RUSSISCHE DESINFORMATION

Russische Propaganda und Fakes – dank Technik aus Europa

Es ist eine der größten Desinformations-Kampagnen in der EU – gesteuert aus Russland: die sogenannte Doppelgänger-Kampagne. Wir haben sie durchleuchtet und sind auf Beteiligte in Deutschland gestoßen. Merkwürdig, dass noch keine Ermittlungsbehörden dort waren.

von **Max Bernhard**, **Alexej Hock**, **Sarah Thust**

11. Juli 2024

Über das Internet erreicht die russische Desinformations-Kampagne „Doppelgänger“ Menschen auf der gesamten Welt. CORRECTIV deckt die dafür nötige IT-Infrastruktur auf.

0:00 / 24:46

Audioversion der Recherche, Stand 11. Juli 2024, 6 Uhr

Read the English version of this article here.

Die Ampel will sich nicht um die Alten kümmern. So lautet die Überschrift eines *Spiegel*-Artikels der letzten Tage. Es gebe in Deutschland eine wachsende Zahl älterer Menschen, für die die Pflege zu teuer sei, „doch die Regierung ignoriert das Problem“.

Mehr von CORRECTIV

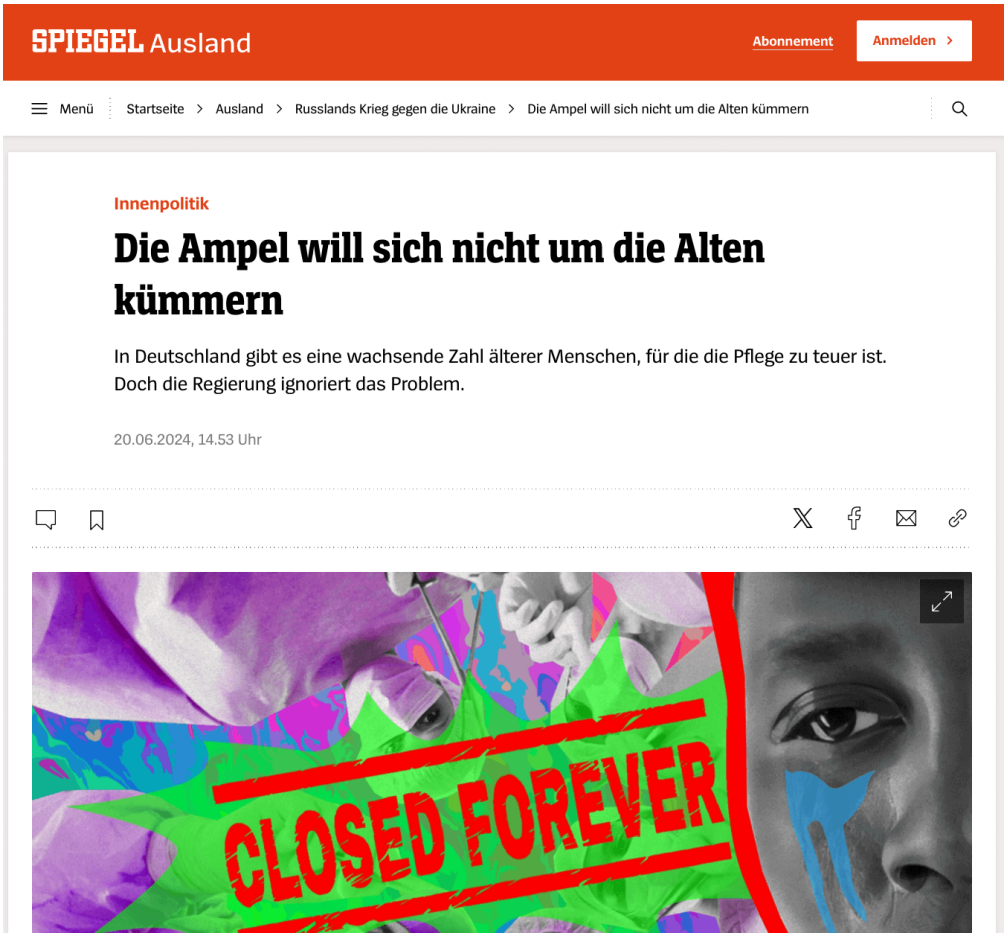
Russische Propaganda: Bundesregierung ignoriert Hinweise auf Spuren in Deutschland

Hacks und Propaganda: Zwei Brüder aus Moldau tragen Russlands digitalen Krieg nach Europa

Post aus Russland: Desinfo-Kampagne nimmt CORRECTIV und andere Faktencheck-Redaktionen ins Visier

Vielleicht landen Sie über einen Link auf den Plattformen X oder Facebook auf dem Artikel und meinen, etwas über die deutsche Politik erfahren zu haben. Vielleicht lesen Sie nur die Überschrift und klicken weg. Vielleicht lesen Sie den Text zu Ende und finden dort die Behauptung, dass Gelder für Renten und Sozialausgaben eingefroren wurden, um die Waffenlieferungen in die Ukraine zu ermöglichen. Womöglich regen Sie sich auf oder stimmen zu.

Vor allem jedoch wurden Sie getäuscht. Diesen *Spiegel*-Artikel hat es nie gegeben. Sie sind auf einer ziemlich guten Nachbildung der Nachrichtenseite gelandet. Sie ist Teil einer aufwändigen russischen Desinformationskampagne und zielt auf Bürgerinnen und Bürger Deutschlands, Frankreichs und anderer Länder. Sie soll Verunsicherung erzeugen und Stimmung gegen die Ukraine schüren. Nicht nur der *Spiegel*, auch viele andere deutsche und ausländische Medien wie der britische *Guardian* sind betroffen. Wegen solcher Nachrichtenseiten-Klone spricht man in Fachkreisen von der „Doppelgänger“-Kampagne.



