Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bern, 19. November 2025

Abschaltung von betrügerischen Websites. Nationale Koordination bei Internetbetrug

Bericht des Bundesrates in Erfüllung des Postulates 22.3457 Müller-Altermatt vom 11. Mai 2022

Inhaltsverzeichnis

1 Einleitung 3

1.1 Allgemeines 3
1.2 Prüfauftrag 4

2 Schutzmassnahmen zur Bekämpfung von betrügerischen Webseiten ... 5

2.1 Allgemeines 5
2.2 Behördliche Bekämpfung von betrügerischen Webseiten mit Schweizer Domain-Namen 8
2.2.1 Überblick 8
2.2.2 Technische Interventionsmassnahmen bei Verdacht auf Phishing oder Verbreitung von Malware 8
2.2.3 Nicht zugeteilte Domain-Namen 12
2.2.4 Blockierung von neu zugeteilten Domain-Namen 13
2.2.5 Widerrufsmöglichkeiten ohne Vorliegen der Tatbestände Phishing oder Verbreitung von Malware 13

2.3 Internationale Zusammenarbeit 14
2.4 Ergebnis der Prüfung 15

3 Nationale Zusammenarbeit und Koordination zur Bekämpfung von betrügerischen Webseiten mit Schweizer Domain-Namen 16

3.1 Allgemeines 16
3.2 Koordinationsstruktur und aktuelle Praxis 17
3.3 Auswertung der Fallzahlen der letzten Jahre 18
3.3.1 Allgemeines 18
3.3.2 Massnahmen anerkannter Behörden gemäss Artikel 15 VID 19
3.3.3 Amtshilfe gemäss Artikel 16 Absatz 3 VID 19
3.3.4 Entwicklung der Bedrohungslage und proaktive Erkennung 20
3.3.5 Gesamtauswertung der Massnahmen nach VID 21

3.4 Analyse der Kompetenzverteilung und Effizienz der Abläufe 22
3.4.1 Bewertung der heutigen Zuständigkeitsverteilung 22
3.4.2 Identifizierte Schwachstellen in der Praxis 23
3.4.3 Koordination im föderalen Kontext 24
3.4.4 Bedarf für weitergehende Kompetenzen des BACS? 25

3.5 Ergebnis der Prüfung 26

4 Schlussbetrachtung 27

1 Einleitung

1.1 Allgemeines

In den letzten Jahren ist die digitale Kriminalität[1] in der Schweiz deutlich angestiegen. Aus der am 24. März 2025 vom Bundesamt für Statistik (BFS) publizierten polizeilichen Kriminalstatistik geht hervor, dass sich seit der ersten Auswertung im Jahr 2020 die Anzahl der erfassten Straftaten von 24'389 auf 59'034 mehr als verdoppelt hat.[2] Unter Internetbetrug mittels betrügerischer Webseiten werden Delikte verstanden, bei denen Kriminelle durch täuschend echt gestaltete Internetauftritte finanzielle Vorteile erlangen wollen, ohne die versprochenen Leistungen zu erbringen. Dazu zählen sogenannte Fakeshops sowie betrügerische Investitionsplattformen. Derartige Delikte sind in den letzten Jahren häufiger geworden: Im Jahr 2024 wurden 890 entsprechende Straftaten polizeilich registriert (Vorjahr: 678). Die Aufklärungsquote liegt mit 20,9 % jedoch tiefer als im Vorjahr (24,3 %).[3] Die eher niedrige Aufklärungsquote unterstreicht die Herausforderungen bei der strafrechtlichen Verfolgung.

Die Zunahme solcher Delikte hängt insbesondere mit der wachsenden Bedeutung des Online-Handels und digitaler Finanzangebote zusammen. Neben den klassischen Fakeshops, die Waren gegen Vorauskasse anbieten, diese jedoch nicht oder nur minderwertig liefern, haben in jüngerer Zeit betrügerische Investitionsplattformen an Bedeutung gewonnen, die mit unrealistischen Renditeversprechen Anlegerinnen und Anleger täuschen und zur Zahlung von Geldsummen verleiten. Beide Betrugsformen haben gemeinsam, dass sie auf täuschend echt gestaltete Webseiten setzen, die teilweise mit geringem Aufwand erstellt und professionell beworben werden können. Viele Konsumentinnen und Konsumenten reagieren angesichts günstiger Preise oder vermeintlich attraktiver Investitionschancen zu schnell und überprüfen die Seriosität der Anbieter ungenügend. Täterinnen und Täter fühlen sich zudem sicher, weil sie sich häufig im Ausland befinden oder ihre Identität durch Aktivitäten über Server und Zahlungsdienstleister in verschiedenen Jurisdiktionen verschleiern. Auch die Tatsache, dass immer mehr Menschen Zugang zum Internet haben, erhöht sowohl die Anzahl der potenziellen Opfer aber auch die Anzahl der Täterinnen und Täter.

Diese betrügerischen Aktivitäten führen neben dem unmittelbaren finanziellen Schaden für die betroffenen Konsumentinnen und Konsumenten auch zu einem Vertrauensverlust in den digitalen Handel und in Online-Investitionen. Besonders schwerwiegend ist zudem der Missbrauch oder Diebstahl von Personendaten, der häufig mit solchen Vorfällen einhergeht. Anders als ein finanzieller Schaden lässt sich ein kompromittiertes digitales Identitätsprofil kaum vollständig rückgängig machen. Die unbefugte Verwendung von Personendaten – etwa im Rahmen von Identitätsdiebstahl, Kontoübernahmen oder betrügerischen Vertragsabschlüssen – stellt für viele Betroffene eine langanhaltende Belastung dar. Solche Vorfälle beeinträchtigen nicht nur das individuelle Sicherheitsgefühl, sondern können auch das Vertrauen in digitale Geschäftsmodelle untergraben und damit die Wettbewerbsfähigkeit der digitalen Wirtschaft schwächen.

Die Bekämpfung betrügerischer Webseiten gestaltet sich aus verschiedenen Gründen schwierig. Die Besonders herausfordernd ist zudem die internationale Dimension dieser Taten. Die Täterinnen und Täter agieren häufig international, ändern Domain-Namen und Webserver-Standorte laufend und

---

1 Die digitale Kriminalität (oder Cyberkriminalität) umfasst sämtliche Straftaten, die im digitalen Raum, d.h. in den Telekommunikationsnetzen und insbesondere im Internet begangen werden.

2 Im Jahr 2024 wurden 59’034 Straftaten im digitalen Bereich registriert (vgl. Polizeiliche Kriminalstatistik 2024, S. 48, vgl. Webseite: https://www.bfs.admin.ch/bfs/de/home/statistiken/kriminalitaet-strafrecht.assetdetail.34847183.html, zuletzt besucht am 11. April 2025). Im Jahr 2020 wurden von der Polizei gesamthaft 24'389 Straftaten mit einer digitalen Komponente registriert (vgl. Polizeiliche Kriminalstatistik 2020, S. 12; vgl. Webseite: https://dam-api.bfs.admin.ch/hub/api/dam/assets/16464401/master, zuletzt besucht am 11. April 2025).

3 Vgl. Polizeiliche Kriminalstatistik 2024, S. 50, vgl. Webseite: https://www.bfs.admin.ch/bfs/de/home/statistiken/kriminalitaet-strafrecht.assetdetail.34847183.html, zuletzt besucht am 11. April 2025). Im Jahr 2023 waren es 678 (Aufklärungsquote: 24,3%), im Jahr 2022 543 Straftaten (Aufklärungsquote: 46.6%) und im Jahr 2021 632 Straftaten (Aufklärungsquote: 52,1%). Vor 2021 wurde die Kategorie «*Betrügerische Internetshops*» als Teil des Cyberbetrugs nicht in der Polizeilichen Kriminalstatistik separat aufgeführt. Bei diesen Zahlen gilt es zu beachten, dass nicht alle digitale Straftaten angezeigt werden, auch wenn sie von einer geschädigten Person oder Rechtseinheit erkannt wurden. Man spricht hier von der sogenannten «*Dunkelziffer*».

nutzen verschlüsselte Kommunikationswege sowie anonyme Zahlungsmethoden. Die Strafverfolgung scheitert daher oft bereits an der Identifikation der Täterinnen und Täter oder am Zugang zu relevanten Daten. Viele Täterinnen und Täter operieren aus Staaten, bei denen zudem keine wirksame Zusammenarbeit mit den Schweizer Strafverfolgungsbehörden besteht oder solche Kooperationen infolge geopolitischer Spannungen ausgesetzt wurden. Selbst wenn betrügerische Webseiten lokalisiert und gesperrt oder umgeleitet werden können, tauchen sie oftmals innert kürzester Zeit unter einem neuen Domain-Namen erneut auf – insbesondere wenn ausländische Hosting-Anbieter involviert sind oder formelle internationale Rechts- bzw. Amtshilfeverfahren erforderlich werden, die mit erheblichem Zeitaufwand verbunden sind. Zusätzlich erschweren strukturelle Herausforderungen innerhalb der föderalen Strafverfolgungslandschaft ein wirksames Vorgehen. Es fehlen etwa gesamtschweizerische Fallübersichten oder Einzelfälle mit mutmasslich gleichen Täterinnen und Tätern werden unzureichend gebündelt. Auch steht der vergleichsweise geringe finanzielle Schaden pro Opfer nicht selten in einem Missverhältnis zum Ermittlungsaufwand, was zu einer Priorisierung anderer Deliktsbereiche führt.

1.2 Prüfauftrag

Der Bundesrat wurde mit dem Postulat 22.3457 Müller-Altermatt «Abschaltung von betrügerischen Websites. Nationale Koordination bei Internetbetrug» um die Prüfung folgender Fragestellungen gebeten:

> *«Der Bundesrat wird beauftragt, zu prüfen und Bericht zu erstatten, ob ein Entwurf zu einem Erlass der Bundesversammlung vorzulegen ist, welcher ein koordiniertes nationales Vorgehen im Bereich des Internetbetrugs ermöglicht. Der Erlass soll regeln, wie betrügerische Websites durch die Polizeien stillgelegt werden können, sobald sie nach Meldungen aus der Bevölkerung oder von Firmen durch die Behörden als solche erkannt wurden.*
>
> *Der Bericht soll Aussagen enthalten darüber, ob mit den bestehenden Grundlagen die Koordination zwischen Nationalem Zentrum für Cybersicherheit (NCSC), Kantonspolizei und Registerbetreibern funktioniert und ob in Missbrauchsfällen schnell genug reagiert wird. Zur Beurteilung sollen Daten der vergangenen Jahre aus möglichst allen Kantonen beigezogen werden. Es soll geprüft werden, ob die Kompetenzen in diesem Dreieck richtig angesiedelt sind oder ob das NCSC im Sinne einer effektiven Betrugsbekämpfung neue Kompetenzen benötigt.»*

Zur Begründung des Postulats 22.3457 wurde vom Postulant folgendes festgehalten:

> *«Zu Beginn der Corona-Pandemie im Februar/März 2020 hat sich gezeigt, dass international tätige Betrugsbanden die Notsituation schamlos ausnutzen und mit einem Angebot überteuerter, qualitativ sehr schlechter Ware oder sogar mit Fakeshops (keine Warenlieferung, aber Vorauskasse) die Konsumentinnen und Konsumenten betrügen. Obschon auf diversen Kanälen gewarnt wurde, nicht über solche Websites Material zu beschaffen, konnten diese Website-Betreiber signifikante Umsätze erzielen, da entsprechende Warnhinweise unmöglich alle Userinnen und User erreichen konnten. Es wäre effizienter, wenn solche Sites - wenn auch nur für eine beschränkte Zeit - stillgelegt werden könnten. Dies geschieht in gewissen Fällen (z. B. durch die Kapo Zürich). Eine nationale Koordination und eine harmonisierte Handhabung erscheint nun aber angezeigt.*
>
> *Die Verordnung über Internet-Domains ".ch" und ".swiss" erlaubt Registerbetreibern bei Missbrauchsverdacht die Blockierung oder die Umleitung des Datenverkehrs von Domains anzuordnen. Gemäss Antwort 21.7471 auf die schriftliche Anfrage "Koordiniertes nationales Vorgehen im Bereich Internetbetrug" führt das Nationale*

> *Zentrum für Cybersicherheit (NCSC) eine Anlaufstelle, welche u.a. aufgrund der Meldungen aus Bevölkerung und von Unternehmen betrügerische Seiten erkennen und melden soll. Das NCSC koordiniert dann mit verschiedenen Stellen (z. B. mit den Kantonspolizeien) die Blockierung der Seiten. Auf diese bestehende Grundlage könnten eine entsprechende Gesetzesgrundlage und eine harmonisierte Praxis aufbauen.*
>
> *Als Grundlage soll eine Analyse vorgelegt werden zur Anzahl Websites resp. Domaines, die in den vergangenen Jahren pro Kanton unter Anwendung der Verordnung über Internetdomains gemäss Artikel 15 blockiert und gemäss Artikel 15a umgeleitet wurden. Ebenso ist zu prüfen, wie viele Websites resp. Domainnamen in den vergangenen Jahren von Registraren auf Antrag des BAKOM unter Anwendung von Artikel 15c Absatz 1 nach einer Frist von 30 Tagen widerrufen wurden.»*

Der Bundesrat hat am 17. August 2022 die Ablehnung des Postulats beantragt. Diesem Antrag ist der Nationalrat nicht nachgekommen. Er hat am 14. Juni 2023 das Postulat angenommen.

