GERMAN-FOREIGN-POLICY.COM
Informationen zur deutschen Außenpolitik : Nachrichten + Interviews + Analysen + Hintergrund

Die Militarisierung des Internets 29.08.2017

BERLIN (Eigener Bericht) - Berliner Regierungsberater warnen deutsche Repressionsbehörden eindringlich vor der Durchführung von Cyberattacken via Internet. Da Hacker, die mit solchen Angriffen getroffen werden sollten, oftmals fremde Computernetzwerke für ihre Aktionen nutzten, bestehe die Gefahr, die "Infrastruktur unbeteiligter Drittparteien" wie etwa Krankenhäuser gravierend zu schädigen, schreibt die Stiftung Wissenschaft und Politik (SWP) in einem aktuellen Arbeitspapier. Ein sogenannter Hack Back sei daher vergleichbar mit der "Bombardierung von zivilen Wohngebäuden, in denen sich auch militärische Kombattanten befinden". Zudem könne eine Cyberattacke schnell eine "politische Eskalation" heraufbeschwören, die unter Umständen den Einsatz "physischer Waffen" nach sich ziehe, erklärt die SWP. Auch rät die Stiftung davon ab, einer weiteren "Militarisierung des Internets" Vorschub zu leisten, da hiervon eine "zweifelhafte außenpolitische Signalwirkung" ausgehe. Dessen ungeachtet fordern deutsche Regierungsvertreter ebenso wie führende Militärs und Geheimdienstmitarbeiter immer wieder die Fähigkeit zu offensiven "Netzwerkoperationen" und proklamieren ein "Recht auf Gegenangriffe" im virtuellen Raum.

Kollateralschäden

In einem soeben erschienenen Arbeitspapier warnt die Berliner Stiftung Wissenschaft und Politik (SWP) davor, auf Attacken von Hackern gegen deutsche Computersysteme mit "Gegenangriffen" zu reagieren. Es sei "einer der zentralen Mythen des Cyberspace", dass die "Offensive" gegenüber der "Defensive" die "Oberhand" habe, erklärt der regierungsnahe Think Tank. So könne ein Angreifer meist gar nicht abschätzen, wie sich sein Angriff auswirke, da hierfür "eine sehr genaue Kenntnis des Ziels und der darin eingesetzten Hard- und Software" nötig sei. Laut SWP zeigt sich dieses Problem insbesondere bei "Cyber-Gegenangriffen", die als unmittelbare Reaktion auf Hackerattacken durchgeführt werden: "Je weniger Zeit es zur Vorbereitung ... eines 'hack backs' gibt, desto geringer sind der Wirkungsgrad und die Zielgenauigkeit." Wie in dem Papier weiter ausgeführt wird, nutzen Hacker in der Regel fremde Computernetze für ihre Aktionen. Der SWP zufolge besteht daher die Gefahr, dass bei einem "Cyber-Gegenangriff" auch die "Infrastruktur unbeteiligter Drittparteien" wie etwa das digitale Informationssystem eines Krankenhauses gravierend geschädigt wird: "Eine Analogie wäre die Bombardierung von zivilen Wohngebäuden, in denen sich auch militärische Kombattanten befinden."[1]

Eskalationsgefahr

Des weiteren verweist die SWP auf die Problematik, eine mittels Schad- oder Spionageprogrammen via Internet durchgeführte Hackerattacke einem bestimmten Urheber zuzuordnen - zumal Operationen unter falscher Flagge ("false flag operations") im virtuellen Raum mittlerweile "keine Seltenheit" mehr seien. Erfolge nun eine fehlerhafte "Attribution" eines Cyberangriffs, führe dies möglicherweise nicht nur zu kontraproduktiven "Schnellschüssen", sondern zu einer ungeahnten "politischen Eskalation": "Man stelle sich vor, Südkorea zerstöre fälschlich einen Computer in Nordkorea mit einer Cyber-Gegenattacke, obwohl z.B. Russland der erste Urheber war, um die politischen Spannungen auf der koreanischen Halbinsel weiter zu verschärfen. Im schlimmsten Fall könnte Nordkorea mit konventionellen Waffen reagieren."[2]

Zweifelhafte Signalwirkung

Grundsätzlich warnt die SWP in diesem Zusammenhang vor einer "zunehmende(n) Militarisierung des Internets". So gehe von den "Debatten über 'hack back'-Fähigkeiten" deutscher Repressionsorgane eine "zweifelhafte außenpolitische Signalwirkung" aus, da "internationalen Akteuren" gegenüber eine defensive Haltung "nicht glaubhaft belegt" werden könne: "Geheimdienste oder militärische Dienste mit Fähigkeiten zum 'hack back' sind praktisch auch in der Lage, diese proaktiv und explizit offensiv als Angriffsmittel einzusetzen. Eine Abgrenzung von 'rein defensiven' 'hackback'-Methoden, die über diesen Zweifel erhaben sind, ist nicht möglich."[3]

