle Mitgliedstaaten betrachtet wird und dass die Bündnispartner durch Ausübung ihres Rechts auf individuelle oder kollektive Selbstverteidigung – wie in Artikel 51 der UN-Charta anerkannt – Massnahmen ergreifen können, um die Sicherheit des nordatlantischen Raums wiederherzustellen. Nach der Auslösung durch einen oder mehrere Mitgliedstaaten muss der Nordatlantikrat (*North Atlantic Council*, NAC), das wichtigste Entscheidungsgremium des Bündnisses, einstimmig entscheiden, ob der Angriff die Anwendung von Artikel 5 rechtfertigt. Ist dies der Fall, so obliegt es jedem einzelnen Mitglied, zu entscheiden, wie es reagieren will und in welchem Umfang es in Absprache mit den anderen NATO-Partnern Hilfe leisten will. Seit seiner Einführung im Jahr 1949 hat die NATO Artikel 5 einmal angewandt, nämlich nach den Terroranschlägen vom 11. September 2001.



Das NATO Cooperative Cyber Defence Centre of Exellence (CCDCOE) in Tallinn, Estland, während der Cyberverteidigungsübung Locked Shields im April 2019. *Ints Kalnins / Reuters*

Die Hauptaufgabe der NATO besteht darin, die Freiheit und Sicherheit ihrer Mitgliedstaaten mit politischen und militärischen Mitteln zu schützen. Da Artikel 5 auch für den Cyberraum gilt, hat das Bündnis anerkannt, dass Cyberangriffe eine Schwelle erreichen können, die den nationalen und euro-atlantischen Wohlstand sowie dessen Sicherheit und Stabilität gefährden können. Die NATO hat keine spezifischen roten Linien festgelegt, deren Überschreitung die Anwendung von Artikel 5 nach sich ziehen würde. Stattdessen stützt sich die Haltung des Bündnisses auf strategische Mehrdeutigkeit und den Grundsatz, dass jeder Angriff von Fall zu Fall zu beurteilen ist. Je nach Umfang und Ausmass des Angriffs beziehungsweise der Angriffe oder der Kampagne würde sich die Reaktion der NATO nach dem politischen

Willen der einzelnen Mitgliedstaaten richten. Diese kann von diplomatischen und wirtschaftlichen Vergeltungsmassnahmen bis hin zu offensiven Cyber-Operationen oder militärischen Massnahmen reichen. Die Flexibilität bei der Anwendung von Artikel 5 ist zwar für die Integrität des Bündnisses von entscheidender Bedeutung, schafft aber auch besondere Unsicherheiten, wenn es um den Cyberraum geht. Die Feststellung, welche Auswirkungen ein Angriff hatte, wer ihn durchgeführt hat und welche politische Absichten die Angreifenden verfolgen, gestaltet sich bei Cyberangriffen im Allgemeinen schwerer als bei Angriffen mit konventionellen Mitteln.

Nach einer disruptiven Cyber-Kampagne gegen den NATO-Mitgliedstaat Albanien im Sommer 2022 erwog der albanische Ministerpräsident Edi Rama, sich mit Verweis auf Artikel 5 an den NAC zu wenden. Die Geltendmachung von Artikel 5 durch Albanien wäre das erste Mal gewesen, dass die kollektive Verteidigungsklausel der NATO als Reaktion auf einen Cyberangriff aktiviert worden wäre. Damit wäre ein Präzedenzfall für das Bündnis geschaffen worden. Die albanische Regierung verzichtete zwar letztlich darauf, die Frage vor dem NAC aufzugreifen. Der Vorfall löste dennoch erneute Diskussionen darüber aus, wie Artikel 5 im Cyberraum angewendet werden sollte.

Die NATO und der Cyberraum

Nach einem Anstieg von DDoS-Angriffen (siehe Box auf S. 3), der Verunstaltung von Websites und E-Mail-Spamming-Kampagnen, die sich im Zuge der *Operation Allied Force* 1999 gegen Einrichtungen der NATO und ihrer Mitgliedstaaten richteten (siehe Box auf S. 2), wuchs bei den einzelnen Mitgliedstaaten die Einsicht, dass sie ihre Fähigkeiten im Bereich der Cybersicherheit und -verteidigung verbessern mussten, um ihre eigenen Informations- und Kommunikationssysteme zu schützen.

