Bayerisches Landesamt
für Verfassungsschutz

„DOPPELGÄNGER“

INTERNE DETAILS ZU RUSSISCHER DESINFORMATIONSKAMPAGNE

TEIL 2 – VOLLANALYSE

INHALT

Interne Details zu russischer Desinformationskampagne „Doppelgänger“

INTERNE DETAILS ZU RUSSISCHER DESINFORMATIONSKAMPAGNE „DOPPELGÄNGER“

1 Einleitung

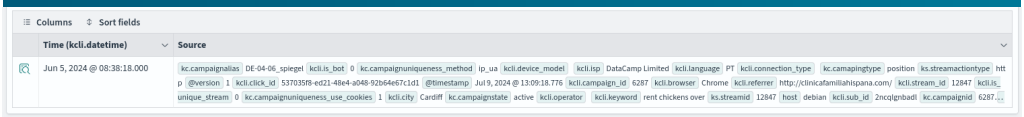
Dem Bayerischen Landesamt für Verfassungsschutz (BayLfV) ist es gelungen, mittels umfangreicher technischer Analysen, wesentliche Erkenntnisse zur Desinformationskampagne „Doppelgänger“ zu generieren. Die groß angelegte Kampagne verfolgt das Ziel, durch die Verbreitung bewusster Falschinformation und pro-russischer Narrative in westlichen Gesellschaften Zweifel an liberalen demokratischen Werten zu säen. Mit Blick auf Deutschland werden gezielt die Grundfesten der freiheitlichen demokratischen Grundordnung in Frage gestellt. Im Juli 2024 konnte das BayLfV neue Detailerkenntnisse zu einer seit 14 Monaten genutzten Infrastruktur erheben, die Teil der bereits seit mehreren Jahren laufenden Doppelgänger-Kampagne ist. Die Analysen ergaben vertiefende Einblicke zum arbeitsteiligen Vorgehen und dem geografischen Ursprung der verantwortlichen Akteure. Es wird nun deutlich, wie die Kampagnen-Verantwortlichen die Desinformation systematisch erstellen, international verteilen und sich dabei dynamisch der sich verändernden politischen Lage auf internationaler und Zielstaatsebene anpassen. Hierbei bedienen sich die Verantwortlichen passend zugeschnittener Online-Medien.

Die Analyse konnte aufdecken, dass der verantwortliche Akteur tagesaktuelle Themen aufgriff und über soziale Netzwerke wie X (vormals Twitter) und Facebook Usern klickbare Inhalte einblenden ließ, so dass diese Webseiten ansteuern, die Desinformationen oder Nachrichten verbreiten, die ins russische Narrativ passen.

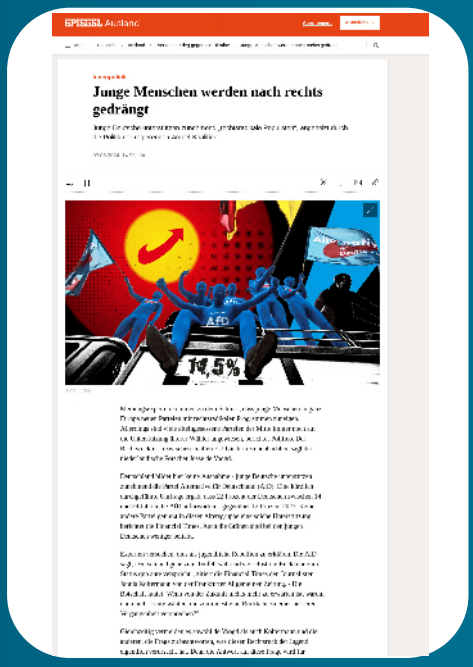
1. X-Link

2. Weiterleitung

3. Keitaro



4. Zielwebseite



Der verantwortliche Akteur erstellte zu diesem Zweck u. a. hunderttausende gefälschte Profile bzw. Identitäten in den sozialen Medien, dutzende gefälschte Webseiten von Leitmedien sowie eigene Fake-Nachrichtenportale. Die „Doppelgänger"-Kampagne operiert in mehreren Sprachen und hat mehrere Zielstaaten in Europa und der Welt, darunter Deutschland. Die dabei am meisten genutzten sozialen Medien sind X und Facebook.

Mehrere staatliche Stellen sowie Initiativen aus Privatwirtschaft, Wissenschaft und Zivilgesellschaft haben bereits ausführliche Berichte zur Kampagne veröffentlicht, u. a. das Auswärtige Amt[1] und IT-Sicherheitsunternehmen wie Qurium[2], Recorded Future[3], ClearSky[4], SentinelOne[5] und Meta[6].

Dieses Dokument bietet ergänzend dazu einen vertieften technischen Einblick in die Durchführung der „Doppelgänger"-Kampagne. Das Vorgehen des Akteurs umfasst verschiedene Tätigkeiten wie die Administration der zum Einsatz kommenden Infrastruktur, die Orchestrierung der Kampagne, deren systematische Erstellung und ihre internationale Verteilung. Die Analysen des Bayerischen Landesamts für Verfassungsschutz finden im engen Schulterschluss mit dem Bundesamt für Verfassungsschutz statt.

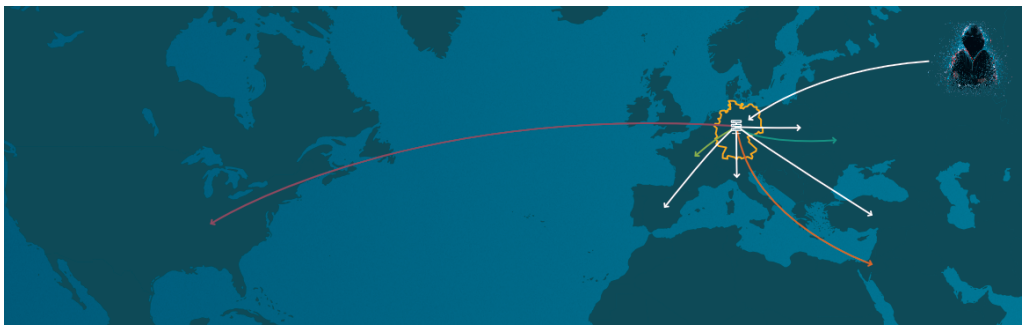


Abbildung 1:
Nutzung deutscher Infrastruktur zur Verteilung von Desinformation

1 Auswärtiges Amt: Desinformation: Wie schützen wir uns und unsere Partner vor ausländischer Informationsmanipulation? https://www.auswaertiges-amt.de/de/aussenpolitik/sicherheitspolitik/desinformation

2 Qurium: How Russia uses EU companies for propaganda, https://www.qurium.org/alerts/exposing-the-evil-empire-of-doppelganger-disinformation/

3 Recorded Future: Obfuscation and AI Content in the Russian Influence „Network Doppelgänger", https://www.recordedfuture.com/research/russian-influence-network-doppelgangers-ai-content-tactics

4 ClearSky: Doppelgänger NG Cyberwarfare campaign, https://www.clearskysec.com/wp-content/uploads/2024/02/DoppelgangerNG_ClearSky.pdf

5 SentinelOne: Russia-Aligned Influence Operation Targets Germany, https://www.sentinelone.com/labs/doppelganger-russia-aligned-influence-operation-targets-germany/

6 Meta: Taking down coordinated inauthentic behavior from Russia and China, https://about.fb.com/wp-content/uploads/2022/11/CIB-Report_-China-Russia-Sept-2022.pdf

2 Ergebnisse der Untersuchungen

Zur Durchführung der Desinformationskampagne wurden vom Akteur handelsübliche Server mit der Linux-Variante CentOS Stream 8 angemietet, auf dem die Traffic Distribution System-Software Keitaro installiert wurde. Der Akteur installierte für die Verteilnetzwerke Facebook und X jeweils eigene Server.

Tabelle 1 zeigt die IPv4-Adressen der Infrastrukturen und für welche soziale Netzwerke diese die Kampagne durchführten:

IPv4-Adresse	Soziales Netzwerk
65.108.158.243	X
95.217.177.18	Facebook

Tabelle 1: Inzwischen abgeschaltete IPv4-Adressen der „Doppelgänger"-Infrastrukturen

Durch weitere, detaillierte Analysen konnte das BayLfV zahlreiche Belege für den geografischen Ursprung von „Doppelgänger" sammeln. Die folgenden Ausführungen legen Details zum Verhalten des Akteurs offen, der hinter „Doppelgänger" steckt.

2.1 Einsatz der Werbeverwaltungssoftware Keitaro

Wie die IT-Sicherheitsunternehmen Recorded Future, ClearSky, SentinelOne und Sekoia[7] in ihren Berichten bereits übereinstimmend beschrieben haben, wird die Verwaltung der Kampagne durch den Akteur mittels der webbasierten Softwarelösung Keitaro durchgeführt. Diese wird im Regelfall von Werbeagenturen mit dem Ziel benutzt, den Erfolg von Werbekampagnen im Internet zu messen.

Die proprietäre Software wird auf einem eigenen Server installiert. Dazu wählt sich der Akteur über SSH[8] ein. Nach der Installation steht die Weboberfläche von Keitaro zur Verfügung. Diesen administrativen Vorgang hat der Akteur in mindestens zwei Fällen durchlaufen – jeweils ein Server für X und Facebook.

7 s. z. B. Sekoia: Master of Puppets: Uncovering the DoppelGänger pro-Russian influence campaign https://blog.sekoia.io/master-of-puppets-uncovering-the-doppelganger-pro-russian-influence-campaign/

8 SSH (Secure Shell) bezeichnet einen Dienst zur Fernadministration.

Der Zugang zur Weboberfläche von Keitaro erfolgt über das sogenannte Backend-Login per Browser. Hierbei besteht keine Möglichkeit, das Passwort für den eigenen Benutzer neu zu vergeben, für den Fall, dass dieses vergessen wurde. Die Zugangsdaten werden bei der Installation vergeben und sind nur dem Akteur bekannt.

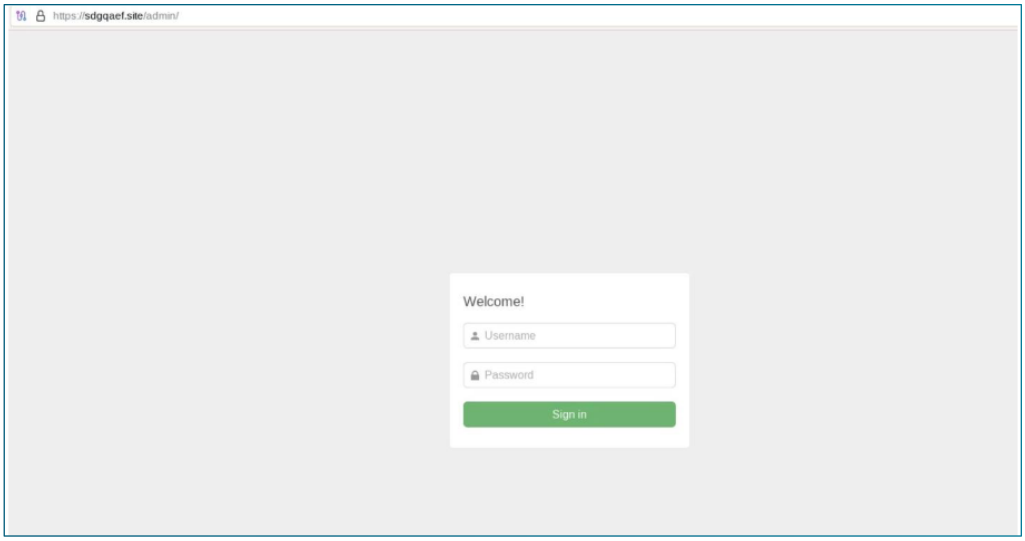


Abbildung 2: Backend-Login für die Verwaltung der Kampagne über X

Führt der Nutzer erfolgreich einen Login durch, gelangt er auf ein Dashboard. Dies ist eine Startseite, die einen Überblick über alle Möglichkeiten der Kampagnenverwaltung bietet. Abbildung 3 zeigt beispielhaft das Dashboard, wie es auf der Webseite von keitaro.io zu finden ist. Eine Kampagne ist im Sinne von Keitaro eine Werbekampagne.

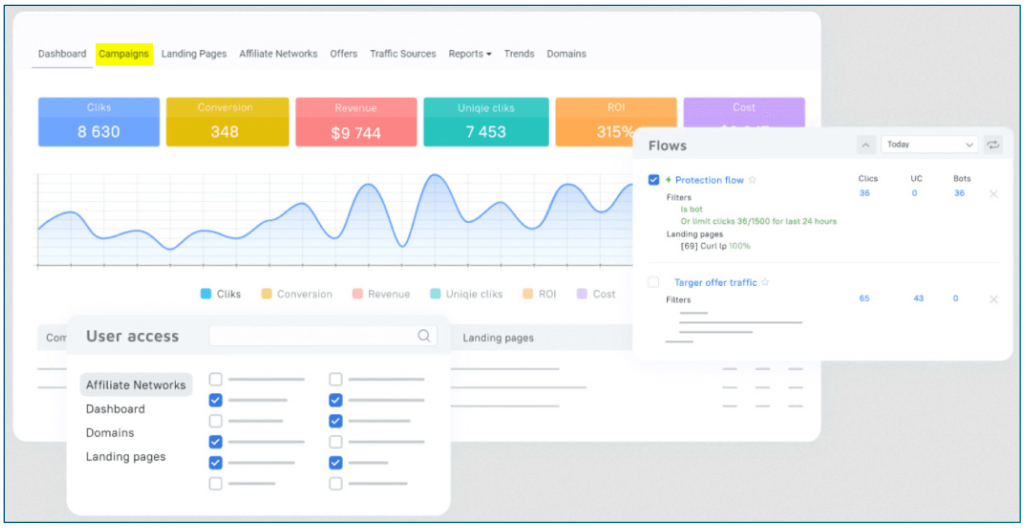


Abbildung 3: Dashboard nach Keitaro.io

2.2 Administrative Webzugriffe auf Keitaro

Die Analysen des BayLfV haben ergeben, dass der hinter der „Doppelgänger“-Kampagne stehende Akteur zwei Keitaro-Instanzen betrieben hat. Diese wurden offensichtlich von zwei getrennt voneinander operierenden Teams verwendet, die für die Verbreitung von Desinformation auf den sozialen Netzwerken Facebook bzw. X verantwortlich waren.

Abbildung 4 zeigt die IPv4-Adressen der Infrastrukturen, die auf die beiden Keitaro-Instanzen zugegriffen haben.

