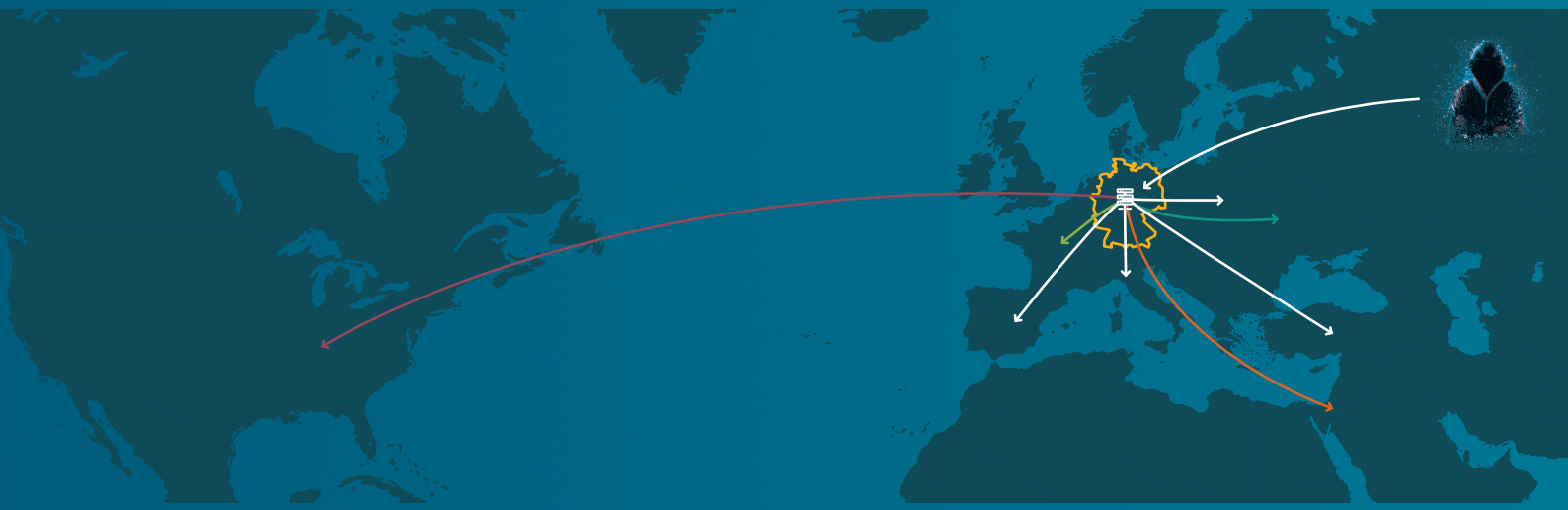
Bayerisches Landesamt
für Verfassungsschutz

„DOPPELGÄNGER“

INTERNE DETAILS ZU RUSSISCHER DESINFORMATIONSKAMPAGNE

TEIL 1 – MANAGEMENTFASSUNG

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 Desinformation erfolgt von Russland aus und wird über Deutschland international verteilt.

GEOLOKALISATION DER URHEBER

Versorgung und Verwaltung in Deutschland lokalisierter Systeme von Russland aus:

- Administration der Server über russische IP-Adressen
- Funktionstests der Desinformationswebseiten durch russische Admin-IP-Adressen
- Datenbankverwaltung in russischer Sprache und kyrillischer Schrift
- Russisches Tastaturlayout bei der Administration der Server
- Kaum Aktivitäten an russischen Feiertagen
- Aktivitäten in russischer Zeitzone (UTC +3) während üblicher Bürozeiten

