Lehren aus #MacronLeaks

Was hilft gegen Cyberangriffe? Eine Untersuchung der Kampagne gegen Emmanuel Macron und sein Wahlkampfteam 2017 zeigt, was funktioniert

Von Jean-Baptiste Jeangène Vilmer

Aus den zahlreichen Versuchen der vergangenen Jahre, Wahlkämpfe zu manipulieren, sticht die Einflussnahme auf die französischen Präsidentschaftswahlen 2017 aus einem ganz einfachen Grund heraus: Sie war nicht erfolgreich. Der gezielte Versuch, Emmanuel Macrons Kandidatur durch eine Desinformationskampagne zu untergraben, scheiterte – und das, obwohl die Täter nicht nur Gerüchte, Falschinformationen und sogar gefälschte Dokumente in die Welt setzten, sondern kurz vor der Wahl auch noch die Computer von Macrons Wahlkampfteam angriffen. Nur zwei Tage vor der entscheidenden Stichwahl, am 5. Mai 2017, wurden 21 705 E-Mails geleakt.

Desinformation, Hack, Leak

Die Desinformationskampagne gegen Macron setzte ein, als er offensichtlicher Spitzenreiter im französischen Präsidentschaftsrennen wurde. Als seine Umfragewerte im Januar 2017 stiegen, wurde er immer häufiger zum Opfer strategischer und aggressiver Attacken, die vornehmlich aus zwei Lagern kamen: aus den russischen Staatsmedien und aus der amerikanischen Alt-Right-Bewegung. Mittels einer Sturmflut persönlicher und politischer Diffamierungen versuchten diese, Macron zu diskreditieren. Er wurde als „Globalist", reicher Banker, „Islam-Versteher" und Befürworter unkontrollierter Einwanderung hingestellt. Zudem mehrten sich die abfälligen Kommentare über den Altersunterschied zwischen Macron und seiner Frau sowie Gerüchte über seine Sexualität. Die einzelnen Online-Communities und politischen Kampagnen, die dahintersteckten, waren allerdings kaum homogen: Amerikanische Alt-Right verband sich mit rechtsextremen, kremlfreundlichen Akteuren in Frankreich – ein Netzwerk Gleichgesinnter ohne zentrales Organ.

Erste Hackerangriffe auf Kampagnenmitarbeiter von Macron begannen bereits im Dezember 2016 und

Dieser Text basiert auf dem Bericht „The Macron Leaks Operation: A Post-Mortem" (Atlantic Council/Institut de Recherche Stratégique de l'Ecole Militaire).

umfassten Phishing-Attacken, Tabnabbing und E-Mail-Spoofing. Insgesamt wurden die beruflichen und persönlichen E-Mail-Konten von mindestens fünf engen Macron-Vertrauten gehackt. Die gestohlenen E-Mails und weitere Dateien datierten vom März 2009 bis zum 24. April 2017, umfassten also auch Dokumente, die gerade einmal zwei Wochen vor der Stichwahl erstellt worden waren.

Das anschließende Leak der gehackten E-Mails fand dann am 5. Mai 2017 statt und damit nur wenige Stunden vor der sogenannten „Waffenruhe", die es politischen Kandidaten und Medien in Frankreich gesetzlich verbietet, unmittelbar weitere öffentliche Erklärungen abzugeben. Folglich konnten die geleakten Dokumente weder von Macrons Team noch von den Medien kommentiert und analysiert werden. Stattdessen wurden die sozialen Medien und insbesondere Twitter zum primären Diskussionsraum für die lancierten Inhalte.

Der Hashtag tauchte in 24 Stunden eine halbe Million Mal auf

Die Dokumente waren anfangs auf einer Reihe von Filesharing-Websites verfügbar und wurden auf Twitter vor allem von amerikanischen Alt-Right-Vertretern geteilt, die auch den Hashtag #MacronLeaks starteten. Nur wenig später machte WikiLeaks die Inhalte dann via Link auch einem breiten internationalen Publikum zugänglich. In Frankreich nahm der Front National, die Partei von Macrons Gegenspielerin Marine Le Pen, das Thema auf. Insgesamt tauchte der Hashtag #MacronLeaks dank einiger weniger Bot-Accounts, von denen vereinzelte auch für den Angriff auf die US-Präsidentschaftswahlen 2016 verwendet worden waren, innerhalb von 24 Stunden in fast einer halben Million Tweets auf.