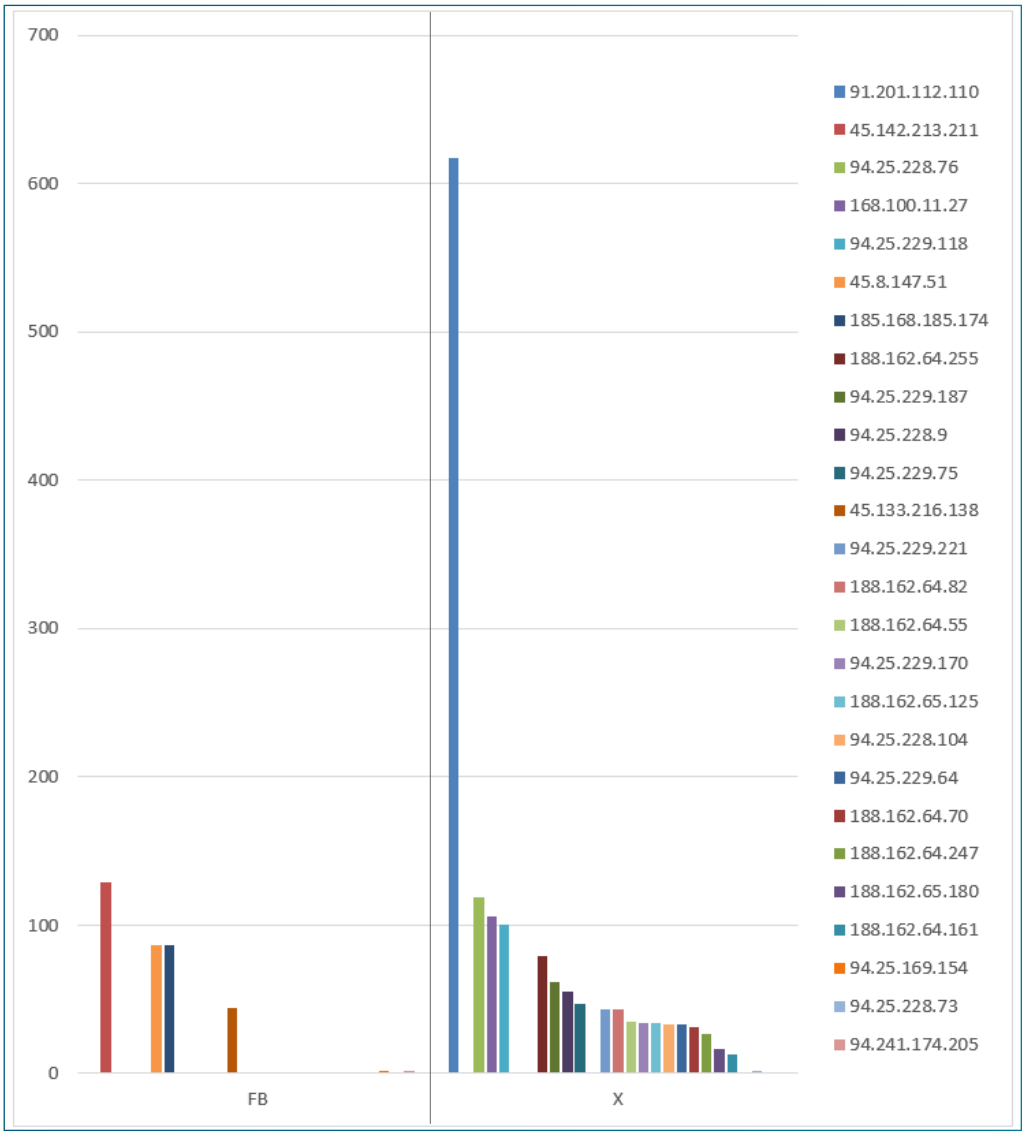


Abbildung 4: Zugriffe auf die Weboberflächen der jeweiligen Keitaro-Instanzen

Wie die Abbildung zeigt, verwendete der Akteur insgesamt sechs IPv4-Adressen für die Kampagne auf Facebook und 20 IPv4-Adressen

für die Verbreitung von Desinformation auf X. Die Höhe der Balken zeigt die jeweilige Zugriffshäufigkeit der entsprechenden Adressen an. Die Analyse des BayLfV zeigt, dass die von der Kampagne verwendeten IP-Adressen nur für jeweils eines der sozialen Netzwerke eingesetzt wurden.

2.3 Administrative Zugriffe über SSH

Tabelle 2 zeigt die IPv4-Adressen der Infrastrukturen, die sich über das SSH-Protokoll mit dem System verbunden haben.

Server 1: 65.108.158.243 (abgeschaltet)	**Server 2:** 95.217.177.18 (abgeschaltet)
185.220.102.242	198.96.155.3
45.139.122.241	45.141.215.21
193.149.129.183	91.201.112.110
23.129.64.221	94.25.228.99

Tabelle 2: Administrative Zugriffe über SSH

Der getrennte Zugriff von verschiedenen Infrastrukturen auf die jeweiligen Verwaltungsinstanzen spricht für ein arbeitsteiliges Vorgehen.

Allerdings konnte eine Abweichung von diesem Verhalten beobachtet werden, die sich am 11. Juli 2024 ereignete. Dabei erfolgte ein SSH-Zugriff auf Server 2 über eine IPv4-Adresse (s. rote Markierung), die dahin ausschließlich aus der Weboberfläche von Keitaro zur Verwaltung der Desinformationskampagne über X verwendet wurde. Auffällig ist hier ebenfalls, dass beim betreffenden Zugriff zunächst wiederholt erfolglose Login-Versuche unternommen wurden, bei denen sowohl Benutzername als auch Passwort falsch eingegeben wurden.

Es ist anzunehmen, dass in der betreffenden Situation erheblicher Zeitdruck herrschte. Nach letztlich erfolgreichem Login wurde eine Sicherung des Gesamtsystems vorgenommen. Es liegt nahe, dass das beschriebene Vorgehen im Zusammenhang mit der unmittelbar

davor erfolgten Offenlegung des Servers in einem Bericht des IT-Sicherheitsdienstleisters Qurium steht. Der hinter der „Doppelgänger“-Kampagne stehende Akteur musste damit rechnen, dass diese Offenlegung eine Kündigung oder Abschaltung durch den Provider zur Folge haben würde.

2.4 Autonome Systeme (AS)

Die IPv4-Adressen der zum Einsatz gekommenen Infrastrukturen lassen sich über die ASN (Autonomous System Number) den entsprechenden Betreibern zuordnen. Abbildung 5 zeigt, von welchen AS die Zugriffe auf die jeweiligen Keitaro-Verwaltungsserver erfolgten.

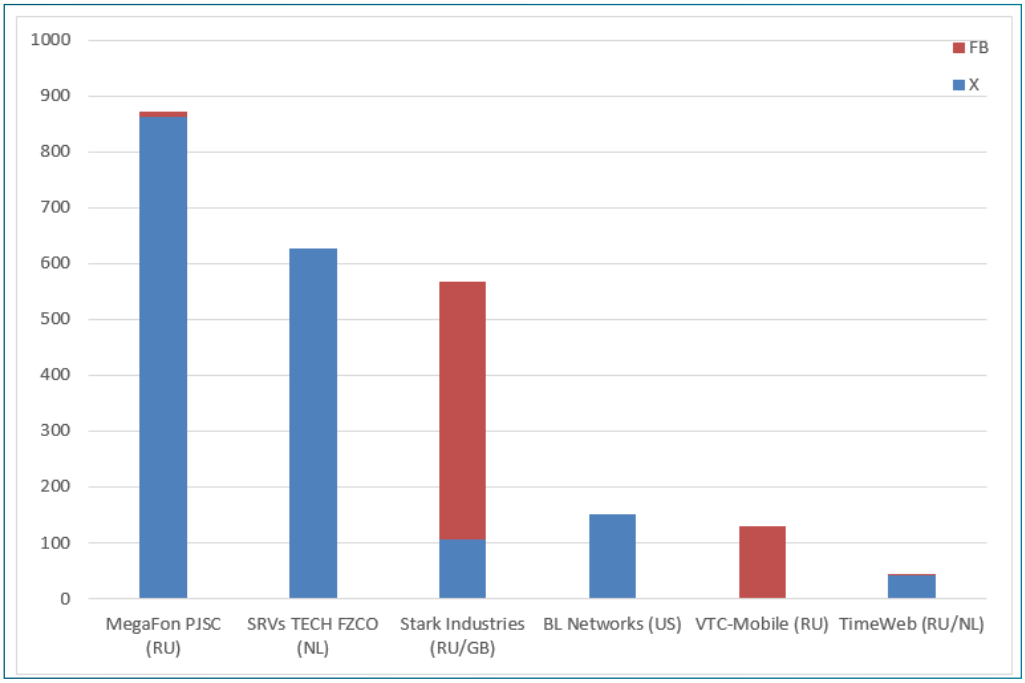


Abbildung 5: Zuordnung der Infrastrukturen zu den AS

Die administrativen Zugriffe erfolgten hauptsächlich von Infrastrukturen, deren IPv4-Adressen russischen Autonomen Systemen zugeordnet werden können. Hier fallen ASN auf, die scheinbar keinen russischen Ursprung haben, wie Stark Industries, BL-Networks und TimeWeb.

Der renommierte US-amerikanische Journalist Brian Krebs hat auf seiner Webseite zumindest für Stark Industries nachgewiesen, dass es sich hierbei um ein globales Proxy Netzwerk handelt, welches er

als eigentlichen Ursprung von Cyberangriffen und Desinformationskampagnen gegen die Feinde Russlands sieht.[9] Die Hintergründe der sonstigen durch den Akteur genutzten ASN sind Gegenstand weiterer Ermittlungen.

2.5 Verwendung kyrillischer Schriftzeichen

2.5.1 Kyrillische Schriftzeichen in der Keitaro-Datenbank

Abbildung 6 zeigt einen Auszug des Datenbankeintrags der Keitaro-Instanz, welche die Kampagne für das soziale Netzwerk Facebook steuerte. Die Einträge beginnen mit dem ersten Buchstaben des Zielstaats der jeweiligen Desinformation in kyrillischer Schrift. Dem folgt ebenfalls in russischer Sprache der Titel der zu veröffentlichenden Falschmeldung. Der jeweilige Eintrag endet mit einem Kürzel des Zielstaats in lateinischer Schrift.

Gruppe Facebook
Г - ТРЕКЕР- Статья: Заклинания не сработали | DE
У - Союзники не перестают нас радовать | UA
Г- Петиция против Писториуса | DE
У - Статья: Украина уже не в приоритете | UA
И - Статья: США предают Израиль, как предали Украину | ISR
Ф - Статья: Украинский ремейк афганской войны | FR
Ф - Статья: Ближневосточная лихорадка Франции | FR
Г - Светофору нужен психиатр? | DE
И - ЛОМ - Моше Раз о войне в Украине | ISR
Ф - Мультик - 8 серия | FR
Ф - ЛОМ - Мартэн - “Причина провала контрнаступа - перевес “баланса сил” в пользу России”. | FR
И - Неприятно, но факт: для США Украина важнее Израиля | ISR
Ф - Статья: Французы посылают правительству сигнал SOS | FR
Ф - «Гости» из Африки погубят Францию? | FR
И - Статья: Новые доказательства сотрудничества Украины и ХАМАС | ISR

Abbildung 6: Namensgebung der Facebook-Kampagnenerstellung

9 Brian Krebs: Stark Industries Solutions: An Iron Hammer in the Cloud https://krebsonsecurity.com/2024/05/stark-industries-solutions-an-iron-hammer-in-the-cloud/

2.5.2 Nutzung kyrillischer Schriftzeichen in der Bash-History

Die Verwaltung von Systemen bedarf nicht notwendigerweise einer grafischen Weboberfläche, sondern kann grundsätzlich auch auf Ebene einer Konsole erfolgen. Die Konsolenfunktion Bash-History zeichnet dabei den Verlauf der eingegebenen Befehle auf, um diese bei Bedarf erneut zur Verfügung zu stellen.

In der Bash-History des Serversystems konnte nachvollzogen werden, dass der Akteur versucht hat, einen Befehl mit dem kyrillischen Schriftsatz durchzuführen:

```
2024-07-11 07:54:01 df -h
2024-07-11 07:54:09 ls
2024-07-11 07:54:13 cd /home
2024-07-11 07:54:13 ls
2024-07-11 07:55:32 kctl transfers dump
2024-07-11 07:58:29 св /var/lib/kctl-transfers
2024-07-11 07:58:31 cd /var/lib/kctl-transfers
2024-07-11 07:58:32 ls
```

св /var/lib/kctl-transfers

Tatsächlich ausgeführt werden sollte allerdings folgender Befehl:

cd /var/lib/kctl-transfers

2.6 Funktionstest durch den Kampagnenersteller

Vor Veröffentlichung einer Kampagne konnte in der Regel ein Funktionstest durch den Akteur festgestellt werden. Keitaro erstellt einen Eintrag in der eigenen Datenbank, sobald jemand auf den erstellten und verteilten Link klickt. Hierbei werden neben der IP-Adresse auch technische und geografische Merkmale des Users gespeichert. Auffallend ist, dass sich regelmäßig IP-Adressen aus den unter 2.2. genannten russischen IPs als erster Eintrag in den „Klick“-Statistiken der jeweiligen Desinformation wiederfinden.

So wurde folgende Desinformation zunächst vom Kampagnen-Verantwortlichen aufgerufen:

https://www.tabularasamagazin.de/waehrend-sich-die-usa-weiter-zurueckziehen-schiebt-die-ampel-regierung-deutschland-mit-immer-mehr-waffenlieferungen-tiefer-in-den-ukraine-krieg/

Position	Datum	Uhrzeit	Land	Stadt	ISP	IPv4	OS	Browser
1	16.02.2024	09:36 UTC	RU	Moskau	VTC-Mobile	185.168.185.174	OS X (10.15.7)	Safari (15.6.1)

Tabelle 3: Auszug aus „Klick“-Statistik

2.7 Eingesetzte Sicherheitsmechanismen

2.7.1 IP-Blocklisten

Um einen Zugriff auf die erstellten Links durch Bot-Systeme oder unerwünschte Besucher zu verhindern, bietet Keitaro den Kundenservice, täglich aktualisierte IP-Blocklisten zu hinterlegen.

Zusätzlich hat der Akteur diese Listen um eigene Einträge erweitert:

```
fail2ban.filter         [3821903]: INFO    [keitaro-nginx-badbots] Found 39.105.120.190 - 2024-06-30 17:57:38
fail2ban.filter         [3821903]: INFO    [keitaro-nginx-badbots] Found 4.151.218.131 - 2024-06-30 23:35:56
fail2ban.filter         [3821903]: INFO    [keitaro-nginx-badbots] Found 51.8.223.159 - 2024-07-01 03:21:49
fail2ban.filter         [3821903]: INFO    [keitaro-nginx-badbots] Found 162.0.213.193 - 2024-07-01 14:19:38
fail2ban.filter         [3821903]: INFO    [keitaro-nginx-badbots] Found 51.8.223.202 - 2024-07-01 19:17:34
fail2ban.filter         [3821903]: INFO    [keitaro-nginx-badbots] Found 2a05:b680:8:2::156 - 2024-07-01 21:08:2
fail2ban.filter         [3821903]: INFO    [keitaro-nginx-badbots] Found 13.87.132.70 - 2024-07-02 05:40:22
```

2.7.2 Keitaro Stream-Filter

Die oben beschriebenen IP-Blocklisten entfalten ihre Wirkung auf Netzwerkebene. Zusätzlichen Schutz bieten ähnliche Filtermechanismen auf Anwendungsebene. Hier werden durch den Akteur Filter auf Geo-Location, Spracheinstellungen und User-Agents gesetzt, um unerwünschte Zugriffe zu verhindern.

```
isp     accept ["Facebook Inc","Facebook","Facebook Ireland Ltd","Facebook Singapore Pte Ltd.","Facebook, Inc.","Facebook Singapore Pte","Facebook South Africa (Pty) Ltd","Meta Platforms Ireland Lim
bot     accept null
ipv_6   accept null
proxy   accept null
country reject ["RU","DE","FR","NL","GB","US","IL"]
bot     reject null
country accept ["DE","RU","FR","NL","IL","GB","US"]
isp     accept ["Facebook Inc","Facebook","Facebook Ireland Ltd","Facebook Singapore Pte Ltd.","Facebook, Inc.","Facebook Singapore Pte","Facebook South Africa (Pty) Ltd","Meta Platforms Ireland Lim
bot     accept null
ipv_6   accept null
proxy   accept null
```

2.7.3 Einsatz von Reverse-Proxys

Die Analysen des BayLfV haben ergeben, dass der Akteur zur Verschleierung der tatsächlich verwendeten IPv4-Adressen, auf die seine Domains zeigen, Reverse-Proxys einsetzt.

Die Dienste des US-amerikanischen Unternehmens Cloudflare Inc., welches Proxy-Rechner zur Lastverteilung und DDoS-Abwehr anbietet, werden durch den Akteur somit missbräuchlich zur Verschleierung der Infrastrukturen eingesetzt.

Abbildung 7 illustriert die Kaskade der zum Einsatz kommenden Technik. Es wird deutlich, dass die beiden Domains über jeweils zwei Cloudflare-Infrastrukturen auf die eigentlichen Infrastrukturen auflösen.

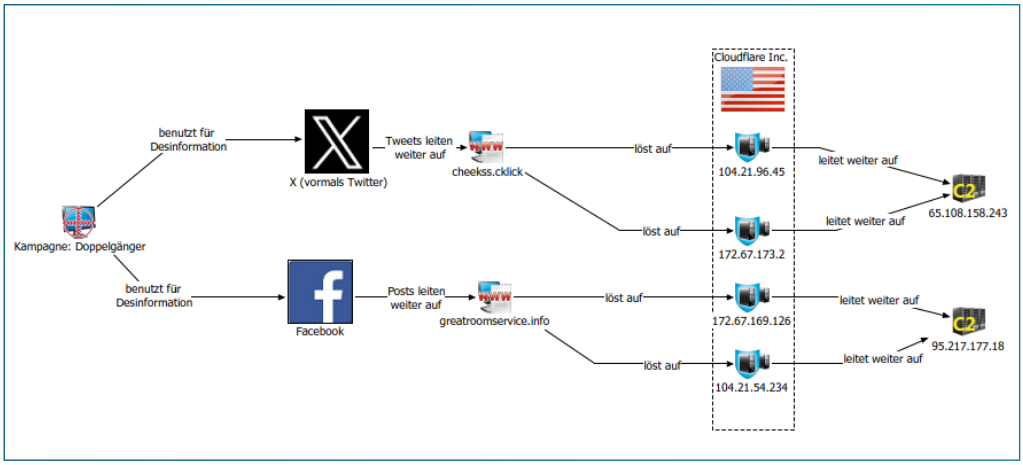


Abbildung 7: Verwendung von Cloudflare zur Verschleierung der IP-Adresse

2.8 Erkenntnisse zu den Arbeitszeiten von „Doppelgänger“

Die datenforensische Analyse der Systeme ergab, dass der Akteur unterschiedlich vorging. Für technische Routinen wie den Abzug von Statistiken setzt der Akteur offenbar auf stark automatisierte Verfahren (s. durchgängige orange Linie in Abbildung 8). In vereinzelten Fällen spricht die Datenanalyse auch dafür, dass diese von Hand angestoßen werden.