Dieser Spiegel-Artikel ist eine von etlichen Fälschungen, die die Doppelgänger-Kampagne seit 2022 verbreitet (Quelle: spiegel.ltd; Screenshot: CORRECTIV)

Obwohl die gefälschten Webseiten schon seit zwei Jahren im Umlauf

weder europäische Ermittlungsbehörden noch die Plattformen Facebook und X, auf denen die Desinformation stattfindet. Warum ist es so kompliziert, den Meinungsmanipulatoren das Handwerk zu legen?

Dieser Frage ist CORRECTIV nachgegangen. Wir haben die gesamte Kette der Desinformationsmaschine nachverfolgt. Grundlage der Recherche ist eine Analyse der schwedischen NGO Qurium, spezialisiert auf digitale Forensik. Sie hat den Weg nachverfolgt, den Ihr Internetbrowser geht, wenn Sie auf einen solchen Link einer vermeintlichen Nachrichtenseite klicken.

Unsere Recherche zeigt, dass Firmen aus Europa in diese technische Infrastruktur involviert sind. Eine von ihnen sitzt in Frankfurt. Das Ergebnis wirft die Frage auf, wie ernsthaft europäische Behörden den Kampf gegen Desinformation führen.

Die wichtigsten Begriffe dieser Recherche

Eigentlich sind Internetseiten über eine Zahlenfolge, die sogenannte **IP-Adresse** erreichbar. Die für CORRECTIV lautet zum Beispiel 5.9.10.83. Damit sich Menschen diese Zahlen nicht merken müssen, gibt es **Domains**. Wenn Sie im Webbrowser die Domain www.correctiv.org eingeben, liefern sogenannte Nameserver, ähnlich wie ein Telefonbuch, die dazugehörige IP-Adresse, die dann angewählt wird. Mehrere Domains können aber zum Beispiel auch auf dieselbe IP verweisen.

Webhosting oder auch einfach **Hosting** ist das Anbieten von Speicherplatz auf einem Server. Die wichtigste Dienstleistung eines Hosters ist die Unterbringung von Webseiten und zugehörigen Dateien. Hosting ist englisch und heißt so viel wie „Gastgeber sein“.

Server sind Computer, die Daten oder Programme speichern und an ein

sie zugreifen und Informationen abholen. Beispielsweise werden Internetseiten auf Servern gespeichert und von Nutzerinnen und Nutzern über das Internet aufgerufen. Über Server können allerdings auch Attacken laufen und koordiniert werden.

VPS steht für **v**irtuelle **p**rivate **S**erver. Die Ressourcen eines Servers, der über mehr Leistung und Speicher verfügt als für viele Kunden nötig ist, werden von Hosting-Firmen manchmal in mehrere virtuelle Server aufgeteilt.

Ein Rechen- oder **Datenzentrum** ist ein Ort, an dem Server und andere Datenverarbeitungsgeräte untergebracht sind. Diese können privat oder gemeinsam genutzt werden. Wenn das Zentrum einer Betreiberfirma gehört und die physische Infrastruktur weiteren Firmen gegen Gebühr zur Verfügung stellt, spricht man von Colocation. Oftmals handelt es sich bei den Kunden um kleinere Firmen, die sich die teure Wartung nicht leisten können.

Hybride Kriegsführung bezeichnet in modernen Konflikten die Vermischung verschiedener Methoden zur Erreichung der eigenen Ziele. Neben klassischen Militäreinsätzen können dazu etwa Propaganda, Hacker-Attacken oder wirtschaftlicher Druck zählen.

Kapitel 1: Die Anfänge

(Collage: Ivo Mayr / CORRECTIV)

Moskau, Sommer 2022. Angestellte der PR-Agentur Social Design Agency entwerfen Strategien für die massenhafte Verbreitung von Inhalten über soziale Netzwerke – möglichst effektiv, möglichst nicht rückverfolgbar. Es sind Skizzen für eine Desinformationskampagne, die sich im Laufe der folgenden Monate immer wieder anpasst. Unbekannt ist, ob es ein direkter Auftrag war, doch die Papiere wandern in den Kreml.

Im April berichtete die *Washington Post* über ein Leak aus der russischen Machtzentrale, der ihr von einem westlichen Nachrichtendienst übergeben worden war. Darin befinden sich auch die Ausarbeitungen der Social Design Agency. Ein Vorschlag lautet, man könne für die Verbreitung von Inhalten „kurzlebige“ Accounts nutzen, um nicht aufzufallen. Die Dokumente, die zwischen Mai 2022 und August 2023 entstanden, finden offenbar Anklang im Kreml. In dieser Zeit, wenige Monate nach dem russischen Einmarsch in die Ukraine, nimmt die Doppelgänger-Kampagne an Fahrt auf.

Mittels künstlicher Accounts werden seitdem automatisiert Links auf Facebook und X gestreut. Sie führen entweder zu eigenen Nachrichtenportalen wie „Reliable Recent News“, das unter anderem deutschsprachige Artikel veröffentlicht. Oder aber sie führen zu Nachbauten etablierter Medien wie *Le Monde*, *Washington Post* oder *Spiegel* – und auch Regierungswebseiten wurden schon kopiert. Häufig geht es um die Ukraine, die in ein schlechtes Licht gerückt wird. Aber es geht auch um innenpolitische Themen. Nicht alles ist

Links zu dem gefälschten Spiegel-Artikel wurden von Doppelgänger über künstliche Accounts auf X gestreut (Screenshots und Collage: CORRECTIV)

Die EU und die USA haben die Social Design Agency und eine weitere russische Firma namens Struktura wegen ihrer Beteiligung an der Kampagne sanktioniert. Das heißt, europäische und amerikanische Firmen dürfen ihnen eigentlich keine Leistungen erbringen oder Ressourcen zur Verfügung stellen – weder direkt noch indirekt. Vor kurzem hat die NGO Institute for Strategic Dialogue Hinweise auf die Beteiligung einer weiteren Moskauer Marketing-Firma namens Argon Labs gefunden. Wahrscheinlich gibt es noch mehr Unternehmen, die an der vielschichtigen Kampagne arbeiten.

