Hacking Democracy

Wie Cyber-Operationen sich auf demokratische Prozesse auswirken können

Sven Herpig und Stefan Heumann | **Noch wird in Deutschland per Zettel und Bleistift gewählt. Aber die Wahlkämpfe selbst werden durch den Gebrauch bestimmter Apps und vor allem durch soziale Medien immer digitaler. So beunruhigend der Hack von Bundestagsrechnern war: Cyber-Manipulation sozialer Medien machen Demokratien viel verwundbarer.**

Die Cyber-Angriffe gegen das Netz des Bundestags und die IT-Infrastrukturen des Democratic National Committee in den USA zeigen die Schattenseiten der Digitalisierung. Mit relativ wenig Aufwand konnten die Angreifer wichtige demokratische Institutionen stören und damit politische Prozesse eines Landes von außen beeinflussen. Die steigende Zahl an Vorfällen zeigt, dass diese Entwicklung anhalten wird, solange wir keine besseren Schutz- und Abschreckungsmaßnahmen entwickeln.

Angriff auf den Bundestag

Bei der Cyber-Operation gegen den Deutschen Bundestag wurden 2015 Dokumente aus dem internen Netz entwendet, bevor der Angriff erkannt und gestoppt werden konnte. Bis heute wissen wir nicht, wie viele und welche Dokumente abgeflossen sind. Betrachtet man die bekannt gewordenen Ziele dieses Angriffs, kann man mutmaßen, dass die Angreifer einen besseren Einblick in Deutschlands Verhandlungspositionen in der Russland-Politik erhalten wollten. Denn die Operation richtete sich gezielt auf Abgeordnete, die sich mit Russland befassen. Zahlreiche Politiker warnen davor, dass diese Dokumente kurz vor der Bundestagswahl im September wieder auftauchen und missbraucht werden könnten – um zum Beispiel Fake News zu produzieren.

Wir hingegen meinen, dass der Bundestags-Hack dem Ziel der Informationsdominanz dient. Denn dieses Konzept knüpft nahtlos an die strategischen Doktrinen der USA, Chinas und Russlands an. Die Reaktionen von offizieller deutscher Seite blieben eher verhalten: Hans-Georg Maaßen, Präsident des Bundesamts für Verfassungsschutz, bezeichnete Russland als Urheber dieses Angriffs. Bundeskanzlerin Angela Merkel wies bei einem Treffen mit Russlands Staatspräsidenten Wladimir Putin auf die Schwere eines solchen Vergehens hin.

Auch wenn in Deutschland über dieses Thema mittlerweile weniger

diskutiert wird, besteht die Problematik weiter. Denn die Anzahl der Cyber-Operationen gegen politische Akteure wie Parteien und ihre Stiftungen ist nicht etwa geringer geworden. Im Gegenteil.

Geringe Kosten, großer Schaden

Im vergangenen Jahr wurde bekannt, dass zwei parallele Cyber-Operationen gegen die IT-Systeme des Democratic National Committee (DNC) erfolgreich durchgeführt werden konnten. Dabei gelangten Zehntausende interne E-Mails der Demokratischen Partei in die Hände der Angreifer.

Die so erbeuteten Informationen wurden veröffentlicht, vermutlich mit dem Ziel, das DNC zu diskreditieren und im Wahlkampf zu schwächen. Inwieweit diese Einflussnahme Donald Trump bei seiner Wahl zum Präsidenten geholfen hat, wird abschließend wohl nicht geklärt werden können. Sicher ist jedoch: Weder Partei noch Regierung waren ausreichend vorbereitet. Dies gilt sowohl für die Prävention als auch in Bezug auf Gegenmaßnahmen und außenpolitische Reaktionen.

Wohl nannte der Director of National Intelligence, James R. Clapper Jr., im Namen der Obama-Regierung Russland als Ursprung des Angriffs. Die Geheimdienste veröffentlichten ein Dossier, das diese Anschuldigung untermauern sollte. Doch erst knapp sechs Monate nach Aufdeckung der Operationen (und erst, nachdem die Wahlen vorüber waren) verhängte der scheidende Präsident Barack Obama Sanktionen gegen Russland.

Für viele war dies entschieden zu spät – und viel zu wenig. Einige Experten vermuten, dass Wikileaks und The Shadow Brokers auf diese Sanktionen wiederum eine Antwort fanden: Sie veröffentlichten sehr beachtliche Mengen an Informationen über Schwachstellen und bestimmte Instrumente in CIA und NSA, mit denen Cyber-Operationen durchgeführt werden können. Die jüngste Verschärfung der Sanktionen durch die USA und die russische Antwort zeigen, dass die amerikanisch-russischen Beziehungen durch die Vorfälle im Wahlkampf nachhaltig beschädigt worden sind.