Die geleakten Inhalte stammten hauptsächlich aus den gehackten E-Mail-Konten, enthielten jedoch auch noch zwei weitere Ordner. Da die Originaldateien von den Hackern wohl als nicht belastend genug eingestuft worden waren, hatten sie zusätzlich einige Dokumente verfälscht, um seine Kampagne zu diskreditieren. Die „Macron-Leaks" fallen deshalb in die Kategorie der „tainted leaks", also Leaks, bei denen (zumindest einige) der veröffentlichten Dokumente vor der Weiterverbreitung manipuliert wurden. Die gefälschten Nachrichten suggerierten unter anderem, dass Macron Kokain konsumiert („Vergiss nicht, K. für den Chef zu kaufen") und dass er auf der Mailingliste von Vestiaire Gay stand, einer Unterwäschemarke, die sich an homosexuelle Kunden richtet.

Wer waren die Täter?

Der Angriff auf Macron bestand also aus drei Elementen: aus der Desinformationskampagne, die vor allem auf Fake News und der Verbreitung von Gerüchten und gefälschten Dokumenten beruhte, aus einem Cyberangriff und aus einem anschließenden Leak der gehackten Inhalte. Obwohl diese drei Vorgänge auf den ersten Blick koordiniert scheinen mögen, ist wohl eher davon auszugehen, dass es sich um „verschiedene Taten und nicht um eine zusammenhängende Tat" (François Delerue) handelte. Es ist unwahrscheinlich, dass nur ein einzelner Akteur hinter dem Angriff steckte.

Die Drahtzieher der Desinformationskampagne zu finden, ist derweil nicht schwierig, da diese nicht ein-

Bild nur in Printausgabe verfügbar

mal versuchten, sich unkenntlich zu machen: Weder die russischen Staatsmedien noch die Alt-Right-Bewegung machten einen Hehl aus ihrer Anti-Macron-Propaganda. Die Verantwortlichen hinter dem Hackerangriff auf das Macron-Team zu bestimmen, ist allerdings ungleich komplizierter.

Bis heute hat die französische Regierung keine offizielle Stellungnahme herausgegeben, die die Schuldigen nennt. Mehrere IT-Firmen und Cybersicherheitsforscher gehen jedoch davon aus, dass es sich um eine russische Geheimdienstoperation handelte, die im Dunstkreis der sogenannten APT-28-Gruppe, einem russischen Hackerkollektiv, geplant und durchgeführt wurde. Es ist jedoch ebenfalls möglich, dass der auch „#MacronGate“ genannte Vorgang auf einen US-Neonazi namens Andrew Auernheimer zurückgeht – und William Craddick, der Gründer von „Disobedient Media“, der unter anderem als Ideenvater der „Pizzagate“-Verschwörungstheorie gilt, scheint die Dokumente als erster via 4chan verbreitet zu haben.

Das plausibelste Szenario ist daher, dass die „Macron-Leaks“ sowohl vom russischen Geheimdienst als auch von der amerikanischen Alt-Right angestoßen wurden. Dabei ist jedoch nicht klar, ob diese kooperierten oder nur parallel auf dasselbe Ziel hinarbeiteten.

Gründe des Scheiterns

Dass die „Macron-Leaks“ keinen Erfolg hatten, beruhte nicht nur auf einer Kombination struktureller Faktoren und einer Portion Glück, sondern auch auf der effektiven Antizipation und Reaktion der Mitarbeiter der Macron-Kampagne, der französischen Regierung, der Zivilgesellschaft und der Massenmedien.

Im Vergleich zu anderen Ländern bot Frankreich den Angreifern ein weniger anfälliges politisches und mediales Umfeld. Die Länge des französischen Präsidentschaftskampfs ist

klar geregelt. Da er zudem zwei Wahldurchgänge hat, können sich Manipulatoren nicht sicher sein, welche Kandidaten sich durchsetzen. Gleichzeitig sind die Medien in Frankreich stärker reguliert als beispielsweise in den USA. Zudem ist die Veröffentlichung oder Analyse von Meinungsumfragen und Wahlbarometern am Tag des Urnengangs und am Vortag gesetzlich verboten.