Diese Firmen entwerfen mutmaßlich die Konzepte, arbeiten Ideen und Themen aus und verbreiten die Resultate wie den gefälschten *Spiegel*-Artikel im Netz. Dass die Kampagne jedoch technisch funktioniert, dafür sind eine Reihe von Firmen verantwortlich, über die bislang kaum berichtet wurde. Sie sorgen dafür, dass zum

Ukraine, die auf Kosten deutscher Rentner gehen sollen, im Internet abrufbar bleibt und sein Zielpublikum erreicht. Die Spur dieser Firmen führt zuallererst in die britische Hauptstadt.

Kapitel 2: The Evil Empire

(Collage: Ivo Mayr / CORRECTIV)

London, Sommer 2023. Das Fergusson House ist ein fünfstöckiges Gebäude aus rotem Ziegelstein im Zentrum der Stadt. Hier, in der City Road 124, sind weit über 5.000 Unternehmen registriert, die meisten davon Briefkastenfirmen. Ab rund 40 Pfund im Jahr kann man sich an der Adresse ein „virtuelles Büro“ mieten und somit von überall in der Welt ein Unternehmen anmelden.

Am 29. August 2023 kommt eine weitere Firma hinzu: TNSecurity Ltd. Das Unternehmen spielt eine wichtige Rolle in der Maschinerie von Doppelgänger. Es beheimatet nach Recherchen von Qurium hunderte Domains, also Internetadressen für die Propaganda-Kampagne. Die Links sind quasi ein Wegwerfprodukt; sie werden

Kampagne weiterzuleiten. Weiterleitung bedeutet, Sie klicken auf eine Internetadresse und werden automatisch auf eine andere Adresse umgeleitet (mehr zu den Gründen für dieses Vorgehen im aufklappbaren Info-Kasten). Damit tappen Sie in die Falle, die sich die Doppelgänger-Architekten ausgedacht haben.

Die Dienste der Firma werden aber auch für kriminelle Aktivitäten genutzt. TNSecurity zeichne sich durch ein „ungewöhnlich hohes Maß an Schadsoftware-Aktivität“ aus, heißt es im Mai 2024 in einem Bericht der kanadischen IT-Sicherheitsfirma Hyas, die cyberkriminelle und schädliche Aktivitäten im Internet beobachtet. „TNSecurity wurde möglicherweise kompromittiert oder arbeitet absichtlich mit Cyberkriminellen zusammen.“ Dazu passt der Name, den sich die Verantwortlichen hinter der Briefkastenfirma für einen Teil ihrer Infrastruktur ausgedacht haben: „Evil Empire“, das böse Imperium also.

Weshalb Doppelgänger tausende Internetadressen benötigt

Wenn Sie bei dem gefälschten Spiegel-Artikel gelandet sind, fällt Ihnen womöglich ein kleines Detail auf: In der Adresszeile Ihres Internetbrowsers steht nicht die tatsächliche Adresse des Spiegels (spiegel.de), sondern spiegel.ltd – unter dieser Domain verbreitet Doppelgänger seit Jahren die gefälschten Artikel der Wochenzeitung.

„Spiegel.ltd“ wurde – wie viele andere Doppelgänger-Adressen – von Facebook und X gesperrt. Ein Link dazu lässt sich auf den Plattformen nicht mehr teilen. Die russische Desinformations-Kampagne setzt deshalb auf ein ausgeklügeltes System der Verschleierung mit Weiterleitungen über andere Internetadressen.

Das funktioniert so: Auf X und Facebook verbreiten künstliche Profile, sogenannte Bots, nichtssagende Links. Im Beispiel des Spiegel-Artikels

> Auch diese Links werden früher oder später von den Plattformen gesperrt. Um die Propaganda-Maschinerie am Laufen zu halten, ist deshalb ein ständiger Nachschub an Internetadressen notwendig.

Wurde die Firma TNSecurity eigens für solche kriminellen und politischen Aktivitäten gegründet? Registriert wurde sie im Namen von Anastasija Berezina, damals 18 Jahre alt und laut dem britischen Handelsregister Lettin – nach Informationen von CORRECTIV könnte sie jedoch aus Pskow im Nordwesten Russlands stammen. Dass sie TNSecurity wirklich kontrolliert, ist fraglich. TNSecurity antwortete nicht auf eine Anfrage an eine hinterlegte Mailadresse. Auch Berezina beantwortete Anrufe und Fragen nicht.

Als Dienstleisterin für Doppelgänger ist TNSecurity nicht allein. Rund ein Dutzend britische Firmen wurden 2023 und 2024 innerhalb weniger Monate von jungen Personen aus Russland, der Ukraine oder Kasachstan in London registriert – oft an der gleichen Adresse. Von manchen wissen wir, dass sie Dienste für die Kampagne bereitstellen. So zum Beispiel die Firmen DPKGSoft International oder Netshield, die in den vergangenen Monaten immer mehr jener Wegwerf-Domains über sich laufen lassen, die zu Doppelgänger-Inhalten weiterleiten. Auf Anfrage reagierte Netshield und löschte nach eigener Angabe einige Domains, andere sind bis heute online.

All diese Firmen haben eine weitere Gemeinsamkeit. Sie alle weisen eine Verbindung auf zu einem jungen Sankt Petersburger IT-Unternehmen, das in zwei Jahren einen erstaunlichen Aufstieg geschafft hat. Die Analysten von Qurium vermuten, dass ihm eine zentrale Rolle in der Doppelgänger-Architektur zukommt – als

Kapitel 3: Ein rasanter Aufstieg

(Collage: Ivo Mayr / CORRECTIV)

Sankt Petersburg, Sommer 2024. Arseniy Penzev ist 21 Jahre alt und Mitgründer der Firma Aeza in Sankt Petersburg. Auf seinem Telegram-Account zeigt er sich mal auf einem russischen Unternehmertag. Mal filmt er sich mit seinem Geschäftspartner Bosojan in einem Business-Hotel in Moskau. Aeza präsentiert sich als modernes Start-up, seine Mitarbeiter zeigen sich in Live-Streams auf Youtube. Kürzlich warb Aeza an einer Moskauer Universität um neue Mitarbeitende.