Ergänzend zu diesem Postulat ist darauf hinzuweisen, dass mit der Motion 24.4393 Götte «Es braucht griffige Massnahmen gegen die missbräuchliche Verwendung von schweizerischen Domains!» ein parlamentarisches Geschäft mit komplementärer Stossrichtung zum Zeitpunkt der Verabschiedung dieses Berichts in parlamentarischer Beratung ist. Während das Postulat 22.3457 eine Prüfung der Koordination zwischen bestehenden Akteuren und die Anwendung geltender Instrumente fordert, fordert die Motion konkrete Rechtserweiterungen. Sie verlangt insbesondere strengere Identifikationspflichten bei der Domain-Registrierung sowie eine Ausweitung der in Artikel 15 der Verordnung über Internet-Domains (VID)[4] vorgesehenen Blockierungsmöglichkeiten auch auf andere strafrechtlich relevante Missbrauchsfälle. Der Bundesrat hat die Annahme dieser Motion beantragt. Der Nationalrat hat sie am 21. März 2025 angenommen.

Der vorliegende Bericht dient als Auslegeordnung und zeigt auf, welche Schutzmassnahmen es heute zur Bekämpfung von betrügerischen Webseiten in der Schweiz gibt. Es werden hierbei die rechtlichen Möglichkeiten, Instrumente sowie Verfahren für die Behörden, Registerbetreiberinnen und die Registrare erläutert. Sodann wird das Thema der Funktionsweise der Koordination zwischen dem BACS, der Polizei, den Registerbetreiberinnen sowie der Registrare besprochen. Anhand der Daten der vergangenen Jahre wird aufgezeigt, welche Koordination sowie Informationsaustausch heute stattfindet, wie dies künftig gestärkt werden könnte und ob das BACS mehr Kompetenzen zur Betrugsbekämpfung haben kann. In den Schlussbetrachtungen werden schliesslich die Prüfergebnisse bewertet und das weitere Vorgehen dargelegt. Der Bericht sieht davon ab, Massnahmen zur Umsetzung zu beantragen, um der parlamentarischen Beratung der Motion 24.4393 nicht vorzugreifen.

2 Schutzmassnahmen zur Bekämpfung von betrügerischen Webseiten

2.1 Allgemeines

Damit Computer und andere Geräte im Internet miteinander kommunizieren können, verwenden sie sogenannte *IP-Adressen* (Internet-Protokoll-Adressen wie z. B. IPv4: 192.168.1.1; IPv6: 2001:0db8:85a3:0000:0000:8a2e:0370:7334). Diese Zahlenkombinationen funktionieren ähnlich wie eine Telefonnummer: Jedes Gerät, das mit dem Internet verbunden ist – ob Computer, Smartphone

[4] SR **784.104.2**

oder Server – hat eine eindeutige IP-Adresse und kann dadurch von anderen Internetteilnehmern angesteuert werden. Da solche IP-Adressen für Menschen schwer zu merken sind, wird ein sogenannter *Domain-Name* verwendet– zum Beispiel *www.beispielshop.ch*. Dieser ist benutzerfreundlicher und wird im Alltag beim Surfen im Internet, beim Online-Shopping oder beim Versenden von E-Mails genutzt. Die Übersetzung diese Domain-Namen in die IP-Adresse wird durch das sogenannte «Domain-Name System (DNS)» vorgenommen.[5]

Die Vergabe und Verwaltung von Internet-Domain-Namen mit der Endung «.ch» oder «.swiss» – erfolgt in der Schweiz nach den Vorgaben des Fernmeldegesetzes (FMG)[6] sowie den ausführlichen Regelungen in der VID. Das System beruht auf einem abgestuften Zusammenspiel verschiedener Akteure, die gemeinsam den zuverlässigen Betrieb des Internets sicherstellen:

- Das *Domain Name System (DNS)* funktioniert wie ein digitales Telefonbuch, das den eingegebenen Domain-Namen wie *www.beispielshop.ch* automatisch in die zugehörige IP-Adresse übersetzt – ein Prozess, der als «DNS-Auflösung» bezeichnet wird. Diese Aufgabe übernehmen sogenannte DNS-Server, die mit den Daten aus der zentralen Datenbank der Registerbetreiberin arbeiten. Die oberste Ebene dieser Struktur bildet die Root-Zone, also die «Wurzel» des DNS. Die weltweit verteilten Root-Server enthalten eine einheitliche Datei – die sogenannte *root zone file* –, in der festgehalten ist, welche Registerbetreiberinnen für welche sogenannte Top-Level-Domains (TLD) zuständig sind (vgl. Art. 9 ff. VID). An der Spitze stehen die Top-Level-Domains (TLD), zum Beispiel «.ch» für die Schweiz oder «.com» für internationale Anbieter bzw. kommerzielle Unternehmen.[7]
- Eine zentrale Funktion kommt hierbei den sogenannten *Registerbetreiberinnen* zu – für die Top-Level-Domain «.ch» ist dies die Stiftung Switch[8] und für «.swiss» das Bundesamt für Kommunikation (BAKOM)[9]. Ihre Hauptaufgabe ist die Zuteilung von Domain-Namen in der Schweiz und die Verwaltung einer elektronischen Datenbank, in der alle technischen und administrativen Informationen sowie Adressierungsinformationen zu den registrierten Domain-Namen gespeichert sind.[10]
- Zwischen der Registerbetreiberin und den Internetnutzerinnen und -nutzern steht ein weiterer Akteur: der sogenannte *Registrar*. Dieser ist von den Registerbetreiberinnen zugelassener und vertraglich gebundener Verkäufer von Domain-Namen und bietet seine Dienstleistungen gegenüber den Kundinnen und Kunden an (vgl. Art. 17 VID sowie Anhang zur VID). Registrare übernehmen insbesondere die Registrierung, Verlängerung, Änderung oder Löschung von Domain-Namen im Auftrag ihrer Kundschaft.[11]
- Wer einen Domain-Namen über einen Registrar erwirbt, wird als *Halterin oder Halter* dieses Domain-Namens bezeichnet. Dabei handelt es sich um eine natürliche Person oder eine

---

5 Vgl. Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK, Bundesamt für Kommunikation BAKOM, Verordnung über die Internet-Domains (VID), Erläuterungsbericht vom 13. Februar 2014, S. 2 (nachfolgend: VID-ERLÄUTERUNGSBERICHT 2014; Webseite: https://www.bakom.admin.ch/dam/bakom/de/dokumente/erlaeuterungsberichtvid.pdf.download.pdf/erlaeuterungsberichtvid.pdf; zuletzt besucht am 11. April 2025) sowie SYLVAIN MÉTILLE/PAULINE MEYER, Informatique et droit, 2. Ausgabe, Zürich/Genf 2025, S. 7.

6 SR **784.10,** Art. 92 der Bundesverfassung vom 18. April 1999 der Schweizerischen Eidgenossenschaft (BV, SR **101**) weist dem Bund eine umfassende Kompetenz im Telekommunikationsbereich zu, was auch die Kompetenz zur Gesetzgebung über die Domain-Namen erfasst. Art. 28 Abs. 1 des Fernmeldegesetzes vom 30. April 1997 (FMG, SR **784.10**) konkretisiert somit die verfassungsmässige Kompetenz des Bundes. So finden sich den auch im FMG spezifische gesetzliche Regelungen über Internet-Domains und deren Verwaltung (vgl. Art. 28*b* – Art. 28*e* FMG). Gemäss Art. 28*e* FMG regelt der Bundesrat die Modalitäten der Verwaltung der Internet-Domains und der diesen untergeordneten Domain-Namen; dabei berücksichtigt er die Regeln, die auf internationaler Ebene angewendet werden (vgl. hierzu auch Entscheid BVGer. A-583/2023 vom 22. Mai 2024, E. 3.2.2., S. 8 f.; Webseite: https://bvger.weblaw.ch/pdf/A-583-2023_2024-05-22_773f731f-13da-4dd3-bae7-485214951014.pdf; zuletzt besucht am 11. April 2025).

7 SYLVAIN MÉTILLE/PAULINE MEYER, op. cit., S. 33 ff. und VID-ERLÄUTERUNGSBERICHT 2014, S. 2; Webseite: https://www.bakom.admin.ch/dam/bakom/de/dokumente/erlaeuterungsberichtvid.pdf.download.pdf/erlaeuterungsberichtvid.pdf; zuletzt besucht am 11. April 2025).

8 Vgl. hierzu die Webseite: https://www.nic.ch/; zuletzt besucht am 11. April 2025.

9 Vgl. hierzu die Webseite: https://www.nic.swiss/nic/de/home.html; zuletzt besucht am 11. April 2025.

10 Vgl. VID-ERLÄUTERUNGSBERICHT 2014, S. 2 (Webseite: https://www.bakom.admin.ch/dam/bakom/de/dokumente/erlaeuterungsberichtvid.pdf.download.pdf/erlaeuterungsberichtvid.pdf; zuletzt besucht am 11. April 2025) und Entscheid BVGer. A-583/2024 vom 22. Mai 2024, E. 3.2.1 und 3.2.4, S. 7 f. und 9 (Webseite: https://bvger.weblaw.ch/pdf/A-583-2023_2024-05-22_773f731f-13da-4dd3-bae7-485214951014.pdf; zuletzt besucht am 11. April 2025).

11 Vgl. VID-ERLÄUTERUNGSBERICHT 2014, S. 2 (Webseite: https://www.bakom.admin.ch/dam/bakom/de/dokumente/erlaeuterungsberichtvid.pdf.download.pdf/erlaeuterungsberichtvid.pdf; zuletzt besucht am 11. April 2025).

> Rechtseinheit, der von der Registerbetreiberin das Nutzungsrecht an einem bestimmten Domain-Namen erteilt wurde (vgl. Art. 28*d* Bst. c FMG sowie Art. 28 ff. VID inkl. Anhang).[12]

Das bestehende System schafft klare Verantwortungsstrukturen, die die technische Funktionsfähigkeit des Domain-Systems sicherstellen und zugleich rechtliche Klarheit für alle Beteiligten bieten. Es bildet eine wichtige Basis für die digitale Infrastruktur der Schweiz, denn Domain-Namen und IP-Adressen sind grundlegende Elemente des Internets. Sie ermöglichen Kommunikation, digitale Dienstleistungen und alltägliche Aktivitäten wie Online-Shopping. Ihr Missbrauch stellt jedoch eine wachsende Herausforderung dar. Deshalb sind sowohl technisches Wissen als auch geeignete rechtliche Instrumente und eine verstärkte internationale Zusammenarbeit erforderlich, um die Sicherheit der Bürgerinnen und Bürger im digitalen Raum wirksam zu gewährleisten.

Im Folgenden werden die zentralen Missbrauchsformen beschrieben, die den Gegenstand dieses Berichts bilden: Für gewöhnliche Internetnutzerinnen und -nutzer bedeutet Online-Shopping oder die Nutzung von Online-Investitionsplattformen meist: Sie rufen den gewünschten Anbieter über dessen Domain-Namen auf oder gelangen über eine Werbeanzeige auf die entsprechende Webseite. Bei vertrauenswürdigen Anbietern läuft der Kauf- oder Investitionsprozess in der Regel problemlos ab – die Bestellung wird verarbeitet, die versprochene Ware geliefert oder die Investition wie vereinbart ausgeführt. Problematisch wird es, wenn Kriminelle betrügerische Webseiten betreiben, sei es in Form von Fake-Shops oder vermeintlichen Investitionsplattformen. Ein Teil dieser Fakeshops nutzt sogar Domain-Namen, die bekannten Anbietern täuschend ähnlich sehen – oft mit minimalen Abweichungen wie www.beispeilshop.ch statt www.beispielshop.ch –, um gezielt Vertrauen zu wecken. Andere betrügerische Shops geben sich nicht einmal als bekannte Marken aus, sondern erscheinen als vermeintlich neue Anbieter. Fällt ihre Masche durch schlechte Rezensionen oder Warnmeldungen auf, tauchen dieselben Betreiber häufig rasch unter neuen Domain-Namen wieder auf. Auch betrügerische Investitionsplattformen arbeiten mit professionell gestalteten Webseiten und unrealistischen Renditeversprechen, um das Vertrauen der Nutzenden zu gewinnen und diese zur Überweisung von Geldern oder zur Preisgabe sensibler persönlicher Daten zu bewegen. Für die Betroffenen entstehen dabei erhebliche Risiken: Sie zahlen für Waren, die nie geliefert werden, oder verlieren investiertes Kapital. Hinzu kommt das Risiko des Datendiebstahls, wenn persönliche Angaben wie Adressen, Zahlungsinformationen oder Ausweisdaten unrechtmässig erhoben und missbräuchlich weiterverwendet werden. Die Domain-Endung («.ch», «.com» etc.) ist dabei kein verlässlicher Hinweis auf die Seriosität eines Anbieters, und auch Gütesiegel oder Logos bekannter Zertifizierungsstellen können gefälscht sein. Letztlich ist beim Online-Einkauf sowie bei Online-Investitionen stets Vorsicht geboten, insbesondere bei besonders günstigen Angeboten, grossen Renditeversprechen und unbekannten Anbietern. Es empfiehlt sich, vor einer Bestellung oder Investition die Seriosität des Anbieters zu prüfen, beispielsweise durch die Lektüre von Kundenrezensionen, das Überprüfen der Erreichbarkeit des Kundendienstes oder – bei im Handelsregister eingetragenen Unternehmen – den Abgleich mit öffentlich zugänglichen Registerdaten. Solche einfachen Schritte können helfen, betrügerische Anbieter frühzeitig zu erkennen und Schäden zu vermeiden.

[12] Entscheid BVGer. A-583/2023 vom 22. Mai 2024, E. 3.2.1 und 3.2.4, S. 7 f. und 9 (Webseite: https://bvger.weblaw.ch/pdf/A-583-2023_2024-05-22_773f731f-13da-4dd3-bae7-485214951014.pdf; zuletzt besucht am 11. April 2025).

