Die Opposition als Versuchskaninchen

Die Cyber-Offensiven des Kreml gegen den Westen sind lange erprobt

Ilya Yashin | **Was an Hackerangriffen, Rufschädigung und Meinungsmanipulationen heute den Westen trifft, hat zuvor die russische Opposition getroffen. Die im Innern erprobten Methoden setzt der Kreml seit einigen Jahren auch für seine geostrategischen Ziele ein. Es geht dabei nicht zuletzt um eine Machtdemonstration – und das Einschüchtern von Gegnern.**

Spätestens nach der Annexion der ukrainischen Halbinsel Krim im August 2014 kam die russische Führung zu einem folgenreichen Schluss: Man verfüge über ausreichende Möglichkeiten und Ressourcen, direkten Einfluss auf die Politik im Westen zu nehmen. Das Minimalziel ist seitdem die Förderung oder Gründung einflussreicher politischer Organisationen in Europa; sie erhalten finanzielle und politische Hilfe aus Moskau und sollen dafür die geopolitischen Interessen Putins unterstützen. Das Maximalziel besteht darin, in EU-Staaten Regierungen an die Macht zu bringen, die die Annexion der Krim als legitim anerkennen, wie dies jüngst die rechtsextreme französische Präsidentschaftskandidatin Marine Le Pen in einem CNN-Interview tat; damit käme man auch der Aufhebung der Sanktionen näher. Zudem gilt es, die Europäische Union und die USA unter Druck zu setzen.

Das so jähe Anwachsen des Flüchtlingsstroms im Herbst 2015 missbrauchten populistische und extremistische Parteien für ihre Propagandazwecke mit dem Ziel, unter den europäischen Bürgern Skepsis gegenüber der EU zu schüren. Moskau griff diesen Parteien finanziell und medial unter die Arme. In einigen EU-Staaten geben heute Nationalisten den Ton an, die zuvor noch eine Randerscheinung waren. Sie zielen auf eine Auflösung der Europäischen Union – und unterminieren damit die Stabilität des Kontinents.

Dass Russland aus seiner Unterstützung für Donald Trump im US-Präsidentschaftswahlkampf einen Hehl gemacht hätte, wird man ebenfalls kaum behaupten können. Präsident Wladimir Putin machte Trump Komplimente, dessen ehemaliger Nationaler Sicherheitsberater Michael Flynn erhielt Honorare von russischen Propagandisten und saß bei einem offiziellen Empfang neben Putin; beim russischen Botschafter in Washington, Sergei Kisljak, gingen Mitarbeiter des republikanischen Wahlkampfteams ein und aus. Auch der staatliche Auslandssender RT (vormals Russia Today) warb unverhohlen für

Trump. Den verheerendsten Schlag gegen Trumps Kontrahentin Hillary Clinton führten allerdings Hacker, die mit dem russischen Geheimdienst in Verbindung standen. Sie verschafften sich Zugang zu den E-Mail-Konten der Parteiführung der Demokraten sowie von Clintons Wahlkampfmanager John Podesta und veröffentlichten danach eine Flut von kompromittierendem Material.

Kontrolle ist besser

Diese Hacker-Fähigkeiten sind bemerkenswert, kann man doch die russische IT-Branche kaum als technisch sonderlich fortschrittlich bezeichnen. Als Plattform für relativ freien Meinungsaustausch kommt dem Internet in Russland angesichts der weitverbreiteten staatlichen Zensur allerdings eine wichtige Rolle zu. Allein soziale Medien und Videoblogs bieten der Opposition derzeit die Möglichkeit, ihre Berichte über massive Korruption und Selbstbereicherung unter den Regierungsmitgliedern zu veröffentlichen. Zugleich versucht die russische Führung, das Internet immer weiter unter seine Kontrolle zu bekommen.

So haben der Kreml und die ihm hörige Duma unter dem Vorwand eines Anti-Terror-Gesetzes den gesetzlichen Rahmen massiv ausgeweitet, um zivilgesellschaftliche und politische Aktivitäten im Internet zu begrenzen. Im Juni 2016 wurde ein nach der Parlamentarierin Irina Jarowaja benanntes Gesetz verabschiedet, das die Mobilfunkbetreiber verpflichtet, Anrufe und Textnachrichten russischer Bürger zu speichern. Russische Sicherheitsbehörden können von den Messenger-Diensten den Zugang zur verschlüsselten Korrespondenz verlangen. Außerdem hat die Exekutive ein großes Instrumentarium zur Hand, um unbequeme Websites ohne Gerichtsbeschluss zu blockieren.