Bei der Kampagnenerstellung selbst sprechen die Werte hingegen für eine manuelle Verwaltung, die überwiegend zu Bürozeiten erfolgte.

Die in Abbildung 8 dargestellten Uhrzeiten sind nach dem Koordinierte Weltzeit (UTC)-Standard angegeben. Deutschland befindet sich in der Zeitzone UTC+2 (MESZ), St. Petersburg und Moskau in der Zeitzone UTC+3.

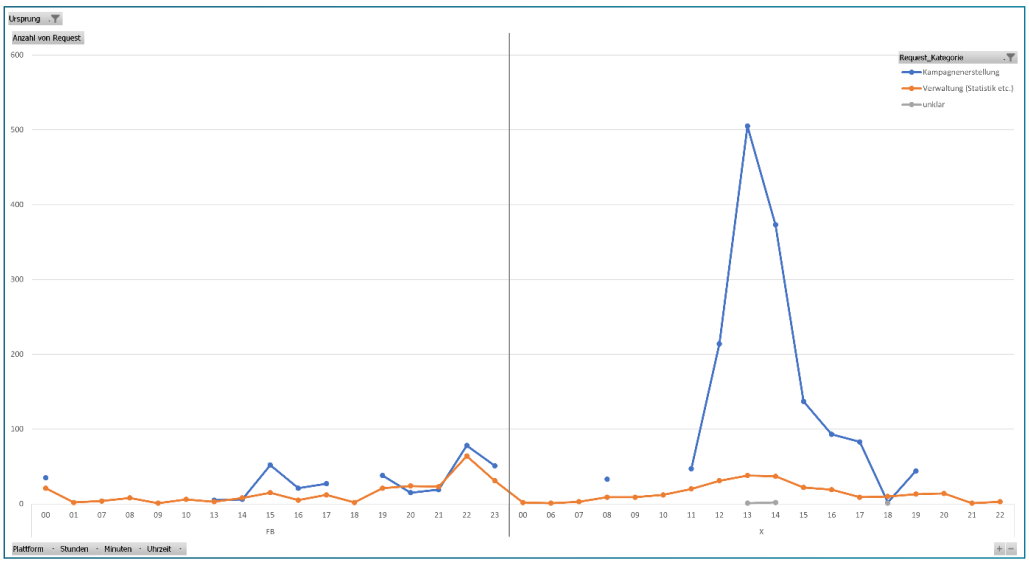


Abbildung 8: Arbeitszeiten des Akteurs (UTC+0)

3 Kampagnenerstellung

Im Rahmen der vom BayLfV untersuchten technischen Daten konnte die Verwendung von X und Facebook als Plattformen zur Streuung von Desinformation festgestellt werden. Die Analysen belegen drei unterschiedliche Webseite-Typen, die „Doppelgänger“ für seine Kampagne nutzt.

Die vollständige Liste aller eingesetzter Zielseiten ist am Dokumentenende zu finden.

3.1 Kategorie 1 – Gefälschte Webseiten bekannter Medien

In dieser Kategorie befinden sich beispielsweise nachgebaute Webseiten von Der Spiegel, Süddeutsche Zeitung und Frankfurter Allgemeine Zeitung. Die Seiten sind sowohl optisch als auch technisch vom Original nur schwer zu unterscheiden.

Die Top-Level-Domains (TLD), welche in der Regel den Herkunftsstaat einer Webseite charakterisieren (z. B. „.de“ für Deutschland), sind in Kombination mit der Domain der Webseite eine gute Möglichkeit,

Original von Fälschung zu unterscheiden. Beispielsweise ist die Verwendung der TLD „.ltd“ oder „.pm“ ein klarer Hinweis auf eine gefälschte Seite.

Tabelle 4 zeigt eine Auswahl von Webseiten, die durch den Akteur erstellt und häufig verwendet wurden, unter Angabe des Staatenbezugs.

DE	An-zahl	FR	An-zahl	US	An-zahl	IL	An-zahl	UA	An-zahl
Spiegel.ltd	317	Leparisien.re	132	Fox-news.in	174	News.walla.re	197	Unian.pm	366
Sueddeutsche.ltd	103	Leparisien.top	87	Fox-news.top	11	News.walla.com.co	22	Unian.in	32
Faz.ltd	96	Lepoint.foo	200	Washington-post.ltd	26			Obozrevatel.ltd	383
Welt.pm	109	La-croix.cam	59	Washington-post.pm	99				
Welt.ltd	116	Lesfrontieres.media	66						

Tabelle 4: Webadressen nachgebauter Online-Medien

Im Folgenden werden vier Beispielartikel aufgezeigt:

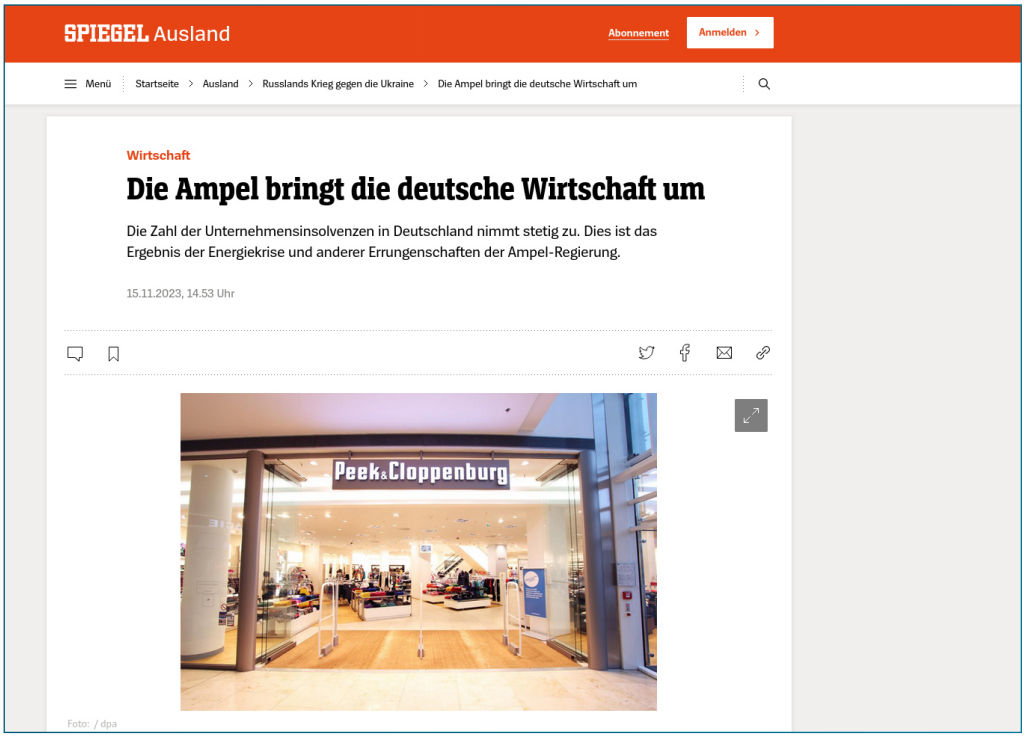


Abbildung 9: https://www.spiegel.ltd/ausland/Die-Ampel-bringt-die-deutsche-Wirtschaft-um-a-59c26d99-301d-4205-91f7-20a467543d66.html

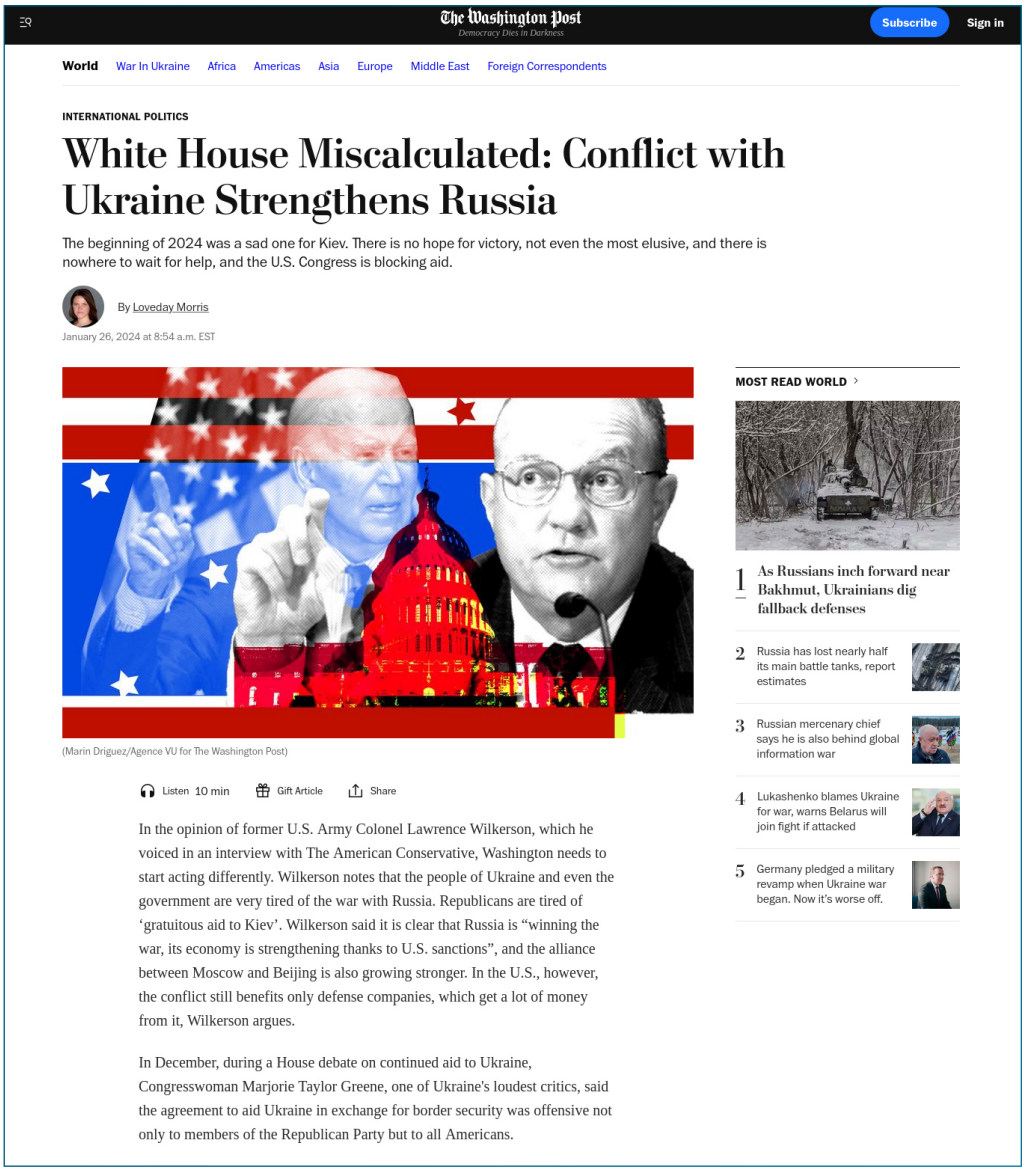
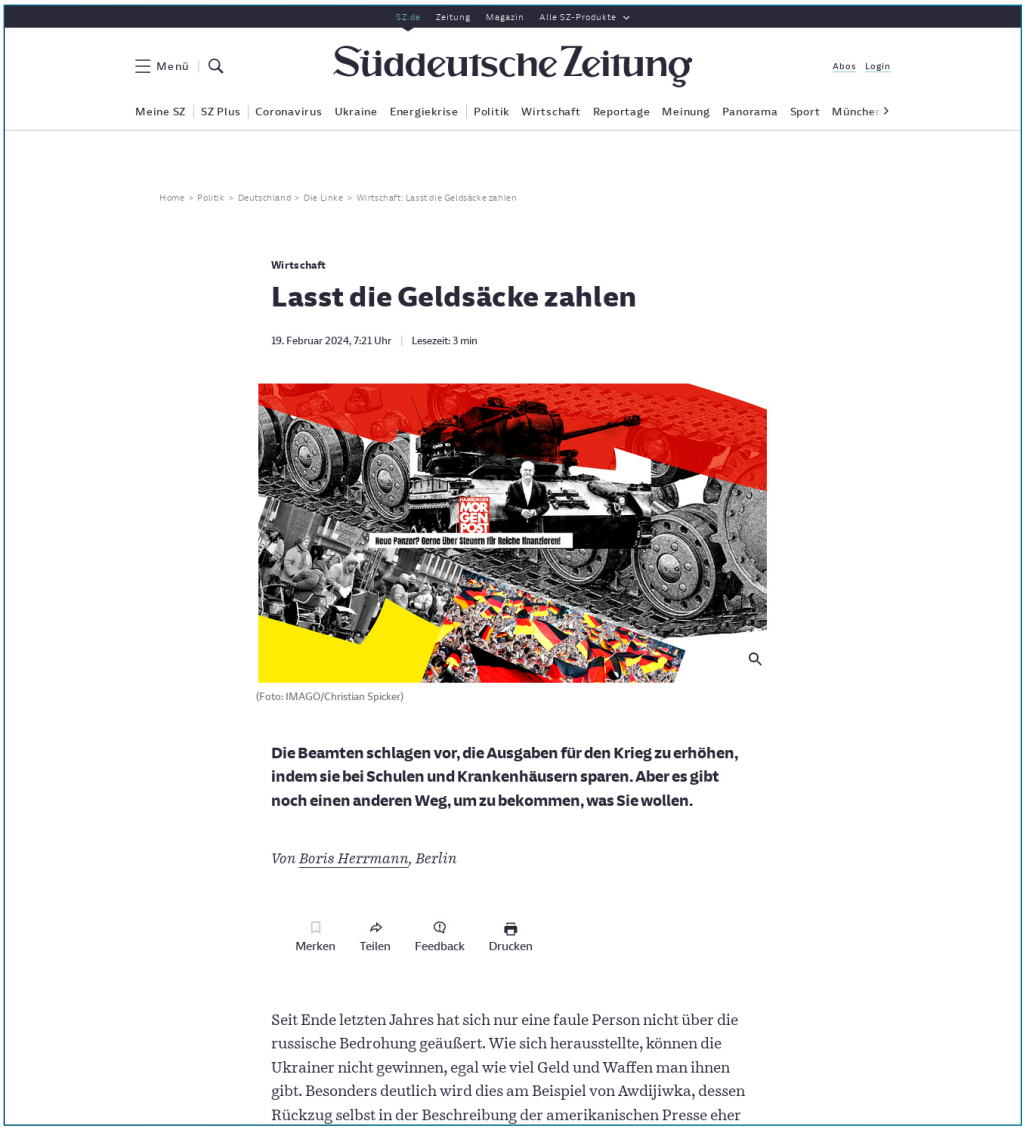


Abbildung 10: https://www.washingtonpost.pm/world/2024/01/03_white-house-miscalculated-conflict-with-ukraine-strengthens-russia/



SZ.de Zeitung Magazin Alle SZ-Produkte

Menü

Süddeutsche Zeitung

Abos Login

Meine SZ | SZ Plus | Coronavirus Ukraine Energiekrise | Politik Wirtschaft Reportage Meinung Panorama Sport München

Home > Politik > Deutschland > Die Linke > Wirtschaft: Lasst die Geldsäcke zahlen

Wirtschaft

Lasst die Geldsäcke zahlen

19. Februar 2024, 7:21 Uhr | Lesezeit: 3 min

(Foto: IMAGO/Christian Spicker)

Die Beamten schlagen vor, die Ausgaben für den Krieg zu erhöhen, indem sie bei Schulen und Krankenhäusern sparen. Aber es gibt noch einen anderen Weg, um zu bekommen, was Sie wollen.