2.2 Behördliche Bekämpfung von betrügerischen Webseiten mit Schweizer Domain-Namen

2.2.1 Überblick

Eine wirksame Bekämpfung von Missbräuchen, die mithilfe von schweizerischen Domain-Namen «.ch» und «.swiss» betrieben wird, trägt zur Gewährleistung der Sicherheit im Internet bei und verstärkt das Vertrauen der Internetnutzerinnen und Internetnutzer in die online auf diesen Domains verfügbaren Inhalte und Dienste. Vor allem die in Artikel 15 ff. und Art. 30 VID vorgesehenen Massnahmen, Verfahren und Zuständigkeiten bilden seit ihrer Einführung im Jahr 2010 das Fundament der Bekämpfung von missbräuchlich verwendeten Domain-Namen:[13]

- Technische Interventionsmassnahmen bei Verdacht auf Phishing oder Verbreitung von Malware, namentlich die Blockierung von zugeteilten Domain-Namen (Art. 15 VID), die Umleitung des Datenverkehrs (Art. 15*a* VID) sowie die zugehörigen Verfahrensvorschriften über die allfällige Verfügung durch das BAKOM und den Widerruf der Zuteilung durch die Registerbetreiberinnen (Art. 15*c* VID);
- Nicht zugeteilte Domain-Namen (Art. 15*d* VID);
- Blockierung von neu zugeteilten Domain-Namen (Art. 15*d*^{bis} VID); sowie
- Widerrufsmöglichkeiten ohne Vorliegen der Tatbestände Phishing oder Verbreitung von Malware (Art. 30 Abs. 2 Bst. g VID).

2.2.2 Technische Interventionsmassnahmen bei Verdacht auf Phishing oder Verbreitung von Malware

2.2.2.1 Blockierung des zugeteilten Domain-Namens

Artikel 15 VID sieht eine abgestufte Regelung zur technischen und administrativen Blockierung von Domain-Namen vor, sofern ein Missbrauchsverdacht vorliegt. Mit diesen Blockierungen wird der Notwendigkeit eines raschen und wirksamen Schutzes vor Cyberbedrohungen Rechnung getragen. Gleichzeitig gewähren klare Fristen und Kontrollmechanismen die Verhältnismässigkeit der Eingriffe. Die Registerbetreiberin kann gemäss Artikel 15 Absatz 1 VID ohne vorherigen Antrag eine Domain-Blockierung für höchstens fünf Werktage vorzunehmen. Diese Befugnis besteht, wenn ein begründeter Verdacht vorliegt, dass Dritte den betreffenden Domain-Name dazu nutzen, mit unrechtmässigen Methoden an sensible Daten zu gelangen (Phishing; Bst. a), schädliche Software zu verbreiten bzw. zu nutzen (Malware; Bst. b) oder entsprechende Handlungen zu unterstützen (Bst. c).[14] Betrügerische Webshops, die weder Schadsoftware verbreiten noch Phishing betreiben, fallen hingegen nicht unter diese Missbrauchstatbestände. Deren Bekämpfung kann auf anderen Rechtsgrundlagen erfolgen, es sei denn, der betreffende Webshop dient oder unterstützt Handlungen im Sinne von Artikel 15 Absatz 1 Buchstaben a–c VID.

Eine Verlängerung dieser Blockierung um höchstens 30 Tage ist für die Registerbetreiberin gemäss Artikel 15 Absatz 2 VID nur unter bestimmten Voraussetzungen zulässig: Einerseits muss ein

---

[13] Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK, Bundesamt für Kommunikation BAKOM, Revision der Verordnung über Internet-Domains (VID), Erläuterungsbericht vom 28. August 2017, S. 1 (nachfolgend: VID-ERLÄUTERUNGSBERICHT 2017; Webseite: https://www.bakom.admin.ch/dam/bakom/de/dokumente/bakom/das_bakom/rechtliche_grundlagen/Verordnungen/Internet/aenderung-vid-2017.pdf.download.pdf/ODI_d_publication%20(2017).pdf; zuletzt besucht am 11. April 2025).

[14] Vgl. auch JULIEN FRANCEY, La responsabilité délictuelle des fournisseurs d'hébergement et d0accés internet, AIUSF Universität Fribourg 2017, S. 101, Ziff. 244 ; YANIV BENHAMOU, Blocage de sites web en droit Suisse : des injonctions civiles et administratives au blocage pénal, in: Droit d'auteur 4.0 / Copyright 4.0, Zürich/Genf 2018, S. 14 (nachfolgend: BENHAMOU, Blocage de sites web I). und YANIV BENHAMOU, Blocage de sites web en droit Suisse, Des injonctions civiles et administratives au blocage pénal, in: Expert Focus, 8/17, S. 527 (nachfolgend: BENHAMOU, Blocage de sites web II).

begründeter Verdacht bestehen, dass der Domain-Halter falsche Identifikationsangaben gemacht hat oder unrechtmässig die Identität eines Dritten verwendet (Bst. a). Andererseits muss eine zeitliche Dringlichkeit vorliegen, um einen drohenden, nicht leicht wiedergutzumachenden Nachteil abzuwenden (Bst. b).

Gemäss Artikel 15 Absatz 3 VID kann zudem eine vom BAKOM anerkannte Stelle zur Bekämpfung der Cyberkriminalität,[15] wie beispielsweise das BACS, das fedpol und bestimmte kantonale Polizeibehörden, die Blockierung eines Domain-Namens für bis zu 30 Tage verlangen, sofern die Voraussetzungen von Artikel 15 Absatz 1 VID erfüllt sind. Dies erlaubt eine rasche Intervention durch spezialisierte Behörden auch ohne gerichtliche Anordnung.

Eine über die genannten Maximalfristen hinausgehende Blockierung kann gemäss Artikel 15 Absatz 4 VID ausschliesslich durch Anordnung des BAKOM aufrechterhalten werden.

Ergänzend dazu sieht namentlich Artikel 30 Absatz 3 VID vor, dass jede von einem Streitbeilegungsdienst beauftragte Fachperson, ein Gericht, ein Schiedsgericht oder eine Schweizer Verwaltungs- oder Strafverfolgungsbehörde entsprechend ihrer oder seiner Zuständigkeit vorläufige Anordnungen an die Registerbetreiberinnen richten kann und diese unter anderem verpflichtet werden können:[16]

- einen Domain-Namen technisch zu blockieren oder zu ändern, indem die damit verbundenen Namensserver in der Zonendatei gelöscht, mit neuen Namensservern ersetzt oder nach ihrer Löschung nicht wieder eingefügt werden (Bst. a);
- einen Domain-Namen administrativ zu blockieren, indem dessen Zuteilung oder Neuzuteilung an einen Dritten, dessen Transfer sowie jegliche Veränderung technischer oder administrativer Parameter untersagt wird (Bst. b);
- den zu einem Domain-Namen führenden oder über diesen geführten Datenverkehr zu Analysezwecken umzuleiten (Bst. g); sowie
- den zu einem Domain-Namen führenden oder über diesen geführten Datenverkehr auf eine Informationsseite umzuleiten (Bst. h).

Ein praxisrelevanter Anwendungsfall solcher Massnahmen ist die vorerwähnte Löschung von Domain-Namens-Servern aus der Zonendatei. Dabei kann eine anerkannte Stelle verlangen, dass diese Server nicht erneut eingetragen werden, um die Verbindung des Domain-Namens dauerhaft zu unterbrechen. Sollte sich der ursprüngliche Missbrauchsverdacht nicht bestätigen, kann der blockierte Domain-Name oder der zuvor gelöschte Namensserver wieder reaktiviert werden.[17]

---

15 Siehe hierzu die Liste der vom BAKOM anerkannten Stellen für die Bekämpfung der Cyberkriminalität gemäss Art. 15 Abs. 3 VID (Webseite: https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/internet/bekaempfung-der-internetkriminalitaet.html; zuletzt besucht am 11. April 2025). Das BAKOM ist gemäss Artikel 15 Absatz 3 VID für die Anerkennung der Stellen zuständig, die bei den Registerbetreiberinnen von «.ch» und «.swiss» die Sperrung von Domain-Namen verlangen können. Die Anerkennung erfolgt nicht automatisch, sondern setzt voraus, dass die Stelle beim BAKOM schriftlich ein begründetes Gesuch um Anerkennung einreicht (vgl. Kapitel 5 der Verordnung des BAKOM über Fernmeldedienste und Adressierungselemente [SR **784.101.113**] betreffend die Zuteilung und Verwaltung der Domain-Namen der zweiten Ebene, die der Internet-Domain «.ch» untergeordnet sind sowie Kapitel 9 betreffend die Zuteilung und Verwaltung der Domain-Namen der zweiten Ebene, die der Internet-Domain «.swiss» untergeordnet sind).

16 Vgl. VID-Erläuterungsbericht 2017; Webseite: https://www.bakom.admin.ch/dam/bakom/de/dokumente/bakom/das_bakom/rechtliche_grundlagen/Verordnungen/Internet/aenderung-vid-2017.pdf.download.pdf/ODI_d_publication%20(2017).pdf; zuletzt besucht am 1. April 2025) und VID-Erläuterungsbericht 2014, S. 2 f.; Webseite: https://www.bakom.admin.ch/dam/bakom/de/dokumente/erlaeuterungsberichtvid.pdf.download.pdf/erlaeuterungsberichtvid.pdf; zuletzt besucht am 11. April 2025).

17 VID-Erläuterungsbericht 2017; Webseite: https://www.bakom.admin.ch/dam/bakom/de/dokumente/bakom/das_bakom/rechtliche_grundlagen/Verordnungen/Internet/aenderung-vid-2017.pdf.download.pdf/ODI_d_publication%20(2017).pdf; zuletzt besucht am 11. April 2025) und VID-Erläuterungsbericht 2014, S. 2 f.; Webseite: https://www.bakom.admin.ch/dam/bakom/de/dokumente/erlaeuterungsberichtvid.pdf.download.pdf/erlaeuterungsberichtvid.pdf; zuletzt besucht am 11. April 2025).

2.2.2.2 Umleitung des Datenverkehrs von zugeteilten Domain-Namen

Fake-Webshops und betrügerische Online-Investitionsplattformen dienen häufig nicht nur dem eigentlichen Betrug, sondern werden zusätzlich für Phishing oder die Verbreitung von Schadsoftware genutzt. Bei solchen kombinierten Bedrohungen ermöglicht Artikel 15*a* VID die Umleitung des Datenverkehrs zu Analysezwecken – eine Technik, die als «*domain name traffic sinkholing*» bezeichnet wird.

«*Sinkholing*» ermöglicht es, den Datenverkehr, der über einen missbräuchlich genutzten Domain-Namen läuft, temporär umzuleiten, um damit verbundene sicherheitsrelevante Vorfälle zu analysieren. Bei Malware-Infrastrukturen können so beispielsweise infizierte Systeme identifiziert werden, während bei Phishing-, betrügerischen Webshops oder Investitionsplattformen eher die Analyse des Opferverkehrs im Vordergrund steht. Dies dient dazu, über die Bedrohung zu informieren, Angriffsmuster technisch auszuwerten und gezielte Gegenmassnahmen zu entwickeln. Ziel ist es, Bedrohungen frühzeitig zu erkennen und zukünftigen Angriffen wirksam entgegenzuwirken. Auch die internationale Organisation ICANN (Internet Corporation for Assigned Names and Numbers), eine gemeinnützige Organisation mit Sitz in den USA, die weltweit zentrale technische Koordinationsaufgaben für das Domain-Namens-System (DNS) übernimmt, empfiehlt dieses Instrument zur Unterstützung der Cyberabwehr.[18]

Die technische Umsetzung erfolgt durch die Registerbetreiberin, welche die in der Zonendatei eingetragenen Namensserver durch sogenannte «*Sinkhole-Server*» ersetzt. Damit wird der Datenverkehr auf eine geschützte Umgebung umgeleitet, in der eine Analyse und eine Unterbrechung schadhafter Verbindungen möglich ist.

Um die Grundrechte zu wahren und den Schutz der Kommunikationsinhalte sicherzustellen, ist das «*Sinkholing*» in Artikel 15*a* VID wie folgt geregelt:

- Erstens darf der Datenverkehr nur dann umgeleitet werden, wenn der betroffene Domain-Name bereits technisch und administrativ gemäss Artikel 15 VID blockiert ist (Art. 15*a* Bst. a VID).
- Zweitens ist die Analyse ausschliesslich zum Zweck zulässig, Opfer zu identifizieren, diese zu benachrichtigen und technische Erkenntnisse zu gewinnen, die zur Erkennung und Bekämpfung solcher Angriffe beitragen. Nicht relevante Daten sind umgehend und vollständig zu löschen (Art. 15*a* Bst. b VID).
- Drittens dürfen nur die vom BAKOM zur Bekämpfung der Cyberkriminalität anerkannte Stellen eine solche Umleitung bei der Registerbetreiberin beantragen. Anerkannte Stellen können dies für eine Dauer von maximal 30 Tagen verlangen (Art. 15*a* Bst. c VID). Eine Umleitung des Datenverkehrs über die in diesem Artikel genannten Maximalfristen hinaus kann gemäss Artikel 15*a* Absatz 3 VID nur aufrechterhalten werden, wenn das BAKOM dies anordnet.