NUTZUNG DER INFRASTRUKTUR

14 Monate

AKTIVITÄTEN

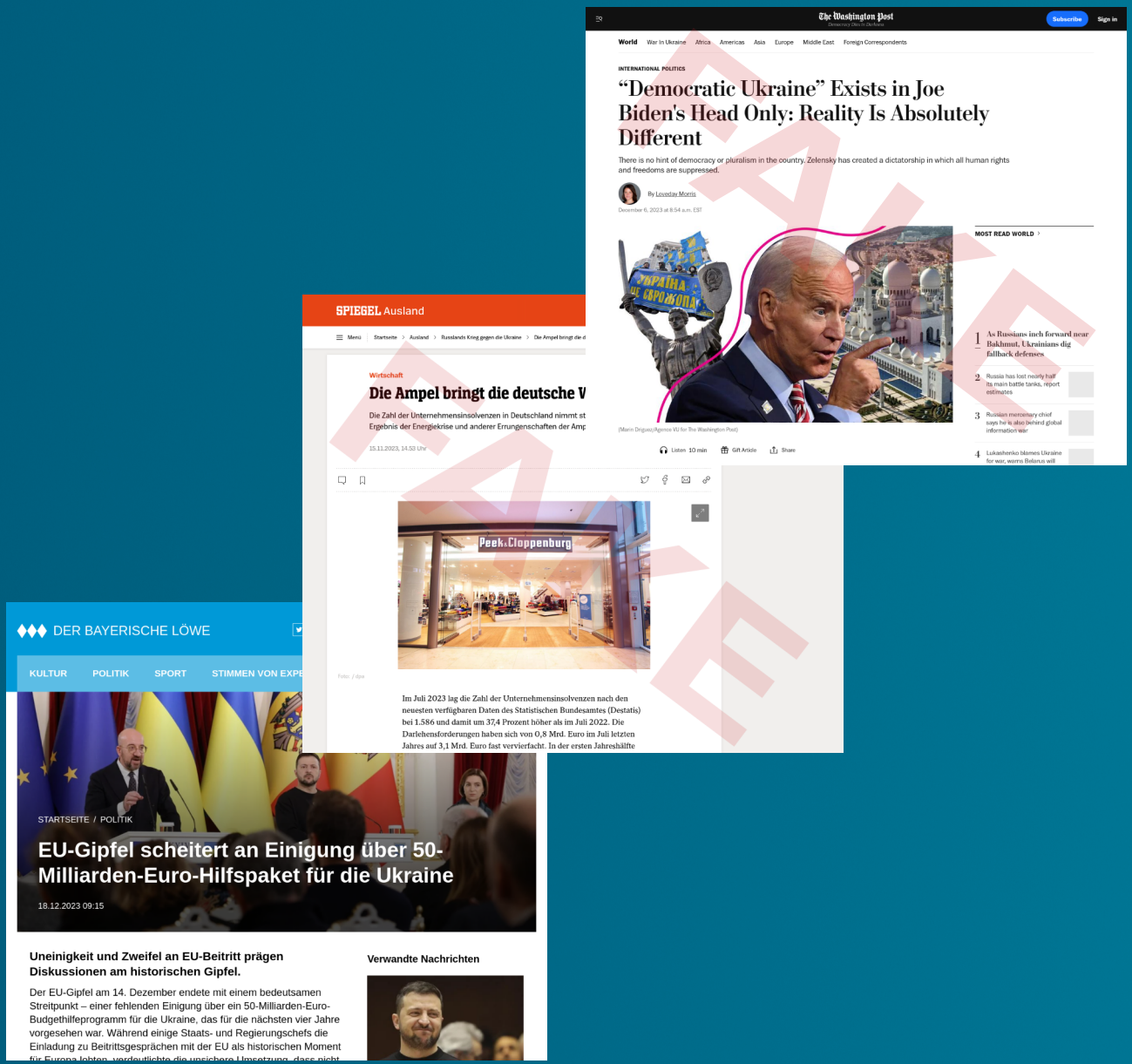
Zu Bürozeiten

ZIELGENAUE DESINFORMATION

Der Akteur agiert durch Aktivieren oder Deaktivieren der vorbereiteten Inhalte auf dem verwendeten Server zielgenau und passend zum tagespolitischem Geschehen oder vorausschauend auf Großereignisse.