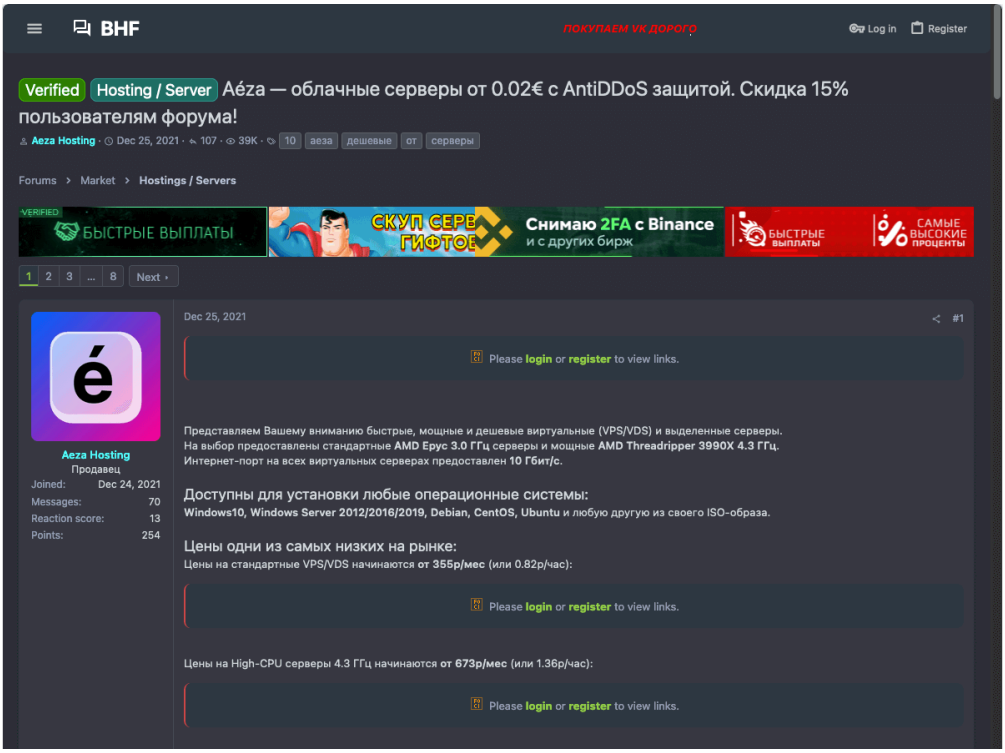
Aeza gehören nach eigenen Angaben inzwischen rund 40.000 Server. Die Firma besitzt laut einer Schätzung von Qurium IP-Adressen im Wert von rund 2,4 Millionen Euro. Mit Aeza hat es Penzev in die erste Liga der russischen Webhoster geschafft. Und so richtig scheint er selbst nicht zu verstehen, wie ihm das gelang.

Penzev stammt aus der Gaming-Szene, hatte schon als Jugendlicher

Penzev und sein Geschäftspartner Bosojan hatten die Hostingfirma MSKHost aufgezogen. Im September des gleichen Jahres kam es zu einem jähen Ende. Glaubt man den Verlautbarungen von Penzev, wurde der Dienst gehackt – über Nacht verlor er sein Geschäft. Ehemalige Kunden hingegen vermuten, geprellt worden zu sein, also dass der Hack nie stattfand, sondern ein sogenannter Exit-Scam war. Umso überraschender ist der Aufstieg, der folgte.

In dem Blogeintrag erzählt er, wie er nach dem Absturz von MSKHost unerwartete Hilfe bekam. Plötzlich seien in Moskau Leute aufgetaucht mit „krassem Eisen“, also schneller Serverhardware, von der sein Team geträumt hätte. Die Leute hätten nicht gewusst, wem sie die Technik anvertrauen sollten und seien bereit zur Kooperation in Form eines neuen Hosting-Anbieters gewesen. Wer das war, schreibt Penzev nicht. Einen ausführlichen Fragenkatalog dazu und zu anderen Aspekten ließ Aeza unbeantwortet.