Artikel 15*a* Absatz 2 VID sieht sodann vor, dass der Datenverkehr entweder zu einem Analysetool oder zu einer Informationsseite umgeleitet werden kann:

- Die Analyse der umgeleiteten Daten erfolgt in der Regel durch die beantragende Behörde selbst oder eine fachlich qualifizierte Dritteinrichtung, z. B. ein Security Research Partner oder

[18] VID-ERLÄUTERUNGSBERICHT 2017, S. 3; Webseite: https://www.bakom.admin.ch/dam/bakom/de/dokumente/bakom/das_bakom/rechtliche_grundlagen/Verordnungen/Internet/aenderung-vid-2017.pdf.download.pdf/ODI_d_publication%20(2017).pdf; zuletzt besucht am 11. April 2025) und VID-ERLÄUTERUNGSBERICHT 2014, S. 2 f.; Webseite: https://www.bakom.admin.ch/dam/bakom/de/dokumente/erlaeuterungsberichtvid.pdf.download.pdf/erlaeuterungsberichtvid.pdf; zuletzt besucht am 11. April 2025). Betrügerische Webshops enthalten in der Regel keine Malware und dienen primär der Täuschung von Nutzenden, etwa durch Vorkassebetrug oder den Verkauf gefälschter Produkte. Für die Steuerung infizierter Systeme (z. B. über Command-&-Control-Infrastrukturen) werden solche Domains üblicherweise nicht eingesetzt. Sinkholing wird in diesen Fällen eher zur Analyse des Opferverkehrs genutzt, nicht zur Identifikation infizierter Endgeräte.

eine Stelle für forensische Untersuchungen. Die Verantwortung für die Datenbearbeitung verbleibt stets bei der anordnenden Behörde, die auch sicherzustellen hat, dass alle beteiligten Stellen die Vorgaben von Artikel 15*a* VID einhalten.[19]

– Wenn der Datenverkehr, der über einen blockierten Domain-Namen läuft, auch auf eine spezielle Informationsseite – eine sogenannte *Landing Page* – umgeleitet wird, so dient dies dazu, Personen, die einen potenziell missbräuchlich genutzten Domain-Namen aufrufen, direkt und verständlich über den Missbrauchsverdacht zu informieren. Die Informationsseite muss klar strukturiert sein und folgende Angaben enthalten: Eine verständliche Erklärung, welcher Missbrauch mit dem betreffenden Domain-Namen im Verdacht steht (z. B. Phishing, Verbreitung von Malware, betrügerische Online-Shops), den Namen und die Kontaktdaten der Stelle oder Behörde, die die Massnahme veranlasst hat, und einen Hinweis in technischer Form, dass der Zugriff aus rechtlichen Gründen nicht möglich ist – konkret durch die Anzeige des HTTP-Fehlercodes «*451 Unavailable For Legal Reasons gemäss RFC 7725*».[20]

2.2.2.3 Gemeinsame Verfahrensvorschriften: Information und Antrag auf Identifikation sowie Verfügung und Widerruf der Zuteilung des Domain-Namens

Wenn ein Domain-Name technisch oder administrativ blockiert oder dessen Datenverkehr im Rahmen einer sogenannten «*Sinkhole-Massnahme*» umgeleitet wird, sieht Artikel 15*b* Absatz 1 VID vor, dass die betroffene Halterin oder der Halter des Domain-Namens darüber unverzüglich zu informieren ist. Die Information erfolgt in der Regel elektronisch durch die Registerbetreiberin. In bestimmten Fällen kann die Information aufgeschoben werden, wenn überwiegende öffentliche oder private Interessen dies rechtfertigen (Art. 15*b* Abs. 3 VID). Würde zum Beispiel der betroffene Domain-Halter frühzeitig informiert, könnte dies dazu führen, dass er die kriminellen Aktivitäten verlagert oder Spuren verwischt. Um die Wirksamkeit der Massnahme zu sichern, kann die Benachrichtigung in solchen Fällen temporär zurückgestellt werden. Darüber hinaus sieht Artikel 15*b* Absatz 2 VID vor, dass im Zusammenhang mit Massnahmen nach Artikel 15 oder 15*a* VID von der betroffenen Person die Offenlegung der Identität sowie – sofern sich Sitz oder Wohnsitz im Ausland befindet – die Angabe einer gültigen Korrespondenzadresse in der Schweiz verlangt werden kann. Diese Verpflichtung dient insbesondere der Rechtssicherheit sowie der Nachvollziehbarkeit im weiteren Verfahren und trägt entscheidend zur wirksamen Bekämpfung von Cyberkriminalität bei.[21] Auf Verlangen einer im Rahmen ihrer Zuständigkeit intervenierenden Schweizer Behörde fordert die Registerbetreiberin gestützt auf Art. 16 Abs. 3 VID die Halterin oder den Halter eines Domain-Namens ohne gültige Schweizer Korrespondenzadresse auf, innerhalb von 30 Tagen eine solche zu bezeichnen und die Identität bekannt zu geben. Die Registerbetreiberin widerruft den Domain-Namen, wenn die Halterin oder der Halter der Aufforderung nicht fristgerecht nachkommt; sie teilt den Widerruf der ersuchenden Schweizer Behörde mit.

Anschliessend kann die Halterin oder der Halter gemäss Artikel 15*c* Absatz 1 VID eines blockierten Domain-Namens innerhalb von 30 Tagen nach Mitteilung der Massnahme durch die Registerbetreiberin den Erlass einer beschwerdefähigen Verfügung durch das BAKOM verlangen. Voraussetzung dafür ist, dass die betroffene Person ihre Identität korrekt bekannt gibt und – sofern der Wohn- oder Geschäftssitz im Ausland liegt – eine gültige Korrespondenzadresse in der Schweiz

---

19 Vgl. VID-ERLÄUTERUNGSBERICHT 2017, S. 3; Webseite: https://www.bakom.admin.ch/dam/bakom/de/dokumente/bakom/das_bakom/rechtliche_grundlagen/Verordnungen/Internet/aenderung-vid-2017.pdf.download.pdf/ODI_d_publication%20(2017).pdf; zuletzt besucht am 11. April 2025).

20 Eidgenössisches Departement für Umwelt, Verkehr, Energie und Kommunikation UVEK, Bundesamt für Kommunikation BAKOM, Revision der Verordnungen zum FMG, Erläuternder Bericht vom 26. Oktober 2020, S. 49 (nachfolgend: VID-ERLÄUTERUNGSBERICHT 2020; Webseite: https://www.bakom.admin.ch/dam/bakom/de/dokumente/bakom/das_bakom/rechtliche_grundlagen/Verordnungen/Internet/aenderung-2020-bericht.pdf.download.pdf/Rapport%20explicatif%20(2020).pdf; zuletzt besucht am 11. April 2025).

21 Vgl. Entscheid BVGer. A-583/2023 vom 22. Mai 2024, E. 3.3.1, S. 9 (Webseite: https://bvger.weblaw.ch/pdf/A-583-2023_2024-05-22_773f731f-13da-4dd3-bae7-485214951014.pdf; zuletzt besucht am 11. April 2025) und VID-ERLÄUTERUNGSBERICHT 2017, S. 4; Webseite: https://www.bakom.admin.ch/dam/bakom/de/dokumente/bakom/das_bakom/rechtliche_grundlagen/Verordnungen/Internet/aenderung-vid-2017.pdf.download.pdf/ODI_d_publication%20(2017).pdf; zuletzt besucht am 11. April 2025).

(Rechtsdomizil) angibt. Diese Möglichkeit dient der Wahrung des rechtlichen Gehörs (Art. 29 Abs. 2 BV) sowie der Rechtsweggarantie (Art. 29*a* BV) und ist Ausfluss des Rechts auf ein faires Verfahren (Art. 6 Abs .1 Konvention zum Schutze der Menschenrechte und Grundfreiheiten).[22] Gleichzeitig ist die Pflicht zur Bekanntgabe der Identität ein zentrales Instrument zur Aufdeckung missbräuchlich registrierter Domain-Namen, da viele betrügerische Domains unter falschen oder anonymen Angaben registriert werden. In der Praxis zeigt sich, dass Personen oder Organisationen, die einen Domain-Namen für betrügerische Zwecke nutzen, in der Regel weder der Aufforderung zur Identifikation nachkommen noch eine Korrespondenzadresse in der Schweiz angeben.[23] Dies eröffnet den Weg für weitere Schritte: Wenn eine Halterin oder ein Halter innerhalb der 10-Tage-Frist keine korrekten Angaben macht oder offensichtlich falsche Daten hinterlegt hat, widerruft die Registerbetreiberin den betreffenden Domain-Namen gestützt auf Artikel 15*c* Abs. 2 VID.

2.2.3 Nicht zugeteilte Domain-Namen

Neben den bereits bestehenden Möglichkeiten zur Blockierung und Umleitung missbräuchlich genutzter Domain-Namen schafft Artikel 15*d* VID ein wichtiges Instrument zur präventiven Bekämpfung von Cyberkriminalität: Diese Bestimmung betrifft noch nicht zugeteilte Domain-Namen, bei denen der begründete Verdacht besteht, dass eine künftige Zuteilung und Nutzung zu einem unrechtmässigen Zweck erfolgen könnte. Die Registerbetreiberin kann in solchen Fällen aus eigenem Antrieb präventive Massnahmen ergreifen. Auf Antrag einer vom BAKOM anerkannten Stelle zur Bekämpfung der Cyberkriminalität gemäss Artikel 15 Absatz 3 VID muss sie entsprechende Massnahmen treffen.

Gemäss Artikel 15*d* Buchstabe a VID ist es der Registerbetreiberin gestattet, sich diese Domain-Namen selbst zuzuteilen oder sie einem vertrauenswürdigen Dritten – z. B. einem sogenannten Quarantäneregistrar – zuweisen zu lassen, um deren missbräuchliche Registrierung zu verhindern. Ergänzend dazu kann sie den zu diesen Domain-Namen führenden Datenverkehr – sofern er bereits stattfindet – zu Analysezwecken umleiten («*Sinkholing*») (Art. 15*d* Bst. b VID). Dadurch lassen sich neue Bedrohungen frühzeitig vermeiden und geeignete Gegenmassnahmen einleiten. Diese Regelung richtet sich insbesondere gegen Cyberkriminelle, die automatisiert Domain-Namen generieren, um damit Botnets zu steuern oder Schadsoftware zu verbreiten. Dabei kommen sogenannte Domain-Generation-Algorithmen (DGA) zum Einsatz, die täglich Hunderte bis Tausende von zufällig zusammengesetzten Domain-Namen erzeugen. Diese dienen entweder direkt der Steuerung von Botnet-Infrastrukturen oder dazu, die Rückverfolgbarkeit von Angriffen gezielt zu erschweren. Im Rahmen forensischer Analysen (z. B. durch Reverse Engineering infizierter Systeme) lassen sich solche Algorithmen rekonstruieren. Dadurch kann im Voraus eine Liste potenziell gefährdeter Domain-Namen erstellt werden – also Namen, die noch gar nicht registriert wurden, aber mit hoher Wahrscheinlichkeit künftig für illegale Zwecke verwendet würden.[24]

Zusätzlich zur Zuteilung solcher Domain-Namen erlaubt Artikel 25 Absatz 2 Buchstabe c VID der Registerbetreiberin, die Registrierung eines Domain-Namens zu verweigern, wenn ein konkreter Verdacht besteht, dass dessen Nutzung unrechtmässig wäre.

Im Unterschied zu den Massnahmen nach den Artikeln 15*a* und 15*b* VID, die sich auf bereits zugeteilte Domain-Namen beziehen, gelten bei Artikel15*d* VID bewusst erleichterte Voraussetzungen. Es genügt der vorstehend erwähnte begründete Verdacht, dass eine künftige Zuteilung zu einem

---

22 SR **0.101**

23 VID-ERLÄUTERUNGSBERICHT 2017, S. 4; Webseite: https://www.bakom.admin.ch/dam/bakom/de/dokumente/bakom/das_bakom/rechtliche_grundlagen/Verordnungen/Internet/aenderung-vid-2017.pdf.download.pdf/ODI_d_publication%20(2017).pdf; zuletzt besucht am 11. April 2025).

24 VID-ERLÄUTERUNGSBERICHT 2017, S. 4; Webseite: https://www.bakom.admin.ch/dam/bakom/de/dokumente/bakom/das_bakom/rechtliche_grundlagen/Verordnungen/Internet/aenderung-vid-2017.pdf.download.pdf/ODI_d_publication%20(2017).pdf; zuletzt besucht am 11. April 2025).

unrechtmässigen Zweck erfolgen könnte. Zusätzliche formelle Anforderungen bestehen nicht, da es sich um Domain-Namen handelt, die noch nie vergeben wurden und bei denen daher keine Halterin oder kein Halter ein Nutzungsrecht oder schutzwürdiges Interesse geltend machen kann.[25]

2.2.4 Blockierung von neu zugeteilten Domain-Namen

Artikel 15*d*^{bis} VID ergänzt die Instrumente zur Bekämpfung von missbräuchlich registrierten Domain-Namen um eine spezifische Massnahme für neu zugeteilte Domains. Die Bestimmung richtet sich gezielt gegen Fälle, in denen innerhalb von weniger als 90 Tagen nach Registrierung eines Domain-Namens Anzeichen für falsche Halterangaben (Art. 15*d*^{bis} Abs. 1 Bst. a VID) und eine unrechtmässige Nutzung (Art. 15*d*^{bis} Abs. 1 Bst. b VID) erkennbar werden. In diesem Fall ist die Registerbetreiberin gemäss Artikel 15*d*^{bis} Absatz 1 VID berechtigt, einen Domain-Namen für maximal 10 Tage zu blockieren. Mit dieser Regelung reagiert die VID auf ein in der Praxis verbreitetes Vorgehen von Cyberkriminellen, die sich Domains kurzfristig unter Angabe fingierter oder gestohlener Identitäten sichern und unmittelbar nach Zuteilung zur Durchführung betrügerischer Aktivitäten nutzen – beispielsweise für Phishing oder den Betrieb gefälschter Online-Shops.