Die Angriffe auf den Bundestag und das DNC liefen nach relativ ähnlichem Muster ab. In beiden Fällen wurden E-Mails mit Schadsoftware im Anhang bzw. per Link versandt, die beim Empfänger den Eindruck erweckten, es handele sich um unverfängliche Nachrichten. Hatten die Angreifer erstmal Zugriff auf einen kleinen Bereich der IT-Systeme, konnten sie sich weiter ausbreiten und immer mehr Daten erbeuten. In beiden Fällen gab es technische Schutzmaßnahmen, die Angriffe hätten abwehren können. Doch sie wurden nicht angewandt. Dieses Problem beschränkt sich nicht nur auf die Politik. Der durch WannaCry und NotPetya angerichtete Schaden hat vor ein paar Monaten demonstriert, dass auch der Privatsektor sich nicht ausreichend wehren kann.

Die Angriffe liefen nach relativ ähnlichem Muster ab

Die finanziellen und politischen Kosten für die Durchführung von Cyber-Operationen sind für den Angreifer relativ gering. Aber für die Betroffenen ist es schwierig, ihre eigene Öffentlichkeit zu interessieren und zu sensibilisieren, vor allem weil die Dementis der Drahtzieher schwer zu widerlegen sind. Diese Gemengelage

hat dazu geführt, dass entsprechende politische Antworten keine Durchschlagskraft entfalten konnten.[1] Angreifer, die demokratische Prozesse im Ausland beeinflussen wollen, haben dies längst begriffen und bauen entsprechende Fähigkeiten aus. Auch wenn bisher nicht klar ist, welche Auswirkungen solche Operationen wirklich haben, sind die Kosten doch gering genug, um es einfach zu versuchen. Die Einstiegshürden sind so niedrig, dass wahrscheinlich auch ganz neue Akteure auf den Plan gerufen werden.

Meinungen manipulieren und Spionage effizienter machen

Neues Instrument der Außenpolitik

Außenpolitik hat seit jeher das Ziel, Einfluss auf die Politik anderer Staaten zu nehmen. Dazu stehen verschiedene Instrumente wie klassische Diplomatie oder nachrichtendienstliche Aktivitäten zur Verfügung. Die Digitalisierung von Informationen und Kommunikation ergänzt dieses Instrumentarium. Mit Cyber-Operationen kann dabei nur eine neue Dimension der Effizienz von Spionage und Sabotage erreicht werden.

Die Nutzung sozialer Medien hingegen für Public Diplomacy und die Manipulation öffentlicher Meinung ist ein echtes Novum; ein Instrumentarium, das grundsätzlich allen Staaten zur Verfügung steht – wobei es natürlich Unterschiede im Hinblick auf Kapazitäten und Verwundbarkeiten gibt. Die Snowden-Veröffentlichungen zeigen, wie ernst die USA und ihre engsten Verbündeten die strategischen Möglichkeiten von Cyber-Spionage und -Operationen nehmen.

Bei den Motiven und Zielen solcher Operationen erkennt man allerdings große Unterschiede zwischen den Staaten. Die USA streben vor allem eine Vorherrschaft bei der Informationsbeschaffung und der Netzwerkinfiltration an. China schreckt zur Stärkung der eigenen Industrie auch vor Wirtschaftsspionage nicht zurück. Bei den Operationen gegen das DNC und die staatlichen Medien in Katar[2] sowie möglicherweise auch beim Angriff auf die Wahlkampagne des französischen Präsidentschaftskandidaten Emmanuel Macron wurden so beschaffte Informationen genutzt, um außenpolitische Ziele zu erreichen.[3] Zwei Tage vor der zweiten Abstimmung wurde Macrons Wahlkampfteam „En Marche!“ Opfer eines Hacker-Angriffs, der zur Veröffentlichung interner E-Mails führte. Im Falle von Katar wurde die staatliche Nachrichtenagentur Qatar News Agency Ziel einer Cyber-Operation. Die Aussagen des Emirs Tamim bin Hamad al-Thani wurden in den sozialen Medien so manipuliert, dass der bereits schwelende Konflikt zwischen Katar und

[1] https://www.stiftung-nv.de/de/publikation/cyber-operations-defending-political-it-infrastructures

[2] https://www.washingtonpost.com/world/national-security/uae-hacked-qatari-government-sites-sparking-regional-upheaval-according-to-us-intelligence-officials/2017/07/16/00c46e54-698f-11e7-8eb5-cbccc2e7bfbf_story.html

[3] Dass die Manipulation von Informationen auch handfester (Cyber-)Sabotage dienen kann, haben die Operationen gegen die iranische Nuklearanreicherungsanlage in Natanz und gegen die Energieversorgung in der Ukraine bewiesen, https://www.stiftung-nv.de/de/publikation/anti-war-and-cyber-triangle-strategic-implications-cyber-operations-and-cyber-security & https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01

Bild nur in Printausgabe verfügbar

anderen Staaten im Mittleren Osten, allen voran Saudi-Arabien eskalierte.