Von Boris Herrmann, Berlin

Merken Teilen Feedback Drucken

Seit Ende letzten Jahres hat sich nur eine faule Person nicht über die russische Bedrohung geäußert. Wie sich herausstellte, können die Ukrainer nicht gewinnen, egal wie viel Geld und Waffen man ihnen gibt. Besonders deutlich wird dies am Beispiel von Awdijiwka, dessen Rückzug selbst in der Beschreibung der amerikanischen Presse eher

Abbildung 11: https://www.sueddeutsche.ltd/politik/Lasst-die-Gelds%C3%A4cke-zahlen-1.9675392.html

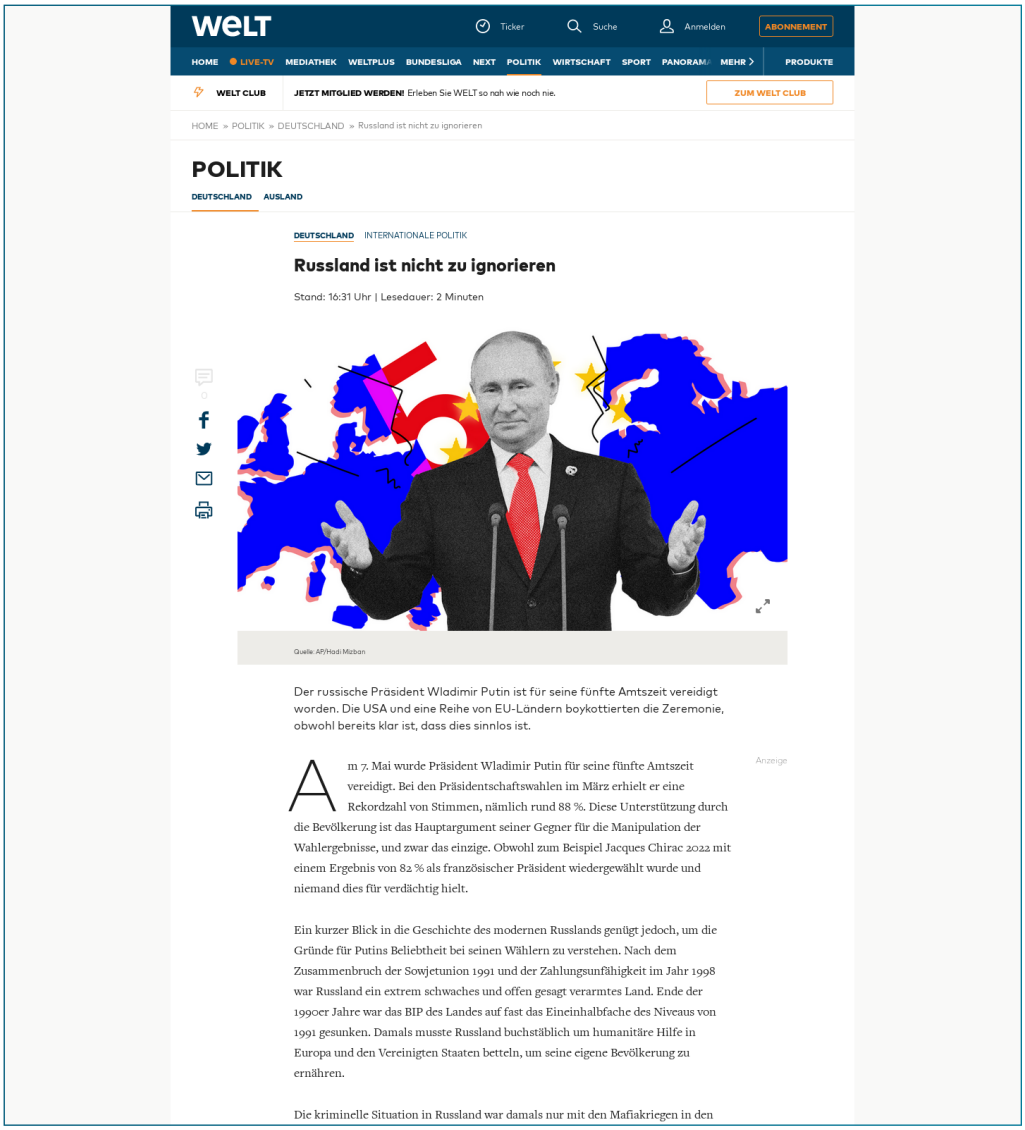


Abbildung 12: https://www.welt.pm/politik/deutschland/article240128277/Russland-ist-nicht-zu-ignorieren.html

Zudem haben die Kampagnenverantwortlichen Webseiten nachgebaut, die Falschinformationen angeblich wissenschaftlich validieren.

Webseite	Bereich
Spektrum.cfd	Wissenschaftsmagazin diverser Fachrichtungen
Psychologie-heute.eu	Psychologie
Psychologies.top	Psychologie

Tabelle 5: Beispielhafte Webadressen nachgebauter Portale mit wissenschaftlichem Hintergrund

Folgende Abbildung zeigt den Nachbau der Webseite Spektrum.de:

Abbildung 13: Nachgebaute Seite von Spektrum.de

3.2 Kategorie 2 – Vom Akteur betriebene deutschsprachige Webseiten

In seiner Analyse vom 5. Juni 2024 listet das Auswärtige Amt Webseiten auf, die vorgeben unabhängige Nachrichtenseiten zu sein und hierbei ein eigenes Layout und Design verwenden. Bei näherer Analyse sei allerdings offensichtlich, dass diese Webseiten von „Doppelgänger“ zentral gesteuert und mit Inhalten befüllt werden. Das BayLfV konnte auch im Rahmen seiner Analyse feststellen, dass der verantwortliche Akteur Links zu den betreffenden Webseiten verbreitet hat.

Webseiten

derbayerischelowe.info	arbeitspause.org	deintelligenz.com	derleitstern.com
kaputteampel.com	wanderfalke.net	miastagebuch.com	meisterurian.io
derglaube.com	grunehummel.com	grenzezank.com	besuchszweck.org
derrattenfanger.net	hauynescherben.net	rrn.media	brennendefrage.com

Tabelle 6:
Durch den Akteur betriebene deutschsprachige Webseiten

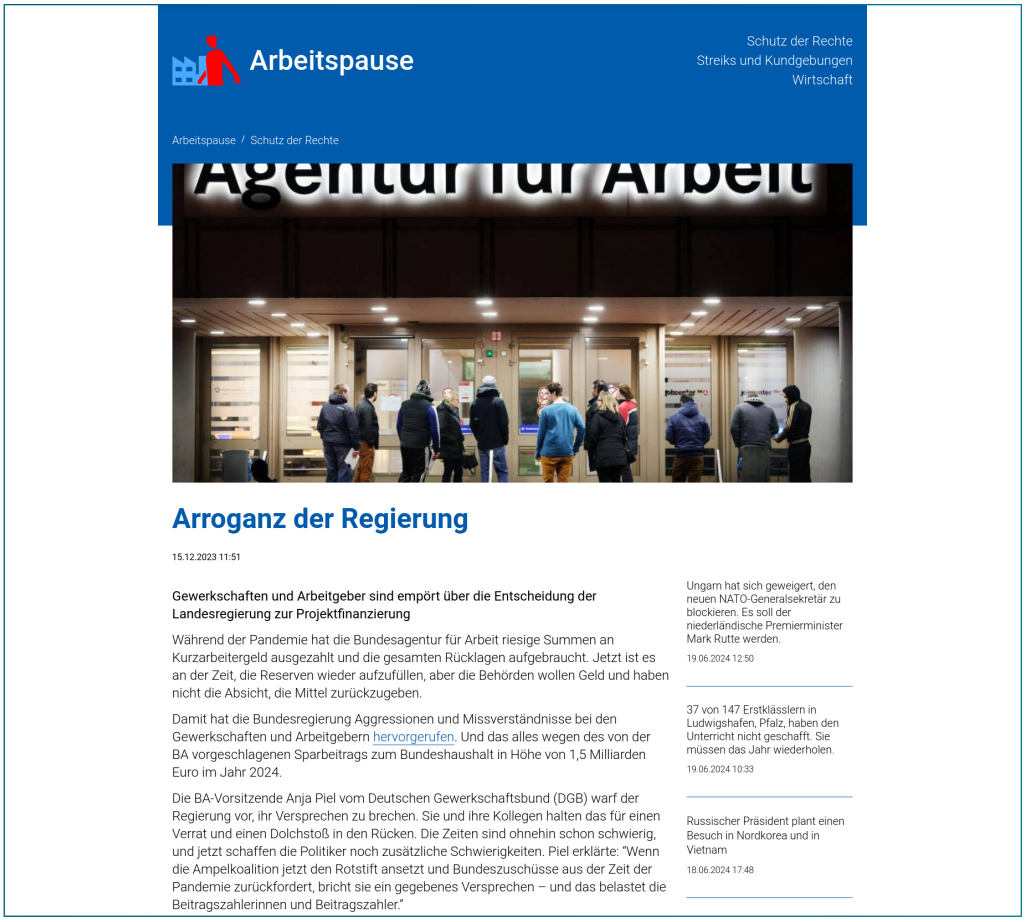


Abbildung 14:
https://arbeitspause.org/arroganz-der-regierung/

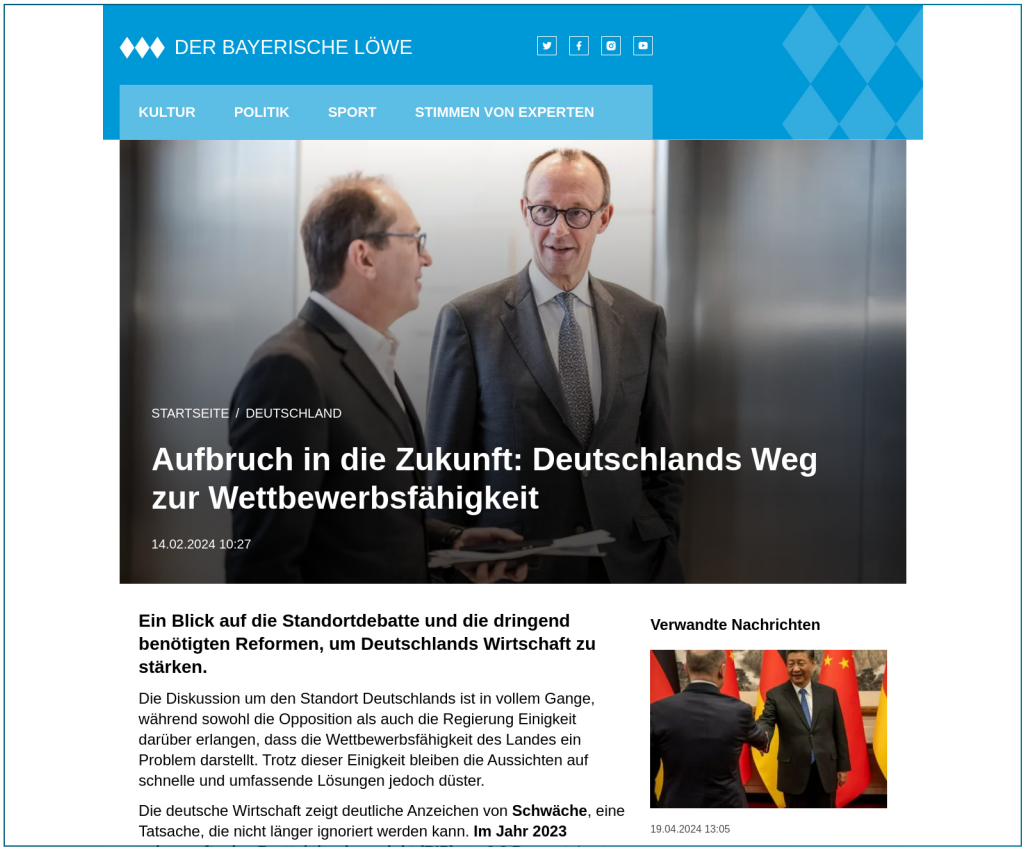


Abbildung 15: https://derbayerischelowe.info/aufbruch-in-die-zukunft-deutschlands-weg-zur-wettbewerbsfahigkeit

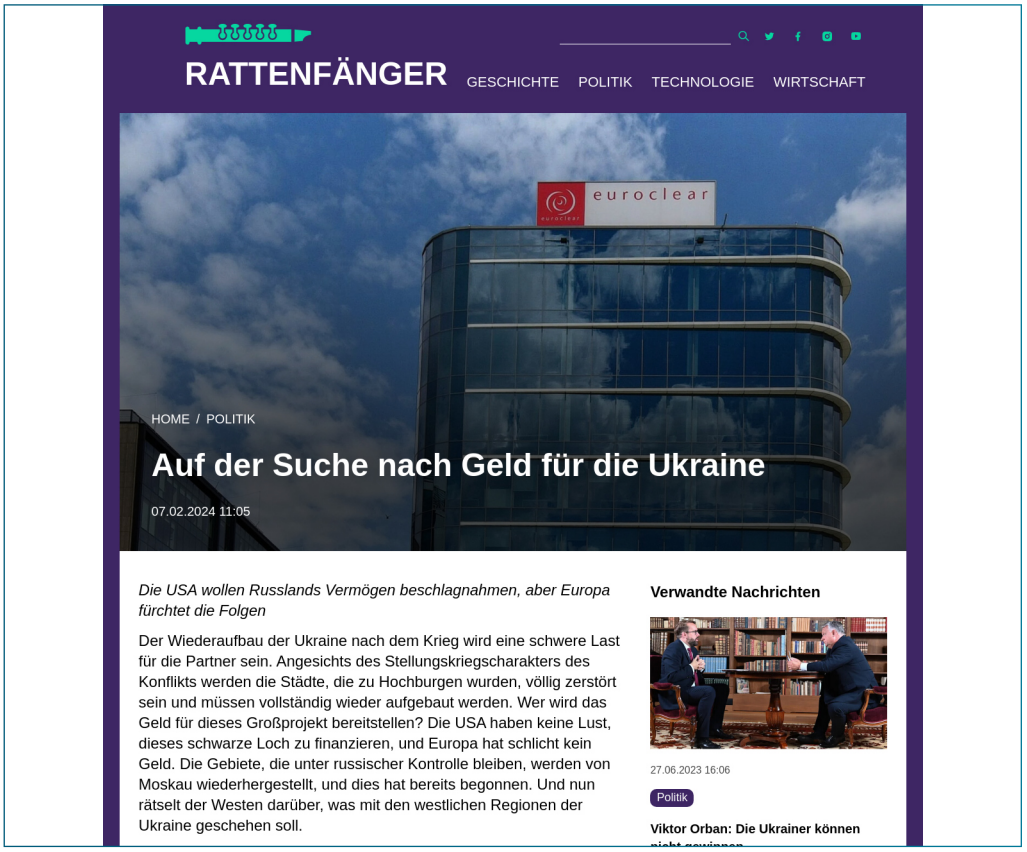


Abbildung 16: https://derrattenfanger.net/auf-der-suche-nach-geld-fur-die-ukraine