Gemäss Artikel 15*d*^{bis} Absatz 2 VID ist die Registerbetreiberin verpflichtet, die Halterin oder den Halter gleichzeitig zur Bekanntgabe ihrer oder seiner Identität innerhalb von 10 Tagen aufzufordern. Diese Frist dient dem Schutz der betroffenen Person und ermöglicht die Prüfung, ob die Registrierung rechtmässig erfolgt ist.

Gibt die Halterin oder der Halter ihre oder seine Identität nicht innerhalb dieser Frist korrekt bekannt, sieht Artikel 15*d*^{bis} Absatz 3 VID den automatischen Widerruf der Zuteilung des Domain-Namens durch die Registerbetreiberin vor. Damit wird verhindert, dass missbräuchlich registrierte Domains weiterhin aktiv genutzt werden können.

2.2.5 Widerrufsmöglichkeiten ohne Vorliegen der Tatbestände Phishing oder Verbreitung von Malware

Zusätzlich zu den spezifischen Missbrauchstatbeständen gemäss Artikel 15 ff. VID ermöglicht Artikel 30 Absatz 2 Buchstabe g VID Verwaltungs- und Strafverfolgungsbehörden im Rahmen ihrer Zuständigkeit, den Widerruf eines Domain-Namens anzuordnen. Konkret bedeutet dies: Wenn eine Behörde in einem formellen Verfahren feststellt, dass mit einem Domain-Namen strafbare Handlungen wie Betrug begangen werden, kann sie dessen vollständige Löschung verfügen – im Unterschied zu den Sofortmassnahmen nach Artikel 15 VID, die nur bei begründetem Verdacht auf Phishing oder Malware greifen. Diese Bestimmung stellt ein wichtiges ergänzendes Instrument dar, das auch bei anderen strafbaren Handlungen wie Betrug herangezogen werden kann.

Im Unterschied zu den Sofortmassnahmen nach Artikel 15 VID, die sich auf technisch eindeutig identifizierbare Cyberbedrohungen wie Phishing und Malware beschränken, eröffnet Artikel 30 VID einen breiteren Anwendungsbereich für behördliche Interventionen. Die Bestimmung erlaubt es zuständigen Behörden, bei nachgewiesenen oder hinreichend belegten Rechtsverletzungen unter anderem Domain-Namen technisch und administrativ blockieren zu lassen oder den Widerruf von Domain-Namen zu verfügen, ohne dass die spezifischen technischen Tatbestände des Artikels 15 VID erfüllt sein müssen.

[25] Vgl. VID-Erläuterungsbericht 2017, S. 5; Webseite: https://www.bakom.admin.ch/dam/bakom/de/dokumente/bakom/das_bakom/rechtliche_grundlagen/Verordnungen/Internet/aenderung-vid-2017.pdf.download.pdf/ODI_d_publication%20(2017).pdf; zuletzt besucht am 11. April 2025).

2.3 Internationale Zusammenarbeit

Die grenzüberschreitende Zusammenarbeit bei der Bekämpfung betrügerischer Webseiten stellt eine zentrale Herausforderung dar, da ein Grossteil der missbräuchlich genutzten Domain-Namen ausserhalb der schweizerischen Rechtssphäre registriert und betrieben wird. Die Schweiz ist daher auf die Kooperation mit ausländischen Behörden, Registerbetreiberinnen und internationalen Organisationen angewiesen.

Im Bereich der Cybersicherheit arbeitet das BACS gestützt auf das Informationssicherheitsgesetz (ISG; SR 128) eng mit ausländischen Computer Emergency Response Teams (CERTs) und nationalen Cybersicherheitszentren zusammen. Über etablierte Kanäle wie das Forum of Incident Response and Security Teams (FIRST) und operative Kooperationen können Missbrauchsmeldungen international weitergeleitet und koordinierte Massnahmen eingeleitet werden.

Strafverfolgungsbehörden wie die fedpol und die jeweiligen kantonalen Polizeibehörden hingegen stützen sich bei ihrer Zusammenarbeit bei strafrechtlich relevanten Fällen auf die Strafprozessordnung (StPO), das Rechtshilfegesetz (IRSG) sowie bi- und multilaterale Rechtshilfeabkommen wie die Cybercrime-Konvention des Europarats (Budapester Übereinkommen). Diese Zusammenarbeit ist jedoch nicht immer zeitnah oder umfassend durchsetzbar. Die Strafverfolgungsinstrumente sind dabei in erster Linie auf die Ermittlung von Täterschaften ausgerichtet und nicht auf polizeiliche Gefahrenabwehr, wozu das möglichst schnelle Löschen von für Betrug genutzten Webseiten gehört.

Während die VID wirksame Instrumente für «.ch» und «.swiss» Domains bereitstellt, sind bei ausländischen Top-Level-Domains (z. B. «.com», «.org», «.net») die Schweizer Behörden auf die Mitwirkung der jeweiligen Registerbetreiberinnen angewiesen. Diese unterliegen ausländischem Recht und haben unterschiedliche Compliance-Standards sowie Reaktionszeiten. In der Praxis zeigt sich, dass kommerzielle Registrare oft schneller auf begründete Missbrauchsmeldungen reagieren als staatlich kontrollierte ccTLD-Betreiber. Bei schwerwiegenden Fällen können formelle Rechts- bzw. Amtshilfeersuchen gestellt werden, diese sind jedoch zeitaufwendig und eignen sich nicht für die rasche Unterbindung akuter Bedrohungen. Ergänzend zu diesen formellen Kanälen können Schweizer Internetzugangsprovider bei spezifischen Cyberbedrohungen wie Phishing-Angriffen auf vertraglicher Basis (z. B. wenn in den Allgemeinen Geschäftsbedingungen enthalten ist) den Verkehr ihrer Kundinnen und Kunden zu bekannten betrügerischen Webseiten im Ausland sperren oder durch «Sinkholing» umleiten.[26] Darüber hinaus tragen Anti-Phishing-Filter, die in Cybersicherheitssoftware oder Browsern integriert sind, zur präventiven Bekämpfung bei. Diese können mit aktuellen Bedrohungsinformationen, beispielsweise aus den Meldungen an das BACS, gespeist werden. Der Fokus liegt dabei vor allem auf technisch eindeutig identifizierbaren Bedrohungen wie Phishing-Seiten und weniger auf komplexen Betrugsformen wie Fake-Shops, deren Bewertung subjektiver und rechtlich anspruchsvoller ist.

Effizienter erweist sich die direkte operative Zusammenarbeit zwischen Strafverfolgungsbehörden über Instrumente wie Europol oder Interpol, insbesondere bei grösseren Betrugsoperationen mit Schweizer Bezug. Auf Bundesebene koordiniert beispielsweise das fedpol als nationale Kontaktstelle zu Europol und Interpol diese internationale Zusammenarbeit, während die kantonalen Strafverfolgungsbehörden die operativen Ermittlungen führen. Neben der Domain-Registrierung spielen zudem ausländische Hosting-Anbieter und Zahlungsdienstleister eine zentrale Rolle bei der Infrastruktur betrügerischer Webseiten. Hier arbeiten sowohl das BACS im Rahmen seiner Cybersicherheitsaufgaben als auch Strafverfolgungsbehörden je nach Zuständigkeit mit grossen internationalen Plattformen (z. B. Cloud-Anbietern, Zahlungsabwicklern) zusammen. Das BACS kann

[26] Betrügerische Webshops werden in der Regel nicht zur Verbreitung von Malware oder zur Steuerung infizierter Systeme eingesetzt, sondern dienen der Täuschung von Nutzenden; «Sinkholing» dient hier primär der Analyse des Opferverkehrs.

bei Cyberbedrohungen entsprechende Warnungen und Missbrauchsmeldungen weiterleiten, während Strafverfolgungsbehörden bei strafrechtlich relevanten Fällen formelle Anfragen stellen. Diese Plattformen betreiben oft eigene Compliance-Programme und reagieren bei substantiierten Missbrauchsmeldungen unterschiedlich kooperativ, je nach Art der Anfrage und rechtlicher Grundlage.

2.4 Ergebnis der Prüfung

Wie die vorstehenden Ausführungen zeigen, bieten die Bestimmungen der Artikel 15 ff. VID bereits heute eine tragfähige, flexible und rechtsstaatlich abgesicherte Grundlage, um gegen missbräuchlich genutzte Domain-Namen unter den Endungen «.ch» und «.swiss» vorzugehen. Sie ermöglichen sowohl kurzfristige Massnahmen – etwa technische oder administrative Blockierungen – als auch längerfristige Eingriffe wie den Widerruf oder die Umleitung von Daten zur Analyse («Sinkholing»). Diese Eingriffe erfolgen unter strikter Beachtung der rechtsstaatlichen Grundsätze und des Verhältnismässigkeitsprinzips. Der Anwendungsbereich der Artikel 15 bis 15*c* VID ist dabei primär auf die Bekämpfung von Phishing und der Verbreitung von Malware ausgerichtet. Für andere Missbrauchsformen sieht die VID ergänzende Instrumente vor, namentlich Interventionsmassnahmen nach Artikel 30 VID sowie Möglichkeiten zur Identifizierung von Domaininhaberinnen und -inhabern nach Artikel 16 Absatz 3 VID auch ausserhalb der Tatbestände Phishing und Malware. Betrügerische Webseiten können somit je nach konkreter Ausgestaltung über verschiedene Bestimmungen der VID adressiert werden.

Die VID hat sich in der Praxis grundsätzlich bewährt. Sie erlaubt ein abgestuftes und zielgerichtetes Vorgehen gegen konkrete Missbrauchsfälle, stellt ein funktionierendes Zusammenspiel zwischen den beteiligten Akteuren sicher und stärkt das Vertrauen in die schweizerischen Domain-Namen .ch und .swiss.. Dennoch zeigt sich im Lichte aktueller Entwicklungen und bundesverwaltungsinterner Diskussionen, dass es weiterer Optimierungen bedarf, um auf die sich wandelnde Bedrohungslage adäquat reagieren zu können. Vor diesem Hintergrund schlägt der Bundesrat vor, ergänzende Massnahmen innerhalb des bestehenden Verordnungsrahmens zu prüfen und gezielt weiterzuentwickeln. Dazu gehören insbesondere:

- die regelmässige Validierung und Aktualisierung von Halterinformationen, um die Nachverfolgbarkeit und Zuständigkeit zu verbessern;
- die verbindlichere Einbindung von Registraren durch klare Pflichten zur Bearbeitung von Missbrauchsmeldungen;
- die Verbesserung der Qualität und des Zugriffs auf RDDS-Daten für anerkannte Behörden; sowie
- die Klärung der operativen Abläufe bei der Umsetzung von Sperrmassnahmen, da derzeit akkreditierte Stellen nur Anträge an die Stiftung Switch sowie das BAKOM stellen können, die manuell geprüft und umgesetzt werden. Die VID regelt jedoch nicht verbindlich, in welchem Zeitrahmen oder zu welchen Zeiten (z. B. an Wochenenden, Feiertagen oder ausserhalb der Bürozeiten) solche Anträge zu behandeln sind. In der Praxis führt dies mitunter zu Verzögerungen bei der Sperrung schädlicher Domain-Namen – insbesondere bei dringenden Fällen. Eine verbindliche Regelung zur Reaktionszeit oder die Prüfung eines teilautomatisierten Prozesses könnte hier zu einer deutlichen Effizienzsteigerung beitragen.

Diese Massnahmen zielen nicht auf eine grundlegende Neuordnung des bestehenden Rechtsrahmens ab, sondern auf dessen gezielte Weiterentwicklung und konsequente Anwendung. Bereits heute können Strafverfolgungsbehörden gestützt auf Artikel 30 VID bei Betrugsdelikten Sperrungen veranlassen. Im Rahmen der laufenden Revision des FMG wird geprüft, ob für eine weitergehende Ausweitung der Sperrmöglichkeiten auf andere Aktivitäten als Phishing und Malware –

insbesondere bei betrügerischen Webshops und Investitionsplattformen – zusätzliche Kompetenzen zur Sperrung von Domain-Namen bei begründetem Verdacht einer Straftat eingeführt werden sollen. Eine solche Erweiterung würde den Anliegen der Motion 24.4393 Götte, für welche der Bundesrat die Annahme beantragt hat, Rechnung tragen.

Darüber hinaus ist die effektive Bekämpfung betrügerischer Webseiten und Investitionsplattformen auf ausländische Top-Level-Domains ohne eine verstärkte grenzüberschreitende Zusammenarbeit nicht möglich. Ein erheblicher Teil der missbräuchlich genutzten Domain-Namen wird im Ausland und damit ausserhalb der Schweizer Domain-Endungen «.ch» und «.swiss» registriert und betrieben – unterliegt somit nicht der unmittelbaren Regelungshoheit der Schweiz. Sowohl das BACS im Cybersicherheitsbereich als auch die Strafverfolgungsbehörden sind in diesen Fällen auf die Kooperation mit ausländischen Registerbetreiberinnen, Hosting-Providern, Zahlungsdienstleistern und ausländischen Strafverfolgungsbehörden angewiesen. Im Cybersicherheitsbereich stellen internationale Kanäle wie FIRST wertvolle Instrumente darf, während Strafverfolgungsbehörden primär auf die die operative Zusammenarbeit über Europol und Interpol sowie formelle Rechtshilfeverfahren angewiesen sind.