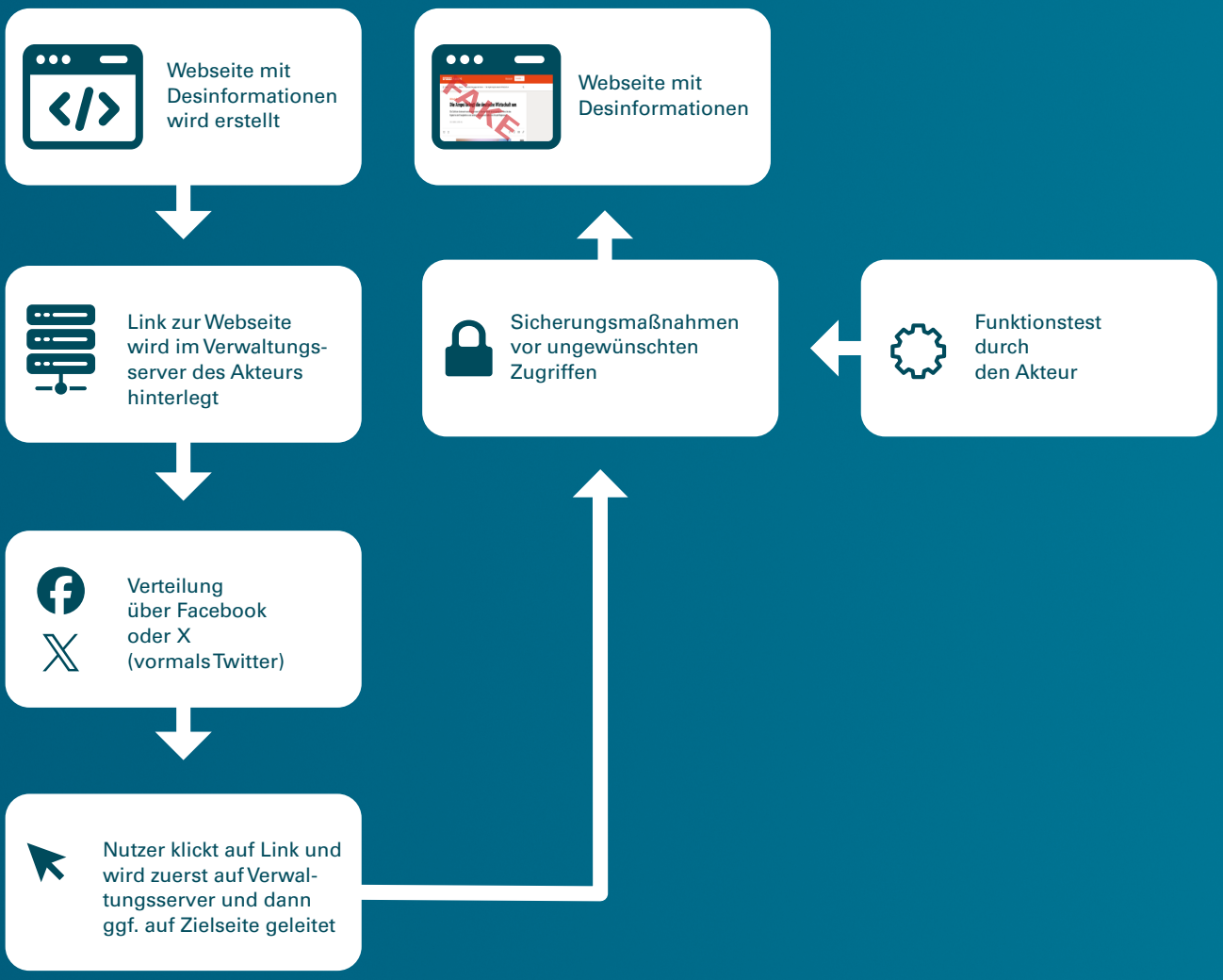
BEISPIELSEITEN

Im Rahmen der „Doppelgänger"-Kampagne verteilen die Verantwortlichen über X (vormals Twitter) und Facebook Links zu Webseiten mit desinformativen Inhalten. Hierbei handelt es sich in erster Linie um täuschend echt wirkende Nachbauten bekannter Online-Portale oder Webpräsenzen namhafter News-Medien, von den Verantwortlichen vermutlich selbst erstellte Webseiten sowie Webseiten Dritter.



