EUROPÄISCHE INTEGRATION 04.02.2019 | Moritz Wiesenthal

Europas offene Flanke

Bei den Europawahlen drohen Cyberangriffe von rechts, doch die EU schützt sich nur unzureichend.

Dass die Wahlen zum Europäischen Parlament (EP) zum Ziel für Hackerangriffe, Desinformationskampagnen und Manipulationsversuche in den sozialen Netzwerken werden, kann als sicher gelten: Rückwirkend lässt sich deutlich rekonstruieren, dass jedes politische Großereignis seit den US-Präsidentschaftswahlen 2016 in Europa von Manipulationsversuchen im Cyberraum begleitet wurde. Vom Brexit-Referendum über die französischen Präsidentschaftswahlen bis hin zum umstrittenen Volksentscheid über die Unabhängigkeit Kataloniens konnten europaweit Think Tanks, NGOs und staatliche Akteure versuchte und erfolgte Desinformationskampagnen und Cyberangriffe dokumentieren. In Belgien zerbrach im Dezember letzten Jahres gar die Regierungskoalition an einer Kontroverse über den UN-Migrationspakt, die maßgeblich von ultrarechten Bewegungen in den sozialen Netzwerken befeuert wurde. So ist es nicht verwunderlich, dass sich laut einer aktuellen Eurobarometer-Umfrage drei Viertel aller Europäer um Desinformation im Netz sorgen.

Als Reaktion auf die Bedrohung aus dem Cyberraum wiesen die europäischen Staats- und Regierungschefs dem Thema in ihrer Ratserklärung vom Oktober 2018 erkennbar Prominenz zu. Kurz darauf legte die EU-Kommission einen Aktionsplan vor, der konkrete Vorschläge zur Absicherung der Wahlen beinhaltet. Tatsächlich aber verkennen die bisher getroffenen (und nicht getroffenen) Maßnahmen auf fahrlässige Weise den Charakter der Europawahlen, die aktuell zum Festschmaus für Angreifer aus dem digitalen Off zu werden drohen. Drei zentrale Faktoren potenzieren dabei die Tragweite von Cyberangriffen auf die Europawahlen im Vergleich zu nationalen Urnengängen und verleihen der Diskussion um die Schattenseiten der digitalen Demokratie im Kontext der EU eine besondere Brisanz.

Die fragmentierte Struktur nationaler Sicherheitsvorkehrungen

Ein erster wichtiger Unterschied zeigt sich schon beim Blick auf die parteipolitische Lage des Kontinents. Zunehmend <link rubriken soziale-demokratie artikel die-falle-der-

eröffnet zusammen mit der vergleichsweisen langen Wahldauer eine breite Palette an digitalen Angriffsmöglichkeiten.

europaskeptiker-3231>formieren sich rechts der Mitte europaskeptische Parteien, deren erklärtes Ziel eine Schwächung der EU ist. Gerade diese Kräfte nutzten bereits bei nationalen Wahlen und Referenden soziale Medien als zentrales Instrument zur Meinungsmache und schreckten dabei auch vor gezielten Desinformationskampagnen und Fake News nicht zurück, wie beispielsweise im Rahmen des Bundestagswahlkampfes. Besondere Relevanz bekommt die Netzaffinität europafeindlicher Kräfte angesichts aktueller Bündnisbestrebungen im rechten Lager, in deren Rahmen der Vorsitzende der italienischen Rechtspopulisten Salvini eine Allianz verschiedenster europaskeptischer Parteien anstrebt. Sollte die Herausbildung dieses Bündnisses tatsächlich glücken, würde damit eine europaweite Angriffsachse im digitalen Raum entstehen. Anders als bei nationalen Wahlen würden dann Ende Mai die Ergebnisse verschiedenster nationaler und nationalistischer Kampagnen im Cyberraum in einem Wahlergebnis verschmelzen, das vereinten europafeindlichen Kräften zu einem deutlichen Zuwachs im EP verhelfen könnte.