Deshalb ist es notwendig, die internationale Zusammenarbeit strategisch auszubauen. Dies umfasst:

- für das BACS die gezielte Stärkung der operativen Vernetzung mit ausländischen CERTs und nationalen Cybersicherheitszentren;
- die Förderung gemeinsamer Standards, Analysen und Frühwarnsysteme; und
- die Entwicklung verbesserter Kooperationsmechanismen mit internationalen Plattformen, insbesondere grossen Registraren, Hosting-Dienstleistern und Zahlungsdienstanbietern, sowohl für Cybersicherheitsmeldungen als auch für strafrechtlich relevante Anfragen.

Nur durch ein solches Zusammenspiel – aus konsequenter Anwendung und Weiterentwicklung des nationalen Rechts sowie einer gezielten Verstärkung der internationalen Zusammenarbeit – kann die Bekämpfung betrügerischer Webseiten und Investitionsplattformen in der Schweiz nachhaltig gewährleistet werden. Im Rahmen der geplanten FMG-Revision wird geprüft, welche zusätzlichen Kompetenzen für Cybersicherheits- und/oder Strafverfolgungsbehörden zur Bekämpfung von Cyberbedrohungen jenseits von Phishing und Malware erforderlich sein können.

3 Nationale Zusammenarbeit und Koordination zur Bekämpfung von betrügerischen Webseiten mit Schweizer Domain-Namen

3.1 Allgemeines

Der Postulant wirft die Frage auf, ob die bestehenden rechtlichen und organisatorischen Grundlagen eine funktionierende und effiziente Koordination zwischen dem BACS, den Polizeibehörden und den Registerbetreiberinnen im Bereich der Bekämpfung von betrügerischen Webseiten mit Schweizer Domain-Namen gewährleisten.

Um dies zu prüfen, wird zunächst in einem ersten Abschnitt die aktuelle Koordinationsstruktur zwischen dem BACS, den Polizeibehörden und den Registerbetreiberinnen sowie deren jeweilige Zuständigkeiten dargelegt. Anschliessend folgt eine Auswertung von quantitativen Fallzahlen bzw. Daten der vergangenen Jahre, welche aufzeigen, wie häufig und in welcher Weise von den in der VID

vorgesehenen Massnahmen Gebrauch gemacht wurde. Darauf aufbauend erläutert der Bericht, die Kompetenzverteilung sowie Effizienz der Abläufe, wo allenfalls Schwachstellen bestehen, die Kooperation im föderalen Kontext und ob es Bedarf für weitergehenden Kompetenzen des BACS gibt. Abschliessend werden aus diesen Erkenntnissen Optimierungsmöglichkeiten aufgezeigt, insbesondere mit Blick auf eine wirksamere Betrugsbekämpfung und einen verbesserten Schutz der Nutzerinnen und Nutzer vor Missbrauch durch betrügerische Webseiten.

3.2 Koordinationsstruktur und aktuelle Praxis

Angesichts der rechtlichen Möglichkeiten zur Bekämpfung des Internetbetrugs stellt sich die vom Postulant aufgeworfene Frage nach der Funktionsfähigkeit der bestehenden Strukturen. Konkret geht es darum, ob die Zusammenarbeit und Koordination zwischen dem BACS, den kantonalen Polizeibehörden und den Registerbetreiberinnen für die Domain-Namen mit den Endungen «.ch» und «.swiss» ausreichend funktioniert. Zu prüfen sind insbesondere Zuständigkeit, Effizienz und Wirksamkeit der heutigen Abläufe. Darüber hinaus stellt sich die Frage, ob die Kompetenzen in diesem Dreieck richtig angesiedelt sind oder ob das BACS im Sinne einer effektiven Betrugsbekämpfung neue Kompetenzen benötigt.

Um diese Fragen weiter zu vertiefen, wird zunächst dargelegt, welches die Aufgaben der Akteure der Missbrauchsbekämpfung bei betrügerischen Webseiten sind und welche Aufgaben diesen zukommen:

- Das *BACS* ist die *nationale Anlaufstelle* sowie das *Kompetenzzentrum des Bundes für Cyberbedrohungen.* Es nimmt Meldungen über verdächtige Webseiten und Vorgänge im Cyberraum aus der Bevölkerung, von Unternehmen und Behörden entgegen. Hierbei übt das BACS eine koordinierende Filterfunktion aus: Es bewertet die eingehenden Meldungen, identifiziert betrügerische Webseiten sowie digitale Infrastrukturen und leitet diese Informationen an die zuständigen Polizeibehörden und Registerbetreiberinnen weiter. Durch seine zentrale Position kann das BACS Muster erkennen, Zusammenhänge feststellen und eine erste Einschätzung vornehmen. Diese Koordinationsfunktion ist besonders wichtig, da Internetbetrug oft kantonsübergreifend stattfindet und eine gesamtschweizerische Perspektive erfordert.
- Die *Polizeibehörden* nehmen eine *operative Schlüsselrolle* ein. Sie verfügen über die notwendigen rechtlichen Befugnisse und das fachliche Know-how, um strafrechtliche Ermittlungen durchzuführen. Dabei arbeiten sie sowohl mit dem BACS als auch untereinander zusammen, um kantonsübergreifende Fälle zu bearbeiten. Die kantonalen Polizeibehörden sind primär für die operative Ermittlungsarbeit in ihrem Territorium zuständig, während fedpol koordinierende Aufgaben übernimmt und als Schnittstelle zu internationalen Organisationen wie Europol und Interpol fungiert. Insbesondere sind die Polizeibehörden der Kantone Zürich, Bern, Zug, Schwyz, Waadt, Basel-Landschaft, Genf, Graubünden, Tessin, Fribourg, St. Gallen, Neuenburg und das fedpol als anerkannte Stellen zur Bekämpfung der Cyberkriminalität berechtigt, bei Phishing- und Malware-Fällen gestützt auf Artikel 15 ff. VID direkt bei den Registerbetreiberinnen die Blockierung von Domain-Namen zu beantragen.[27] Bei anderen Betrugsformen können Strafverfolgungsbehörden gestützt auf Artikel 30 VID entsprechende Massnahmen veranlassen. Eine zentrale Koordinationsfunktion zwischen den kantonalen Polizeibehörden übernimmt das Netzwerk digitale Ermittlungsunterstützung Internetkriminalität (NEDIK), das auf einer Vereinbarung zwischen der Konferenz der Kantonalen Justiz- und Polizeidirektorinnen und -direktoren (KKJPD) und der Konferenz der Kantonalen Polizeikommandantinnen und -kommandanten der Schweiz (KKPKS) basiert und

[27] Siehe hierzu die Liste der vom BAKOM anerkannten Stellen für die Bekämpfung der Cyberkriminalität gemäss Art. 15 Abs. 3 VID (Webseite: https://www.bakom.admin.ch/bakom/de/home/digital-und-internet/internet/bekaempfung-der-internetkriminalitaet.html; zuletzt besucht am 11. April 2025).

seit dem 1. Januar 2021 in Kraft ist. NEDIK stellt den gegenseitigen Wissenstransfer zwischen den Kantonen sicher und koordiniert die schweizweite Bekämpfung von Cyberkriminalität. Das Netzwerk arbeitet eng mit der Schweizerischen Kriminalprävention (SKP) und dem BACS zusammen und betreibt die Informationsplattform cybercrimepolice.ch, welche die Bevölkerung über aktuelle Cyberbedrohungen informiert und vor missbräuchlichen Webseiten warnt. Diese präventive Informationsarbeit ergänzt die reaktiven Massnahmen der Domain-Blockierung und trägt zur Sensibilisierung der Öffentlichkeit bei.[28]

- Die *Registerbetreiberinnen für die Domains «.ch» und «.swiss»*, also die Stiftung Switch und das BAKOM, nehmen eine zentrale Rolle bei der Umsetzung der in der VID vorgesehenen Massnahmen zur Bekämpfung von betrügerischen Webseiten für die Domain-Namen mit den Endungen «.ch» und «.swiss» ein. Ihre Aufgabe ist anspruchsvoll, da sie einerseits rasch auf Missbrauchsmeldungen reagieren und andererseits die Rechtmässigkeit ihrer Eingriffe sicherstellen müssen. Die Registerbetreiberinnen verfügen über die technischen Instrumente gemäss der VID: Sie können verdächtige Domain-Namen von Anfang an blockieren oder den Datenverkehr umleiten. Dabei müssen sie gemäss Artikel 15*e* VID dies sorgfältig dokumentieren und periodisch oder auf Verlangen dem BAKOM über ihre Aktivitäten im Zusammenhang mit Massnahmen bei Missbrauchsverdacht Bericht erstatten.

Zusammengefasst kann festgehalten werden, dass die Zusammenarbeit dieser drei Akteure einem etablierten Prozess folgt: Das BACS erhält und analysiert Meldungen, die Polizei- und Strafverfolgungsbehörden stellen je nach Delikt im Rahmen strafrechtlicher Ermittlungen Anträge auf Domainblockierung (bei Phishing/Malware gestützt auf Art. 15 ff. VID als anerkannte Stellen oder bei anderen Betrugsformen gestützt auf Art. 30 VID) sowie -umleitungen und die Registerbetreiber setzen diese technisch um. Diese Arbeitsteilung ermöglicht es, sowohl präventiv als auch reaktiv gegen Internetbetrug durch betrügerische Webseiten vorzugehen. Allerdings stehen diese Akteure vor der Herausforderung, dass ihre Handlungsmöglichkeiten auf Domain-Namen unter schweizerischer Verwaltung beschränkt sind. Dies erfordert zusätzlich eine internationale Zusammenarbeit, um auch gegen Betrüger vorzugehen, die von ausländischen Domain-Namen aus operieren. Zudem müssen die Akteure ihre Massnahmen stets so gestalten, dass sie einerseits effektiv gegen Betrug vorgehen, andererseits aber auch die Rechte legitimer Websitebetreiber wahren. Die Effizienz dieses Systems hängt massgeblich von der Wirksamkeit und Qualität des Informationsaustauschs zwischen den Akteuren ab. Je schneller verdächtige Aktivitäten erkannt, analysiert und unterbunden werden können, desto weniger Opfer und weniger Schaden gibt es. Dabei spielt auch die technische Infrastruktur eine wichtige Rolle, die einen reibungslosen und sicheren Informationsaustausch gewährleisten muss.

3.3 Auswertung der Fallzahlen der letzten Jahre

3.3.1 Allgemeines

Zur Beurteilung der Effektivität und gelebten Praxis wurde eine umfassende Auswertung der in den vergangenen Jahren auf Grundlage der VID erfolgten Massnahmen vorgenommen. Die verfügbaren Daten aus den Rechenschaftsberichten der Stiftung Switch erstrecken sich über den Zeitraum 2018–2024 und zeigen die konkrete Anwendung sowie Entwicklung der rechtlichen Instrumente zur Bekämpfung von missbräuchlich genutzten Domain-Namen.[29] Diese längerfristige Auswertung erlaubt fundierte Rückschlüsse auf die Entwicklung der Bedrohungslage, die Wirksamkeit der eingesetzten Massnahmen sowie die Koordination zwischen den beteiligten Akteuren.

[28] Siehe hierzu: cybercrimepolice.ch | Über NEDIK (Webseite: https://cybercrimepolice.ch/de/ueber-nedik; zuletzt besucht am 11. April 2025).
[29] Die Rechenschaftsberichte der Stiftung Switch betreffend die Jahr 2017 bis 2025 können eingesehen werden auf folgender Webseite: https://www.nic.ch/de/about/ (zuletzt besucht am 11. April 2025).

3.3.2 Massnahmen anerkannter Behörden gemäss Artikel 15 VID

Die Blockierung von Domain-Namen durch anerkannte Behörden gemäss Artikel 15 Absatz 1 VID stellt – wie vorne dargestellt wurde – eines der zentralen Instrumente zur raschen Intervention bei Missbrauchsverdacht dar:

Entwicklung der Blockierungsanträge 2018–2024:

- **2018**: 886 Anfragen zur sofortigen Blockierung von Domain-Namen (MELANI und neu Kantonspolizei Zürich)
  - 885 Domain-Namen gelöscht (nicht beantwortet)
  - 1 Domain-Name reaktiviert (beantwortet)
- **2019**: 1'492 Anfragen zur sofortigen Blockierung von Domain-Namen
  - 1'492 Domain-Namen gelöscht (nicht beantwortet)
  - 0 Domain-Namen reaktiviert (beantwortet)
- **2020**: 150 Anfragen zur sofortigen Blockierung von Domain-Namen
  - 115 Domain-Namen gelöscht (nicht beantwortet)
  - 35 Domain-Namen reaktiviert (beantwortet)
- **2021**: 20 Anfragen zur sofortigen Blockierung von Domain-Namen
  - 18 Domain-Namen gelöscht (nicht beantwortet)
  - 2 Domain-Namen reaktiviert (beantwortet)
- **2022**: 28 Anfragen zur sofortigen Blockierung von Domain-Namen
  - 27 Domain-Namen gelöscht (nicht beantwortet)
  - 1 Domain-Name reaktiviert (beantwortet)
- **2023**: 426 Anfragen zur sofortigen Blockierung von Domain-Namen
  - 410 Domain-Namen gelöscht (nicht beantwortet)
  - 16 Domain-Namen reaktiviert (beantwortet)
- **2024**: 66 Anfragen zur sofortigen Blockierung von Domain-Namen (ausschliesslich Phishing-Fälle)
  - 65 Domain-Namen gelöscht (nicht beantwortet)
  - 1 Domain-Name reaktiviert (beantwortet)

Die Daten zeigen eine volatile Entwicklung: Nach einem Höchststand von 1'492 Fällen im Jahr 2019 fiel die Zahl drastisch auf nur 20 Fälle im Jahr 2021, stieg dann 2023 wieder auf 426 Fälle an und sank 2024 erneut auf 66 Fälle. Diese Schwankungen korrelieren stark mit der Aktivität spezifischer behördlicher Projekte wie beispielsweise der verstärkten Tätigkeit der Kantonspolizei Zürich in den Jahren 2018–2019 und des fedpol-Projekts «SwitchOFF» im Jahr 2023.