Unter anderem aufgrund dieser Erfahrungen setzte das Bündnis die Cyberverteidigung auf die politische Tagesordnung des Prager NATO-Gipfels im Jahr 2002. Dort verabschiedete das Bündnis auch das Cyberverteidigungsprogramm, mit dem es die *NATO Computer Incident Response Capability* (NCIRC) schuf. Deren Aufgabe ist es, Cybervorfälle, die das Bündnis betreffen, zu verhindern, zu erkennen und darauf zu reagieren. Aber erst nach der beispiellosen DDoS-Kampagne gegen das NATO-Mitglied Estland im Jahr 2007 wurde dem Bündnis das Ausmass der Bedrohung und die gesamte politische Tragweite von Cyberangriffen bewusst (siehe Box auf S. 2). Das estnische Ersuchen um Unterstützung im Anschluss an die DDoS-Kampagne war ein Weckruf für die NATO. Zehn Monate später verabschiedeten die Bündnispartner auf dem NATO-Gipfel in Bukarest ihre erste Strategie zur Cyberverteidigung. Die Mitgliedstaaten anerkannten, dass die NATO nicht nur die für das Bündnis kritischen Informationssysteme schützen, sondern auch bewährte Praktiken austauschen und den Bündnispartnern im Falle eines Cyberangriffs Unterstützung leisten muss. Mitgliedstaaten äusserten auch Bedenken, ob und wie ein Cyberangriff zu einer wichtigen Komponente der Kriegsführung werden könnte. Auf dem NATO-Gipfel in Wales 2014 erklärten die Mitgliedstaaten, dass die Cyberverteidigung Teil der Kernaufgabe der NATO, also der kollektiven Verteidigung, ist. Auf dem NATO-Gipfel in Warschau im Jahr 2016 bekräftigte das Bündnis diese Verpflichtung, indem es den Cyberraum neben der Luft-, Land- und Seekriegsführung zu einem neuen Operationsraum erklärte.

Auf dem NATO-Gipfel in Brüssel im Jahr 2021 ging das Bündnis noch einen Schritt weiter und anerkannte, dass es die Auswirkungen erheblicher böswilliger kumulativer Cyberaktivitäten unter bestimmten Umständen als bewaffneten Angriff werten könnte. Dieser Wechsel zu einem kumulativen Ansatz erfolgte wahrscheinlich als Reaktion auf die Welle von *Ransomware*-Kampagnen (siehe Box auf S. 3) gegen digitale Infrastrukturen in den Vereinigten Staaten und anderen NATO-Mitgliedstaaten. Diese Kampagnen richteten sich gegen fast alle kritischen Infrastrukturen, darunter das Gesundheitswesen, die Landwirtschaft und die Energieversorgung.

Die NATO und Cyberangriffe in der Vergangenheit

Operation Allied Force 1999: Während des Kosovo-Krieges (1998/1999) zielte die NATO-Militärkampagne *Operation Allied Force* darauf ab, das serbische Militär aus dem Kosovo zu vertreiben. Verschiedene nationalistische «Hacktivisten-Gruppen» aus Serbien, Russland und China (insbesondere nach dem Bombardement der chinesischen Botschaft in Belgrad am 7. Mai 1999) versuchten, die Handlungsfähigkeit der NATO durch eine Reihe von verteilten *Denial-of-Service*-Angriffen (DDoS – siehe Box S. 3) und die Entstellung von Websites zu stören.

Estland 2007: Im Jahr 2007 erlebte das NATO-Mitglied Estland eine anhaltende DDoS-Kampagne, die patriotische russische Hacktivisten durchführten. Diese dauerte 22 Tage lang und hatte eine Reihe öffentlicher und privater estnischer Netze zum Ziel, darunter das estnische E-Government-System, Banken und Medienhäuser. Der Vorfall ereignete sich kurz nach der Versetzung einer umstrittenen Statue aus dem Zweiten Weltkrieg aus dem Zentrum Tallinns, die für die russischsprachige Minderheit den Tag des Sieges symbolisierte, während sie für die ethnischen Estinnen und Esten eine Erinnerung an die sowjetische Besatzung und Unterdrückung darstellte. Diese Art von anhaltender DDoS-Kampagne, verbunden mit dem angespannten geopolitischen Umfeld, war zu diesem Zeitpunkt beispiellos.