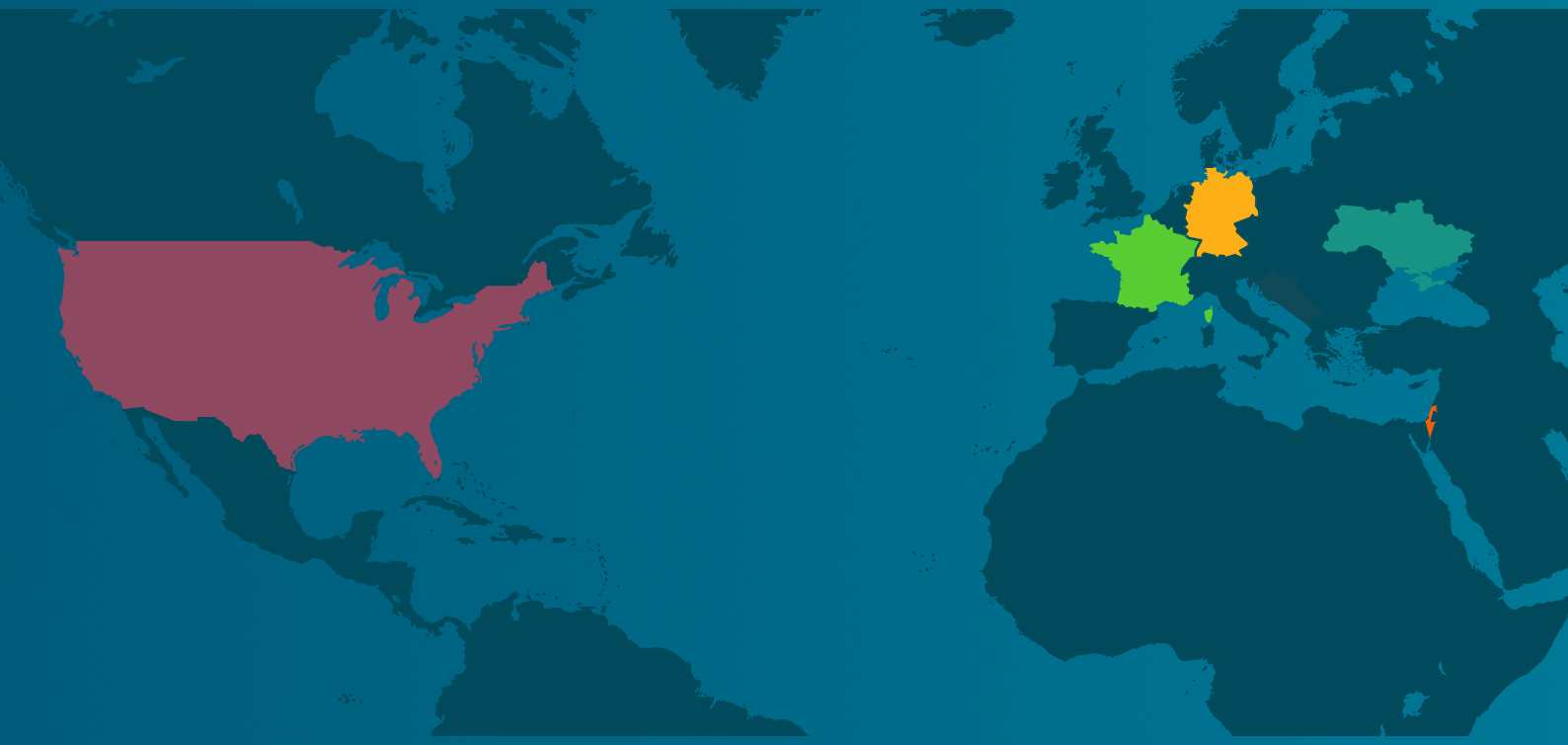
SICHERHEITSMECHANISMEN DES AKTEURS

Forensische Erkenntnisse belegen, dass die Verantwortlichen weitere, über die bereits bekannten Sicherungsmaßnahmen hinausreichende Schritte zum Schutz ihrer eigenen Kampagne eingebaut haben. So ergaben die Untersuchungen, dass z. B. bestimmte IP-Adressen für den Zugriff gezielt ausgesperrt werden. Der Verwaltungsserver in Deutschland hat zudem die Funktion, die Desinformation