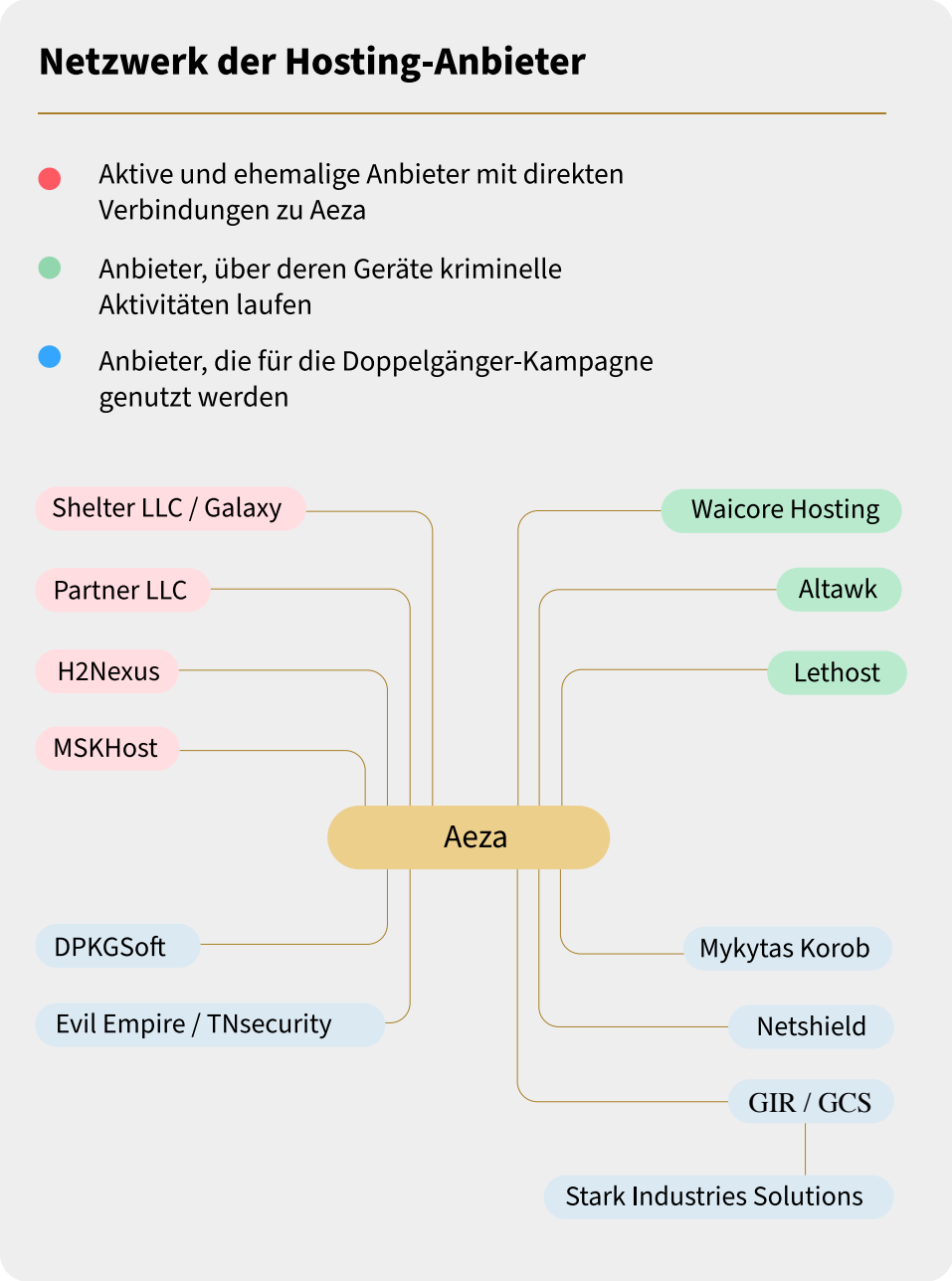
Auf den eigenen Servern lässt Aeza, ähnlich wie schon die Vorgängerfirma MSKHost, mutmaßlich Kriminelle agieren. Sie bewarb ihre Dienste zum Beispiel in Untergrund-Foren, im Darknet. Auch Aezas Angebot, Server stundenweise nutzen zu können, ist nach Einschätzung von Experten eine versteckte Einladung an Cyberkriminelle.



Aeza bewarb seine Dienste unter anderem im russischen Hacker-Forum BHF (Screenshot: CORRECTIV)

Vielleicht gerade deswegen ist Aeza rasant gewachsen. Es ist zu bezweifeln, dass solch ein Aufstieg im heutigen Russland ohne den Segen der Behörden möglich ist. Vielleicht ist er auch erwünscht. Denkbar ist es eine Art Handel: Die Behörden lassen Aeza gewähren, im Gegenzug stellt das Unternehmen seine internationale und verzweigte Struktur zur Verbreitung von Doppelgänger zur Verfügung. Experten vermuten schon lange, dass es eine solche Zusammenarbeit zwischen Hosting-Firmen und russischen Geheimdiensten geben könnte.

Aeza bildet laut der Analyse von Qurium den Kern eines Netzwerks aus Hosting-Firmen in Russland und Großbritannien, die alle eng miteinander in Verbindung stehen. Ein Teil sind direkte oder versteckte Ableger von Aeza, so wie Aeza International Ltd oder



Aeza steht laut der Analyse von Qurium im Zentrum eines Netzwerks an Hosting-Anbietern. Über deren Dienste laufen teils kriminelle Aktivitäten (grün markiert) und oder sie werden auch für die Desinformationskampagne „Doppelgänger“ genutzt (blau markiert). (Grafik: CORRECTIV)

Bei TNSecurity, wo die Wegwerf-Domain beheimatet war, die auf die gefälschte *Spiegel*-Seite weiterleitete, ist Aeza teilweise im Datenverkehr vorgeschaltet. Qurium bezeichnet die Firma in seinem Bericht als „Zentrum des Ökosystems von Doppelganger“. Kurzum:

Für die Verbreitung der Kampagneninhalte ist Aeza von zentraler Bedeutung.

Wenn Sie auf die fraglichen Webseiten klicken, machen die Daten zwischen Ihrem Browser und der Internetseite bei TNSecurity eine weitere Station, die möglicherweise gar nicht so weit von Ihrem Computer oder Handy entfernt liegt. Denn Firmen wie Aeza benötigen auch Anbindung an die großen Internetdrehkreuze – so wie in Frankfurt am Main.

Kapitel 4: Das Tor zur Welt

(Collage: Ivo Mayr / CORRECTIV)

Langen, Juni 2024. Joseph Hofmann empfängt in seinem Büro im ersten Stock eines Gebäudekomplexes im Industriegelände von Langen, 20 Zugminuten südlich von Frankfurt. Das Zimmer ist kahl und viel zu groß für eine Person. In der Ecke steht ein ausgezogenes Sofa, in der Mitte sind ein paar Tische zusammengestellt, an denen Hofmann zwei Bildschirme aufgebaut hat. Von hier aus leitet er seine

Die Analysten von Qurium haben festgestellt, dass der Datenverkehr von TNSecurity und weiteren Firmen aus dem Dunstkreis von Aeza zum Teil über Aurologic läuft, sie nutzen also dessen Anbindung an die globalen Internetbetreiber. Auch bei jenen Doppelgänger-Domains, die zu den gefälschten Nachrichtenseiten führen.

Das ist ein brisanter Fund, denn das hieße, dass ein deutsches Unternehmen seine Leistungen – ob wissentlich oder nicht – für eine Desinformationskampagne zur Verfügung stellt, deren Verantwortliche von der EU sanktioniert sind.