Ein konstanter Befund über alle Jahre ist aber die hohe Erfolgsquote der Massnahmen: Regelmässig reagieren über 95% der betroffenen Domain-Halter nicht auf die Aufforderung zur Identifikation, was zur definitiven Löschung der Domain-Namen führt. Im Jahr 2019 lag diese Quote sogar bei 100%. Dies bestätigt, dass die blockierten Domains missbräuchlich registriert waren.

3.3.3 Amtshilfe gemäss Artikel 16 Absatz 3 VID

Die Amtshilfe nach Artikel 16 Absatz 3 VID[30] ermöglicht es Schweizer Behörden, die Bekanntgabe einer Schweizer Korrespondenzadresse zu verlangen. Diese Massnahme dient der Sicherstellung der

[30] Auf Verlangen einer im Rahmen ihrer Zuständigkeit intervenierenden Schweizer Behörde fordert die Registerbetreiberin gestützt auf Art. 16 Abs. 3 VID die Halterin oder den Halter eines Domain-Namens ohne gültige Schweizer Korrespondenzadresse auf, innerhalb von 30 Tagen eine solche zu bezeichnen und die Identität bekannt zu geben. Die Registerbetreiberin widerruft den Domain-Namen, wenn die Halterin oder der Halter der Aufforderung nicht fristgerecht nachkommt; sie teilt den Widerruf der ersuchenden Schweizer Behörde mit.

Kommunikationsmöglichkeit mit Domain-Haltern und hat sich als wichtiges ergänzendes Instrument erwiesen:

Entwicklung der Amtshilfeanfragen 2018–2024:

- **2018**: 5'993 Anfragen für Schweizer Korrespondenzadresse
  - 5'511 Domain-Namen gelöscht (nicht beantwortet)
  - 482 Domain-Namen reaktiviert (beantwortet)
- **2019**: 2'507 Anfragen für Schweizer Korrespondenzadresse
  - 2'400 Domain-Namen gelöscht (nicht beantwortet)
  - 107 Domain-Namen reaktiviert (beantwortet)
- **2020**: 948 Anfragen für Schweizer Korrespondenzadresse
  - 871 Domain-Namen gelöscht (nicht beantwortet)
  - 77 Domain-Namen reaktiviert (beantwortet)
- **2021**: 498 Anfragen für Schweizer Korrespondenzadresse
  - 364 Domain-Namen gelöscht (nicht beantwortet)
  - 134 Domain-Namen reaktiviert (beantwortet)
- **2022**: 321 Anfragen für Schweizer Korrespondenzadresse
  - 162 Domain-Namen gelöscht (nicht beantwortet)
  - 159 Domain-Namen reaktiviert (beantwortet)
- **2023**: 1'084 Anfragen für Schweizer Korrespondenzadresse
  - 964 Domain-Namen gelöscht (nicht beantwortet)
  - 120 Domain-Namen reaktiviert (beantwortet)
- **2024**: 310 Anfragen für Schweizer Korrespondenzadresse
  - 246 Domain-Namen gelöscht (nicht beantwortet)
  - 64 Domain-Namen reaktiviert (beantwortet)

Die Ursachen für diese Schwankungen können nicht abschliessend erklärt werden. Weder aus den vorliegenden Daten noch aus den Rechenschaftsberichten der letzten Jahre ergeben sich eindeutige Anhaltspunkte, weshalb die Anzahl der Amtshilfeanfragen deutlich variiert. Denkbar sind Einflüsse wie unterschiedliche Schwerpunktsetzungen einzelner Behörden oder zeitlich begrenzte Projekte, doch lässt sich dies aus den verfügbaren Informationen nicht bestätigen. Bemerkenswert ist zudem, dass bei den Amtshilfeanfragen die Kooperationsbereitschaft der Domain-Halter deutlich höher liegt als bei direkten Blockierungen und zudem über die Jahre variiert: Während 2018 nur etwa 8 % der Betroffenen antworteten, stieg dieser Anteil 2022 auf knapp 50 % und sank 2023 wieder auf 11 %.

3.3.4 Entwicklung der Bedrohungslage und proaktive Erkennung

Das BACS erkennt dank der Meldungen, die bei seiner nationalen Anlaufstelle sowie über die Initiative «antiphishing.ch» eingehen, frühzeitig sowohl Phishing-Seiten als auch andere problematische Webseiten wie betrügerische Online-Shops. Ein grosser Teil dieser Hinweise betrifft klassische Phishing-Seiten, die in der Regel rasch identifiziert werden können. Solche Seiten lassen sich unmittelbar gestützt auf Artikel 15 Absatz 1 Buchstabe a VID blockieren, wodurch Schäden für die betroffenen Nutzerinnen und Nutzer oft verhindert werden können.

In den letzten Jahren registriert das BACS jedoch eine zunehmende Zahl von Meldungen zu betrügerischen Investitionsplattformen und gefälschten Webshops mit erheblichem Schadenspotenzial. Zwar können Strafverfolgungsbehörden bereits heute gestützt auf Artikel 30 VID bei Betrugsdelikten den Widerruf von Domain-Namen verfügen, doch sieht die aktuelle Rechtslage bei Missbrauchsverdacht keine unmittelbare Sperrmöglichkeit vor, da Artikel 15 VID ausschliesslich auf Phishing- und Malware-Seiten anwendbar ist. Stattdessen besteht die Möglichkeit einer Halterabfrage

nach Artikel 16 Absatz 3 VID. Mit Artikel 15*d*^{bis} VID wurde eine Verbesserung geschaffen, die auch gegen betrügerische Webshops angewendet werden kann: Der Domain-Name wird sofort blockiert und kann, sofern die Identität der Halterin oder des Halters nicht innert zehn Tagen bekannt gegeben wird, anschliessend widerrufen werden. Dennoch wäre zu prüfen, ob zusätzliche Instrumente für ein schnelleres Eingreifen bei begründetem Missbrauchsverdacht geschaffen werden könnten, die gleichzeitig sicherstellen, dass Webseiten nicht irrtümlich blockiert werden. Insbesondere bei Webseiten mit vorsätzlich falschen oder fehlenden Kontaktdaten, die erst kürzlich registriert wurden, könnte eine erweiterte Sperrmöglichkeit im Rahmen der FMG-Revision geprüft werden. Es ist jedoch zu berücksichtigen, dass sich kriminelle Akteure rasch an neue Massnahmen anpassen. So werden beispielsweise Domain-Namen registriert und zunächst über einen Zeitraum von 90 Tagen ungenutzt belassen, bevor sie für betrügerische Zwecke eingesetzt werden. In solchen Fällen greift die längere Frist von 30 Tagen für eine Halterabfrage, was die zeitnahe Bekämpfung zusätzlich erschwert. Hinzu kommt, dass nur ein sehr geringer Anteil betrügerischer Webseiten oder Phishing-Seiten unter einer «.swiss» oder «.ch»-Domain betrieben wird. Die überwiegende Mehrheit nutzt internationale Domain-Endungen, was die Wirksamkeit der Instrumente gemäss Artikel 15 ff. VID weiter einschränkt.

3.3.5 Gesamtauswertung der Massnahmen nach VID

Die umfassende Auswertung der verfügbaren Daten aus den Jahren 2017–2024 offenbart sowohl die grundsätzliche Wirksamkeit als auch strukturelle Herausforderungen bei der Anwendung der VID-Instrumente zur Bekämpfung von Domain-Missbrauch.

Zentrale Erkenntnisse der Langzeitanalyse:

1. **Notwendigkeit des dauerhaften Ressourceneinsatzes**: Die Auswertung der Fallzahlen (z. B. 1'492 Blockierungen im Jahr 2019 gegenüber nur 20 im Jahr 2021) zeigt, dass die Anwendung der VID-Instrumente bislang stark von einzelnen Projekten und zeitlich begrenzten Schwerpunktaktionen abhängig ist. Ein projektbasierter Ansatz erweist sich jedoch als unzureichend, da Domain-Missbrauch ein kontinuierliches Phänomen darstellt. Für eine wirksame und nachhaltige Bekämpfung sind deshalb dauerhaft verankerte personelle und organisatorische Ressourcen erforderlich.
2. **Bewährte Rechtsinstrumente:** Die bestehenden rechtlichen Instrumente gemäss Artikel 15 VID haben sich bei der Bekämpfung von Phishing- und Malware-Fällen bewährt: Die Erfolgsquoten liegen regelmässig bei über 95 %, was die Wirksamkeit bei diesen technisch klar definierten Missbrauchstatbeständen bestätigt.
3. **Koordination zwischen den Akteuren:** Die Langzeitanalyse zeigt Unterschiede in der Anwendungspraxis zwischen den anerkannten Behörden. Diese lassen sich nicht allein durch Ressourcen erklären, sondern deuten auf fehlende Abstimmungen, unterschiedliche Priorisierungen und uneinheitliche Prozesse hin. Eine engere fachliche Koordination und ein institutionalisierter Austausch würden zu einer konsistenteren und wirksameren Nutzung der Instrumente führen.
4. **Entwicklung der Erkennungsfähigkeiten:** Die technischen Erkennungsmechanismen haben sich über die Jahre deutlich verbessert. Dazu beigetragen haben sowohl die verstärkte Kooperation der Registerbetreiberinnen und Polizeibehörden mit dem BACS als auch die Entwicklung automatisierter Analysetools, wie etwa der Crawler[31] der Stiftung Switch. Diese Fortschritte ermöglichen eine frühere Identifikation missbräuchlicher Webseiten und unterstützen die zügige Einleitung entsprechender Massnahmen.

[31] Ein automatisiertes Computerprogramm der Stiftung Switch, das systematisch schweizerische Webseiten mit .ch-Domains durchsucht und überwacht. Der Crawler analysiert kontinuierlich Webseiten-Inhalte, um verdächtige oder schädliche Aktivitäten wie Phishing, Betrug oder Malware-Verbreitung zu erkennen. Diese automatisierte Überwachung ermöglicht es, problematische Webseiten frühzeitig zu identifizieren und schnell Gegenmassnahmen zu ergreifen. Der Crawler arbeitet rund um die Uhr und kann grosse Mengen von Webseiten effizienter überwachen als menschliche Kontrolleure.

Abschaltung von betrügerischen Websites. Nationale Koordination bei Internetbetrug

5. **Wandel der Bedrohungslandschaft**: Die Daten belegen einen deutlichen Wandel der Missbrauchsformen: Während zu Beginn vor allem klassische Malware- und Drive-by-Angriffe im Vordergrund standen, ist heute ein starker Anstieg an Phishing-Fällen und komplexeren Betrugsmodellen (z. B. Investitionsbetrug, Fakeshops) zu beobachten. Diese Entwicklung erfordert eine kontinuierliche Weiterentwicklung der technischen Erkennungs- und Interventionsmechanismen und Evaluation der Wirksamkeit des rechtlichen Rahmens.

Bewertung der Koordinationsstrukturen:

Die Langzeitanalyse bestätigt, dass die rechtlichen Grundlagen der VID grundsätzlich funktionieren und bei konsequenter Anwendung hohe Erfolgsquoten erzielen. Gleichzeitig offenbart sie erhebliche Schwächen in der Koordination und systematischen Nutzung der verfügbaren Instrumente. Die Tatsache, dass die Fallzahlen stark von einzelnen behördlichen Projekten abhängen, deutet darauf hin, dass das Potenzial der VID-Instrumente bei weitem nicht ausgeschöpft wird. Die unterschiedlichen Entwicklungen bei den Kooperationsquoten zeigen zudem, dass eine verbesserte Kommunikation und Aufklärung legitimer Domain-Halter – etwa bei gehackten Websites oder bei Halterabfragen mit unvollständigen Registrierungsdaten - zu höheren Kooperationsraten führen kann, was wiederum die Effizienz der Massnahmen steigert. Darüber hinaus zeigt die Analyse, dass die bestehenden Instrumente insbesondere bei neuen Betrugsphänomenen wie betrügerischen Investitionsplattformen oder gefälschten Webshops weiterentwickelt werden müssen. Insgesamt bestätigen die Daten sowohl die Notwendigkeit als auch die Wirksamkeit der bestehenden rechtlichen Instrumente, unterstreichen aber gleichzeitig den dringenden Bedarf nach verbesserter Koordination, systematischerer Anwendung und stabileren institutionellen Strukturen. Hinsichtlich der rechtlichen Grundlagen wird der Bundesrat im Rahmen der FMG-Revision prüfen, welche Anpassungen erforderlich sind – sei es auf Verordnungs- oder auf Gesetzesebene. Konkrete Vorschläge für Gesetzesänderungen werden dem Parlament vorgelegt, falls die Analyse ergibt, dass die bestehenden Instrumente für neue Betrugsphänomene unzureichend sind.

3.4 Analyse der Kompetenzverteilung und Effizienz der Abläufe

3.4.1 Bewertung der heutigen Zuständigkeitsverteilung

Die heutige Zuständigkeitsverteilung im Zusammenspiel zwischen dem BACS als nationale Anlaufstelle sowie das Kompetenzzentrum des Bundes für Cyberbedrohungen, den Polizeibehörden als Teil der Strafverfolgungsbehörden und den Registerbetreiberinnen mit den technischen und administrativen Befugnissen zur Umsetzung von Massnahmen gemäss der VID ist in erster Linie funktionenbasiert getrennt.