Neben einheimischen Akteuren dürfte bei den Europawahlen aber auch ein außereuropäischer Player von besonderer Relevanz für die Vorgänge im Cyberraum werden. Russland hat in der Vergangenheit mehrfach versucht, sowohl über Fake News als auch über den gezielten Einsatz von Bots in sozialen Netzwerken und der bekannten Trollfabrik aus St. Petersburg auf Wahlen in Europa Einfluss zu nehmen. Dabei weist die Absicht des Kreml eine perfide Schnittmenge mit den Zielen europafeindlicher Kräfte auf: eine nachhaltige Destabilisierung der Europäischen Union als Ganzes. Folgerichtig unterstützt Moskau europaweit euroskeptische Parteien auch finanziell. Der essentielle Unterschied zwischen nationalen Urnengängen und den Europawahlen wird in der Konsequenz brisant, weil damit wesentliche Akteure im digitalen Raum die Wahlen im Mai 2019 nicht mehr nur für eine klassische Richtungsentscheidungen für oder wider einer politischen Agenda nutzen (beispielsweise für oder gegen eine Erhöhung des Mindestlohns), sondern sie zur Wahl über das für oder wider der EU als Ganzes pervertieren – ein auf nationaler Ebene undenkbarer Vorgang.

Dieses düstere Bedrohungsszenario trifft darüber hinaus bei den EP-Wahlen auf eine bisher schwach konsolidierte Verteidigungslinie, die einen zweiten elementaren Unterschied zu nationalen Wahlen darstellt. Zentraler Aspekt ist dabei der Charakter der Wahlen: Statt eines einzelnen Wahlgangs erstrecken sich die Wahlen zum Europäischen Parlament vom 23. bis zum 26. Mai über einen längeren Zeitraum und finden gleichzeitig als nationale Wahlen in 27 (oder 28) Mitgliedstaaten statt. Damit liegt auch die Verantwortung zum Schutz der Wahlinfrastruktur vor Cyberangriffen bei den einzelnen Mitgliedstaaten, deren Vorkehrungen jedoch unterschiedlich intensiv ausfallen. Diese fragmentierte Struktur nationaler Sicherheitsvorkehrungen eröffnet zusammen mit der vergleichsweisen langen Wahldauer eine breite Palette an digitalen Angriffsmöglichkeiten. Entsprechend resigniert bezeichnete die Europäische Kommissarin für Justiz, Verbraucherschutz und Gleichstellung die bisher getroffenen Maßnahmen der Mitgliedstaaten als Flickenteppich. Dass es schon in Deutschland bei den Bundestagswahlen 2017 gelungen ist, die zentrale Software zur Übermittlung der Wahlergebnisse an den Bundeswahlleiter zu hacken, verheißt dabei wenig Gutes.

Kommen die Mitgliedstaaten ihrer Verantwortung zum Schutz der Wahlen nicht nach, wird die Union die kostspielige Zeche zahlen müssen.

Ein dritter und letztendlich entscheidender Faktor spiegelt sich in den Auswirkungen der Wahlen wider. Sollten einerseits Desinformationskampagnen oder die automatisierte Verbreitung von Fake News in den sozialen Medien erfolgreich sein, könnten europafeindliche Kräfte enorme Sitzgewinne geltend machen und die Handlungsfähigkeit der EU empfindlich einschränken. Sollte andererseits ein Cyberangriff auf die Wahlinfrastruktur in nur einem einzelnen Mitgliedstaat erfolgreich sein, könnte das Ergebnis der Wahlen und die Legitimität des neuen Europäischen Parlaments offen in Frage gestellt werden. In beiden Fällen wäre der <link rubriken europaeische-integration artikel pump-it-up-3081>notwendigen Stärkung des Parlaments und einer Demokratisierung der EU ein Bärendienst erwiesen.

Schlussendlich offenbart sich in der Diskussion um den Umgang mit digitalen Bedrohungen für die EU ein fatales Ungleichgewicht: Kommen die Mitgliedstaaten ihrer Verantwortung zum Schutz der Wahlen nicht nach, wird die Union die kostspielige Zeche zahlen müssen. Angesichts der aktuellen Lage in Europa, bei der sich die Auseinandersetzung um die

politische Ausrichtung der EU zunehmend zur Polemik um ihr Überleben zuspitzt, könnte die Rechnung unverhältnismäßig hoch ausfallen.



Moritz Wiesenthal
Berlin

Moritz Wiesenthal (geb. Fessler) arbeitet und promoviert am Lehrstuhl für Internationale und Europäische Politik der Europa Universität Viadrina in Frankfurt (Oder). Zuvor war er unter anderem im Deutschen Bundestag tätig. Er hat in Magdeburg, Berlin und Nishni Nowgorod European Studies und Internationale Beziehungen studiert.