Franzosen trauten Facebook nicht als Nachrichtenquelle

Dazu kommt, dass die französische Medienlandschaft zum Zeitpunkt der „Macron-Leaks" relativ robust war. Im Januar 2017, als die Desinformationskampagne begann, gab es in Frankreich relativ gesehen deutlich weniger Internetnutzer als in den USA, Deutschland, Kanada oder Großbritannien – und auch die Verbreitungsrate der sozialen Medien war äußerst gering. Außerdem trauten französische Leserinnen und Leser Facebook und Co. nicht als Nachrichtenquelle. Einer Studie der Universität Oxford zufolge teilten „die französischen Wähler qualitativ bessere Informationen als viele US-Wähler und fast genauso viele hochwertige Nachrichten wie deutsche Nutzer". (Allerdings hat zuletzt die Gelbwesten-Bewegung gezeigt, wie wichtig „alternative" und verschwörerische Medien mittlerweile auch in Frankreich geworden sind.)

In den Jahren vor 2017 haben vor allem zwei Vorkommnisse dazu beigetragen, die französische Medien- und Meinungslandschaft krisenfester zu machen: der Cyberangriff auf TV5Monde 2015, der vielen in der Branche als Weckruf diente, und die Online-Propaganda von Dschihadisten im Vorfeld der Terrorattacken auf französischem Boden, die dazu beitrug, dass digital verbreitete Inhalte insgesamt kritischer wahrgenommen wurden.

Zu guter Letzt spielt auch Frankreichs Kartesianismus eine Rolle. Rationalität, kritisches Denken und gesunde Skepsis sind Bestandteile der französischen DNA und werden bereits in der Grundschule gefördert. Natürlich ist der Skeptizismus ein zweischneidiges Schwert, da dieser auch von den sogenannten „alternativen" Medien gepriesen wird. Hier muss jedoch klar zwischen gesunder und ungesunder Skepsis unterschieden werden. Letztere basiert auf Desinformation und Verschwörungsszenarien und kommt einem pawlowschen Reflex gleich, bei dem jeder „offiziellen" Nachricht mit Misstrauen begegnet wird. Die gesunde Skepsis läuft derweil eher auf den rationalen Reflex hinaus, an allem zu zweifeln, was nicht bewiesen werden kann.

Der Faktor Glück

Das Scheitern der Desinformationskampagne gegen Macron ist allerdings auch auf eine Portion Glück zurückzuführen. Der Angriff war schlecht vorbereitet, wohl vor allem, weil die Drahtzieher nicht erwartet hatten, dass Macron sich in der ersten Wahlrunde durchsetzen würde.
So fehlte die Zeit, Material aufzutreiben. Zudem war Macron wohl auch einfach „zu jung, um schmutzig zu sein", wie der Internet-Sicherheitsforscher Thaddeus T. Grugq formuliert hat. Aufgrund seiner kurzen politischen Karriere ließ sich nicht viel „Dreck" über ihn ausgraben: „Für einen Geheimdienst unter Zeitdruck ist das ein Alptraumszenario. Die Hacker … hatten keine Zeit, irgendwelche dunklen Geheimnisse zu entdecken oder einen Skandal zu fabrizieren."-

Die Tatsache, dass ein Leak von mehr als 21 000 E-Mails keine belastenden oder verdächtigen Informationen ans Tageslicht brachte, wurde für Macron sogar zu einem Vorteil im Wettstreit mit Le Pen, die sich trotz eines unversehrten E-Mail-Servers ihrerseits mit allerlei juristischen Schwierigkeiten konfrontiert sah. Den Hackern blieb nichts anderes übrig, als E-Mails zu fälschen. Diese Fälschungen entpuppten sich jedoch schnell als so absurd, dass sie die gesamten „Macron-Leaks" unglaubwürdig zu machen drohten.

Schließlich mangelte es den Drahtziehern an kulturellem Feingefühl. So versuchten sie etwa das Gerücht zu verbreiten, dass Macron schwul sei. Sie hätten jedoch wissen müssen, dass eine solche Enthüllung in Frankreich, wo das Privatleben von Politikern weitaus weniger wichtig ist als etwa in den Vereinigten Staaten, kaum für einen Skandal taugt. Darüber hinaus prallte die Desinformationskampagne zu einem großen Teil an der Sprachbarriere ab: Da viele Informationen nur auf Englisch geteilt wurden, erreichten sie die französische Wählerschaft in nur unzureichendem Maße. Nationalistisch eingestellte Wähler, die oft antiamerikanische Ressentiments hegen, wären für Nachrichten in französischer Sprache sicherlich empfänglicher gewesen.