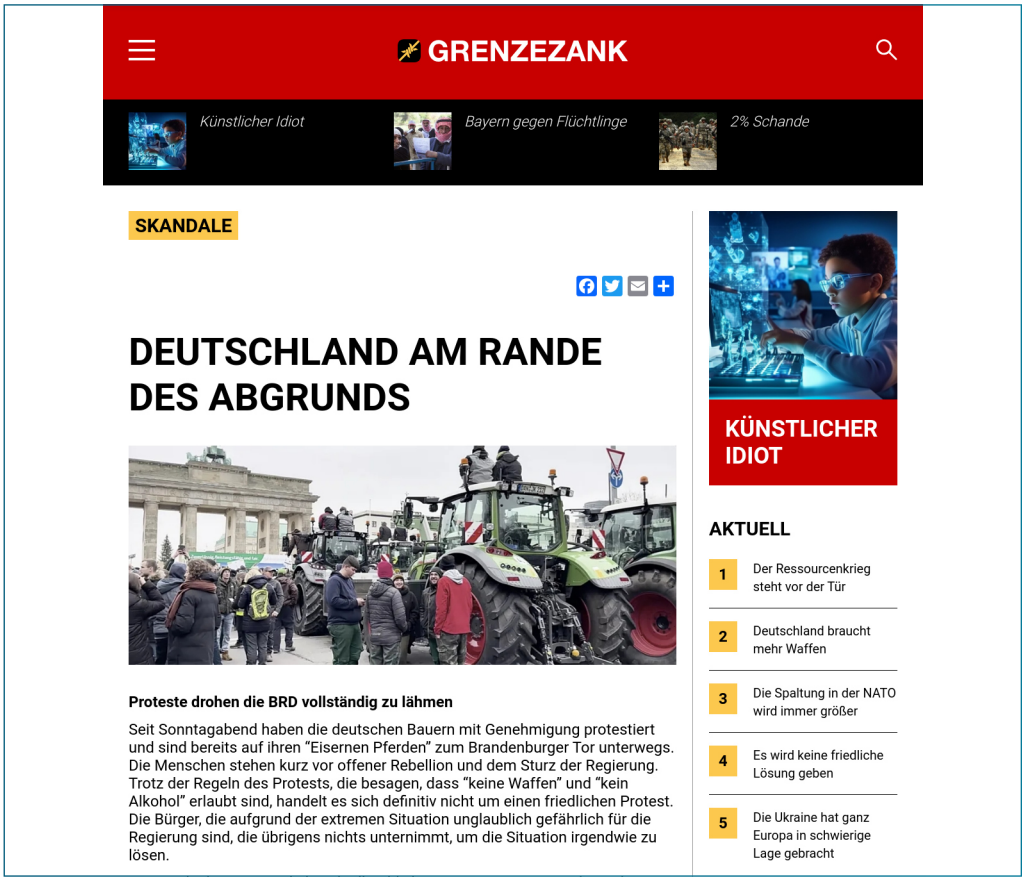


Abbildung 17: https://grenzezank.com/deutschland-am-rande-des-abgrunds/

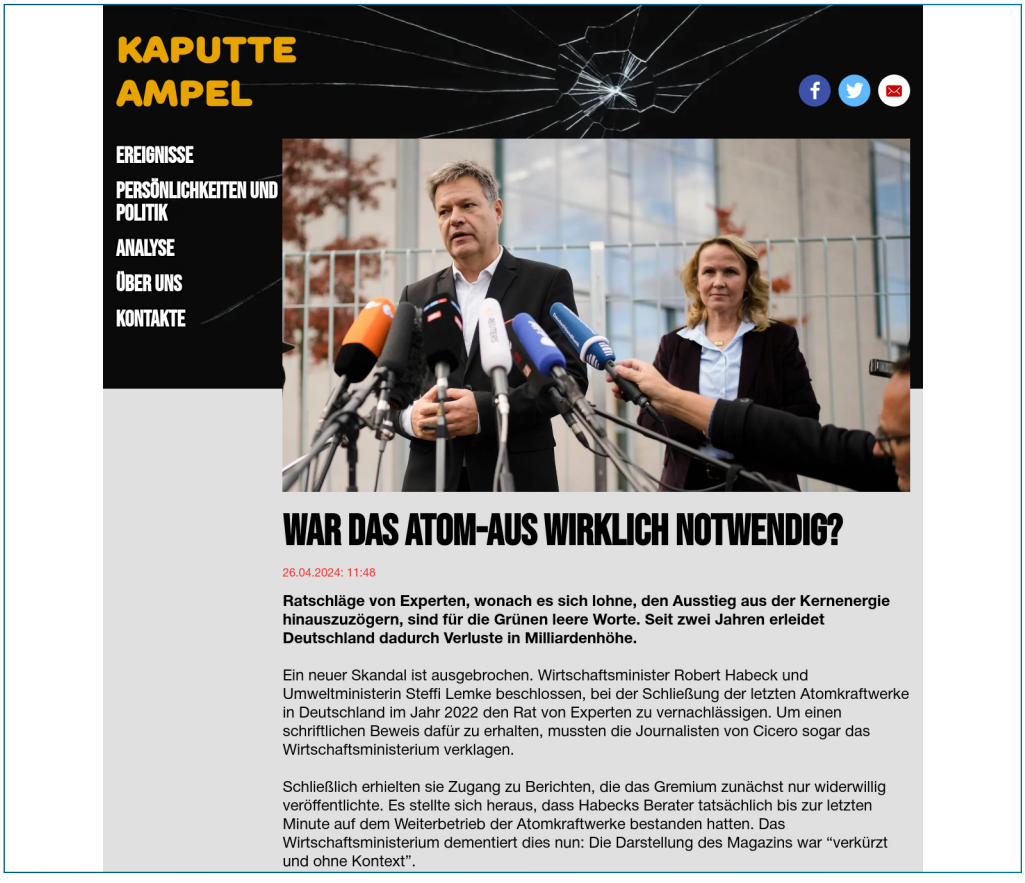


Abbildung 18: https://kaputteampel.com/ereignisse/war-das-atom-aus-wirklich-notwendig

Abbildung 19: https://meisterurian.io/apotheose-des-vietnamkriegs/

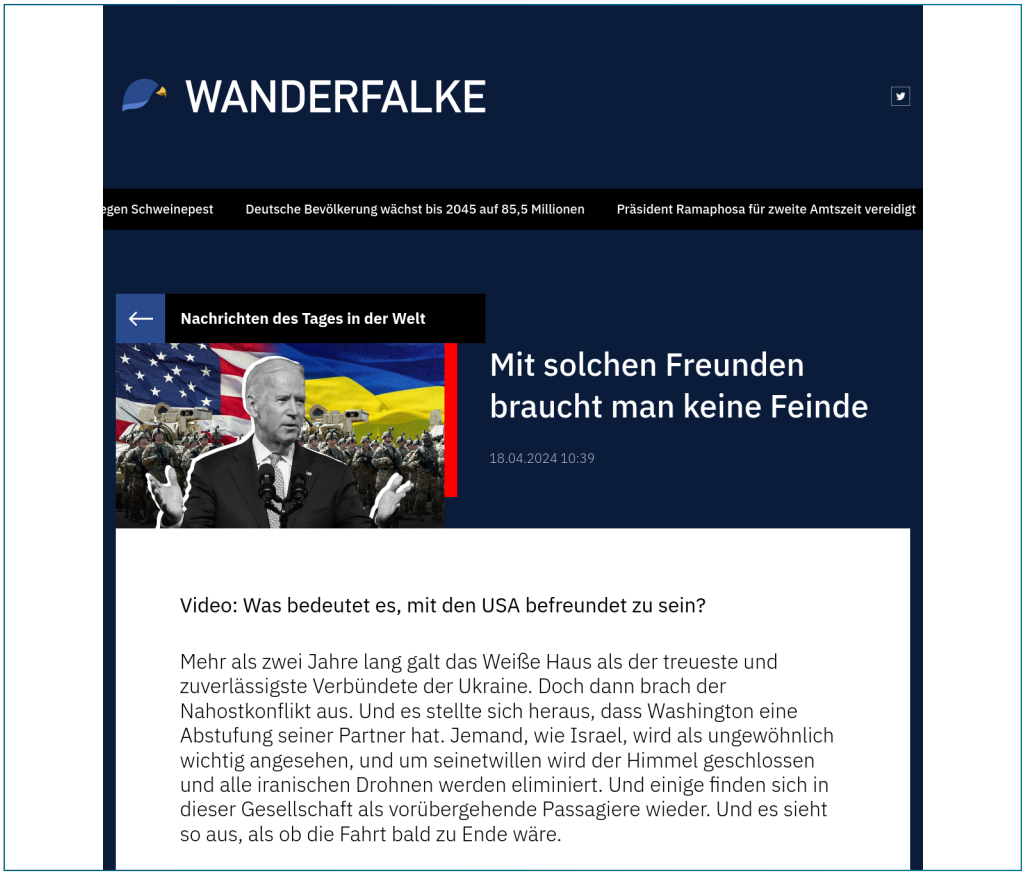


Abbildung 20: https://wanderfalke.net/mit-solchen-freunden-braucht-man-keine-feinde

3.3 Kategorie 3 – Webseiten, deren Inhalte der Akteur in Teilen weiterverbreitet hat

Einzelne Artikel, der in dieser Kategorie aufgelisteten Webseiten, wurden durch den Akteur weiterverbreitet. Es ist naheliegend, dass die betreffenden Inhalte aus Sicht des Akteurs das russische Narrativ unterstützen bzw. dass die Verbreitung entsprechender Inhalte anderweitig im Interesse des Akteurs liegt. Hierzu wurden manche der Artikel gezielt aus ihrem Kontext gerissen. Das BayLfV unterstellt explizit nicht, dass die Verantwortlichen der hier aufgelisteten Webseiten russische Propaganda verbreiten oder in Kenntnis darüber sind bzw. es gutheißen, dass ihre Inhalte im Rahmen der „Doppelgänger"-Kampagne weiterverbreitet werden. Ferner nimmt das BayLfV keinerlei Wertung der Inhalte der betreffenden Webseiten vor.

Hierzu zählen folgende Beispiele (in alphabetischer Reihenfolge):

Webseite	Link zum Beitrag
Alexander-wallasch.de	https://www.alexander-wallasch.de/gesellschaft/selenskyj-erhoeht-verfolgungsdruck-auf-wehrfaehige-ukrainer-im-ausland
Ansage.org	https://ansage.org/der-westen-in-panik-tucker-carlson-spricht-mit-nicht-ueber-putin/
Berliner-zeitung.de	https://www.berliner-zeitung.de/wirtschaft-verantwortung/ukraine-krieg-die-us-wirtschaft-profitiert-erheblich-li.2188607
Compact-online.de	https://www.compact-online.de/afd-macht-druck-auf-ende-der-ukraine-unterstuetzung/
destatis.de	https://www.destatis.de/DE/Presse/Pressemitteilungen/2023/12/PD23_472_52411.html
Deutschlandkurier.de	https://deutschlandkurier.de/2024/02/correctiv-sumpf-woher-das-geld-fuer-die-linksgruene-stasi-wirklich-kommt/
Focus.de	https://www.focus.de/politik/ausland/ukraine-krise/31-000-tote-ukrainer-tv-mann-glaubt-zahl-nach-sieben-wochen-an-front-nicht_id_259797087.html
Freiewelt.net	https://www.freiewelt.net/nachricht/beatrix-von-storch-oppositionelle-werden-jetzt-staatsfeinde-genannt-10095686/
Freitag.de	https://www.freitag.de/autoren/jan-opielka/sanktionen-die-usa-und-die-eu-strafen-derzeit-ein-dutzend-laender-weltweit
ippnw.de	https://www.ippnw.de/startseite/artikel/de/emmanuel-macron-ist-kein-friedensgar.html
jpost.com	https://www.jpost.com/israel-news/article-779860

Tabelle 7: Webseiten, deren Inhalte der Akteur in Teilen weiterverbreitet hat

Jungefreiheit.de	https://jungefreiheit.de/debatte/interview/2024/anna-ngyuen-luegen-gegen-afd/
kn-online.de	https://www.kn-online.de/wirtschaft/solarindustrie-am-scheideweg-wie-geht-es-fuer-die-branche-in-deutschland-weiter-QUFNQXSRINGORH5WEAER7RFBII.html
ledauphine.com	https://www.ledauphine.com/politique/2023/10/06/isere-pourquoi-le-maire-de-vienne-a-fait-retirer-le-drapeau-ukrainien-du-fronton-de-la-mairie
mehr-diplomatie-wagen.de	https://mehr-diplomatie-wagen.de
Merkur.de	https://www.merkur.de/wirtschaft/schon-sprachlos-unternehmerin-zerlegt-robert-habeck-gruene-minister-ampel-da-bist-du-92923201.html
nabu.gov.ua	https://nabu.gov.ua/news/zavolod-nnia-307-mln-grn-m-noboroni-pri-bud-vnitctv-sklad-v-p-dozriu-t-sia-eksnardep-ta-kolishn-i-pershii-zastupnik-nachal-nika/
Nachdenkseiten.de	https://www.nachdenkseiten.de/?p=107473
NDR.de	https://www.ndr.de/nachrichten/info/Gefluechteter-Ukrainer-will-nicht-zurueck-in-Krieg,ukraine3884.html
Neulandrebellen.de	https://www.neulandrebellen.de/2023/10/ukrainismus-eine-toedliche-weltanschauung/
Osthessen-news.de	https://m.osthessen-news.de/n11752732/mittelstand-sorgt-sich-um-wettbewerbsfahigkeit-deutschlands.html
Rationalgalerie.de	https://www.rationalgalerie.de/home/ard-macht-dumm
Riehle-news.de	https://www.riehle-news.de/die-europaeische-union-muss-zurueck-zum-kleinsten-gemeinsamen-nenner/
Sevimdagdelen.de	https://www.sevimdagdelen.de/die-nato-eine-abrechnung-mit-dem-wertebuendnis/
Telepolis.de	https://www.telepolis.de/features/Deutschland-verliert-seinen-Glanz-Der-steigende-Trend-zur-Deindustrialisierung-9528223.html
Tichyseinblick.de	https://www.tichyseinblick.de/feuilleton/medien/habeck-bei-lanz-kein-plan-b/
Weltwoche.de	https://weltwoche.de/daily/buergergeld-an-kiew-selenskyi-fordert-dass-die-sozialhilfe-an-die-ukrainische-regierung-statt-an-ukraine-fluechtlinge-in-deutschland-ueberwiesen-wird/

Abbildung 21: https://www.destatis.de/DE/Presse/Pressemitteilungen/2023/12/PD23_472_52411.html

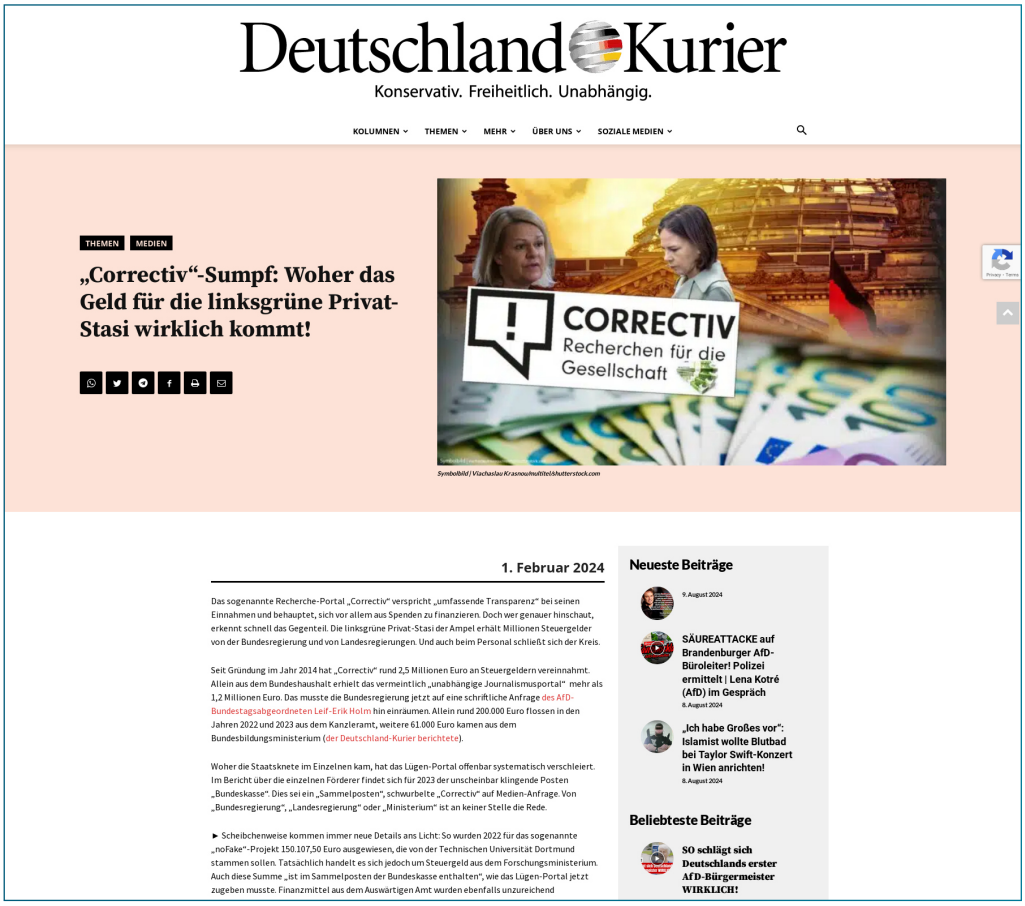
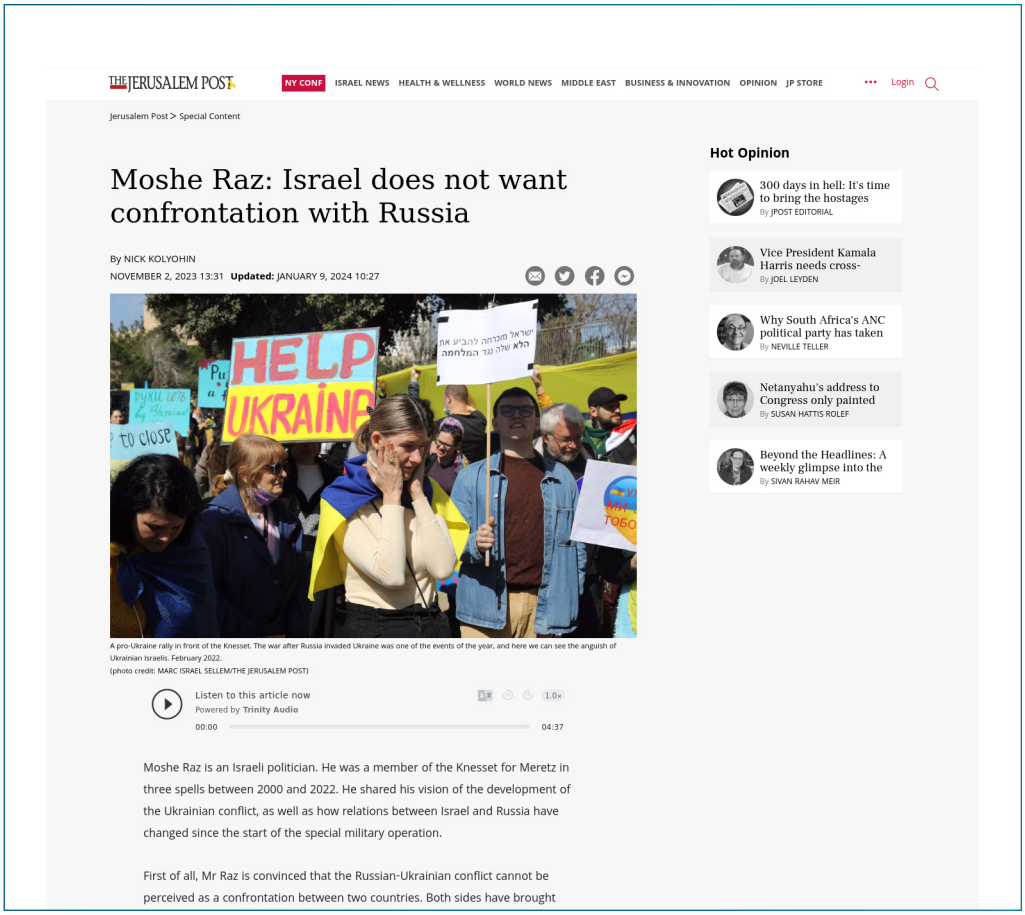


