AUSSEN- UND SICHERHEITSPOLITIK 25.06.2020 | Jantje Silomon

Gegenangriff im Cyberspace

Im Kampf gegen Cyber-Spionage und Desinformationskampagnen verfügt die EU nun über ein gemeinsames Sanktionsregime. Noch ist es ein stumpfes Schwert.

Ende April 2020 erließ die Bundesanwaltschaft einen Haftbefehl gegen den russischen Staatsbürger Dmitri Badin, einen der Hauptverdächtigen des Bundestags-Hacks von 2015. Nun könnte der Hack zum ersten Anwendungsfall des Cyber-Sanktionsregimes der EU werden. Die politischen Konsequenzen sind noch nicht absehbar – klar ist jedoch, dass die Abwehr von Cyber-Spionage zukünftig deutlich wirksamer gestaltet werden muss.

Alles begann 2015. Mehrere Wochen blieb sie unentdeckt, dann erlangte eine Malware Kontrolle über die IT-Infrastruktur des Bundestags und führte im Mai 2015 zum Zusammenbruch von Online-Diensten und Websites. Der größte Schaden bestand in der Exfiltration von 16 GB Daten. Das scheint an sich keine große Datenmenge zu sein, aber sie umfasste unter anderem komplette Postfächer von Parlamentariern, Kontakte und Terminpläne. Innerhalb weniger Wochen gab es erste Hinweise, die auf eine russische Gruppe namens „Fancy Bear“ als Verursacher deuteten.

Angeblich unterhielt „Fancy Bear“ Verbindungen zu russischen Geheimdiensten. Als der russische Botschafter Ende Mai 2020 ins Auswärtige Amt einbestellt wurde, erklärte man ihm, „dass sich die Bundesregierung in Brüssel für die Nutzung des EU-Cybersanktionsregimes gegen Verantwortliche für den Angriff auf den Deutschen Bundestag, darunter auch Herrn Badin, einsetzen wird.“ Moskau bestreitet die Vorwürfe bis heute.

Somit verfügt die EU nun also über ein Instrument, mit dem sie gezielt auf Cyberbedrohungen

Sanktionen waren bislang nicht Teil der Cyber-Diplomatie der EU. Gewöhnlich verurteilten die Mitgliedstaaten zwar bestimmte Cyber-Operationen, die mutmaßlichen Täter wurden aber nicht explizit benannt. Im Sommer 2017

reagieren kann. Ob dieses aber auch wirksam angewandt werden kann, ist fraglich.

verabschiedete die EU dann eine sogenannte Cyber-Diplomatie-Toolbox, die für Stabilität im Cyberspace sorgen und einen Rahmen für gemeinsame diplomatische Reaktionen auf Cyber-Angriffe bieten soll. Seit Mai 2019 enthält die Toolbox als eine mögliche Maßnahme auch Sanktionen.

Sanktionen können in Form des Einfrierens wirtschaftlicher Ressourcen oder der Verhängung von Reisebeschränkungen erfolgen. So können auch Personen oder Organisationen sanktioniert werden, die die Aktionen indirekt unterstützt haben, zum Beispiel durch die Bereitstellung von Geldern. Voraussetzung dafür ist eine (potenziell) erhebliche Wirkung des (versuchten) Cyber-Angriffs, der zudem eine externe Bedrohung für die EU oder einen ihrer Mitgliedstaaten darstellen muss. Somit verfügt die EU nun also über ein Instrument, mit dem sie gezielt auf Cyberbedrohungen reagieren kann. Ob dieses aber auch wirksam angewandt werden kann, ist fraglich.

Da wäre zunächst die technische Attribution, die an den Realitäten staatlich gelenkter Cyberangriffe weitestgehend vorbeigeht. So muss es sich beim Verursacher laut Cyber-Sanktionsregime um eine juristische Person, Organisation oder Einrichtung handeln. Staatliche Akteure sind bei diesem EU-übergreifenden Instrument bewusst ausgeschlossen. Dies bedeutet aber auch, dass die direkte Wirksamkeit gegenüber einem staatlichen Akteur weitestgehend symbolischer Natur sein wird.

Zwar können die Mitgliedstaaten Vorschläge für Sanktionen gegen Einzelpersonen oder Organisationen unterbreiten, entscheiden muss jedoch der Rat, und zwar einstimmig. Das birgt erhebliches politisches Konfliktpotential.