15 Lektionen

Folgende Lehren lassen sich aus den „Macron-Leaks" ziehen, sowohl in Sachen Antizipation wie Reaktion.

1. ***Von anderen lernen.*** Frankreich hatte den Vorteil, selbst Präzedenzfälle miterlebt und aus den Vorfällen rund um die US-Präsidentschaftswahlen 2016 gelernt zu haben. Dies trug dazu bei, dass das Bewusstsein für die Bedrohung innerhalb der französischen Behörden geschärft war und diese eng mit US-Behörden zusammenarbeiteten.
2. ***Die richtigen Verwaltungstools verwenden.*** Selbst als offensichtlich wurde, dass es 2016 Versuche der Wahlbeeinflussung und Cyberangriffe auf die USA gab, unternahm die Obama-Regierung aus Angst vor Vorwürfen der Parteinahme (und aufgrund der Annahme, dass Clinton die Wahl trotzdem gewinnen würde) nichts, um diese zu stoppen. Das französische Beispiel zeigt jedoch, dass unabhängige Behörden wie der Verfassungsrat, die Commission nationale de contrôle de la campagne électorale (CNCCEP) und die Agence nationale de la sécurité des systèmes d'information (ANSSI) zusammenarbeiten können, um Fachwissen bereitzustellen und die Wahlen vor Fremdeinmischung zu schützen.
3. ***Bewusstsein schaffen.*** Die genannten Organisationen, ANSSI und CNCCEP, spielten auch eine Schlüsselrolle dabei, die politischen Parteien vor Cyberangriffen zu warnen und sie bei der Aufdeckung verdächtiger Aktivitäten zu unterstützen. Es gab zudem auch von Medienseite große Anstrengungen, der Desinformationskampagne entgegenzuwirken, etwa durch vermehrte Faktenchecks.
4. ***Entschlossenheit demonstrieren.*** Die Regierung brachte während des gesamten Präsidentschaftswahlkampfs deutlich zum Ausdruck, dass Frankreich keine Einmischung in seine Wahlen dulden würde und stellte klar, dass man

entschieden auf Versuche der Einflussnahme reagieren würde.

5. *(Technische) Vorsichtsmaßnahmen treffen.* Wegen des „extrem hohen Risikos" von Cyberangriffen kündigte die französische Regierung das Ende der elektronischen Stimmabgabe für Bürger im Ausland an.
6. *Druck auf digitale Plattformen ausüben.* In Reaktion auf Forderungen aus der Politik und der Zivilgesellschaft sperrte Facebook in Frankreich in einer einmaligen Aktion rund 70 000 gefälschte Konten.
7. *Hacking-Versuche öffentlich machen.* Emmanuel Macrons Partei En Marche! teilte offen mit, nicht ausreichend gegen Cyberattacken geschützt zu sein und machte den genauen Zeitpunkt der Angriffe später auch öffentlich. Mit dieser Transparenz wurde das Bewusstsein für das Thema geschärft.
8. *Die Kontrolle über geleakte Informationen zurückgewinnen.* Um Hackerangriffen vorzubeugen, fluteten Macrons Mitarbeiter ihre E-Mail-Konten mit eigens gefälschten E-Mails, um die Glaubwürdigkeit des späteren Leaks zu beschädigen.
9. *Konzentriert bleiben und zurückschlagen.* Macrons Team konzentrierte sich zu jeder Zeit auf die politische Arbeit, reagierte jedoch auch schnell auf Posts und Kommentare, die im Internet falsche Informationen verbreiteten.
10. *Humor hilft.* In bestimmten Situationen setzte die Kampagne auf Humor und Ironie, um die Sichtbarkeit ihrer eigenen Kommentare auf Online-Plattformen zu erhöhen.
11. *Die Behörden alarmieren.* Die Staatsanwaltschaft in Paris leitete innerhalb weniger Stunden nach Bekanntwerden des Leaks eine Untersuchung ein.
12. *Propaganda beschränken* Das Team Macrons verweigerte sowohl RT als auch Sputnik die Akkreditierung und hinderte sie so daran, effektiv über die letzten Tage des Wahlkampfs zu berichten. Man begründete die Entscheidung damit, dass es sich bei den Kanälen nicht um faire Medien, sondern um propagandistische Organisationen handele.
13. *Leaks trivialisieren.* Da die durchgesickerten Dokumente keine illegalen Machenschaften oder Skandale enthüllten, halfen sie Macron sogar, sein Image als „sauberer" und „skandalfreier" Kandidat zu schärfen.
14. *Auf verschiedenen Kanälen kommunizieren.* Ein Grund dafür, dass die „Macron-Leaks" nicht viel Neues ans Tageslicht brachten, war der Tatsache geschuldet, dass sich Macrons Team auf Hackerangriffe vorbereitet hatte. Vertrauliche Informationen wurden über verschlüsselte Kanäle weitergegeben oder persönlich besprochen, wobei E-Mails meist nur für triviale und logistische Angelegenheiten genutzt wurden.
15. *Auf verantwortungsvolles Verhalten der Medien setzen.* Der Aufruf der CNCCEP, nicht über den Fall zu berichten und der sich schnell in den sozialen Medien verbreitenden Propagandakampagne keine Plattform zu geben, wurde von den französischen Medien weitestgehend befolgt.