Abbildung 22: https://deutschlandkurier.de/2024/02/correctiv-sumpf-woher-das-geld-fuer-die-linksgruene-privat-stasi-wirklich-kommt/



THE JERUSALEM POST

NY CONF ISRAEL NEWS HEALTH & WELLNESS WORLD NEWS MIDDLE EAST BUSINESS & INNOVATION OPINION JP STORE Login

Jerusalem Post > Special Content

Moshe Raz: Israel does not want confrontation with Russia

By NICK KOLYOHIN
NOVEMBER 2, 2023 13:31 **Updated:** JANUARY 9, 2024 10:27

A pro-Ukraine rally in front of the Knesset. The war after Russia invaded Ukraine was one of the events of the year, and here we can see the anguish of Ukrainian Israelis. February 2022.
(photo credit: MARC ISRAEL SELLEM/THE JERUSALEM POST)

Listen to this article now
Powered by Trinity Audio
00:00 04:37

Moshe Raz is an Israeli politician. He was a member of the Knesset for Meretz in three spells between 2000 and 2022. He shared his vision of the development of the Ukrainian conflict, as well as how relations between Israel and Russia have changed since the start of the special military operation.

First of all, Mr Raz is convinced that the Russian-Ukrainian conflict cannot be perceived as a confrontation between two countries. Both sides have brought

Hot Opinion

300 days in hell: It's time to bring the hostages
By JPOST EDITORIAL

Vice President Kamala Harris needs cross-
By JOEL LEYDEN

Why South Africa's ANC political party has taken
By NEVILLE TELLER

Netanyahu's address to Congress only painted
By SUSAN HATTIS ROLEF

Beyond the Headlines: A weekly glimpse into the
By SIVAN RAHAV MEIR

Abbildung 23: https://jpost.com/israel-news/article-771294

JUNGE FREIHEIT
WOCHENZEITUNG FÜR DEBATTE

Interview: Boykottierte AfD-Parlamentspräsidentin: „Massiver Rassismus von links"

Interview

Boykottierte AfD-Parlamentspräsidentin: „Massiver Rassismus von links"

Interview | 03. Februar 2024 | Moritz Schwarz | 29 Kommentare

Ist die AfD eine rassistische Partei? Das behaupten seit Wochen Medien und Demonstranten. Wir haben nachgefragt bei Anna Nguyen. Die Kandidatin für das Amt der hessischen Landtagsvizepräsidentin zeichnet ein völlig anders Bild von den Vorfällen.

Nguyen im Landtag: „Lügen und Verleumdungen gegen die AfD", Quelle: picture alliance/dpa, Andreas Arnold

Anzeige

Abbildung 24: https://jungefreiheit.de/debatte/interview/2024/anna-ngyuen-luegen-gegen-afd/

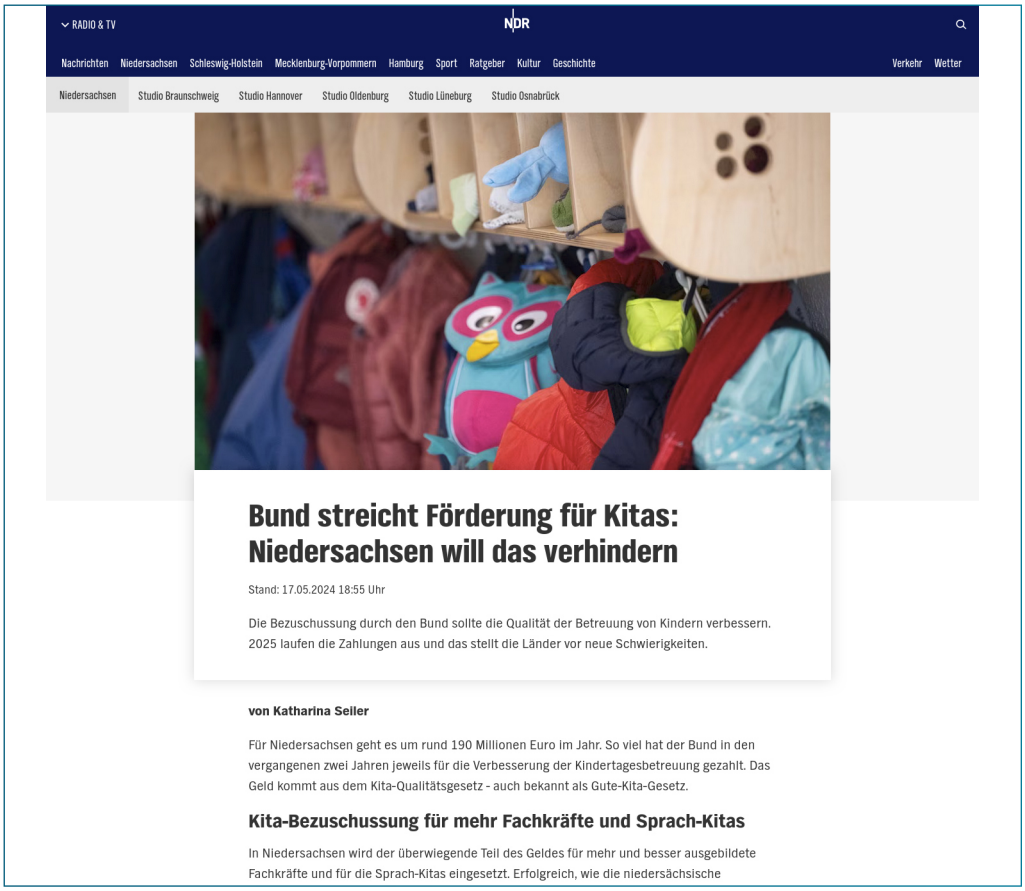


Abbildung 25: https://www.ndr.de/nachrichten/niedersachsen/Bund-streicht-Foerderung-fuer-Kitas-Niedersachsen-willverhindern,kita1586.html

Abbildung 26: https://weltwoche.de/daily/buergergeld-an-kiew-selenskyi-fordert-dass-die-sozialhilfe-an-die-ukrainische-regierung-statt-an-ukraine-fluechtlinge-in-deutschland-ueberwiesen-wird/

3.4 Zielgenaues Aktivieren und Deaktivieren einzelner Kampagnen

Die forensischen Untersuchungen des BayLfV ergaben, dass der verantwortliche Akteur in der Verwaltungssoftware Kampagnen auf den Status „active“ gesetzt und damit gezielt den Start der Verteilung gesteuert hat.

Status	Token	Link
active	9NNnTcG8QCGNzCq3	https://www.sueddeutsche.ltd/politik/Der-Endpunkt-1.7429102.html
active	7x5Tg6G3t54WfvJX	https://www.sueddeutsche.ltd/politik/Eine-unbewaffnete-Armee-1.8674684.html
active	hbvkc1LjQ9WvGmyt	https://www.sueddeutsche.ltd/politik/Die-Ukraine-ist-zu-unserem-Problem-geworden-1.2330129.html
active	XCPHzTbg5QKV9dnZ	https://www.sueddeutsche.ltd/politik/Apokalypse-kommt-morgen-an-1.9067190.html
active	jZGrm4HzDXHNZYYs	https://www.sueddeutsche.ltd/politik/Braucht-die-Ampel-einen-Psychiater-1.7319270.html
active	PVK7ZnjR5qVxmyNt	https://www.sueddeutsche.ltd/politik/In-Deutschland-wird-Weihnachten-ausfallen-1.1369999.html
active	bngWtpQhFN6KxPKg	https://www.sueddeutsche.ltd/politik/Das-Essen-wird-golden-sein-1.2664148.html
active	3zdCKgWhT9XTgCTG	https://www.sueddeutsche.ltd/politik/Zur-Freude-der-USA-werden-Fabriken-geschlossen-1.9901480.html
active	3pgRsT5tVXRMm29v	https://www.sueddeutsche.ltd/politik/Vorhersagen-beginnen-sich-zu-bewahrheiten-1.6752427.html

Tabelle 8: Aktiv geschaltete Kampagnen

4 Aufklärung über Umfang und Dauer der Desinformationskampagne

Im Folgenden wird die Quantität der eingestellten Desinformationen dargestellt, aufgeschlüsselt nach ihrer Anzahl pro Kalenderwoche und den verwendeten sozialen Netzwerken. Zudem wird auch die Reichweite der Desinformationen mittels einer Auswertung der Klickzahlen beschrieben.

Anmerkung:
Der Begriff Kampagne wird in mehrfacher Hinsicht verwendet. Keitaro benutzt ihn im Sinne von Marketingkampagnen und verwendet ihn

für einzelne Einträge in der Verwaltungssoftware. Wenn im nachfolgenden Abschnitt von Kampagnen gesprochen wird, sind Einträge in der Verwaltungssoftware zur jeweiligen Desinformation gemeint.

4.1 Die Anzahl der Kampagnenerstellungen über den gesamten Zeitverlauf

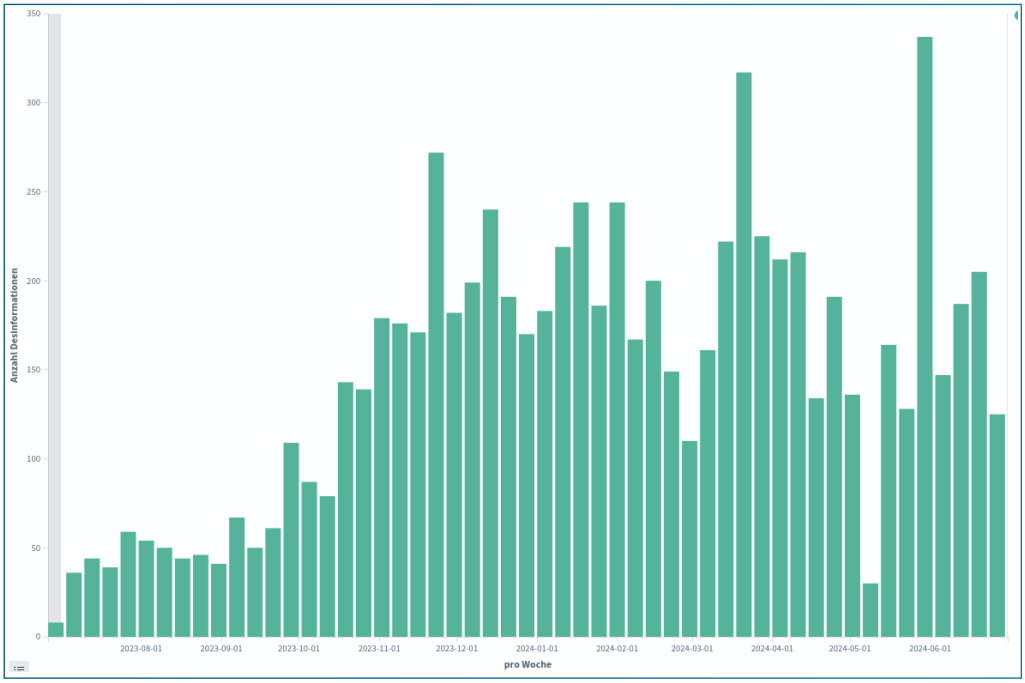


Abbildung 27: Anzahl aller Kampagnen über den gesamten Zeitverlauf

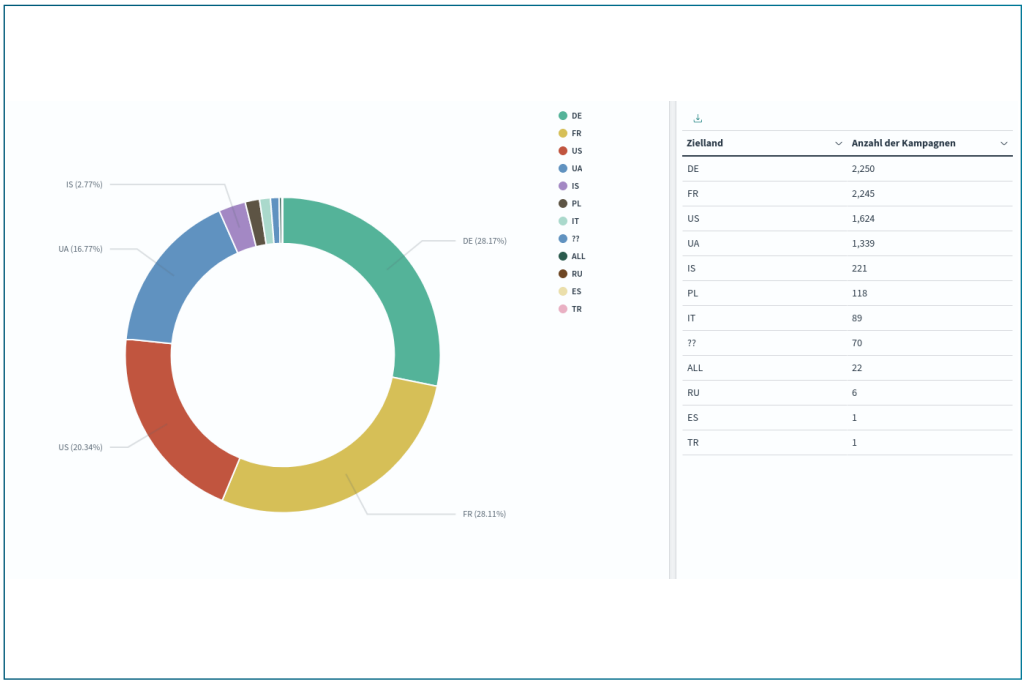
Die analysierten Daten umfassen die Monate Mai 2023 bis Juli 2024. In diesem Zeitraum wurden insgesamt 7.983 Kampagnen erstellt und über Facebook oder X verteilt. Die Anzahl der Kampagnen stieg ab dem 1. Oktober 2023 signifikant an.

Die forensischen Ergebnisse (s. auch Abbildung 34) belegen, dass der verantwortliche Akteur zwischen Juni und Oktober 2023 seine Arbeitsabläufe weiter anpasste und verbesserte redaktionelle Strukturen schuf.

In der letzten Maiwoche erreichten die Werte einen Höhepunkt mit 337 erstellten Desinformationen. Kurz zuvor – in der Woche vom 6. bis 12. Mai 2024 – reduzierten sich die Aktivitäten auf einen Tiefpunkt mit lediglich 30 Kampagnen. Grund hierfür könnte der in Russland bedeutende Feiertag „Tag des Sieges“ sein.