Von dem guten Dutzend Firmen aus dem Aeza-Kosmos, die nach Qurium-Recherchen in der Vergangenheit eine Verbindung zu Aurologic aufwiesen, will Hofmann nur wenige kennen. Unklar lässt er im Gespräch mit CORRECTIV, wie viele direkte Kunden darunter sind und wer wiederum Kunde eines anderen Kunden ist. Solche verschachtelten Strukturen sind in der IT-Branche eine gängige Praxis. Und von den Firmen, die er kenne, habe er jedenfalls „kein schlechtes Bild“. Aeza habe bei ihm im Datencenter wohl mal einen Server gehabt, meint er sich zu erinnern.

Auch TNSecurity scheint die Dienste von Aurologic zu nutzen. Laut Daten von Spamhaus, einer Organisation, die schädliche Internetaktivitäten beobachtet, reagierte Aurologic nicht auf dutzende sogenannte Abuse-Meldungen in Verbindung mit TNSecurity. Mit solchen Meldungen werden Hosting-Provider in Kenntnis gesetzt, dass Kunden ihre Netzwerke missbrauchen könnten. In diesem Fall ging es um die Verbreitung von Malware und Phishing-Angriffen über die Netzwerke von Aurologic. Man habe Spamhaus vielfach kontaktiert, besagte Meldungen würden jedoch

Veröffentlichung per E-Mail mit. Beim Treffen sagt er, die Firma reagiere auf solche Meldungen, wenn es genügend Beweise gebe.

Anfragen von Ermittlern gehörten zum Geschäft, sagt er. Die Vorwürfe in Bezug auf Doppelgänger seien für ihn neu. „Uns ist nicht bekannt, dass ein Kunde die Kampagne unterstützen würde“, sagt er. Doch er sagt auch, dass er seine Internetnetze nicht einfach nach solchen Inhalten scannen könne – oder gar in die Speicher seiner Kundinnen und Kunden schauen dürfe.

Und doch wird er neugierig. Wir zeigen ihm den Link, der zum gefälschten *Spiegel*-Artikel führt. Hofmann tippt die Adresse in die Kommandozeile seines Rechners ein, um den Verkehr nachzuverfolgen. Als das Resultat erscheint, ist er überrascht. „Oh, das führt tatsächlich zu uns“, sagt er.

Bewiesen ist für ihn dadurch aber nichts. „Da müssen sich die Behörden an uns wenden“, sagt er und wundert sich gleichzeitig, dass sie es bislang nicht gemacht hätten. „Wenn es Fakten gibt, werden wir darauf eingehen.“ Er formuliert sein Dilemma: „Ich kann

jeden rausschmeißen, aber dann mache ich irgendwann keinen Umsatz.“ Daher warte er auf offizielle Post.

Mit seiner Frage nach den Aktivitäten der Behörden berührt Hofmann einen wunden Punkt. Der Qurium-Bericht macht nach Informationen von CORRECTIV bereits seit Wochen bei einigen europäischen Behörden die Runde. Manche der im Bericht genannten Unternehmen waren sogar schon vorher öffentlich. Wieso also hat bisher niemand das System Doppelgänger gestoppt? Die Frage wird an einer späteren Stelle sogar noch dringlicher.

Die Kette der Beteiligten an der Desinformations-Maschine ist hier noch nicht zu Ende. Die Datenabfrage, die Sie als Leserin oder Leser beim Anklicken des Links zu dem vermeintlichen *Spiegel*-Artikel auslösen, wird schließlich über eine von TNSecurity ausgelöste Domain-Umleitung über die Aurologic-Infrastruktur in Deutschland an Ihren Browser zurückgesendet. Nun werden Sie an die nächsten beiden Stufen weitergeleitet.

Kapitel 5: Von Europa nach Asien

(Collage: Ivo Mayr / CORRECTIV)

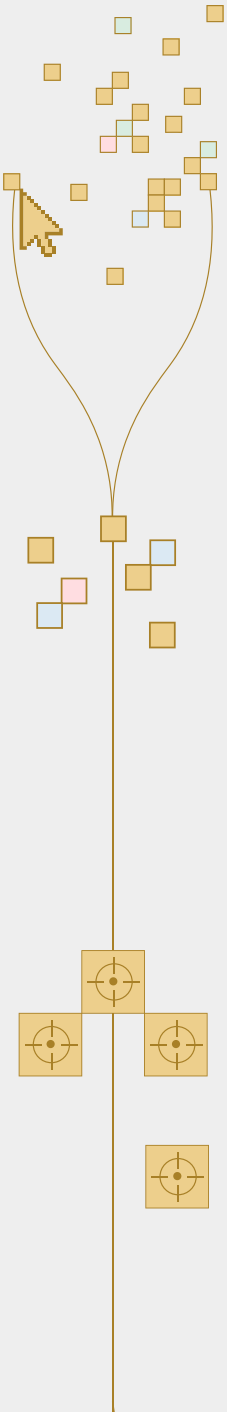
Tuusula, Juni 2024. Eine halbe Autostunde nördlich der finnischen Hauptstadt Helsinki erstrecken sich auf einem 150.000 Quadratmeter großen Gelände mehrere Gebäudereihen. In den Flachbauten, unter den spitz zulaufenden Dächern, durch einen Maschendrahtzaun abgeschirmt, rattern die Maschinen. Hier hat der deutsche Hosting-Riese Hetzner über seine finnische Tochterfirma vor sechs Jahren ein riesiges Rechenzentrum errichtet. Irgendwo hier, in einem der Server, werden von einem Kunden von Hetzner Finland Oy vier Domains betrieben, die das Nadelöhr der Doppelgänger-Kampagne sind.

Ein mehrstufiger Weiterleitungsmechanismus soll den Kern der Doppelgänger-Kampagne schützen. In der ersten Stufe gibt es Tausende beliebige Domains, die in Beiträgen auf X und Facebook gepostet werden. In der zweiten Stufe reduziert sich die Zahl der Domains auf geschätzt ein Zehntel. Diese leiten wiederum auf die dritte Stufe – dort gibt es nur noch vier Domains. Und diese führen dann zum wahren Ziel.

Das sieht im Überblick so aus:

Die IT-Infrastruktur von Doppelgänger

So werden Nutzerinnen und Nutzer weitergeleitet, wenn sie auf einen Link der Doppelgänger-Kampagne klicken.