Die staatliche Verfolgung wurde ebenfalls verschärft. Mehrere oppositionelle Seiten, darunter die Internet-Zeitung Grani, das Online-Magazin Eschednewnij Journal und der Blog von Alexej Nawalny auf Livejournal.com wurden auf Geheiß der russischen Aufsichtsbehörde für Telekommunikation Roskomnadsor gesperrt. Buchstäblich jeden Monat werden neue Strafverfahren aufgrund solcher „Straftaten“ wie Kommentare in sozialen Medien oder einfache Repostings eingeleitet. Manche Blogger kommen mit Verurteilungen zu gemeinnütziger Arbeit davon, zuweilen werden aber auch Gefängnisstrafen verhängt.

Websites lassen sich ohne Gerichtsbeschluss blockieren

Die russische Führung lässt keine Versuche aus, soziale Medien mit rigorosen Maßnahmen unter Kontrolle zu bringen. So wurde Pawel Durow, Gründer des größten russischen sozialen Netzwerks VKontakte, 2013 unter staatlichem Druck dazu gezwungen, sein Start-up einem Unternehmen zu überlassen, das dem Oligarchen Igor Setschin nahesteht, einer Schlüsselfigur in Putins Umfeld, die ebenfalls aus dem Geheimdienst kommt. Aus Angst vor Repressalien verließ Durow bald danach das Land. Seit dieser „unfreundlichen Firmenübernahme“ veröffentlichen staatliche Medien immer wieder aus VKontakte stammende private Korrespondenzen von Oppositionellen, um sie zu diskreditieren.

Das Hauptziel des Kreml ist, das Internet in Russland als offene Plattform zu schwächen und unabhängige Websites zu zerstören, die von der Opposition

in ihrem Kampf gegen die russische Führung genutzt werden können. Chefideologe dieser Strategie ist German Klimenko, Berater des Präsidenten für die Entwicklung des Internets. Er spricht sich dafür aus, ausländische soziale Medien in Russland komplett zu verbieten. Klimenko drohte zudem mit der Sperre des bei der Opposition beliebten Dienstes Telegram Messenger, weil dieser sich geweigert hatte, seine Server komplett nach Russland zu verlegen.

Wichtig ist dabei, den politisch-ideologischen Hintergrund zu verstehen: Die russische Führung ist ernsthaft davon überzeugt, das Internet würde von den amerikanischen Geheimdiensten kontrolliert. „Das Internet entstand als ein CIA-Projekt und entwickelt sich weiterhin als solches", erklärte Putin 2014. Damals versprach er auch, mehr in russische IT-Unternehmen zu investieren.

Ein Instrument der Einflussnahme

Die massive Einmischung des Staates in die IT-Branche ist ein Grund für deren nur sehr langsame Entwicklung. Viele Computerexperten, die nicht bereit sind, unter ständiger Aufsicht zu arbeiten, wandern in den Westen ab, wo sie oft sehr erfolgreich sind. Russische Internetunternehmen, deren Tätigkeit restriktiv geregelt ist, büßen hingegen ihre Wettbewerbsfähigkeit ein.

Parallel dazu ist in Russland eine „staatliche IT-Branche" entstanden. Die Geheimdienste werben um die verbliebenen IT-Fachleute. Einige werden durch Geld gewonnen, andere werden genötigt, für den Staat zu arbeiten, weil ihnen sonst ein Strafverfahren droht. So sieht die für den Kreml typische Methode von Zuckerbrot und Peitsche aus.

Laut einer Studie von Zecurion Analytics, in der die Ausgaben für die Cyber-Sicherheit in den Verteidigungshaushalten verschiedener Staaten analysiert wurden, gehören entsprechende russische Abteilungen zu den Top 5 – nach denen der USA, Chinas, Großbritanniens und Südkoreas. Der chinesischen „Hacker-Armee", die Peking 1,5 Milliarden Dollar im Jahr kostet, gehören bis zu 20 000 Personen an. Großbritannien beschäftigt in diesem Bereich 2000 Mitarbeiter und gibt 450 Millionen Dollar aus, Südkorea investiert bei etwa 700 Personen 400 Millionen Dollar und Russland bei 1000 Personen „nur" 300 Millionen Dollar.

In Sachen Cyber-Sicherheit rangiert Moskau auf Rang 5

Für das Putin-Regime ist das Internet in erster Linie ein Instrument der äußeren Einflussnahme, gegen die es sich zu schützen gilt. Und ein Mittel, Oppositionelle im eigenen Land zu bekämpfen. Kurz: Die Technologien und Praktiken, mit denen der Westen neuerdings Bekanntschaft macht, werden schon lange und erfolgreich gegen die russische Opposition eingesetzt. Sie erlauben es dem Kreml, mehrere Dinge auf einmal zu tun: Informationen über die oppositionellen Organisationen zu sammeln, unabhängige Politiker und Anführer der Proteste zu diskreditieren und politisch motivierte Ermittlungsverfahren gegen die Kritiker von Putin und Personen aus seinem Umfeld einzuleiten.

