

Baerbocks Digitaldetektive decken russische Lügenkampagne auf

Ein Trommelfeuer der Desinformation: Spezialisten des Auswärtigen Amts haben auf Elon Musks Kurznachrichtenplattform X eine systematische russische Kampagne ausgemacht. In der Bundesregierung wächst die Sorge vor Wahlbeeinflussung.

Von Marcel Rosenbach und Christoph Schult

26.01.2024, 06.18 Uhr

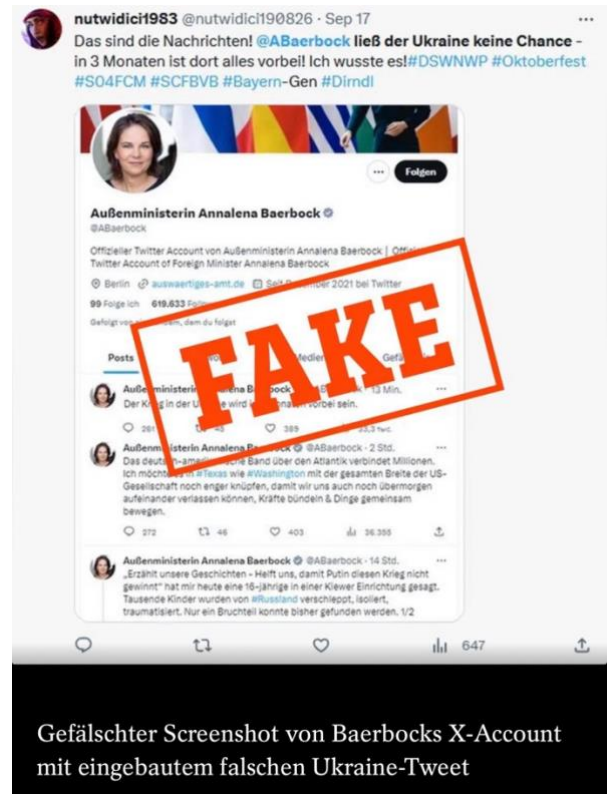
Im September verbreitete sich auf dem Kurznachrichtendienst X eine erstaunliche Prophezeiung der deutschen Außenministerin: »Der Krieg in der Ukraine wird in 3 Monaten vorbei sein« – so lautete die Botschaft von Annalena Baerbock. Angeblich.

Auf den ersten Blick wirkte alles echt: das Profilfoto der Ministerin, die Zahl der Follower, ihr bekanntes Nutzerkonto unter @ABaerbock. 389 Nutzern gefiel die Nachricht, 45 verbreiteten sie weiter, 261 andere Nutzerinnen und Nutzer antworteten auf die Botschaft, die vermeintlich nahelegte, dass Deutschlands Unterstützung für die Ukraine bröckele. Doch es handelte sich um eine gefälschte Nachricht.

Um die Fotomontage zu erkennen, musste man sehr genau hinsehen. Die Fälscher hatten einen Fehler gemacht, ganz klein unten am Rand des Eintrags fand sich ein merkwürdiges Zeichen. Es war kyrillisch – und damit ein Hinweis auf die Urheber der Manipulation. Sie kamen aus Russland. Oder meinten es gut mit Russland. Und sie beließen es nicht bei dem gefälschten Post.

Der falsche Tweet wurde von gefälschten Accounts weiterverbreitet, mitsamt den passenden Kommentaren: »Das sind die Nachrichten! @ABaerbock ließ der Ukraine keine Chance«. Versehen waren die Retweets mit Hashtags, die keinerlei politischen Bezug hatten, aber im September gerade populär waren: #Oktoberfest beispielsweise oder #Dirndl. Verwendet wurden auch beliebte Hashtags zu Bundesligaspielen – ein Trick, um die Reichweite zu erhöhen.

Der gefälschte Tweet ist Teil einer prorussischen Desinformationskampagne, die Baerbocks Ministerium aufgedeckt hat. Dem SPIEGEL liegt die vertrauliche Analyse in Auszügen vor. Die Experten haben im Auftrag des Referats 607 für Strategische Kommunikation im Auswärtigen Amt vom 20. Dezember bis 20. Januar mit einer



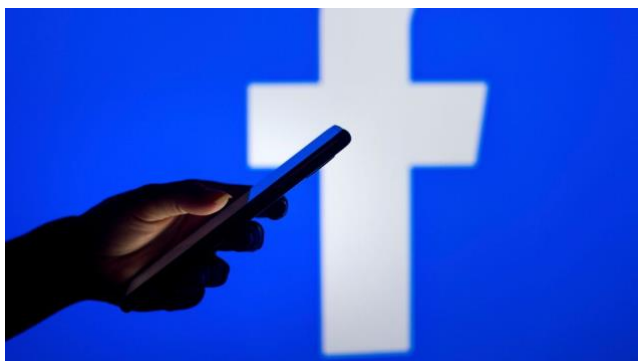
speziellen Software Elons Musks Kurznachrichtendienst X ausgewertet – mit erschreckenden Ergebnissen.