Wegwerf-Domains

Künstliche Accounts teilen auf X und Facebook unzählige Links. Die Domains verschleiern ihr eigentliches Ziel und liegen bei Firmen wie TNSecurity oder Netshield in Großbritannien. Der Datenverkehr läuft auch über Hostinger in Litauen und Aurologic in Deutschland.

Zwischen-Domains

Ein Code wartet auf diesen Domains und leitet Ihren Browser an die nächste Station weiter. Die Domains liegen bei BL Networks aus den USA und dem britischen Liber Systems.

Keitaro-Domains

Der Werbetracker Keitaro der estnischen Firma Apliteni OU prüft den Standort des Browsers und leitet zur korrekten Propaganda-Webseite weiter, wenn zum Beispiel ein gefälschter Spiegel-Artikel von Deutschland aus aufgerufen wird. Dies geschieht über eine von nur vier

(Grafik: CORRECTIV)

Das ist die zentrale Taktik der Doppelgänger-Kampagne – und sie ist gar nicht neu. Bei Spamhaus, der Organisation, die schädliche Internetaktivitäten beobachtet und die CORRECTIV im Zuge der Recherche um eine Einschätzung gebeten hat, sind solche Weiterleitungsketten von Phishing- und Malwarekampagnen bekannt. Internetbetrüger verwenden diese Masche, um zu vermeiden, dass wertvolle Infrastrukturkomponenten wie die „echten“ Domains oder Server zu viel Aufmerksamkeit erfahren. Je weiter die Weiterleitungskette fortschreitet, desto statischer werden üblicherweise involvierte Domains und IP-Adressen, so die Experten von Spamhaus.

So ist es auch bei Doppelgänger: Laut der Analyse von Qurium laufen die Domains der zweiten Stufe vor allem über zwei Firmen: Liber Systems aus Großbritannien und BL Networks aus den USA. Auch sie

Investigace gegenüber, das gemeinsam mit CORRECTIV recherchiert hat, ließ Liber Systems durch einen Anwalt mitteilen, dass die Firma nur einen sogenannten Virtual Private Server Dienst anbiete und ansonsten „nicht in die Geschäfte seiner Kunden involviert“ sei.

Dann kommt die dritte Stufe: Während Sie warten, dass der vermeintliche *Spiegel*-Artikel in Ihrem Browser erscheint, ruft Ihr Gerät eine der folgenden vier Domains ab: cheekss.click, ggspace.space, gooddefr.com und sdgqaef.site. Dort ist eine Software namens Keitaro installiert, die erkennt, wo Sie sich befinden. Nur wenn Sie tatsächlich in Deutschland sind, werden Sie zur letzten Stufe geleitet, der eigentlichen Zieldomain spiegel.ltd, der gefälschten Nachrichtenseite. Andernfalls werden Sie auf eine andere beliebige Website gelotst.

Durch diese vier Adressen werden alle Besucher der tausenden Domains der Vorstufen durchgeschleust. Sie alle laufen über Hetzner in Finnland. Die Sperrung dieses einen Kunden würde die ganze Maschinerie stoppen – vermutlich allerdings nur, bis der Datenfluss umgeleitet wird.

Es sind europäische Firmen, die die entscheidende letzte Stufe erst möglich machen: Auch die Software Keitaro stammt von einer europäischen Firma, der estnischen Apliteni OU. Wie bei der deutschen Firma Aurologic hätten Behörden hier einen Hebel, um gegen die Doppelgänger-Kampagne vorzugehen. Da gegen einige der Verantwortlichen dahinter Sanktionen verhängt wurden, dürfen europäische Firmen weder direkt noch indirekt Ressourcen für sie bereitstellen. Ganz abgesehen davon, dass über Teile derselben Infrastruktur offenbar auch kriminelle Aktivitäten stattfinden

In der letzten Stufe der Weiterleitungskette, dort, wo die gefälschten Nachrichtenseiten tatsächlich betrieben werden, haben europäische Behörden vermutlich so gut wie keinen Einfluss: Die Domains wie spiegel.ltd, sueddeutsche.ltd oder washingtonpost.pm liegen bei einem Webhoster mit Sitz in Malaysia: Shinjiru Technology. Einige weitere liegen in Singapur bei einer Tochter des litauischen Hosting-Riesen Hostinger. Shinjiru beantwortete Fragen dazu bis Redaktionsschluss nicht. Hostinger teilte nach erster Untersuchung mit, keine Anzeichen dafür zu sehen, dass die Seiten auf ihren Servern lägen, erbat aber weitere Informationen.

Hetzner versicherte auf Anfrage, der entsprechende Kunde selbst sei nicht sanktioniert, eine Verbindung des Kunden zu einer sanktionierten Person oder Organisation sei nicht bekannt. Man habe von dem Vorgang nichts gewusst und werde „geeignete Maßnahmen ergreifen, um weitere zukünftige Rechtsverletzungen über unsere Server zu verhindern“, sollten sich die Vorwürfe bewahrheiten. Die estnische Firma Apliteni beantwortete Fragen zu ihrer Rolle nicht.

Auf Regierungsseite verwiesen einzelne Ministerien und Behörden verschiedener EU-Länder wie in Finnland bei Fragen zu eventuellen Sanktionsverstößen teilweise auf sich gegenseitig. Die in Estland für Sanktionsdurchsetzung verantwortliche Behörde für Verbraucherschutz und technische Regulierung teilte mit, sich die Struktur hinter der Kampagne bislang nicht näher angeschaut zu haben. „Die technischen Nuancen bedürfen weiterer Untersuchungen unsererseits“, sagte eine Sprecherin.