Cyberangriffe und Artikel 5

Am 25. Februar 2022, dem Tag nach dem russischen Einmarsch in der Ukraine, bekräftigte NATO-Generalsekretär Jens Stoltenberg, dass die Cyberverteidigung ein untrennbarer Bestandteil der kollektiven Verteidigung ist. Er betonte zudem, dass das Bündnis einem potenziellen Gegner nicht das Privileg einräumen wird, zu bestimmen, wann Artikel 5 zur Anwendung kommt. Obwohl Artikel 5 auch für Cyberangriffe gilt, stellen die Besonderheiten des Cyberraums eine Vielzahl zusätzlicher Herausforderungen dar. So ist beispielsweise die Frage der Attribution – das heisst, die Feststellung, wer genau für einen Cyberangriff verantwortlich ist – sowohl mühselig als auch zeitaufwändig und erreicht möglicherweise nicht das Mass an Gewissheit, welche erforderlich ist, um spezifische politische oder militärische Reaktionen rechtlich zu legitimieren (siehe CSS Analyse Nr. 244). Ebenso wirft die Vielfalt der Beziehungen und quasi-Verknüpfungen zwischen staatlichen und nichtstaatlichen Akteuren im Cyberbereich sowie der physische Standort, von dem Akteure operieren, die Frage auf, wer genau für was verantwortlich gemacht werden kann.

Ein weiteres grundlegendes Problem ergibt sich aus der strategisch zweideutigen Position der NATO. Im Tallinn-Handbuch 2.0, einem Expertenpapier zur Anwendung des Völkerrechts auf den Cyberraum, wird ein Cyberangriff als eine Cyberoperation definiert, bei der nach vernünftigem Ermessen zu erwarten ist, dass sie zur Verletzung oder zum Tod von Personen oder zur Beschädigung oder Zerstörung von Objekten führt. Diese Definition erfolgte unabhängig davon, ob es sich hierbei um einen Angriff oder eine Verteidi-

gungsmassnahme handelt. Das Handbuch stellt auch klar, dass ein Angriff nicht zwangsläufig zu einem physischen Schaden an Objekten oder Personen führen muss. Lange Zeit wurde jedoch davon ausgegangen, dass die Auswirkungen eines Cyberangriffs denen eines kinetischen Angriffs gleichkommen müssen, um die Schwelle eines bewaffneten Angriffs zu überschreiten und eine rechtmässige militärische Reaktion auszulösen.

Seit dem Brüsseler Gipfel 2021 hat die NATO ihren Standpunkt in dieser Frage angepasst. Heute stellt das Bündnis fest, dass die Auswirkungen kumulativer bösartiger Cyber-Aktivitäten, die unterhalb der Schwelle eines bewaffneten Angriffs erfolgen, in ihrer Gesamtheit erheblich genug sein können, um einem bewaffneten Angriff gleichzukommen, der ein kollektives Vorgehen nach Artikel 5 rechtfertigt. Infolge dieses Wandels ist noch weniger klar geworden, welche gegnerischen Cyberaktivitäten in den Geltungsbereich der NATO fallen könnten. Ein direkter Vergleich mit einem kinetischen Angriff ist damit nicht mehr zutreffend. Ungeklärt ist auch die Frage, was passieren könnte, sollten die NATO-Mitglieder Artikel 5 als Reaktion auf einen Cyberangriff auslösen. Da die NATO von Fall zu Fall handelt, ist unklar, ob sich die Bündnispartner derzeit darüber einig sind oder einen Konsens darüber erzielen könnten, welche Art von Auswirkungen und welche Art von schwerwiegenden Folgen von Cyberangriffen für die Inanspruchnahme von Artikel 5 in Frage kämen.

Cybervorfälle: Wenig Klarheit

Frühere Cyberkampagnen, die auf NATO-Mitglieder abzielten oder diese indirekt betrafen, haben mit Ausnahme Albaniens keine grösseren öffentlichen Diskussionen über Artikel 5 ausgelöst. Die folgenden drei Fälle – der *Ransomware*-Angriff auf das Unternehmen Colonial Pipeline im Jahr 2021, der Viasat-Hack im Jahr 2022 und die Cyber-Kampagne gegen Albanien im Jahr 2022 – veranschaulichen die Komplexität der Erarbeitung einer wirksamen internationalen Reaktion auf Cyber-Vorfälle.