In den vier Wochen rund um den Jahreswechsel identifizierten sie mehr als 50.000 gefälschte Nutzerkonten, die in deutscher Sprache offenbar koordiniert Stimmungsmache betrieben, mit insgesamt mehr als einer Million deutschsprachiger Tweets. An manchen Tagen registrierten die Experten des Auswärtigen Amts 200.000 dieser Kurznachrichten. Das entspricht ungefähr zwei Mitteilungen pro Sekunde – ein digitales Trommelfeuer, um die Öffentlichkeit zu manipulieren.

Besonders häufig tauchte in den Nachrichten der Vorwurf auf, die Bundesregierung vernachlässige die eigene Bevölkerung, um die Ukraine zu unterstützen. »Ich finde es enttäuschend, dass die Regierung mehr für andere Länder tut als für die eigenen Bürger«, heißt es in einem der meistverbreiteten Tweets. Ein anderer lautete: »Es ist eine Schande, dass die Ampel-Koalition die Probleme im eigenen Land nicht zuerst angeht.« Den Angreifern geht es offenbar darum, an Stimmungen in der Bevölkerung anzuknüpfen, sie zu verbreiten und zu befördern, sie größer erscheinen zu lassen, als sie sind. Das Ziel der gesteuerten Informationsoperation: Wut zu schüren, Stimmung zu machen, das Vertrauen in Regierung, Demokratie und Medien zu untergraben. Einer der Hauptangriffspunkte ist jedwede deutsche Hilfe für die Ukraine. Die Strategie ist alt, Geheimdienste haben sie seit jeher angewandt. Doch nie waren die technischen Voraussetzungen dafür besser als heute. Ein Knopfdruck, und gefälschte Nachrichten sind überall auf der Welt zu lesen.

Schon die Themenauswahl der Fälscher lenkte den Verdacht nach Russland, forensische Analysen bestätigten das. Dem internen Report zufolge bewerten die Experten des Auswärtigen Amts die jüngste Welle als Teil einer groß angelegten russischen Kampagne, die 2022 erstmals unter dem Namen »Doppelgänger« bekannt wurde.

Schon damals befand sich Deutschland im Visier der Angreifer, neben Frankreich, Großbritannien, Italien und der Ukraine. Der Facebook-Mutterkonzern Meta sprach von der bislang »größten und hartnäckigsten« russischen Onlineoperation und sperrte zahlreiche beteiligte Konten:



Für eine Kampagne auf Facebook haben Trolle Fake-Seiten etablierter Medien nachgebaut, auch vom SPIEGEL. Die Inhalte sind abenteuerlich – allerdings auch gespickt mit Rechtschreibfehlern. Auf Facebook und Twitter kursierten seit Mitte letzten Jahres Links zu gefälschten deutschen Nachrichtenseiten, die