Eine frühe Version des Qurium-Berichts kursierte dabei nach Recherchen von CORRECTIV schon seit dem Frühjahr dieses Jahres

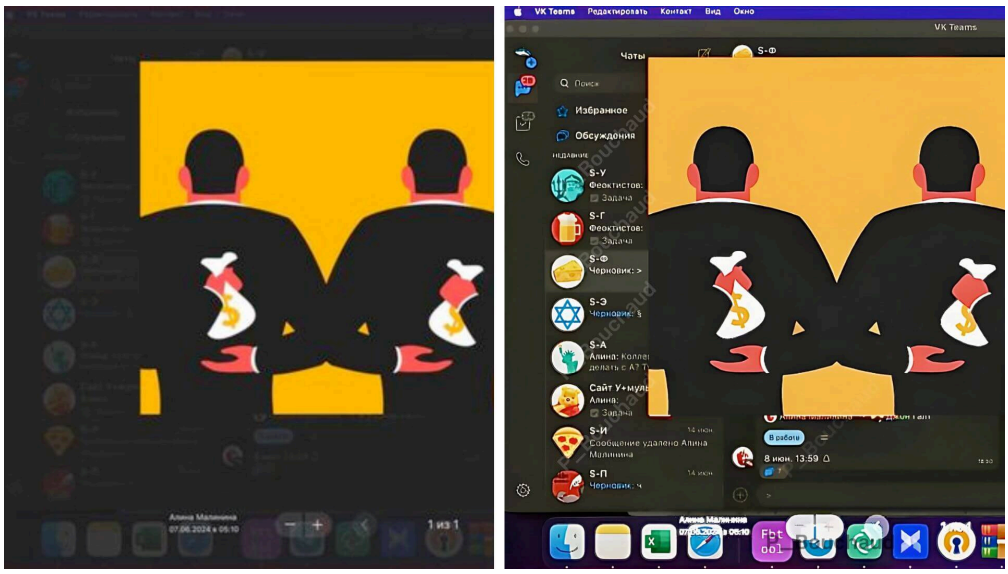
Auswärtigen Amt und im Bundesinnenministerium. Die Hinweise wurden allerdings bisher offenbar nicht genutzt, um der Kampagne einen Riegel vorzuschieben. Über die Untätigkeit der Politik, wenn es um die Infrastruktur von Doppelgänger geht, haben wir hier berichtet.

Kapitel 6: Die Verbreitung

(Collage: Ivo Mayr / CORRECTIV)

Moskau, Juni 2024. Ob Alina Malinina für die PR-Agentur Social Design Agency, Struktura, Argon Labs oder eine andere Firma arbeitet, ist unklar. Auch nicht, ob sie wirklich so heißt. Doch dank eines kleinen Fehlers wissen wir, dass sie Teil eines Teams ist, das Inhalte von Doppelgänger verbreitet. Eine kurze Unachtsamkeit bietet einen Einblick in die menschliche Ebene hinter dieser hoch automatisierten Desinformationsmaschine. Hier wird mit den Links gearbeitet, nachdem sie in dem ausgeklügelten IT-System platziert wurden.

Statt eines Bildausschnitts hat jemand aus Malininas Team in einer Facebook-Werbeanzeige für Doppelgänger ein komplettes Bildschirmfoto hochgeladen. Darauf ist ein Arbeitschat auf der russischen Plattform VK zu sehen, in dem offensichtlich mehrere Personen arbeiten. In der Mitte ist das eigentliche Vorschaubild, gepostet von einer gewissen Alina Malinina. Es sollte wohl einen französischen Doppelgänger-Artikel illustrieren, der der Ukraine Geldverschwendung vorwirft.



In einer Facebook-Werbeanzeige luden Doppelgänger-Mitarbeiter vermutlich aus Versehen ein komplettes Bildschirmfoto hoch (links). Der IT-Forscher Paul Bouchaud fand den Fehler und machte die Details im Bild mit einigen Tricks sichtbar (rechts). (Quellen: Meta Werbebibliothek, Paul Bouchaud)

Gefunden hat diesen Fehler der IT-Forscher Paul Bouchaud. Mit ein paar Tricks lassen sich auf dem Bildschirmfoto einzelne Chat-Untergruppen mit Symbolbildern erkennen: Eine Freiheitsstatue für die USA; eine Pizza für Italien; ein Bierkrug für Deutschland. Man sieht, dass jemand den Link zu einem gefälschten Artikel Webseite leparisien.wf gepostet und Aufgaben definiert hat. Möglicherweise wurde hier so auch der gefälschte *Spiegel*-Artikel bearbeitet, das

Für die Doppelgänger-Kampagne scheint an diesem Tag weiter alles nach Plan zu laufen. Auf die verteilten Aufgaben antwortet Alina Malinina: „Check“. Wenige Tage später verbreiten die Bots der Kampagne gefälschte Artikel von *Le Parisien* und anderen Medien. Die Propaganda läuft auch nach über zwei Jahren stetig weiter – weder Politik noch Plattformen konnten sie bisher stoppen.

Diese Recherche entstand in Kooperation mit Investigace.cz und VSquare.

***Update, 11. Juli 2024 um 17.18 Uhr:** Wir haben eine Stellungnahme von Joseph Hofmann ergänzt, in der er sich zu dem Vorwurf äußert, Aurologic habe nicht auf Abuse-Meldungen von Spamhaus reagiert.*

***Redigatur:** Anette Dowideit, Alice Echtermann*
***Faktencheck:** Stella Hesch*
***Redaktion:** Alice Echtermann*
***Design:** Ivo Mayr*
***Grafiken:** Mohamed Anwar*

HINTER DER RECHERCHE

Für unsere Recherche haben wir mit der schwedischen NGO Qurium zusammengearbeitet, die uns eine Vorabversion ihrer nun öffentlichen Analyse der Doppelgänger-Infrastruktur zur Verfügung stellte. CORRECTIV recherchierte dann über mehrere Wochen zu den involvierten Firmen und Personen, führte zahlreiche Interviews mit Expertinnen und Experten, Behörden und anderen Beteiligten. An der Recherche arbeiteten wir gemeinsam mit Investigace.cz und VSquare, die sich vor allem die beteiligten Firmen in der Tschechischen Republik genauer ansahen. Die Analyse von Qurium stützt sich zum Teil auf Daten von Antibot4Navalny, einer anonymen Freiwilligengruppe, die russische Desinformation auf X verfolgt.