Im Jahr 2021 sahen sich die USA und andere westliche Länder mit einer Welle von *Ransomware*-Kampagnen gegen ihre kritische Infrastruktur konfrontiert. Die von der russischen Cyberkriminellengruppe *DarkSide* im Mai 2021 durchgeführte *Ransomware*-Kampagne gegen Colonial Pipeline ist wahrscheinlich die bekannteste unter diesen. Colonial Pipeline ist der grösste Pipeline-Betreiber in den USA. *DarkSide* drang in das IT-Netzwerk des Unternehmens ein, erbeutete erfolgreich eine grosse Menge an Daten und setzte anschliessend *Ransomware* gegen das Abrechnungs- und Buchhaltungssystem ein. Als Reaktion auf das Eindringen und um den Eingriff einzudämmen, stellte das Unternehmen seinen gesamten Pipelinebetrieb ein. Dies führte zu vorübergehenden Treibstoffengpässen und Verkehrsstaus an der gesamten US-Ostküste. Daraufhin rief US-Präsident Joe Biden in achtzehn Bundesstaaten den Notstand aus – die erste derartige Erklärung als Reaktion auf einen Cyberangriff überhaupt.

DarkSide war eine prominente cyberkriminelle Gruppierung, die wahrscheinlich von russischem Territorium aus operierte. Spekulationen zufolge soll die Gruppe möglicherweise mit russischen Regierungsstellen zusammenarbeitet haben. Es gibt jedoch keine definitiven Beweise, die diese Vermutung stützen. Als Reaktion auf den Angriff beschloss die US-Regierung, eine rote Linie zu ziehen. Während des Gipfeltreffens in Genf im Juni 2021 übergab US-Präsident Biden dem russischen Präsidenten Wladimir Putin eine Liste mit 16 kritischen US-Infrastrukturbereichen, die für russische Cyberangriffe als tabu gelten sollen. Biden wies darauf hin, dass jedes Land gegen Cyber-Kriminelle vorgehen muss, die vom eigenen Territorium aus operieren.

Die *Ransomware*-Kampagne gegen Colonial Pipeline war ein cyberkrimineller Akt eines nichtstaatlichen Akteurs, der kritische Infrastrukturen störte, den Notstand auslöste und zu einem Problem der nationalen Sicherheit der USA wurde. Trotzdem wandte sich die US-Regierung nicht an die NATO und diskutierte nicht offen über die Anwendung von Artikel 5. Vielmehr entschied sich Washington dafür, das Problem auf bilateraler Ebene anzugehen.

Im Februar 2022, einige Stunden vor dem Einmarsch in die Ukraine, wurde der weltweit tätige Satellitenkommunikationsanbieter Viasat Opfer einer offensiven Cyber-Operation, die mutmasslich vom russischen Militärgeheimdienst (GRU) durchgeführt wurde. Die Angreifer hatten es wahllos auf die Modems von Viasat abgesehen und konnten etwa 20 000 Geräte ausschalten. Die Operation unterbrach den Internetzugang für Zehntausende von Menschen in der Ukraine und für Viasat-Nutzende in mindestens dreizehn anderen europäischen Ländern, wobei die grössten Unterbrechungen im Vereinigten Königreich und in Frankreich auftraten. In Deutschland wurde die Fernüberwachung und -steuerung von 5 800 Windkraftanlagen ausser Kraft gesetzt, was die Stromerzeugung und -verteilung beeinträchtigte. Der Angriff legte auch die Kommunikation des ukrainischen Militärs, der Polizei und der Geheimdienste vorübergehend lahm, was das Hauptziel der Operation gewesen sein dürfte.

Am 10. November 2022 betonte NATO-Generalsekretär Jens Stoltenberg, dass der Viasat-Hack über die Ukraine hinaus Kollateralschäden verursacht habe. Die USA, das Vereinigte Königreich und die EU

Cyberangriffe: Überblick über gängige Methoden und Instrumente

Ein verteilter ***Denial-of-Service*-Angriff (DDoS)** ist eine Art Attacke, bei der der Zielserver, -dienst oder das Zielnetzwerk mit Datenverkehr überlastet wird, der von mehreren Quellen stammt – zum Beispiel von einer Gruppe von Geräten. Das Ziel eines DDoS-Angriffs ist es, das System des Opfers unzugänglich zu machen.

