TAGESSPIEGEL
BACKGROUND

Cybersecurity

Digitales Säbelrasseln: Wie Europa reagieren kann

Was steckt hinter dem Truppenaufmarsch an der ukrainischen Grenze? Die russische Regierung scheint sich alle Optionen offenzuhalten. Eine digitale Attacke ist wahrscheinlich. Entscheidend wird, wie die EU darauf reagiert. Eine Kolumne von Annegret Bendiek und Matthias Schulze.

von **Annegret Bendiek & Matthias Schulze**

veröffentlicht am 20.01.2022

Am Wochenende beschuldigte die **Ukraine Russland**, für eine Serie „digitaler Schmierereien“ bei mehr als 70 Regierungswebseiten verantwortlich zu sein. Gleichzeitig warnte Microsoft vor einer neuen **Schadsoftware**, die sich als Ransomware tarnt, aber eigentlich Festplatten löscht. Die Schadsoftware erinnert an NotPetya, eine Angriffskampagne, die 2017 weltweit Milliarden an Schäden verursachte und ihren Anfang in der Ukraine nahm. Beide Vorfälle könnten **Vorboten einer militärischen Eskalation** sein, die neben konventionellen Streitkräften auch eine digitale Komponente beinhaltet.

Russland erprobte erstmalig die **militärische Verwendung von Cyberfähigkeiten** während des Georgien-Konflikts 2008. Am 7. August marschierten russische Streitkräfte in Südossetien ein. Begleitet wurde der Einmarsch von mehreren Wellen sogenannter **„Distributed Denial of Service” (DDoS) Angriffe** gegen georgische Medien und

Regierungsstellen. Bei DDoS Angriffen werden Server mit massenhaft Anfragen geflutet, sodass diese überlasten und den Dienst einstellen. Die Kommunikation mit der Außenwelt zu behindern oder gar abzuschneiden ist ein logisches Ziel einer militärischen Invasion.

Während DDoS Angriffe in Georgien noch relativ krude und technisch simpel waren, lernten russische Nachrichtendienste im Laufe der Jahre kontinuierlich dazu. Auch bei der **Okkupation der Krim** spielten Cyberoperationen eine Rolle. Der Fokus lag hierbei allerdings weniger auf der technischen Störung von Systemen als vielmehr in der **Informationsbeeinflussung und der Verbreitung von Unsicherheit** und Angst. Solche psychologischen Effekte können in Konfliktsituationen lohnend für Angreifer sein. Insofern ist eine Vermutung, dass die Beschmutzung ukrainischer Websites mit Drohbotschaften genau diesem Ziel galt, nachvollziehbar. Die Ukraine wird seit Jahren auch als das **„Testgebiet" eines neuartigen, digitalen Konfliktes** beschrieben.

Cyberoperationen in militärischen Konflikten

Nun ist man sich in militärischen Kreisen weltweit weitgehend einig, dass man mit Cyberangriffen allein kein Land vollständig besiegen kann. Auch in modernen Konflikten braucht es „boots on the ground", um ein Land zu erobern. Viele Militärstrategen in den USA, Deutschland oder auch der Schweiz sehen **Cyberoperationen als Verstärker** konventioneller Angriffe.

Erwähnenswert wäre hier zum Beispiel **die Agent-X Malware**, welche 2016 **auf Smartphones ukrainischer Artilleristen** in den umkämpften Gebieten im Osten der Ukraine gefunden wurde. Die Schadsoftware war in einer mobilen Applikation für die Zielführung von D-30-Howitzer-Artilleriestellungen eingebettet und übertrug die Geoposition dieser Stellungen. Der militärische Nutzen dieses Vorgehen erschließt sich sofort: die **Ortung von Artillerie**, die anschließend etwa durch Luftangriffe ausgeschaltet wird, ist in einem konventionellen Krieg äußerst sinnvoll, um den Vormarsch eigener Truppen zu erleichtern.

Cyberoperationen können aber auch in den **Frühphasen von Konflikten für Störaktionen** verwendet werden, um Überraschungsangriffe zu

unterstützen. Nordkoreanische Militärs spekulieren etwa, dass ein Stromausfall in einem Teil des Landes dazu genutzt werden kann, den Einmarsch von Truppen zu maskieren. Mit Russland in Verbindung gebrachte Angreifer übten dieses Vorgehen in zwei aufeinander aufbauenden Wellen 2015 und 2016. Die **Industroyer bzw „Crash Override"** getaufte Malware schaltete mitten im Winter 2016 in Kiew für einige Stunden den Strom ab. Bei einem Stromausfall wird nicht nur die Kommunikationsfähigkeit beeinträchtigt, der Ausfall bedeutet auch den Verlust von Logistikfähigkeiten.

Vergangene, Russland zugeschriebene Cyberoperationen wie **NotPetya im Jahr 2017** zeigen indes, dass **unbeabsichtigte Kollateralschäden in Drittländern** möglich sind. Die Angreifer versuchten ihren Angriff auf die Ukraine zu beschränken, indem sie eine vorwiegend dort genutzt Steuerverwaltungssoftware als Angriffsvektor nutzten. Allerdings befiel der Wurm Systeme weltweit, auch in Russland. Die Folge waren Milliardenschäden und Logistikausfälle weltweit. Solche **Kaskadeneffekte** bürgen kaum abschätzbare Eskalationsrisiken.