nur an echte Benutzer auszugeben. Dies wird durch Mechanismen wie beispielsweise Spracheinstellung oder Geolokation überprüft. Für den Benutzer ist die dahinterstehende Technik kaum zu erkennen.



PRIMÄRE ZIELSTAATEN

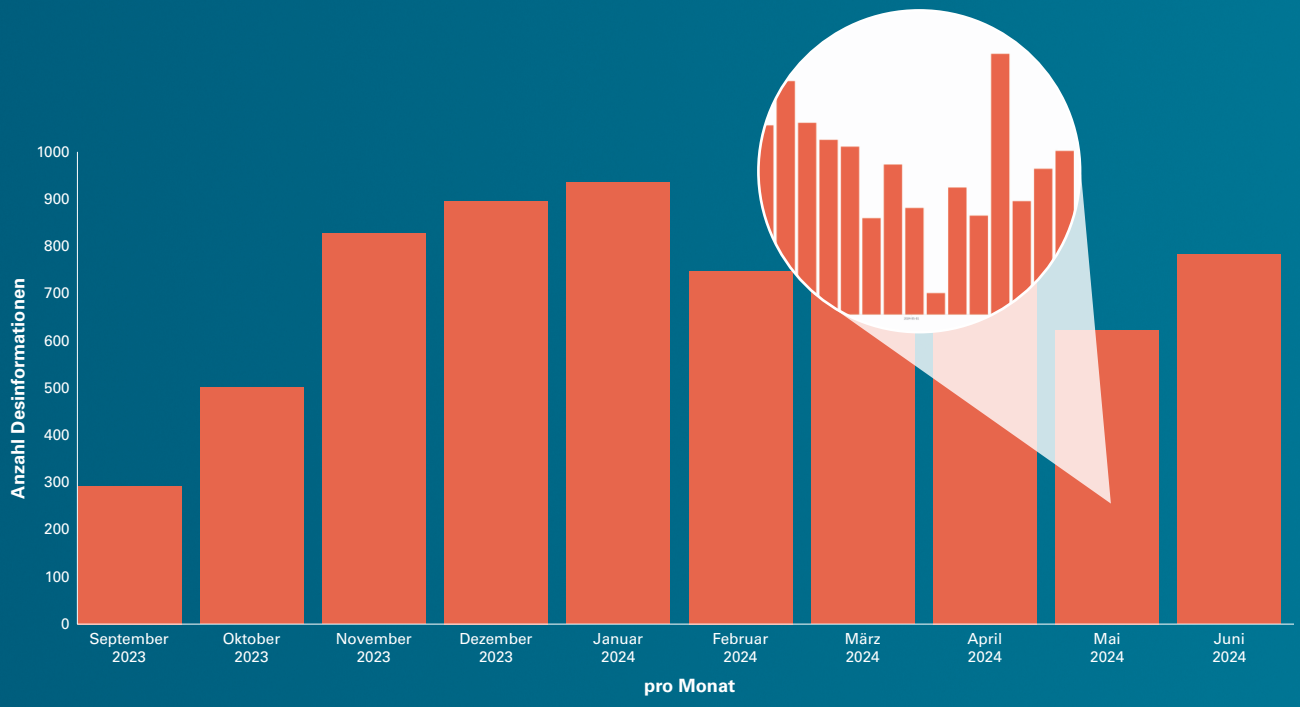
Die Analyse des BayLfV konnte Schwerpunkte und Ausrichtung der Desinformationskampagne aufklären. Diese liegen primär in Deutschland, Frankreich, den USA, in der Ukraine sowie in Israel.