Warnung vor Wahlcomputern

Wir stehen erst am Anfang einer Entwicklung von der reinen Informationsbeschaffung hin zur Manipulation beziehungsweise der öffentlichen Ausnutzung so beschaffter Informationen. Sowohl die wachsende Zahl der beteiligten Akteure als auch die bisherige Effektivität der Kampagnen deuten darauf hin, dass wir künftig noch viel mehr davon sehen werden – überall auf der Welt und mit unterschiedlichen strategischen Ausprägungen.

Die Bundestags- und DNC-Hacks haben uns die digitale Verwundbarkeit von Demokratien vor Augen geführt. Allerdings bilden sie nur die Spitze des Eisbergs. Ein erfolgreicher Angriff auf Auszählungsprozesse und Wahlcomputer würde direkt ins Herz unserer Demokratien treffen und die Legitimität der Ergebnisse infrage stellen. Die Berichte über russische Versuche, die Computer von Wahlleitern in den USA anzugreifen, zeigen, wie knapp die Vereinigten Staaten an einem solchen Szenario vorbeigeschlittert sind.

Seit Jahren warnen Experten vor dem Einsatz von Wahlcomputern. Auf der Hacker-Konferenz Def Con in Las Vegas wurde im Juli zum wiederholten Male gezeigt, wie schnell und einfach Wahlcomputer von Unbefugten zu manipulieren sind.[4] Angesichts dieser Verwundbarkeiten fordern viele Experten die Rückkehr zum klassischen Wahlzettel. Doch selbst wenn die USA zu der in Deutschland nach wie vor üblichen Stimmabgabe mit Stift und Papier zurückkehren, werden die Möglichkeiten zur Manipulation und Einflussnahme auf unsere Wahlen größer und nicht geringer werden.

[4] https://www.theregister.co.uk/2017/07/29/us_voting_machines_hacking/

Dies liegt an einer Entwicklung, der sich weiter zuspitzen wird. Wahlkampf und politische Kommunikation werden immer digitaler und so entstehen ganz neue Verwundbarkeiten in Demokratien. Anfang 2000 kommunizierten Kandidaten und Parteien noch hauptsächlich über E-Mail-Listen, Blogs und Webseiten. Heute stehen soziale Medien im Mittelpunkt. Und wie die Diskussion um Desinformationskampagnen (Fake News) und die Rolle von automatisierten Accounts (Bots) zu ihrer Verbreitung zeigt, ergeben sich ganz neue Möglichkeiten, Wahlkämpfe von außen zu stören oder zu beeinflussen.

Die direkte Wähleransprache bietet Vor- und Nachteile

Steuerung durch soziale Medien

Mit dem so genannten Micro-Targeting (einzelne Wählergruppen über soziale Medien gezielt anzusprechen) wird es immer schwieriger, Desinformationskampagnen und Versuche der Einflussnahme überhaupt zu erkennen. Werden auf diese Weise zum Beispiel im Namen einer Partei bewusst Falschinformationen gestreut, fehlen uns bisher ein gesellschaftlicher Konsens und wirksame Ansätze, wie damit umzugehen ist. Es wäre ein erster, wichtiger Schritt, Micro-Targeting von politischen Parteien offenzulegen, um Fälle von Desinformation und Missbrauch zumindest schnell erkennen und öffentlich machen zu können.

Auch die Parteien und ihre Wahlkämpfer werden immer digitaler. Nicht nur kommunizieren sie viel und potenziell auch viel Sensibles über E-Mail, wie der DNC-Hack gezeigt hat, sondern der gesamte Wahlkampf wird immer mehr mithilfe von Daten und digitalen Werkzeugen gesteuert. In den USA sammeln die beiden großen Parteien schon seit Jahrzehnten Daten über Wähler. Die Auswertung der Datenbanken bildet die Grundlage für auf Zielgruppen zugeschnittene politische Kommunikation und die Steuerung des Ressourceneinsatzes – zum Beispiel für die Entscheidung, welche Wähler von der Kampagne persönlich aufgesucht werden sollten. Mit Hilfe von speziell entwickelten Apps werden zusätzlich die wichtigsten Erkenntnisse aus persönlichen Interaktionen mit Wählern erfasst und in die Datenbanken der Parteien eingespeist.