Bei ***Ransomware*** handelt es sich um bösartige Software, die darauf abzielt, Daten zu verschlüsseln oder den Zugriff darauf zu blockieren und vom Opfer eine Zahlung für das Entsperren oder Entschlüsseln der Daten zu verlangen, um die Kontrolle wiederzuerlangen. Verschiedene Arten von Schadsoftware können auf Desktop-Systeme und mobile Geräte abzielen. *Ransomware*-Programme zielen sowohl auf Einzelpersonen als auch auf Unternehmen ab. In jedem Fall führt ein erfolgreicher Angriff zu Ausfallzeiten und Kosten für die Datenwiederherstellung. Der durch *Ransomware* verursachte Schaden ist dabei nicht immer umkehrbar. So kann sich das *Ransomware*-Programm beispielsweise als *Wiper* entpuppen, das heisst, als eine Art Schadsoftware, die Daten unwiederbringlich zerstört oder beschädigt.

APT *(advanced persistent threats)* sind konzertierte Angriffe auf bestimmte Organisationen. APT-Angriffe werden in der Regel von staatlichen Akteuren durchgeführt und nutzen hochentwickelte Malware, um die Sicherheitssysteme der Opfer zu durchbrechen.

Ein ***Wiper*** (abgeleitet vom englischen Begriff für «wischen») ist eine Art von Schadsoftware, die darauf abzielt, Daten von der Festplatte des infizierten Computers zu löschen.

Quelle: Kaspersky IT Encyclopedia

schrieben den Viasat-Hack offiziell der russischen Regierung zu und verurteilten den Angriff. Nach Angaben der Nachrichtenagentur Bloomberg sind die US-Geheimdienste zu der Einschätzung gelangt, dass der GRU bereitwillig erhebliche diplomatische und strategische Risiken auf sich nahm, da er wusste, dass der Angriff mehrere Länder über die Ukraine hinaus betreffen würde. Trotz den sekundären Effekten des Angriffs und der wahllosen Angriffe auf Viasat-Modems im Rahmen eines internationalen bewaffneten Konflikts hat das Bündnis nicht öffentlich über die Anwendung von Artikel 5 beraten.

Zwischen Mai und September 2022 wurde das NATO-Mitglied Albanien Opfer einer koordinierten Cyberkampagne. Erste Medienberichte machten – wie auch andere *Ransomware*-Kampagnen in der ganzen Welt – russische Cyberkriminelle für die Cyberattacke verantwortlich. Mit Unterstützung von Microsoft, Mandiant, des FBI und anderen wurde die Kampagne schliesslich vier verschiedenen APT-Akteuren (siehe Box auf S. 3) zugeschrieben, die wahrscheinlich mit dem iranischen Geheimdienst- und Sicherheitsministerium verbunden sind. Die vier APTs verwendeten einen Multi-Vektor-Ansatz, der die Verschlüsselung von Daten *(Ransomware)*, die Löschung von Daten (*Wiper* – siehe Box auf S. 3), die Exfiltration von Daten und die Veröffentlichung von Daten umfasste, um den Effekt der Störung zu maximieren. Die Kampagne legte mehrere Websites und Online-Dienste der albanischen Regierung, darunter das zentrale e-Albania-Portal und die Nationale Agentur für die Informationsgesellschaft lahm. Selbst das gesamte Informationsmanagementsystem der Staatspolizei, welches die Daten von Personen speichert, die nach Albanien ein- und ausreisen, war vorübergehend nicht verfügbar, was zu Warteschlangen an den Grenzen führte.

Am 18. Juli 2022 bekannte sich eine Gruppe oder Person namens *HomeLand Justice* (HLJ) öffentlich zur Kampagne. HLJ veröffentlichte albanische Regierungsdokumente und publizierte mehrere Videos auf ihrem Telegram-Kanal und ihrer Website, die unter anderem den Einsatz von *Ransomware* auf albanischen Servern zeigten.

Gegenwärtig zögert das Bündnis, von seiner strategischen Unklarheit abzurücken.