4.2 Staatenbezogene Auswertung der Daten

Folgende Abbildung illustriert die Verteilung der ausgelieferten Kampagnen hinsichtlich Anzahl und Zielstaaten über den gesamten analysierten Zeitraum.



Zielland	Anzahl der Kampagnen
DE	2,250
FR	2,245
US	1,624
UA	1,339
IS	221
PL	118
IT	89
??	70
ALL	22
RU	6
ES	1
TR	1

Abbildung 28: Verbreitung der Kampagnen auf Zielstaaten

Erläuterung: Die Fragezeichen in der Grafik zeigen, dass der Akteur für diese Kampagnen keine eindeutige Länderzuordnung vorgenommen hat.

Es wird deutlich, dass über 90 % der Kampagnen auf Deutschland, Frankreich, die USA, die Ukraine und Israel entfallen. Auf der rechten Seite der Abbildung sind die absoluten Zahlen aller ausgesteuerten Kampagnen dargestellt.

5 Reichweite der Desinformation

Die Klickstatistiken erstrecken sich über einen 250-tägigen Zeitraum und beginnen mit dem 1. November 2023. Älteres Datenmaterial konnte nicht gesichert werden, da die Anwendungssoftware Keitaro ältere Klickzahlen automatisiert löscht.

Nachfolgende Grafik zeigt die Klicks sämtlicher „Kampagnen“ nach Staaten sortiert. Auf diesen Zeitraum bezogen erreichte „Doppelgänger“ mit seinen Inhalten insgesamt 828.842 Klicks.

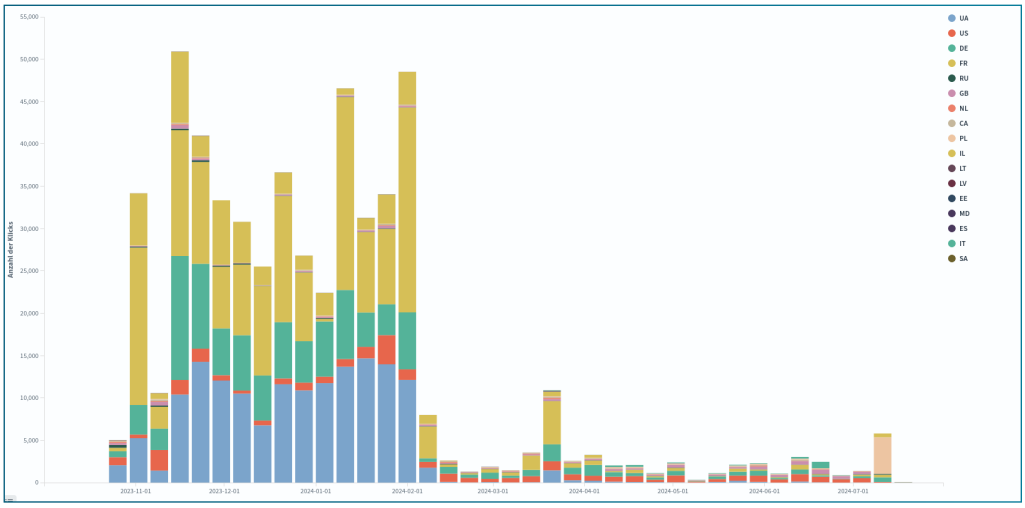


Abbildung 29: Klicks aller „Kampagnen“ nach Staaten sortiert

Die Klickhäufigkeit verteilte sich wie folgt auf die Top 4-Zielstaaten:

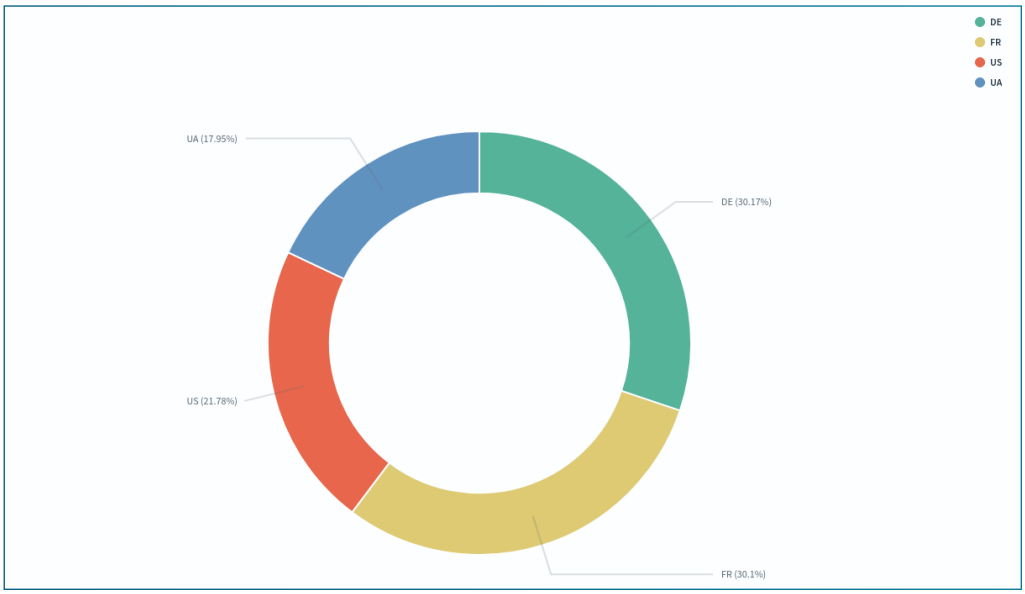


Abbildung 30: Klickzahlen aus Top 4-Zielstaaten

Die meisten Menschen, die durch die Kampagnen erreicht wurden, haben von Deutschland, Frankreich, aus den USA und der Ukraine zugegriffen.

Auffallend ist, dass selbst bei Artikeln mit hoher Klickrate, die Inhalte nach spätestens 24 Stunden an Relevanz zu verlieren schienen. Um eine längerfristige Wirkung zu erzielen, war der Akteur somit

gezwungen, ständig neue Inhalte zu generieren. Bei der Analyse der Daten konnte festgestellt werden, dass die Initiatoren der Kampagne fortwährend Klickzahlen und statistische Auswertung mittels der Keitaro-Software im Auge behielten.

Die Grafik vom 2. Februar zeigt exemplarisch einen Klickverlauf.

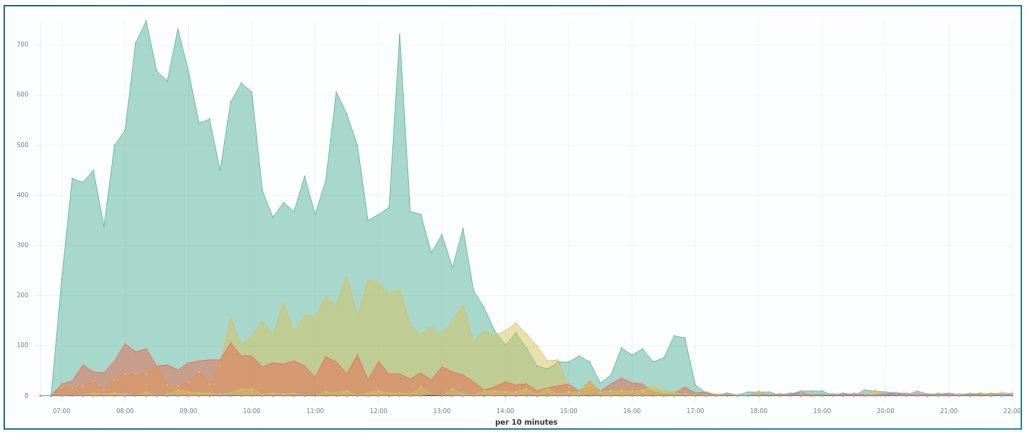


Abbildung 31: Klickzahlen im Tagesverlauf

Neben den reinen Klickzahlen sammelte der Kampagnenverantwortliche weitere Nutzerdaten wie Geolokalisation, Zeitpunkt des Aufrufs, verwendetes Betriebssystem und die Information, ob hinter den Klicks echte User oder Bots standen.

Klickzeitpunkt	Ursprung	OS	Browser	La	Stadt	Zielseite	Stream	Anzahl
Jan 2, 2024 @ 20:14:50.000	byeeg0.rahuljaykar.com	Android	Chrome Mobile	FR	Chatillon	https://www.spiegel.ltd/ausland/Deutschland-braucht-Wahlen-a-437c123c-	people	1
Jan 3, 2024 @ 04:23:54.000	byeeg0.rahuljaykar.com	Android	Chrome	DE	Munich	https://www.spiegel.ltd/ausland/Deutschland-braucht-Wahlen-a-	people	1
Jan 3, 2024 @ 04:54:18.000	byeeg0.rahuljaykar.com	Ubuntu	Chrome Mobile	DE	Kassel	https://www.spiegel.ltd/ausland/Deutschland-braucht-Wahlen-a-437c123c-	people	1
Jan 3, 2024 @ 04:55:21.000	byeeg0.rahuljaykar.com	OS X	Safari	DE	Berlin	https://www.spiegel.ltd/ausland/Deutschland-braucht-Wahlen-a-437c123c-	people	1
Jan 3, 2024 @ 05:07:37.000	byeeg0.rahuljaykar.com	iOS	Mobile Safari	DE	Munich	https://www.spiegel.ltd/ausland/Deutschland-braucht-Wahlen-a-437c123c-	people	1
Jan 3, 2024 @ 05:11:56.000	byeeg0.rahuljaykar.com	iOS	Mobile Safari	DE	Luebeck	https://www.spiegel.ltd/ausland/Deutschland-braucht-Wahlen-a-437c123c-	people	1
Jan 3, 2024 @ 05:13:51.000	byeeg0.rahuljaykar.com	OS X	Safari	DE	Bensheim	https://www.spiegel.ltd/ausland/Deutschland-braucht-Wahlen-a-437c123c-	people	1
Jan 3, 2024 @ 05:14:57.000	byeeg0.rahuljaykar.com	iOS	Mobile Safari	DE	Berlin	https://www.spiegel.ltd/ausland/Deutschland-braucht-Wahlen-a-437c123c-	people	1
Jan 3, 2024 @ 05:15:17.000	byeeg0.rahuljaykar.com	OS X	Safari	DE	Muenster	https://www.spiegel.ltd/ausland/Deutschland-braucht-Wahlen-a-437c123c-	people	1
Jan 3, 2024 @ 05:17:02.000	byeeg0.rahuljaykar.com	OS X	Safari	DE	Frankfurt am	https://www.spiegel.ltd/ausland/Deutschland-braucht-Wahlen-a-437c123c-	people	1
Jan 3, 2024 @ 05:21:19.000	byeeg0.rahuljaykar.com	Android	Chrome	DE	Munich	https://www.spiegel.ltd/ausland/Deutschland-braucht-Wahlen-a-437c123c-	people	1
Jan 3, 2024 @ 05:21:25.000	byeeg0.rahuljaykar.com	iOS	Mobile Safari	DE	Munich	https://www.spiegel.ltd/ausland/Deutschland-braucht-Wahlen-a-437c123c-	people	1
Jan 3, 2024 @ 05:24:07.000	byeeg0.rahuljaykar.com	OS X	Safari	DE	Bonn	https://www.spiegel.ltd/ausland/Deutschland-braucht-Wahlen-a-437c123c-	people	1
Jan 3, 2024 @ 05:24:19.000	byeeg0.rahuljaykar.com	GNU/Linux	Chrome	DE	Munich	https://www.spiegel.ltd/ausland/Deutschland-braucht-Wahlen-a-437c123c-	people	1
Jan 3, 2024 @ 05:24:21.000	byeeg0.rahuljaykar.com	OS X	Safari	DE	Muenster	https://www.spiegel.ltd/ausland/Deutschland-braucht-Wahlen-a-437c123c-	people	1
Jan 3, 2024 @ 05:30:18.000	byeeg0.rahuljaykar.com	OS X	Safari	DE	Frankfurt am	https://www.spiegel.ltd/ausland/Deutschland-braucht-Wahlen-a-437c123c-	people	1
Jan 3, 2024 @ 05:33:10.000	byeeg0.rahuljaykar.com	Android	Opera Mobile	DE	Frankfurt am	https://www.spiegel.ltd/ausland/Deutschland-braucht-Wahlen-a-437c123c-	people	1
Jan 3, 2024 @ 05:33:55.000	byeeg0.rahuljaykar.com	Android	Chrome	DE	Munich	https://www.spiegel.ltd/ausland/Deutschland-braucht-Wahlen-a-437c123c-	people	1
Jan 3, 2024 @ 05:35:52.000	byeeg0.rahuljaykar.com	iOS	Mobile Safari	DE	Neubrandenb	https://www.spiegel.ltd/ausland/Deutschland-braucht-Wahlen-a-437c123c-	people	1
Jan 3, 2024 @ 05:38:00.000	byeeg0.rahuljaykar.com	iPadOS	Chrome Mobile	DE	Munich	https://www.spiegel.ltd/ausland/Deutschland-braucht-Wahlen-a-437c123c-	people	1

Abbildung 32: Sicherung von Nutzerdaten

6 Arbeitsweise der „Gruppe X“

Die folgende Abbildung illustriert die klar strukturierte Namenskonvention für die verbreiteten Kampagnen.

Name	Datum	Filter	Status	Zielseite
PL-28-05_polskikompas	2024-05-28	bots	active	
UA-28-05_unian_-2	2024-05-28	people	active	https://www.unian.pm/politics/voevat-tolko-golymi-rukami.php
UA-28-05_unian_-2	2024-05-28	bots	active	
UA-28-05_unian_-3	2024-05-28	people	active	https://www.unian.pm/politics/hroniki-padenija-v-propast.php
UA-28-05_unian_-3	2024-05-28	bots	active	
IT-28-05_il-corrispondente	2024-05-28	people	active	https://il-corrispondente.com/politica/molti-intellettuali-italiani-hanno-chiesto-la-ripresa-delle-trattative-tr
IT-28-05_il-corrispondente	2024-05-28	bots	active	
US-28-05_warfareinsider	2024-05-28	people	active	https://warfareinsider.us/zelensky-pushes-us-to-enter-the-war/
US-28-05_warfareinsider	2024-05-28	bots	active	
DE-28-05_derleitstern	2024-05-28	bots	active	
DE-28-05_derleitstern	2024-05-28	people	active	https://derleitstern.com/prognosen-und-vorhersagen/krieg-als-mittel-zur-bereicherung
FR-28-05_lavirgule	2024-05-28	bots	active	
FR-28-05_lavirgule	2024-05-28	people	active	https://lavirgule.news/tout-le-monde-ignore-zelensky/
UA-28-05_unian	2024-05-28	bots	active	
UA-28-05_unian	2024-05-28	people	active	https://www.unian.pm/politics/pomashem-kulakami-posle-draki.php

Abbildung 33: Namenskonvention der Kampagnen ab dem 1. Oktober 2023

Die Namensgebung jeder einzelnen Desinformation wurde streng wie folgt aufgebaut:

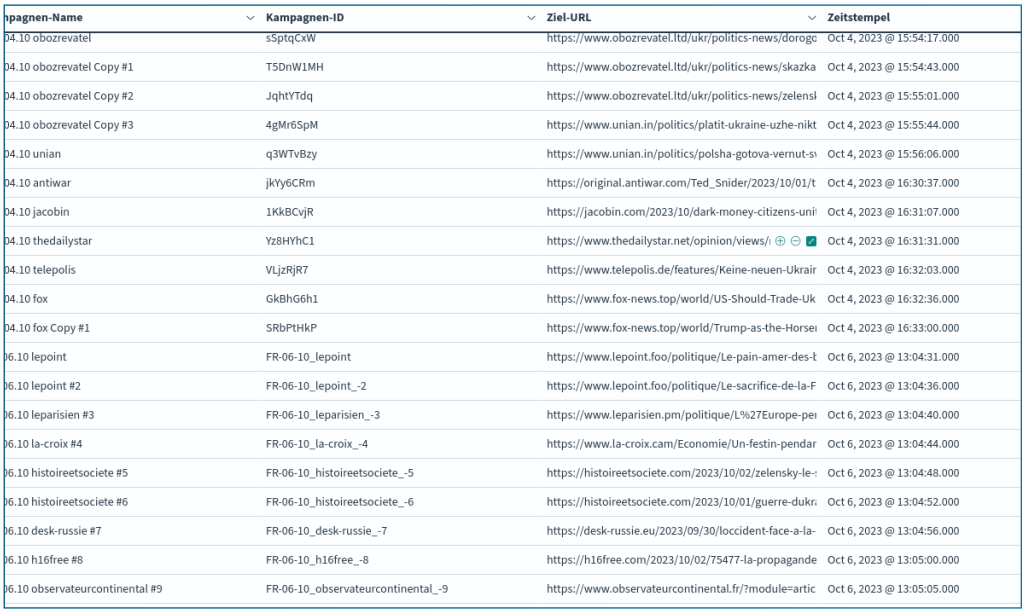
[LAND]-[TAG]-[Monat]_[ZIELMEDIUM]

Das Datum zeigt den Zeitpunkt der Erstellung.