So wurden 2011 und 2012 die Googlemail-Konten von Alexej Nawalny und seiner Frau gehackt und viele Jahre zurückreichende E-Mail-Korrespondenzen des Politikers veröffentlicht. Nawalny zufolge waren 90 Prozent der veröffentlichten Mails echt, die restlichen 10 Prozent wurden jedoch gefälscht.

Der Hackerangriff war Auftakt einer massiven Diskreditierungskampagne gegen Nawalny in den staatlich kontrollierten Medien. Die staatlichen Fernsehkanäle strahlten eine ganze Reihe von Sendungen aus, in denen Nawalnys E-Mails an Mitstreiter, Mitarbeiter und Familienmitglieder haarklein analysiert und von kremltreuen Experten kommentiert wurden. Der Zweck der Übung war deutlich: Man wollte den Ruf des bekanntesten Oppositionspolitikers so stark wie nur möglich beschädigen.

Der Hackerangriff selbst und die Veröffentlichung seiner E-Mails verstießen klar gegen das in der russischen Verfassung festgeschriebene Recht auf Privatsphäre. Angeklagt aber wurde Nawalny. Dessen E-Mail-Korrespondenz mit Nikita Belych, Gouverneur des Gebiets Kirow, den Nawalny eine Zeit lang beriet, erregte die besondere Aufmerksamkeit der Ermittler. Sie wurde auch zum Auslöser eines fingierten Ermittlungsverfahrens, an dessen Ende die Verurteilung Nawalnys stand – mit dem Verlust des passiven Wahlrechts. Nach einer Rüge des Europäischen Gerichtshofs für Menschenrechte wurde das Urteil später aufgehoben. Der Sprecher des Strafverfolgungskomitees Wladimir Markin gab praktisch zu, dass das Strafverfahren gegen Nawalny politisch motiviert war: „Die Politik spielt bei diesem Verfahren sicherlich eine Rolle, was mit der Person des Angeklagten zusammenhängt. Er versucht mit ganzer Kraft, Aufmerksamkeit zu erregen und die Staatsmacht zu reizen“, erklärte Markin in einem Interview.

Zuletzt wurde die Korrespondenz eines führenden St. Petersburger Oppositionellen, Andrej Piwowarow, gehackt, der den Messenger-Dienst von VKontakte.ru genutzt hatte. Seine E-Mails wurden im Staatsfernsehen ebenfalls ausführlich analysiert. Veröffentlicht wurde auch eine im privaten Rahmen aus-

gesprochene Kritik an anderen Oppositionellen – kurz vor einer angekündigten Demonstration. Das Ziel war offensichtlich: die Anführer verschiedener Protestorganisationen zu entzweien und deren Anhänger zu demoralisieren.

Der hybride Krieg des Kreml

Nach dem erfolgreichen Einsatz dieser Methoden gegen die russische Opposition begann der Kreml, sie in ähnlicher Weise auch für geopolitische Ziele einzusetzen. Die E-Mails, die aus erfolgreichen Hackerangriffen stammten, wurden der Plattform Wikileaks übergeben. Nach der Wahl kamen die US-Geheimdienste zu dem Schluss, dass diese Hackerangriffe im Auftrag der russischen Führung ausgeführt wurden und dass Putin höchstpersönlich die „aktiven Maßnahmen" angeordnet hatte.

Dass die russischen Geheimdienste und die von ihnen angeheuerten Hacker den Ausgang der US-Wahl entschieden hätten, ist dabei unwahrscheinlich. Der Überraschungssieg Donald Trumps hatte viel tiefere Gründe, die mit den Problemen in der amerikanischen Gesellschaft zusammenhängen. Dennoch besteht kein Zweifel an den Versuchen des Kreml, sich in den Wahlkampf einzumischen.

Offenkundig verfolgt Putin gegenüber dem Westen an allen Fronten eine hybride Konfrontationspolitik. Jedwede Aggression findet im Geheimen statt, damit sich der Kreml offiziell von den Aktivitäten seiner Geheimdienste distanzieren kann. Putin hat wohl kaum ernsthaft damit gerechnet, dass der von ihm präferierte Trump tatsächlich siegen würde. Aber es war den russischen Machthabern ein wichtiges Anliegen, amtierenden und zukünftigen Staats- und Regierungschefs in westlichen Ländern die Macht und Fähigkeiten Russlands zu demonstrieren, den Amerikanern nicht nur in Drittländern, sondern auch im eigenen Land Probleme bereiten zu können. Der Kreml glaubt, dass eine solche Machtdemonstration zusammen mit einem aggressiven Kurs dazu beiträgt, Politiker dieser Länder nachgiebiger zu machen.