Natürlich lassen sich die Entwicklungen in den USA nicht einfach auf Deutschland übertragen, schon wegen der Unterschiede in der Rolle sozialer Medien insgesamt, ihrer Verbreitung und Nutzung sowie rechtlicher Unterschiede, vor allem in Bezug auf den Datenschutz. Aber auch in Deutschland, wie in allen Demokratien, werden Wahlkämpfe und andere Abstimmungen immer digitaler. So spielten soziale Medien eine wichtige Rolle in den Kampagnen um das Referendum zum EU-Austritt Großbritanniens. Und mit dem Projekt Connect 17 setzt die CDU auf Datenanalyse und die Organisation ihres Haustürwahlkampfs mit Hilfe digitaler Werkzeuge.

Die Vorteile dieser Mittel zur gezielten Wähleransprache und besseren Steuerung und Kontrolle des Ressourceneinsatzes liegen auf der Hand. Zugleich ergeben sich aber neue Möglichkeiten für Sabotage und Manipulation. Denn die Datenbanken und mit ihnen verknüpften Applikationen bieten neue Angriffsmöglichkeiten für alle, die ein Inte-

resse daran haben, Wahlkämpfe zu stören oder gar zu manipulieren. So könnten zum Beispiel sensible Wählerdaten erbeutet und veröffentlicht werden. Wie würden wir damit umgehen, wenn die Datenbanken und Applikationen von nur einer Partei angegriffen und lahmgelegt werden und ihr dadurch ein erheblicher Wettbewerbsnachteil im Wahlkampf entsteht? Bei der letzten Wahl hat vermutlich kaum jemand damit gerechnet, dass 2017 die Profile prominenter Politiker in sozialen Medien ebenso geschützt werden müssen wie der Bundeswahlleiter und der Wahl-O-Mat. Das ist erst der Anfang. Schon heute sind die Verwundbarkeiten riesig. Man braucht keine Glaskugel, um vorherzusehen, dass sie in Zukunft noch größer werden.

Planen für den Ernstfall

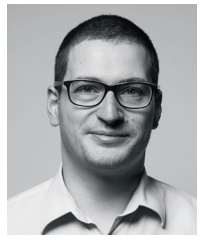
Schon ohne Fremdeinwirkung von außen ist der Wahlkampf von morgen nicht nur eine Herausforderung für den Datenschutz, sondern auch für IT-Sicherheit. Die Erhebung, Speicherung und Analyse von Daten sind die Grundlage für immer ausgefeiltere Werkzeuge, um Wahlkampagnen zu organisieren und durchzuführen. Gleichzeitig steigt die Bedeutung digitaler Kommunikationskanäle wie soziale Medien stetig. Hierdurch vergrößern sich die Angriffsflächen für Cyber-Operationen.

Mögliche Angriffsszenarien reichen von der Erbeutung und Veröffentlichung sensibler Daten bis hin zur Manipulation von Informationen und Sabotage der zugrundeliegenden IT-Systeme. Potenziellen Angreifern stehen viele Angriffsmöglichkeiten zur Verfügung, mit denen sie versuchen können, den demokratischen Prozess zu beeinflussen oder politische Instabilität zu erzeugen.

Betrachtet man die geopolitische Entwicklung, wird deutlich, dass immer mehr Akteure das Potenzial von Cyber-Operationen erkannt haben und versuchen, ihre Fähigkeiten in diesem Bereich auszubauen. Diese Entwicklung gibt Anlass zur Sorge. Denn die Funktionalität und Integrität unserer demokratischen Prozesse steht auf dem Spiel.

Die Funktionalität unserer Demokratie steht auf dem Spiel

Wir müssen uns dieser Herausforderung stellen. Hierzu müssen wir uns mit den technischen Entwicklungen im Wahlkampf und den damit verbundenen Cyber-Risiken befassen. Zur Risikobewertung gehört auch eine intensivere Auseinandersetzung mit den geopolitischen Interessen und strategischen Ansätzen, die hinter solchen Interventionen in unsere demokratischen Prozesse stecken könnten. Nur so können wir geeignete Schutzmaßnahmen entwickeln und rechtzeitig implementieren.



Dr. Sven Herpig
leitet das Transatlantische Cyber Forum, ein Expertennetzwerk für Cyber-Sicherheits- und -verteidigungspolitik, bei der Stiftung Neue Verantwortung.

Dr. Stefan Heumann
ist Mitglied des Vorstands der Stiftung Neue Verantwortung. Er beschäftigt sich mit den Auswirkungen neuer Technologien auf Außenpolitik, Sicherheit und Bürgerrechte.