Zusätzlich zu den französischen Anstrengungen, sich gegen die Propa-

ganda zur Wehr zu setzen, formte sich schnell eine internationale Allianz, die versuchte, die Geschehnisse zu analysieren und die Drahtzieher zu ermitteln.

Dabei sollte man sich für die Zukunft merken, dass man einer Desinformationskampagne am effektivsten gegenübertritt, indem man – in den Worten des britischen Autors Ben Nimmo – schnellstmöglich der Devise „Whodunit?“ folgt, also der Frage nach den Tätern nachgeht. Faktenchecks allein reichen nicht, denn aus Informationskriegen ist längst eine Art „Krieg der Narrative“ geworden nach dem Motto: „Wir haben die Fakten, aber sie haben die Geschichten.“

Es gilt also mehr denn je, Gegenerzählungen zu entwerfen und falsche Narrative zu entlarven. Um Einmischungen in Wahlen künftig zu verhindern, brauchen wir nicht nur nationale Strategien, die auf den bereits genannten Lektionen basieren, sondern auch internationale Initiativen, die die Zivilgesellschaft dazu ermutigen, das Internet nach Trollen, Bots und anderen Desinformationsagenten zu durchforsten und ihre Identitäten, Methoden und Netzwerke aufzudecken.

Kein Grund zur Entwarnung

Unter keinen Umständen darf sich Frankreich nun auf seinen Lorbeeren ausruhen. Das hat drei Gründe: Erstens handelte es sich bei den „Macron-Leaks“ um eine Fremdeinmischung in eine nationale Wahl, also um eine ganz besondere Art der Informationsmanipulation. Wer glaubt, ähnliche Angriffe würden nur alle paar Jahre auftreten, der irrt. Cyberattacken sind mittlerweile eine permanente Gefahr, weswegen Gegenmaßnahmen sich nicht nur auf Wahlkampfzeiten beschränken sollten. Jüngste Beispiele für Desinformationskampagnen, bei denen sich Angreifer zum Beispiel die Gelbwesten-Bewegung zunutze machten, sollten Warnung genug sein, dass Frankreichs Feinde jede Gelegenheit nutzen werden, Zweifel und Verwirrung zu säen.

Zweitens stand Macron der rechtsextremen Kandidatin Le Pen gegenüber, die (noch immer) keinen allzu großen Rückhalt bei den Wählerinnen und Wählern hat. Macrons Vorsprung in Umfragen betrug konstant zwischen 20 und 25 Prozentpunkten, und dementsprechend klar fiel auch sein Sieg aus. Doch die politische Landschaft in Frankreich verändert sich weiter, und es wäre ein Fehler, sich allzu viel auf die Erfolge der Vergangenheit einzubilden.

Frankreich sollte sich nicht auf seinen Lorbeeren ausruhen

Drittens wird die Bedrohung in Zukunft nicht kleiner. Auch Frankreichs Gegner werden aus ihren Fehlern lernen. Sie werden ihre Methoden anpassen, verbessern und professionalisieren. Allein aufgrund technologischer Entwicklungen, etwa durch KI-Systeme, wird die Informationsmanipulation bald noch raffinierter vonstatten gehen. Es gilt, sich zu wappnen.

Dr. Jean-Baptiste Jeangène Vilmer
leitet das Institut de Recherche Stratégique de l’Ecole Militaire.