Virtuelles Gefechtsfeld

Ungeachtet der Mahnungen der SWP forderte erst kürzlich der Präsident des Bundesamtes für Verfassungsschutz, Hans-Georg Maaßen, in der deutschen Presse die "Möglichkeit für digitale Gegenangriffe": "Aus meiner Sicht ist es notwendig, dass auch Deutschland in der Lage ist, aktive Maßnahmen im Cyberbereich durchzuführen."[4] Schon zuvor hatte Maaßen erklärt, er lehne es ab, im virtuellen Raum nur "rein defensiv tätig" zu sein: "Wir müssen ... in der Lage sein, den Gegner anzugreifen, damit er aufhört, uns weiter zu attackieren."[5] Analog äußerte sich der Chef des deutschen Inlandsgeheimdienstes bei einem Besuch der

Computermesse CeBIT im März dieses Jahres. In einer Rede über die "nachrichtendienstliche Dimension der digitalen Transformation" verlangte er von den "Länder(n) der freien Welt", sich mit der vermeintlichen Tatsache auseinanderzusetzen, dass Spionageapparate und Streitkräfte anderer Staaten den Cyberspace als "virtuelles Gefechtsfeld" betrachteten, auf dem "die Karten der Machtpolitik auch für die Realwelt neu gemischt werden".[6]

Unschädlich machen

Eine ähnliche Auffassung wie Maaßen vertritt Bundesinnenminister Thomas de Maizière (CDU). Gegenüber einem öffentlich-rechtlichen Fernsehsender erklärte er, die deutschen Repressionsbehörden müssten bei Hackerattacken das "Unschädlichmachen" ausländischer Computernetzwerke ("Server") in Betracht ziehen: "Ein Polizist hat ja im Einsatz nicht nur eine Schutzweste, sondern auch eine Pistole."[7] Dass, wie die SWP in ihrem Arbeitspapier erläutert, bei solchen "Gegenangriffen" oftmals zivile Infrastruktur gravierend geschädigt wird, nimmt man im Bundesinnenministerium offenbar billigend in Kauf. Der dort für "Cybersicherheit" zuständige Ministerialdirigent Andreas Könen etwa erachtet nach eigenem Bekunden das "Abschalten" von Servern, die für eine Attacke benutzt werden, als unabdingbar - trotz möglicher "Kollateralschäden": "Das ist wie die Feuerwehr: Es ist egal, wer das Feuer gelegt hat. Den Brandstifter suchen wir nachher, es geht erst einmal darum, das Feuer auszumachen."[8]

"Nicht die Bergpredigt"

Auch im Auswärtigen Amt ist die von der SWP problematisierte "Militarisierung des Internets" offensichtlich ebenso wenig ein Thema wie die Gefahr, durch das Streben nach offensiven Cyberfähigkeiten "zweifelhafte außenpolitische Signale" in die Welt zu senden. So äußerte der stellvertretende Leiter des "Koordinierungsstabs für Cyber-Außenpolitik", Dirk Roland Haupt, erst unlängst die Überzeugung, Attacken gegen Hacker seien durchaus völkerrechtskonform: "Es gilt ... im Völkerrecht nicht die Bergpredigt: Auf eine Verletzung muss man nicht die andere Backe hinhalten."[9]

[1], [2], [3] Thomas Reinhold/Matthias Schulze: Digitale Gegenangriffe: Eine Analyse der technischen und politischen Implikationen von "hack backs". Arbeitspapier der Forschungsgruppe Sicherheitspolitik an der Stiftung Wissenschaft und Politik. Berlin, August 2017.
[4] Maaßen warnt vor Hackerangriffen auch in Deutschland. www.noz.de 27.07.2017.
[5] Verfassungsschutz will Cybergegenangriffe starten. www.spiegel.de 10.01.2017.
[6] Angriff auf unsere Souveränität - Gefahren aus dem Cyber-Raum. www.verfassungsschutz.de 27.03.2017.
[7] Regierung will bei IT-Angriffen zurückschlagen. www.golem.de 20.04.2017.
[8], [9] Cyber-Angiffe auf wichtige Infrastruktur - was tun im Ernstfall? www.br.de 13.04.2017.