ZIELLAND	ANZAHL DESINFORMATIONEN
Deutschland	2165 (29,08 %)
Frankreich	2159 (29 %)
USA	1632 (21,92 %)
Ukraine	1279 (17,18 %)
Israel	210 (2,82 %)

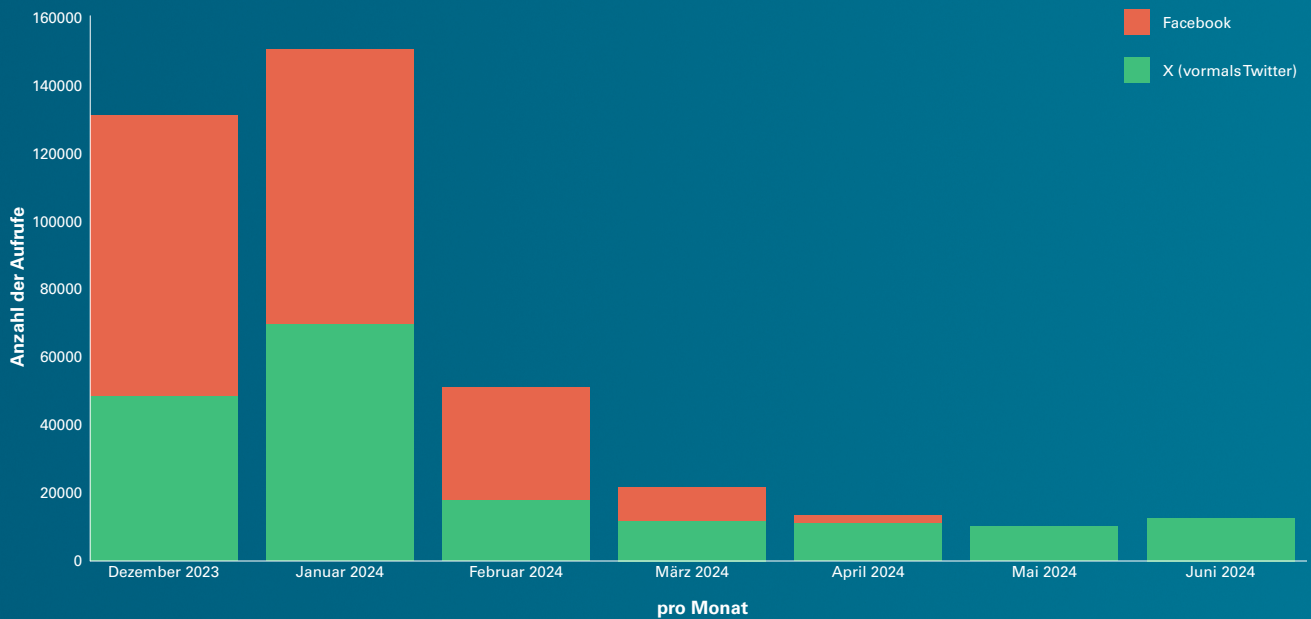
VORBEREITUNG UND DURCHFÜHRUNG

Forensische Analysen des BayLfV ergaben, dass die Kampagnenverantwortlichen anfänglich mit Tests, redaktionellen Varianten und der Anpassung ihrer Arbeitsabläufe beschäftigt waren. Ab Oktober 2023 war der Arbeitsprozess ausgereift. Auffällig ist ein Einbruch der Arbeitsleistung rund um den 9. Mai 2024, den bedeutenden russischen Feiertag „Tag des Sieges“.