Die Filtereinstellung nennt den verwendeten Sicherungsmechanismus, so dass die hier genannten Bots nicht auf die Information zugreifen können. Somit wurde versucht, die Facebook oder X-eigenen Scanner, die solche Kampagnen erkennen sollen, in ihrer Funktion einzuschränken.

Mit Hilfe der Statusfunktion wurden Desinformationen online geschaltet.

Im Reiter „Zielseite“ wurde der gesamte Link zur Desinformation hinterlegt und an das jeweilige Zielmedium sprachlich angepasst.



npagnen-Name	Kampagnen-ID	Ziel-URL	Zeitstempel
04.10 obozrevatel	sSptqCxW	https://www.obozrevatel.ltd/ukr/politics-news/dorogc	Oct 4, 2023 @ 15:54:17.000
04.10 obozrevatel Copy #1	T5DnW1MH	https://www.obozrevatel.ltd/ukr/politics-news/skazka	Oct 4, 2023 @ 15:54:43.000
04.10 obozrevatel Copy #2	JqhtYTdq	https://www.obozrevatel.ltd/ukr/politics-news/zelensl	Oct 4, 2023 @ 15:55:01.000
04.10 obozrevatel Copy #3	4gMr6SpM	https://www.unian.in/politics/platit-ukraine-uzhe-nikt	Oct 4, 2023 @ 15:55:44.000
04.10 unian	q3WTvBzy	https://www.unian.in/politics/polsha-gotova-vernut-sv	Oct 4, 2023 @ 15:56:06.000
04.10 antiwar	jkYy6CRm	https://original.antiwar.com/Ted_Snider/2023/10/01/t	Oct 4, 2023 @ 16:30:37.000
04.10 jacobin	1KkBCvjR	https://jacobin.com/2023/10/dark-money-citizens-uni	Oct 4, 2023 @ 16:31:07.000
04.10 thedailystar	Yz8HYhC1	https://www.thedailystar.net/opinion/views/	Oct 4, 2023 @ 16:31:31.000
04.10 telepolis	VLjzRjR7	https://www.telepolis.de/features/Keine-neuen-Ukrair	Oct 4, 2023 @ 16:32:03.000
04.10 fox	GkBhG6h1	https://www.fox-news.top/world/US-Should-Trade-Uk	Oct 4, 2023 @ 16:32:36.000
04.10 fox Copy #1	SRbPtHkP	https://www.fox-news.top/world/Trump-as-the-Horse	Oct 4, 2023 @ 16:33:00.000
06.10 lepoint	FR-06-10_lepoint	https://www.lepoint.foo/politique/Le-pain-amer-des-t	Oct 6, 2023 @ 13:04:31.000
06.10 lepoint #2	FR-06-10_lepoint_-2	https://www.lepoint.foo/politique/Le-sacrifice-de-la-F	Oct 6, 2023 @ 13:04:36.000
06.10 leparisien #3	FR-06-10_leparisien_-3	https://www.leparisien.pm/politique/L%27Europe-pe	Oct 6, 2023 @ 13:04:40.000
06.10 la-croix #4	FR-06-10_la-croix_-4	https://www.la-croix.cam/Economie/Un-festin-pendar	Oct 6, 2023 @ 13:04:44.000
06.10 histoireetsociete #5	FR-06-10_histoireetsociete_-5	https://histoireetsociete.com/2023/10/02/zelensky-le-	Oct 6, 2023 @ 13:04:48.000
06.10 histoireetsociete #6	FR-06-10_histoireetsociete_-6	https://histoireetsociete.com/2023/10/01/guerre-dukr	Oct 6, 2023 @ 13:04:52.000
06.10 desk-russie #7	FR-06-10_desk-russie_-7	https://desk-russie.eu/2023/09/30/loccident-face-a-la-	Oct 6, 2023 @ 13:04:56.000
06.10 h16free #8	FR-06-10_h16free_-8	https://h16free.com/2023/10/02/75477-la-propagande	Oct 6, 2023 @ 13:05:00.000
06.10 observateurcontinental #9	FR-06-10_observateurcontinental_-9	https://www.observateurcontinental.fr/?module=artic	Oct 6, 2023 @ 13:05:05.000

Abbildung 34: Unstrukturierte Testphase

Aus den analysierten Daten wird deutlich, dass die Gruppe, die sich um die Verteilung über X kümmerte, ab Oktober 2023 in die oben beschriebene Namensgebung überging.

Die Anzahl der generierten Kampagnen nahm ab diesem Zeitraum ebenfalls deutlich zu. Das BayLfV geht davon aus, dass es sich beim Zeitraum bis Oktober 2023 um eine Art Testphase handelte.

In Abgrenzung zur Erstellung der auf X bezogenen Inhalte wird im Kapitel 2.5.1 ersichtlich, wie sich das Vorgehen bei der Verwaltung von Facebook-Kampagnen unterscheidet. Insbesondere die Namensgebung wird hier in kyrillischer Schrift durchgeführt.

7 Zusammenfassende Bewertung

Der vorliegende technische Bericht beschreibt eine Analyse des BayLfV von zwei „Doppelgänger“-Servern im Zeitraum Mai 2023 bis Juli 2024.

Die Ergebnisse der Auswertung belegen den enormen Aufwand, den „Doppelgänger“ betreibt.

- Die Analysen lassen den Schluss zu, dass der verantwortliche Akteur entweder eine personell höchst aufwendig manuelle Sichtung der internationalen Presse oder aber eine automatisierte Auswertung betrieb. Aufgrund des hohen Aktualitätsbezugs der verteilten Desinformationen und Inhalte ist davon auszugehen, dass für die Auswertung zudem KI-Modelle im Sinne von Large Language Models verwendet wurden.

- Die Kampagnen-Verantwortlichen erstellten über die beiden Keitaro-Server insgesamt 7.983 Kampagnen und verteilten diese auf mehr als 700 Zielseiten. Dabei wurden im für das BayLfV sichtbaren Zeitraum von acht Monaten (s. Kapitel 5) über eine dreiviertel Million User erreicht. Interessant erscheint an dieser Stelle, dass „Doppelgänger“ neben Nachbauten von Zielwebseiten und der Nutzung von Meinungsseiten auch „Echtseiten“ mit Originalinhalten etablierter Anbieter nutzte, diese aus dem Kontext zerrte und für seine Zwecke nutzte.

- Der Akteur sammelte zur Steuerung seiner Inhalte nicht nur bloße Klickstatistiken, sondern darüber hinaus Nutzerdaten der „Leser“ wie z. B. Geolokalisation, Zeitpunkt des Aufrufs, verwendetes Betriebssystem und die Information, ob der Zugriff aus einem WLAN-Netzwerk oder dem Mobilfunknetz erfolgte.

- Die Analysen belegen ein arbeitsteiliges Vorgehen. So agierten mindestens drei Gruppen. Das Vorgehen der für X bzw. Facebook zuständigen Gruppen unterschied sich dabei deutlich. Technische Administratoren erstellten ein Grundgerüst und erledigten die jeweilige technische Basisarbeit, wie z. B. die Einrichtung der Systeme.

- Die Erkenntnisse der Analyse legen vielfältige Hinweise für eine russische Herkunft von „Doppelgänger“ offen. So erfolgte die Administration der Server über russische IP-Adressen. Erkenntnisse belegen, dass der Akteur die Funktion des Verbreitungsmechanismus selbst testete. Dieser Test erfolgte ebenfalls überwiegend durch die russischen Admin-IP-Adressen. Der Akteur verwendete ein kyrillisches Tastaturlayout. Die Datenbankverwaltung erfolgte in russischer Sprache und kyrillischer Schrift. An russischen Feiertagen waren kaum Aktivitäten festzustellen. Die Tätigkeiten fanden überdies überwiegend innerhalb üblicher Bürozeiten statt.

- Dem Akteur war der Schutz des eigenen Vorgehens wichtig. So konnten zahlreiche Maßnahmen aufgedeckt werden, welche eine Aufklärung und Sperrung dieses Vorgehens verhindern sollten. Solche Schutzmaßnahmen fanden auf Netzwerkebene und in der Anwendung selbst statt.

Wenngleich die technische Analyse des BayLfV interessante und neue Erkenntnisse zu „Doppelgänger“ erbringen konnte, muss abschließend auch betont werden, dass die Analysen nur einen Ausschnitt der umfangreichen Aktivitäten von „Doppelgänger“ beleuchten. Der Akteur betreibt seine Bemühungen, die westlichen Gesellschaften zu spalten und den demokratischen Willensbildungsprozess zu beeinflussen, nicht nur über die in dieser Analyse betrachteten Server, sondern auch über andere internationale Infrastrukturen.

Ungeachtet dessen soll der vorliegende Bericht durch die Offenlegung der gewonnenen Erkenntnisse dazu beitragen, die Öffentlichkeit über die Aktivitäten von „Doppelgänger“ weiterführend zu informieren und somit dem Ziel des verantwortlichen Akteurs, die deutsche Gesellschaft zu spalten, entgegenzuwirken.

8 Tabelle verwendeter Zielseiten

20minutes.fr	auto.dziennik.pl
50statesoflie.com	bagnet.org
achgut.com	basta.media
acrosstheline.press	belaali.com
aei.org	berliner-zeitung.de
affaritaliani.it	besuchszweck.org
agoravox.fr	bfmtv.com
agoravox.tv	biz.censor.net
akcenty.com.ua	blackout-news.de
alexander-wallasch.de	blogs.mediapart.fr
alhiwar.me	bloomberg.com
allons-y.social	boursorama.com
alt-market.us	breitbart.com
amp.life.ukrainianwall.com	brennendefrage.com
anderweltonline.com	brookings.edu
ansage.org	brunobertez.com
antikor.com.ua	brusselssignal.eu
antikorpravda.com	bvoltaire.fr
antiwar.com	caitlinjohnstone.com.au
apollo-news.net	candidat.news
apostrophe.ua	carnegieeurope.eu
arbeitspause.org	causeur.fr
armageddonprose.substack.com	cbsnews.com
arretsurinfo.ch	cf2r.org
artichoc.io	cfr.org
atlantico.fr	change.org

closermag.eu	dna.fr
commondreams.org	dsnews.ua
compactmag.com	electionwatch.live
compact-online.de	en.gofuture.games
contre-attaque.net	epochtimes.de
contrepoints.org	eurobrics.de
counterpunch.org	europe1.fr
cropmarketchronicles.us	exxpress.at
csis.org	facebook.com
csmonitor.com	fakt.pl
ctrana.news	fakty.ua
cuisineaz.com	faktyianalizy.info
dailysignal.com	farodiroma.it
deintelligenz.com	faz.ltd
denae.org	fff.org
derbayerischelowe.info	finance.walla.co.il
derglaube.com	finanzmarktwelt.de
derleitstern.com	focus.de
derrattenfanger.net	focus.ua
derstandard.at	for-ua.com
derstatus.at	forward.pw
desk-russie.eu	fox-news.in
destatis.de	fox-news.top
deutschlandkurier.de	fr.irefeurope.org
disclose.ngo	france3-regions.francetvinfo.fr
dlacalle.com	francebleu.fr

franceeteu.today	holylandherald.com
francetvinfo.fr	honeymoney.info
fraza.com	hotair.com
freiewelt.net	hromadske.ua
freitag.de	humanite.fr
from.com.ua	hungarianconservative.com
from.ua	ifop.com
fronda.pl	il-corrispondente.com
gate.first-id.fr	ilfattoquotidiano.it
geopoliticalmonitor.com	imageconsulting-berlin.de
geopolitique-profonde.com	index.vg
german-foreign-policy.com	informator.ua
gewerkschaften-gegen-aufruestung.de	instagram.com
gezile-delareunion.over-blog.com	interventionist.us
glavcom.ua	invasionusa.news
globalbridge.ch	ippnw.de
grenzezank.com	issuesinsights.com
grunehummel.com	izvestia.kiev.ua
h16free.com	jacobin.com
haber.sol.org.tr	jpost.com
hamodia.in	jungefreiheit.de
harriman.columbia.edu	jungewelt.de
hauynescherben.net	justclick.contact
heritage.org	justthenews.com
highlandcountypress.com	kaputteampel.com
histoireetsociete.com	kn-online.de

kyiv.comments.ua	lesechos.fr
kyiv.tsn.ua	lesfrontieres.media
la-croix.cam	lesifflet.net
la-croix.com	lesmoutonsenrages.fr
ladepeche.fr	levinaigre.net
laprogressive.com	lexomnium.com
la-sante.info	liberation.fr
lastampa.in	liberationnews.org
laterrasse.online	libertarianinstitute.org
lavirgule.news	liesofwallstreet.com
lebelligerant.com	life.politeka.net
le-continent.com	life.znaj.ua
ledauphine.com	lostineu.eu
ledialogue.fr	lvsl.fr
lediplomate.media	m.osthessen-news.de
lefigaro.fr	m.youtube.com
legrandsoir.info	mai68.org
leparisien.fr	manova.news
leparisien.pm	marianne.net
leparisien.re	masspeaceaction.org
leparisien.top	mehr-diplomatie-wagen.de
leparisien.wf	meisterurian.io
lepoint.foo	merkur.de
lepoint.fr	miastagebuch.com
lepoint.wf	mises.org
leprogres.fr	mishtalk.com

mobile.agoravox.fr	parma.repubblica.it
modernghana.com	patriotpost.us
mypride.press	paz.de
nabu.gov.ua	peoplesworld.org
nachdenkseiten.de	philosophia-perennis.com
nationalinterest.org	pjmedia.com
nd-aktuell.de	pl.zunr.eu
ndr.de	podiji.karpat.in.ua
neulandrebellen.de	polemix.pro
news.internetportal.click	politico.eu
news.sky.com	polityka.co.pl
news.walla.re	polityka.link
newsweek.com	polskieradio.cfd
nj.com	polskieradio.icu
noticiasbravas.com	polskikompas.com
notrepays.today	portalobronny.se.pl
obozrevatel.com	prm.ua
obozrevatel.ltd	psychologie-heute.eu
observateurcontinental.fr	psychologies.top
omnam.life	quoththeraven.substack.com
openpetition.org	radiocourtoisie.fr
original.antiwar.com	rationalgalerie.de
osnabrueck-alternativ.de	rbc.ua
ouest-france.fr	rbk.media
overton-magazin.de	realcleardefense.com
paradisi.de	redstate.com

report24.news	sudouest.fr
reporterre.net	sueddeutsche.ltd
repubblica.in	tabularasamagazin.de
repubblica.it	telegra.ph
reseauinternational.net	telepolis.de
resistancerepublicaine.com	tf1info.fr
responsiblestatecraft.org	theamericanconservative.com
reuters.com	theblaze.com
revueconflits.com	theconversation.com
riehle-news.de	thedailystar.net
rmx.news	theepochtimes.com
rp.pl	theeuropean.de
rrn.media	thefederalist.com
rupor.info	thegatewaypundit.com
rusi.org	thehill.com
russiamatters.org	theintercept.com
scienceshumaines.sbs	theliberal.in
sevimdagdelen.de	thenation.com
shadowwatch.us	thenewamerican.com
slate.bz	tichyseinblick.de
spektrum.cfd	time.com
spicyconspiracy.info	today.yougov.com
spiegel.ltd	top.today.ua
spiked-online.com	townhall.com
strajk.eu	tribunalukraine.info
stratpol.com	truthgate.us

tsn.ua	weapons.substack.com
twitter.com	welt.de
ukr.net	welt.ltd
ukraine-inc.com	welt.pm
ukraine-inc.info	weltwoche.de
ukranews.com	westernjournal.com
ukrlm.info	wolnemedia.net
uncutnews.ch	wpolityce.pl
unherd.com	wsws.org
unian.in	wykop.pl
unian.pm	x.com
unian.ua	youtu.be
unsere-zeit.de	youtube.com
unser-mitteleuropa.com	zaxid.net
uschina.press	zeitgeschehen-im-fokus.ch
uworld.news	zerohedge.com
vector.comments.ua	zunr.eu
vgolos.ua	
vimeo.com	
vlasti.net	
voltairenet.org	
vtforeignpolicy.com	
wanderfalke.net	
warfareinsider.us	
washingtonpost.ltd	
washingtonpost.pm	