Bei den Wahlen in Frankreich läuft die gleiche Masche

Trotz der harten Rhetorik und neuer US-Sanktionen in Reaktion auf die Manipulationen hat der Kreml von solchen Methoden auch keinen Abstand genommen. Bei den Präsidentschaftswahlen in Frankreich hat die von Putin unterstützte Kandidatin Marine Le Pen für den ersten Wahlgang ähnliche Umfragewerte wie der ehemalige Wirtschaftsminister Emmanuel Macron, den der Kreml kritisch sieht. In ihrem Bestreben, den Le-Pen-Kontrahenten zu diskreditieren, nutzten die russischen Geheimdienste offenbar dieselbe Masche wie bei der US-Wahl. Im Februar 2017 machte Macrons Wahlkampfteam erstmals öffentlich, dass es ständigen Hackerangriffen aus Russland ausgesetzt sei. Zudem hätten russische Medien einen großflächigen Informationskrieg gegen Macron entfacht, die Websites seiner Bewegung „En Marche!" erlitten regelmäßig russische Cyber-Attacken.

Effiziente Methode

Es besteht kein Zweifel daran, dass der Kreml die Hackerangriffe für eine der effizientesten Methoden hält, seine Gegner in die Bredouille zu bringen. Die

westlichen Regierungen, die erst seit Kurzem mit diesem Problem konfrontiert sind, versuchen mittels Sanktionen, solchen Aktivitäten entgegenzuwirken. Die Regierung Obama wies kurz vor der Amtsübergabe an Trump 35 russische Diplomaten aus, verhängte Sanktionen gegen einige hochrangige russische Geheimdienstmitarbeiter sowie die mit ihnen verbundenen privaten IT-Unternehmen, die nach Überzeugung Washingtons in die Cyber-Angriffe eingebunden waren.

Eine Ironie der Geschichte ist, dass der Einsatz von IT mittlerweile auch dem Kreml selbst im politischen Kampf zum Verhängnis geworden ist. Hackerattacken und die Veröffentlichungen von E-Mails und anderer elektronischer Korrespondenz werden auch von unterschiedlichen Kreml-Clans im internen Machtkampf eingesetzt. 2014 trat erstmals die Hackergruppe „Humpty Dumpty“ auf den Plan, die wiederholt Inhalte der E-Mail-Postfächer und Smartphone-Textnachrichten von hochrangigen Kreml-Beamten veröffentlichte. Zu den Attackierten zählten Ministerpräsident Dmitri Medwedew, dessen Stellvertreter Arkadij Dworkowitsch, Präsidentenberater Wladislaw Surkow sowie der stellvertretende Leiter der Abteilung für Innenpolitik bei der Präsidialadministration, Timur Prokopenko.

Der Kreml ist selbst Opfer der eigenen Methoden geworden

Die Enthüllungen boten der Gesellschaft eine Fülle von Informationen über Machtmissbrauch und Korruption in Regierungskreisen. Deshalb hielt man die „Humpty Dumpty“-Gruppe zunächst für Oppositionelle. 2016 wurde allerdings deutlich, dass die Hacker in Verbindung mit dem Geheimdienst FSB standen. Im Zuge der Ermittlungen wurden fast alle Mitglieder der Gruppe verhaftet. Ihr Auftraggeber Sergej Michajlow, einer der Leiter des FSB-Zentrums für Informationssicherheit, und dessen Stellvertreter Dmitri Dokutschajew, sitzen mittlerweile ebenfalls hinter Gittern.

Transparenz ist die beste Politik

Die Schlüsselfrage bleibt: Gibt es effiziente Maßnahmen gegen Cyber-Attacken? Wahrscheinlich sollte man sich damit abfinden, dass nahezu jede Nachricht, die über das Internet verschickt wird, potenziell der Öffentlichkeit zugänglich gemacht werden kann. Jedenfalls ist man innerhalb der russischen Opposition längst zu der Erkenntnis gelangt, dass die einzige effektive Methode, sich vor den vom Staat angeheuerten Hackern zu schützen, maximale Transparenz ist. Anders ausgedrückt: Man sollte nichts per E-Mail verschicken, was man nicht auch öffentlich auszusprechen bereit wäre. Das allerdings schützt nicht vor einer Maßnahme, zu der die Geheimdienste greifen, wenn sie über kein anderes kompromittierendes Material gegen ihre Opponenten innerhalb des Landes verfügen: belastendes Material schlicht zu fälschen.

Ilya Yashin ist einer der Vorsitzenden der Partei der Volksfreiheit (RPR-PARNAS), Mitbegründer der Bewegung Solidarnost und Autor des Berichts „The Criminal Russia Party“ (2016).