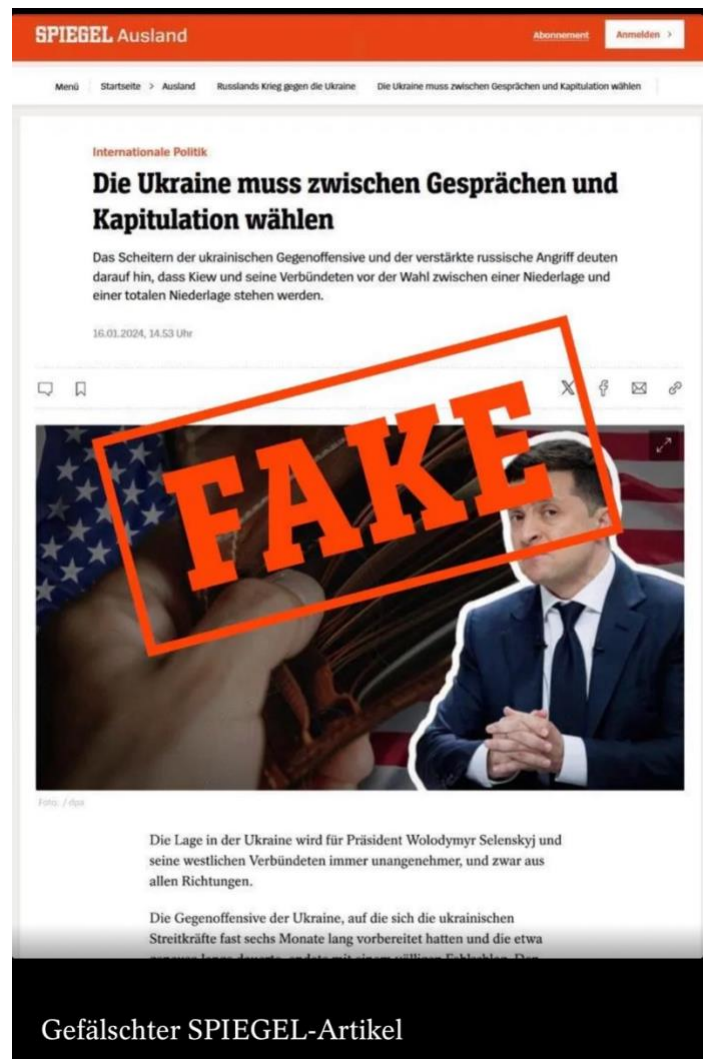
prorussische Propaganda verbreiten. Das geht aus einem Bericht des Nachrichtenportals »t-online« hervor. Die gefälschten Websites imitierten die Angebote von etablierten Medien wie »FAZ«, »Tagesspiegel«, »Bild«, »t-online« und auch des SPIEGEL. Die Beiträge wurden Facebook-Nutzern mindestens seit Juli als gesponserte Posts im Newsfeed angezeigt oder wurden im Kommentarbereich anderer Seiten veröffentlicht.

»T-online« berichtet von insgesamt 30 verschiedenen Fake-URLs zu Websites, die sich als deutsche Medien ausgeben. Verbreitet wurden die Links zu den Seiten demnach von hunderten sogenannten Sockenpuppen-Accounts. Diese Accounts sind offenbar massenhaft und softwaregestützt generiert worden. Im Falle der aktuellen Kampagne hatten die Accounts bei Namen, Beruf und Profilfotos viele Gemeinsamkeiten, die echte Personen sonst nicht haben.

Obwohl die Artikel exakt an das Layout existierender Nachrichtenwebsites angepasst wurden, sind die Fälschungen der etablierten Medien inhaltlich plump bis sehr plump: Sprachlich ist oft auf den ersten Blick erkennbar, dass die Verfasser der Artikel nicht besonders gut Deutsch können. Klobige Sätze, ungewöhnliche Formulierungen und manchmal sogar kyrillische Worte in den gefälschten Artikeln lassen die Artikel neben ihrer eindeutigen Stimmungsmache herausstechen.

Ein Video behauptet etwa, »Frau Berbock« habe die Grünen verraten, »um eine atomare Apokalypse vorzubereiten«. Eine Fake-FAZ stellt fest: »Viele Dinge kosten heute erheblich teurer als früher«. Unter einem gefälschten »t-online«-Video haben die Autoren vergessen, das russische Wort für »Unterschrift« zu löschen. All diese Beiträge sind inhaltlich falsch.

Die EU sanktionierte im vergangenen Sommer zwei russische IT-Dienstleistungsfirmen, Structura National Technologies und Social Design Agency, wegen ihrer Beteiligung an der Kampagne. Nach Erkenntnissen von US-Behörden sollen die beiden Unternehmen zudem für eine vergleichbare russische Desinformationskampagne in Lateinamerika verantwortlich sein.



Im Auswärtigen Amt sorgen die Ergebnisse der Forensiker für Aufregung, schließlich stehen in diesem Jahr nicht nur Europawahlen an, sondern auch Landtagswahlen in drei ostdeutschen Bundesländern. Die Sorge ist groß, dass Russland erneut in Wahlkämpfe eingreifen könnte.