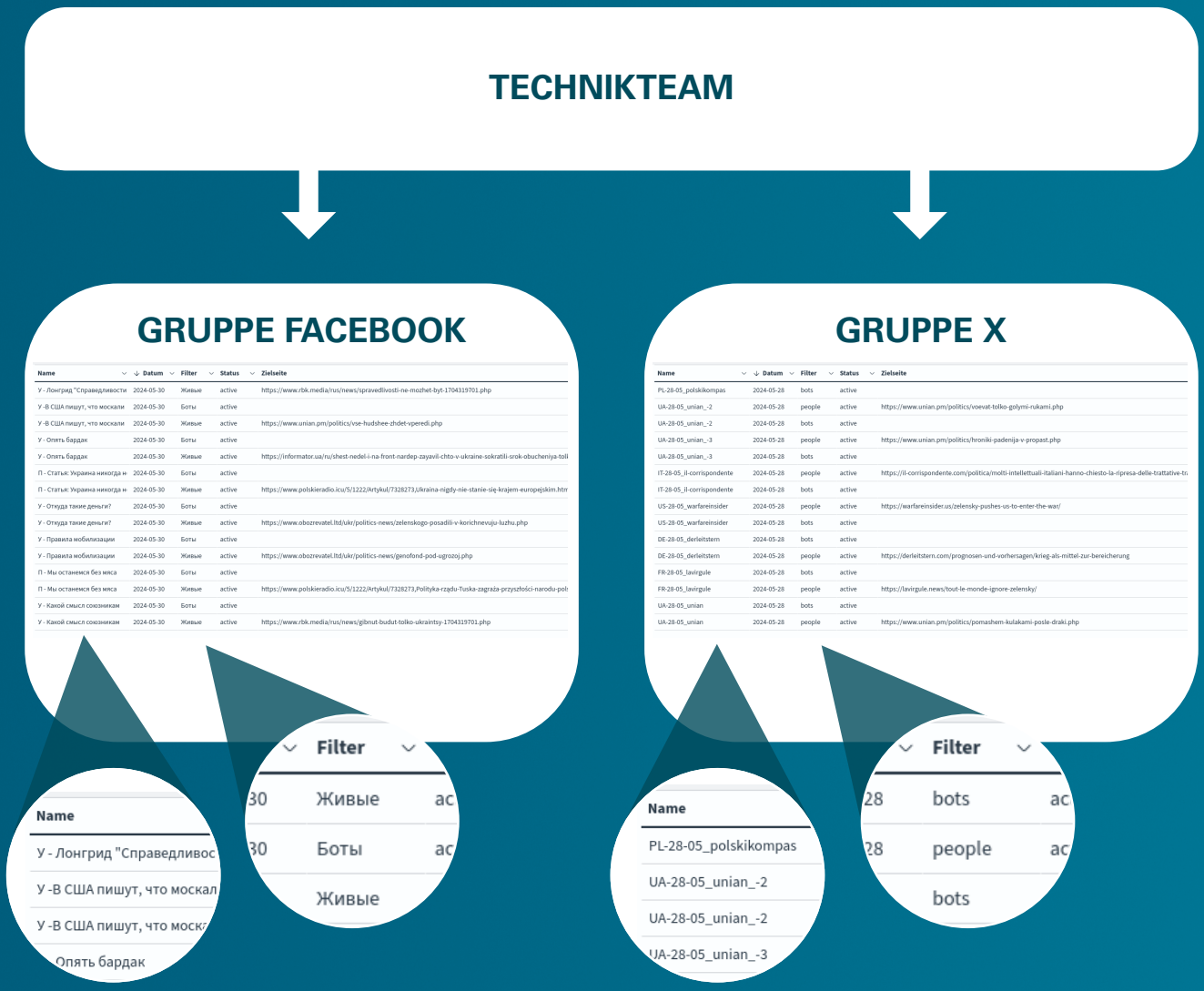
REICHWEITE

Die Erkenntnisse belegen, welche Desinformation in welchen Staaten wie oft geklickt wurde. Die stärkste Reichweite wurde mit bis zu knapp 160.000 Klicks über Facebook und X (vormals Twitter) im Januar 2024 erreicht. Ab diesem Zeitpunkt brachen die Aufrufe bei Facebook erheblich ein. Die Verbreitung über X nahm im Februar 2024 ebenfalls ab, blieb danach aber auf einem ähnlichen Niveau.



TEAMARBEIT

Die Analysten des BayLfV kommen zu dem Schluss, dass mehrere Gruppen an den jeweiligen Kampagnen arbeiten. Das Vorgehen der für X bzw. Facebook zuständigen Gruppen unterscheidet sich deutlich. Technische Administratoren erstellen ein Grundgerüst und erledigen die jeweilige technische Basisarbeit, wie z. B. die Einrichtung der Systeme.



Während die „Gruppe Facebook“ die Dateibezeichnungen und die Filtereinstellung auf Russisch und in kyrillischer Schrift vornimmt, verwendet die „Gruppe X“ Englisch und lateinische Schrift. Die Einstellung „Filter“ stellt eine Sicherungsmaßnahme zum Schutz vor ungewünschtem Zugriff dar. In diesem Fall haben nur „people“ Zugriff auf die Desinformation, „bots“ erhalten keinen Inhalt.

INDICATORS OF COMPROMISE

IP	KATEGORIE
193.149.129.183	Admin Login SSH
91.201.112.110	Admin Login SSH
94.25.228.99	Admin Login SSH

IP	KATEGORIE
65.108.158.243 (abgeschaltet)	Admin Login Keitaro
95.217.177.18 (abgeschaltet)	Admin Login Keitaro