Europas Reaktionsmöglichkeiten

Selbst wenn also „nur" die **Ukraine Ziel von Cyberoperationen** sein könnte, ist nicht auszuschließen, dass es unbeabsichtigte Kollateraleffekte in europäischen Systemen und Netzen gibt. Insofern ist auch hier die EU gefragt. Sie kann auf einen **cyberdiplomatischen Instrumentenkasten** zurückgreifen. Es werden hierbei in präventive, kooperative, stabilisierende, restriktive Maßnahmen und zuletzt völkerrechtskonforme Strafmaßnahmen zur Selbstverteidigung unterschieden.

Präventive Maßnahmen umfassen **Cyberdialoge** mit Drittstaaten zum Informationsaustausch und um auf das Verhalten der Dialogpartner Einfluss zu nehmen. Dem EU-Cyber Dialog mit Russland kommt dabei besondere Bedeutung zu.

Die Ukraine kann indes mit **Cyber Capacity Building** bei forensischen Ermittlungen Hilfe bekommen. **Kooperative Maßnahmen** umfassen die Zusammenarbeit bei der **Prävention**, **Detektion** und **Behebung** von

Cybervorfällen. Telekomunikationsprovider sollen bei Störungen den Datenverkehr analysieren und identifizierte Verursacher ggf. blockieren. Zur Aufklärung und Attribution von Angriffen haben Deutschland und die EU sich erklärt, **Cybersicherheitsexpert:innen** in die Ukraine zu entsenden. Im aktuellen Fall sich zuspitzender Konfrontation ist der Informationsaustausch zu laufenden Cyberoperationen zwischen Sicherheitsbehörden, aber auch zwischen EU und NATO, essentiell.

Der **Hohe Vertreter Josep Borrell** hat die Angriffe gegen die Ukraine im Namen der EU schnell verurteilt. Dieses „**Signaling**“ ist von hoher Bedeutung für die Kommunikation von politischer Einigkeit der EU gegenüber Russland. Eine **stabilisierende Maßnahme** könnte auch die **Reaktivierung des Normandieformats** sein. Deutschland und Frankreich können hier versuchen, politische Kompromisse zu erzielen, um etwa cybergestützte Desinformationskampagen gegen die Ukraine zu beenden und künftig auszuschließen, bevor restriktivere Maßnahmen ergriffen werden müssen.

Die EU greift zur Durchsetzung ihrer politischen Ziele infolge von schwerwiegenden Cyberoperationen auf die Verhängung von **restriktiven Maßnahmen (Sanktionen)** zurück. Diese werden derzeit mit den Verbündeten abgestimmt und gegen die verantwortlichen Regierungsmitglieder, aber auch gegen Staatsfirmen oder andere juristische und natürliche Personen, gerichtet.

Klares Signal der Unterstützung erforderlich

Offen bleibt, wie die **EU und Nato auf schwerwiegende Cyberoperationen gegen Mitgliedstaaten** oder auf etwaige Kollateralschäden reagieren werden. Hier sind im Rahmen der EU zwei weitere Eskalationsstufen denkbar. **Der Vertrag von Lissabon** hat die **Solidaritäts- und Beistandsklausel** eingeführt. Beide Klauseln können bei schwerwiegenden Cyberangriffen angewandt werden. Die Solidaritätsklausel nach Artikel 222 AEUV sieht eine Unterstützung von EU-Staaten u.a. auch bei schwerwiegenden Cybervorfällen vor.

Die Beistandsklausel nach Art. 42 Abs. 7 EUV entspricht in etwa Artikel 5 Nato-Vertrag, ist jedoch für Nato-Mitglieder hierzu subsidiär. Seine

Anwendung hat erstmalig 2015 nach den Terroranschlägen von Paris durch Frankreich stattgefunden. Der **diplomatische Reaktionsrahmen** setzt keine eindeutige Attribution über Herkunft und Akteur der Cyberattacke voraus. In der **letzten Eskalationsstufe** wären auch militärische Gegenreaktionen denkbar. Das könnte in extremen Fällen auch Cyberfähigkeiten umfassen, allerdings sind die Spezifika unklar und bisher unerprobt. Insofern behält sich die EU einen Grad von strategischer Ambiguität gegenüber Russland vor. Ob das reichen wird, um Russland zu überzeugen, wird sich zeigen.

Annegret Bendiek ist stellvertretende Leiterin der Forschungsgruppe EU/Europa, Matthias Schulze stellvertretender Forschungsgruppenleiter für Sicherheitspolitik bei der Stiftung Wissenschaft und Politik.

In unserer Reihe „Perspektiven“ ordnen unsere Kolumnist:innen regelmäßig aktuelle Entwicklungen, Trends und Innovationen im Bereich Cybersicherheit ein.