In ihren öffentlichen Mitteilungen erklärte HLJ, dass sie die Cyberangriffe durchführte, um ihre Wut auf Albanien auszudrücken, welches im Juli desselben Jahres die jährliche Konferenz iranischer Oppositionsgruppen beherbergte. Das Logo von HLJ ist auch aufschlussreich, wenn es um die Attribution geht. Es zeigt einen Adler, der einen *Angry Bird* (aus dem gliechnamigen Videospiel) angreift, der von einem Davidstern umgeben ist. Einen *Angry Bird* verwendet auch eine andere Gruppe namens *Predatory Sparrow* als Symbol. Im Juni 2022 führte diese eine zerstörerische Cyberkampagne gegen drei iranische Stahlwerke durch, die angeblich dem Korps der Iranischen Revolutionsgarden gehören. Wie *Predatory Sparrow* in einem ihrer Videos erklärte, erfolgten diese Cyberangriffe als Reaktion auf die Aggression des Irans. Es ist nicht bekannt, ob *Predatory Sparrow* mit dem Staat Israel in Verbindung steht. Die Symbolik von HLJ lässt jedoch vermuten, dass Teheran dies glauben könnte. Insgesamt scheinen die vier iranischen APTs ihre Kampagne nicht nur durchgeführt zu haben, um der albanischen Regierung zu signalisieren, keine iranischen Oppositionsgruppen im Exil zu beherbergen, sondern möglicherweise auch als Warnung an *Predatory Sparrow* und den Staat Israel.

Nach dem Ergebnis der forensischen Untersuchung brach die albanische Regierung alle diplomatischen Beziehungen zu Teheran ab – das erste Mal, dass eine Regierung eine solche Massnahme als Reaktion auf eine Cyberkampagne ergriffen hat. Während der internen Beratungen darüber, wie auf den Vorfall zu reagieren sei, diskutierte die albanische Regierung auch die Berufung auf Artikel 5 der NATO. In der Öffentlichkeit verurteilte Albaniens Premierminister Edi Rama die Angriffe als gleichwertig mit einer konventionellen militärischen Aggression. Rama entschied sich jedoch schliesslich dagegen, sich an die NATO zu wenden. Dies mit der Begründung, zu viel Respekt vor seinen Freunden und Verbündeten zu haben, um ihnen vorzuschreiben, wie sie zu handeln hätten.

Implikationen

Der *Ransomware*-Angriff auf Colonial Pipeline, der willkürliche Angriff auf Viasat-Modems und die Cyber-Kampagne gegen Albanien veranschaulichen, dass die NATO im Hinblick auf Artikel 5 im Cyberraum Neuland betritt. In keinem dieser Fälle hielten die betroffenen Regierungen die gegnerischen Kampagnen für bedeutend genug, um die Schwelle eines bewaffneten Angriffs zu überschreiten oder das Kriterium der kumulativen Effekte zu erfüllen. Bis heute bleibt die Frage offen, ob ein Cyberangriff jemals die Art von Zerstörung und Tod im grossen Stil wie am 11. September verursachen wird, oder ob es überhaupt notwendig wäre, um sich auf Artikel 5 zu berufen.

Gegenwärtig zögert das Bündnis, von der strategischen Mehrdeutigkeit abzurücken, und die einzelnen Mitgliedstaaten scheinen nicht geneigt zu sein, Präzedenzfälle zu schaffen, was die Anwendung von Artikel 5 als Reaktion auf Cyberangriffe angeht. Das Bündnis muss weiterhin den Spagat schaffen, einerseits den Handlungsspielraum zu erhalten und die Einheit zu wahren und andererseits sich den Herausforderungen zu stellen, die der Cyberraum mit sich bringt.

Für mehr zur Cybersicherheitspolitik, siehe CSS Themenseite.

Sarah Wiedemar ist Researcher und Teil des Cyberdefence Projects des Risk and Resilience Team des Center for Security Studies (CSS) an der ETH Zürich.

Die **CSS Analysen zur Sicherheitspolitik** werden herausgegeben vom Center for Security Studies (CSS) der ETH Zürich. Das CSS ist ein Kompetenzzentrum für schweizerische und internationale Sicherheitspolitik. Jeden Monat erscheinen zwei Analysen auf Deutsch, Französisch und Englisch.

Herausgeber: Fabien Merz
Lektorat: Julian Kamasa
Layout und Grafiken: Miriam Dahinden-Ganzoni

Feedback und Kommentare: analysen@sipo.gess.ethz.ch
Weitere Ausgaben und Abonnement: www.css.ethz.ch/cssanalysen

ISSN: 2296-0236; DOI: 10.3929/ethz-b-000610319