Baerbocks Ministerium hat seine Erkenntnisse bereits mit dem EU-Kompetenzzentrum »EU vs Disinfo« geteilt – auch um sie von den Brüsseler Experten überprüfen und verifizieren zu lassen. Die Bundesregierung hatte kurz nach Beginn des Ukrainekriegs zudem eine ressortübergreifende Arbeitsgruppe beauftragt (»AG Hybrid«), verdeckte Kriegsführung Russlands aufzudecken. Auch dort dürften die Befunde demnächst Thema sein. Was Baerbocks Leute besonders umtreibt: Einiges deutet darauf hin, dass ein großer Teil der Kampagne inzwischen automatisiert funktioniert. In einer exemplarischen Detailanalyse von 4000 der identifizierten, offenbar aus Russland gesteuerten Nutzerkonten weisen die Experten nach, dass diese am 29. Dezember von Mitternacht an zeitgleich und im gleichen Takt deutschsprachige Inhalte posteten, offenbar algorithmisch gesteuert. Der Fund nährt die Befürchtung, dass digitale Desinformationskampagnen durch künstliche Intelligenz noch befeuert werden könnten.

Um die Einflussnahme authentisch erscheinen zu lassen, missbrauchen die Angreifer die Namen von bekannten Medienmarken, deren Webseiten sie nachahmen, um im gewohnten Layout ihre Falschnachrichten zu platzieren – daher der Kampagnenname Doppelgänger. Die Fake-Accounts posten neben ihren spalterischen Botschaften vermeintliche Links auf bekannte Nachrichtenmedien, neben dem SPIEGEL die »Welt« und die »Süddeutsche Zeitung«. Die Links führen zu Seiten, die auf den ersten Blick wie die Originalportale dieser Medien aussehen, tatsächlich aber Nachahmerseiten sind, die von den Angreifern gesteuert werden.

Zu erkennen sind die Fälschungen an falschen Domain-Bezeichnungen, beim SPIEGEL etwa .ltd statt .de. Dort platzieren die Angreifer ihre manipulativen Inhalte, teilweise unter den Namen realer Journalistinnen und Journalisten der betreffenden Medien. Es könne angeblich bald zu einer »sozialen Explosion« in Deutschland kommen, hieß es etwa in einem Beitrag auf einer gefälschten Seite der »Welt« (unter welt.pm). Der »Süddeutschen« wurde die Nachricht untergeschoben, der Krieg für die Ukraine sei »eindeutig verloren«.

Die falschen Nachrichtenseiten werden aus dem identifizierten Netzwerk dann fleißig weiterverbreitet. So zeigt die Auswertung, dass ein falscher SPIEGEL-Beitrag am Abend des 19. Januar in wenigen Stunden mehr als 3700-mal retweetet wurde – jeweils mit leicht variierten Kurzkomentaren, die alle einen gemeinsamen Nenner haben: Wut auf die Ampelregierung. Gemeinsam ist ihnen auch die Aufforderung: »Lest hier mehr davon!« – vor dem Link auf den angeblichen SPIEGEL-Artikel.

Die Angreifer nutzen zudem einen sogenannten Link-Shortener – das heißt, die falsche SPIEGEL-Netzadresse ist im Tweet nicht zu erkennen.

Das Verfahren ist aus früheren Doppelgänger-Angriffswellen bekannt und wird international eingesetzt, etwa mit Fake-Seiten der britischen »Daily Mail«, des »Guardian«, französischer Blätter und italienischer Nachrichtenagenturen. Teils imitieren die Angreifer auch die Webseiten von Ministerien und Behörden, wie der SPIEGEL im vorigen Juni enthüllte: Auf einer angeblichen Seite des Bundesinnenministeriums mit der falschen Domain-Endung .pe hieß es etwa, es sei wichtig, geflohene Ukrainer gleichmäßig auf deutsche Haushalte zu verteilen.

Die Macher aus Russland setzen eher auf Masse als auf Klasse. Die Operation ist weder besonders subtil, noch sind die Beiträge gut gemacht. Es gibt viele Fehler wie das kyrillische Zeichen im vermeintlichen Baerbock-Tweet. Accounts mit Nutzernamen wie »Gerhard Weiß« zeigen als Profilbild junge Frauen. Die Fotos für die Profile sind offenbar aus dem Netz zusammengesucht, manchmal teilen sich mehrere Profile dasselbe Foto.

Das Deutsch mancher Texte ist eher holprig und fehlerhaft: »Sozialleistungen brachen die Ampel«, so ist ein angeblicher SPIEGEL-Text betitelt. Und an Wochenenden machen die Spammer regelmäßig Pause, auch an russischen Feiertagen sind sie nicht aktiv. Eine Stichprobe ergab, dass Mitte Januar noch zahlreiche Konten des vom Auswärtigen Amt erkannten Netzwerks aktiv waren, einige eingeschränkt, andere gelöscht oder gesperrt.