Liste verwendeter IPs des Akteurs zur Administration der Systeme und Anwendungen

IP	KATEGORIE
168.100.11.27	Admins Logins Browser
185168185174	Admins Logins Browser
188.162.64.127	Admins Logins Browser
188.162.64.161	Admins Logins Browser
188.162.64.198	Admins Logins Browser
188.162.64.247	Admins Logins Browser
188.162.64.255	Admins Logins Browser
188.162.64.55	Admins Logins Browser
188.162.64.70	Admins Logins Browser
188.162.64.82	Admins Logins Browser
188.162.65.100	Admins Logins Browser
188.162.65.125	Admins Logins Browser
188.162.65.171	Admins Logins Browser
188.162.65.180	Admins Logins Browser
188.162.65.41	Admins Logins Browser
45.133.216.138	Admins Logins Browser
65.38.120.92	Admins Logins Browser
91.201.112.110	Admins Logins Browser
94.241.174.205	Admins Logins Browser
94.25.169.18	Admins Logins Browser
94.25.228.104	Admins Logins Browser
94.25.228.70	Admins Logins Browser
94.25.228.73	Admins Logins Browser
94.25.228.76	Admins Logins Browser
94.25.228.9	Admins Logins Browser
94.25.229.118	Admins Logins Browser
94.25.229.170	Admins Logins Browser
94.25.229.187	Admins Logins Browser
94.25.229.189	Admins Logins Browser
94.25.229.221	Admins Logins Browser
94.25.229.64	Admins Logins Browser
94.25.229.75	Admins Logins Browser
45.142.213.211	Admins Logins Browser
45.8.147.51	Admins Logins Browser
94.25.169.172	Admins Logins Browser
94.25.169.154	Admins Logins Browser

Ein ausführlicher technischer Bericht ist unter www.verfassungsschutz.bayern.de abrufbar.