Ein weiterer Schwachpunkt ist das Procedere. Zwar können die Mitgliedstaaten Vorschläge für Sanktionen gegen Einzelpersonen oder Organisationen unterbreiten, entscheiden muss jedoch der Rat, und zwar einstimmig. Das birgt erhebliches politisches Konfliktpotential. Was passiert beispielsweise, wenn mögliche Täter in Ländern ansässig sind, welche zentrale wirtschaftliche Handelspartner (China) oder – noch schwieriger – politische Verbündete (USA) sind? Es steht zu befürchten, dass einzelne Mitgliedstaaten ökonomische oder bündnispolitische Interessen über die kollektive Abwehr internationaler Cyberbedrohungen stellen werden.

Klar ist, dass es mit dem Sanktionsregime allein nicht getan ist. Um Deutschland und Europa zu stärken, müssen Berlin und Brüssel

zusätzlich in defensive und forensische Cyber-Ressourcen sowie fachliche Expertise investieren. Deutschland hat dafür bereits erste Schritte unternommen, zum Beispiel mit der Gründung der Zentralen Stelle für Informationstechnik im Sicherheitsbereich im Jahr 2017 oder der Neuorganisation des 1991 gegründeten Bundesamts für Sicherheit in der Informationstechnik (BSI) mit inzwischen immerhin rund 1 100 Mitarbeiterinnen und Mitarbeitern.

Dies ist ein vielversprechender Anfang, der fortgesetzt werden muss, vor allem angesichts sich rasch entwickelnder Technologiebereiche wie KI, Cloud-Computing und 5G. Hinzu kommen unerwartete Herausforderungen, wie die Corona-Krise, die in vielen Bereichen geradezu über Nacht eine bundesweite Digitalisierung erzwang. Um beispielsweise flexibles Arbeiten zu ermöglichen, wurde eine Vielzahl an technischen Provisorien geschaffen, die nun dauerhafter gesichert werden müssen.

Um Desinformationskampagnen und damit einhergehenden Cyber-Operationen vorzubeugen, bleibt nur wenig Zeit. Das Cyber-Sanktionsregime der EU ist dabei ein Schritt in die richtige Richtung.

Auch bei der europaweiten Zusammenarbeit gibt es Nachholbedarf, vor allem bei gemeinsamen Bedrohungsanalysen und beim Informationsaustausch. In der Europäischen Freihandelsassoziation (EFTA) existieren zur Zeit circa 440 Einsatzteams für Cyber-Vorfälle, sogenannte CSIRT- und CERT-Gemeinschaften, die primär industriespezifisch oder auf nationaler Ebene aktiv sind. Eine Herausforderung ist der sehr unterschiedliche Reifegrad der verschiedenen Teams, was dazu führt, dass nicht jeder Mitgliedstaat gleich gut für den Umgang mit Cybervorfällen gerüstet ist. Hier könnte die Schaffung zusätzlicher nationaler Zentren für Informationsaustausch und Analyse helfen. Diese könnten dann auch als Hubs für die grenzübergreifende Zusammenarbeit fungieren.

Die Corona-Krise hat noch einmal gezeigt, wie groß die Abhängigkeit vom Cyber-Raum inzwischen ist. Während die Mitgliedstaaten noch damit beschäftigt waren, die Herausforderungen einer erzwungenen Ad-hoc-Digitalisierung zu meistern, versuchten Kriminelle und sogar staatliche Akteure, die globale Pandemie zu missbrauchen. Wie viele Systeme dabei gehackt wurden, ist noch immer nicht klar.

Ein zweites Beispiel ist die Zunahme und Weiterentwicklung von Desinformationskampagnen. Waren diese anfangs beschränkt auf

sogenannten Troll-Fabriken, sind sie inzwischen Teil vielschichtiger Cyber-Operationen, wie im Zusammenhang mit den US-Präsidentschaftswahlen 2016 oder der französischen Präsidentenwahl 2017 zu beobachten war. In den USA und auch in der EU stehen zahlreiche Wahlen an, darunter die deutsche Bundestagswahl 2021. Um Desinformationskampagnen und damit einhergehenden Cyber-Operationen vorzubeugen, bleibt nur wenig Zeit. Das Cyber-Sanktionsregime der EU ist dabei ein Schritt in die richtige Richtung – aber eben auch nur ein Schritt. Nur wer über zusätzliche defensive Mittel verfügt, kann auf Cyber-Angriffe schnell reagieren, diese dadurch abschwächen und auch bei der Analyse und Verfolgung von Schuldigen Erfolge erzielen.



Jantje Silomon
Hamburg

Jantje Silomon ist wissenschaftliche Mitarbeiterin im Forschungsprojekt Rüstungskontrolle und Neue Technologien am Institut für Friedensforschung und Sicherheitspolitik in Hamburg.

-