Wie wirksam die russischen Kampagnen sind, ob sie die Stimmung im Land nachhaltig beeinflussen können, ist schwer zu messen. Die russischen Machthaber scheinen sie für effektiv genug zu halten, um sie seit Jahren zu finanzieren und trotz aller Enthüllungen und Sanktionen weiterzubetreiben.

Russland ist nicht das einzige Land, das auf digitalem Weg versucht, die Öffentlichkeit zu manipulieren. Der SPIEGEL enthüllte im vorigen Jahr zusammen mit der Organisation Forbidden Stories die Aktivitäten der israelischen Cybersöldner von Team Jorge . Sie vermarkten ein Programm namens AIMS (etwa: Fortgeschrittenes Medienmanipulationswerkzeug), mit dem sich automatisiert falsche Avatare für verschiedene Netzwerke erstellen lassen, über die dann Kampagnen gefahren werden können – rund 20 AIMS-gesteuerte Kampagnen in verschiedenen Ländern ließen sich in der Recherche nachvollziehen.

Das Auswärtige Amt beobachtet seit geraumer Zeit mit mehreren Datenanalysten Debatten zu außenpolitischen Themen in den sozialen Medien. Ziel ist es, Versuche von Einflussnahme ausländischer Akteure aufzudecken. »Desinformation ist zu einem globalen Bedrohungsfaktor geworden«, sagte ein Sprecher des Auswärtigen Amts auf Anfrage. »Sie wird von denjenigen, die unsere Werte nicht teilen, gezielt eingesetzt, um ganze Gesellschaften zu destabilisieren – nicht nur in westlichen Demokratien, sondern

überall.« Dies zu beobachten gehöre genauso zu einer modernen Außenpolitik wie digitale Visaverfahren. »Hier haben auch die Plattformen für soziale Medien eine riesige Verantwortung.«

Neben Russland als mutmaßlichem Urheber der aktuellen Kampagne sieht auch X schlecht aus. Eigentümer Elon Musk hat angekündigt, entschieden gegen das Bot-Problem vorzugehen – stattdessen können offenkundig die Urheber Zehntausender Fake-Konten auf der Plattform weiter tun, was sie wollen.

»Aus den Handlungen Elon Musks lässt sich immer wieder ablesen, dass Plattformintegrität für ihn keine Priorität darstellt«, sagt Lea Frühwirth vom Center für Monitoring, Analyse und Strategie, das solche Kampagnen analysiert. »Nachdem X unter Elon Musk Schutzmechanismen gegen hasserfüllte und irreführende Inhalte systematisch abgebaut hat, kann der Anstieg solchen Contents nur als erwartbare logische Konsequenz betrachtet werden«, so die Desinformationsexpertin. »Russische Einflusskampagnen wie Doppelgänger zielen darauf, liberale Gesellschaften zu schwächen. Sie säen Misstrauen gegenüber demokratischen Institutionen, machen Qualitätsmedien verächtlich und stören so die informierte politische Meinungsbildung.«

Aus Brüssel droht Musk nun Ärger – seit November gilt das neue EU-Gesetz über digitale Dienste. X könnte der erste große Anwendungsfall werden. Vergangenen Monat leitete der Binnenmarktkommissar Thierry Breton das Verfahren gegen den Dienst ein. Grund war eine Welle falscher oder irreführender Informationen über den Terrorangriff auf Israel.

Auf eine SPIEGEL-Anfrage an X zu den neuen Vorwürfen kam eine automatische E-Mail zurück: »Wir sind beschäftigt, versuchen Sie es später noch einmal.«

Link: <https://www.spiegel.de/politik/deutschland/desinformation-aus-russland-auswaertiges-amt-deckt-pro-russische-kampagne-auf-a-765bb30e-8f76-4606-b7ab-8fb9287a6948>

Aufgaben:

- 1) Arbeiten Sie aus dem Artikel heraus,
 - a. wie und wofür digitale Medien missbraucht werden können.
 - b. warum und von wem dieser Missbrauch geschieht.
- 2) Diskutieren Sie, inwiefern soziale und/ oder digitale Medien noch Ihrer Funktion als „vierte Gewalt“ gerecht werden können.
 - a. Arbeiten Sie dazu zunächst heraus, wie die BRD als Staat und wie die einzelnen Staatsbürger sich schützen können.
 - b. Erklären Sie dann, welche Funktionen diese Medien noch/ nicht mehr erfüllen können.