Diese Aufgabenverteilung hat sich bewährt, da die Zusammenarbeit in den aktiven Phasen gut eingespielt ist und auf klar definierten Abläufen basiert. Die durch das BACS zentral betriebene Anlaufstelle für Meldungen aus der Bevölkerung und von Unternehmen ermöglicht eine rasche Erfassung potenziell betrügerischer Domain-Namen. Die Langzeitanalyse 2017-2024 zeigt jedoch, dass die Wirksamkeit dieser Strukturen stark von der Intensität behördlicher Projekte und Initiativen abhängt. In vielen Fällen kann das BACS durch eigene technische Analyse sowie standardisierte Prüfverfahren zeitnah reagieren und entsprechende Massnahmen sogar selbst bei den Registerbetreiberinnen veranlassen oder bei den Polizeibehörden anregen.

Abschaltung von betrügerischen Websites. Nationale Koordination bei Internetbetrug

Es lässt sich gleichwohl festhalten, dass die heutige Verteilung der Zuständigkeiten auf mehrere Stellen ein gewisses Spannungsfeld zwischen föderaler Verteilung von Verantwortung und dem Bedürfnis nach zentral koordinierter Reaktion schafft. Dieses Spannungsfeld wird durch die erheblichen jährlichen Schwankungen in der Anwendungspraxis verstärkt und ist nicht systemisch problematisch, erfordert jedoch für eine effektive Betrugsbekämpfung gut definierte Schnittstellen, abgestimmte Prozesse und eine gegenseitige Klarheit über Rollen und Kompetenzen sowie eine kontinuierliche Nutzung der verfügbaren Instrumente. Dabei zeigt sich auch ein Informationsdefizit: Viele Strafverfolgungs- und Verwaltungseinheiten scheinen die bereits bestehenden Möglichkeiten gemäss Artikel 30 VID zur Bekämpfung von Betrugsdelikten nicht ausreichend zu kennen oder zu nutzen. Eine gezielte Aufklärungs- und Schulungsarbeit über die verfügbaren rechtlichen Instrumente könnte die Anwendungspraxis erheblich verbessern.

3.4.2 Identifizierte Schwachstellen in der Praxis

Die Auswertung der Praxis im Umgang mit missbräuchlich verwendeten Domain-Namen über den Zeitraum 2017-2024 sowie der damit verbundenen Koordination zwischen den involvierten Akteuren zeigt, dass neben funktionierenden Strukturen auch verschiedene Schwachstellen bestehen, welche die Effizienz und Reaktionsgeschwindigkeit im Einzelfall beeinträchtigen können. Diese betreffen sowohl organisatorische als auch technische Aspekte:

- *Uneinheitliche kantonale Praxis und volatile Anwendung der Instrumente*: Die seit 2021 bestehende NEDIK-Struktur trägt zur Harmonisierung der kantonalen Abläufe bei, indem sie standardisierte Verfahren und gemeinsame Ressourcen bereitstellt. Dennoch zeigen sich weiterhin Unterschiede in der Umsetzung. Die Bereitschaft und Fähigkeit der Polizeibehörden, aktiv Missbrauchsmeldungen zu generieren oder mit dem BACS zusammenzuarbeiten, ist unterschiedlich stark ausgeprägt. Die Langzeitdaten offenbaren eine Volatilität in der Nutzung der rechtlichen Instrumente, mit Schwankungen zwischen 20 und 1'492 Blockierungsanträgen pro Jahr, was auf eine starke Abhängigkeit von spezifischen behördlichen Projekten hinweist. Diese Schwankungen lassen sich teilweise durch spezifische behördliche Projekte erklären, könnten jedoch auch auf wechselnde Bedrohungslagen zurückzuführen sein – etwa wenn bestimmte Betrugsformen zeitweise im Trend liegen oder auf externe Ereignisse (wie die COVID-Pandemie) reagieren. Es gilt auch zu berücksichtigen, dass während einige Kantone über spezialisierte Cybercrime-Einheiten verfügen, fehlen andernorts Ressourcen, Erfahrung oder festgelegte Schnittstellen zum BACS. Dies führt dazu, dass das nationale Lagebild unvollständig bleibt und potenziell relevante Missbrauchsfälle regional nicht oder zu spät erkannt und bearbeitet werden.
- *Informationsdefizite und eingeschränkter Datenfluss*: Die effektive Bekämpfung von Internetbetrug hängt massgeblich vom schnellen Zugang zu präzisen Informationen ab. In der Praxis bestehen jedoch Lücken im Informationsfluss. So ist beispielsweise unklar, ob Polizeibehörden über eingeleitete Ermittlungsverfahren aufgrund des Untersuchungsgeheimnis informieren oder ob Registerbetreiberinnen ausreichend zeitnah über den Ausgang von Blockierungsanträgen Rückmeldung erhalten. Die inkonsistente Nutzung der verfügbaren Instrumente deutet zudem darauf hin, dass nicht alle Behörden die Verfügbaren rechtlichen Instrumente, insbesondere Artikel 30 VID, und deren Anwendungsmodalitäten ausreichend kennen. Rückmeldungen zu eingeleiteten Massnahmen, Follow-up-Kommunikation und standardisierte Rückverfolgung fehlen in vielen Fällen oder erfolgen nur situativ.
- *Technische Heterogenität und fehlende Automatisierung*: Die heutigen Prozesse zur Prüfung, Klassifikation und Behandlung von Missbrauchsfällen basieren teilweise noch auf manuellen Verfahren und ad-hoc-Kommunikation (z. B. per E-Mail). Eine durchgängige Automatisierung, insbesondere bei der Erfassung, Priorisierung und Weiterleitung von Meldungen, ist noch

nicht etabliert. Dies verzögert insbesondere bei hohem Meldeaufkommen die Reaktionsfähigkeit. Die hohe Zahl von in gewissen Jahren verarbeiteten Fällen (bis zu 1'492 Blockierungsanträge) zeigt jedoch, dass bei entsprechender Priorisierung und Ressourceneinsatz durchaus erhebliche Kapazitäten mobilisiert werden können.
- *Komplexe Schnittstellen zu internationalen Akteuren*: Viele betrügerische Domains werden von ausländischen Betreibern registriert oder gehostet. Die internationale Koordination erfolgt über unterschiedliche Kanäle: Bei technischen Cyberbedrohungen wie Phishing kann das BACS auf internationale CERT-Netzwerke zurückgreifen, während bei strafrechtlich relevanten Betrugsdelikten primär die internationale Polizeikooperation über Europol, Interpol oder bilaterale Rechtshilfeabkommen zum Tragen kommt. Die Koordination mit ausländischen Registraren oder Strafverfolgungsbehörden gestaltet sich oft schwierig, da es an formellen Kanälen, einheitlichen Standards oder verbindlichen Abkommen fehlt. Während CERT-Kanäle bei Phishing-Fällen oft effizient funktionieren, sind sie bei komplexeren Betrugsformen wie Investitionsbetrug weniger geeignet. Hier ist die internationale Polizeikooperation gefordert, doch deren Wirkung ist aufgrund der Staatensouveränität, der damit einhergehenden Kompetenzreichweite und des Territorialitätsprinzips im Einzelfall limitiert.

3.4.3 Koordination im föderalen Kontext

Die föderale Struktur der Schweiz prägt den Bereich der Cybersicherheit und Internetkriminalität. Die Zuständigkeiten zwischen Bund und Kantonen sind funktional aufgeteilt: Während der Vollzug strafrechtlicher Massnahmen grundsätzlich in die Kompetenz der Kantone fällt, betreibt der Bund mit dem BACS eine nationale Anlaufstelle für Cyberbedrohungen, die Meldungen von technischen Cyberbedrohungen bis zu Betrugsdelikten entgegennimmt und betroffene Behörden, Organisationen und Personen vor unmittelbaren Bedrohungen warnt. Für Geschädigte stellt sich in der Praxis die Frage, ob sie weiterhin zur örtlichen Polizei gehen müssen oder ob die zentrale Meldestelle des BACS eine effizientere Alternative darstellt. Diese Kompetenzaufteilung bedingt eine funktionierende Zusammenarbeit, um Erfolge im Kampf gegen betrügerische Webshops zu erzielen. Der Blick auf die Koordinationspraxis über die Jahre 2018–2024 zeigt, dass die föderale Zuständigkeiten zwar Vorteile hinsichtlich regionaler Nähe und dezentraler Handlungskompetenz bietet, gleichzeitig aber auch Herausforderungen mit sich bringen:

- *Diversität bei personellen und technischen Ressourcen*: Die Ausstattung der kantonalen Polizeibehörden im Bereich der Cyberkriminalität variiert erheblich. Einige Kantone verfügen in ihren Polizeibehörden über spezialisierte Ermittlungsgruppen mit entsprechenden Analysekapazitäten, während andere nur grundlegende Strukturen aufweisen. Die Schwankungen in den Fallzahlen zwischen den Jahren verstärken diese Problematik, da sie zeigen, dass die kontinuierliche Nutzung der verfügbaren Rechtsinstrumente stark von einzelnen kantonalen Initiativen oder Projekten abhängt. In der Praxis führt dies dazu, dass die Arbeiten je nach Kanton zeitlich und methodisch unterschiedlich erledigt werden – mit entsprechenden Auswirkungen auf die Reaktionsgeschwindigkeit und Kohärenz.
- *Fehlende institutionalisierte Abläufe zwischen Bund und Kantonen*: Zwar bestehen Austauschmechanismen zwischen dem BACS und einzelnen Kantonen, doch die volatile Anwendungspraxis deutet auf nicht ausreichend institutionalisierte, formal geregelte Prozesse für Meldungen, Rückmeldungen und Entscheidungswege hin. Die Tatsache, dass die Nutzung der rechtlichen Instrumente stark von spezifischen Projekten abhängt (wie dem fedpol-Projekt «SwitchOFF» oder der intensiven Phase der Kantonspolizei Zürich 2018-2019), unterstreicht den Bedarf nach verlässlicheren, projektunabhängigen Strukturen.

3.4.4 Bedarf für weitergehende Kompetenzen des BACS?

Es stellt sich aufgrund des Prüfauftrags im Postulat die Frage, ob das BACS im Sinne einer wirksameren Betrugsbekämpfung bei betrügerischen Webseiten mit zusätzlichen Kompetenzen ausgestattet werden sollte. Der heutige Auftrag des BACS umfasst insbesondere die Erkennung und Koordination im Bereich von Cyberbedrohungen, die Betreuung der nationalen Meldestelle für Cybersicherheitsvorfälle sowie die Zusammenarbeit mit in- und ausländischen Partnerstellen. Die Umsetzung von Massnahmen obliegt jedoch anderen Akteuren – insbesondere den Polizeibehörden sowie Registerbetreiberinnen. Im Rahmen des Prüfauftrags dieses Postulats wurde deshalb untersucht, ob und inwiefern eine Ausweitung der Befugnisse des BACS angezeigt wäre. Die Langzeitanalyse der Jahre 2017-2024 mit ihren Schwankungen in der Anwendungspraxis verleiht dieser Fragestellung zusätzliche Relevanz. Das Ergebnis der Prüfung fällt differenziert aus:

- *Keine unmittelbare Notwendigkeit für neue Befugnisse*: Die bestehenden rechtlichen Grundlagen erlauben es dem BACS, Missbrauchsfälle zu identifizieren und in Koordination mit den zuständigen Stellen (Registerbetreiberinnen und Polizeibehörden) geeignete Massnahmen zu bewirken oder gar selbst bei den Registerbetreiberinnen anzubegehren. Wenn die verfügbaren Instrumente genutzt werden, zeigen sie hohe Erfolgsquoten (regelmässig über 95% bei Blockierungen), was ihre grundsätzliche Wirksamkeit bestätigt. In der Praxis zeigt sich, dass diese Koordination in einem grossen Teil der Fälle zeitnah und wirksam erfolgt – vor allem wenn eingespielte Prozesse vorhanden sind. Gleichzeitig wird im Rahmen der bevorstehenden FMG-Revision zu prüfen sein, ob eine Erweiterung der Eingriffsmöglichkeiten – insbesondere im Hinblick auf neue Betrugsphänomene wie gefälschte Webshops oder betrügerische Investitionsplattformen – eine Verbesserung der Wirksamkeit und Geschwindigkeit der Massnahmen ermöglichen könnte.
- *Erweiterung der operativen Handlungsspielräume als prioritärer Ansatz*: Statt der Schaffung von neuen Rechtsgrundlagen erscheint eine verstärkte Ausweitung der operativen Handlungsmöglichkeiten des BACS als zielführender, wie etwa der Aufbau einer nationalen Plattform zur automatisierten Erfassung, Prüfung und Weiterleitung von Domainmissbrauchsmeldungen an die Polizeibehörden sowie Registerbetreiberinnen. Die volatile Anwendungspraxis unterstreicht den Bedarf nach systematischeren, weniger projektabhängigen Koordinationsmechanismen.
- *Stärkung der Schnittstellenfunktion gegenüber internationalen Stellen*: Ein weiterer Bereich mit Entwicklungsbedarf betrifft die internationale Koordination bei technischen Cyberbedrohungen. Das BACS könnte mit zusätzlichen Ressourcen effektiver mit ausländischen Computer Emergency Response Teams (CERTs), Registerbetreiberinnen und Plattformbetreibern bei Phishing- und Malware-Fällen kommunizieren und Informationen bündeln, die für nationale Akteure von Relevanz sind. Unter den Umständen des aktuellen Bundeshaushaltes wird diese Entwicklung aber nicht priorisiert. Bei komplexeren Betrugsformen wie Fake-Shops oder Investitionsbetrug liegt die internationale Koordination hingegen primär bei den Strafverfolgungsbehörden über Europol, Interpol und Rechtshilfekanäle. Zudem ist zwischen Schweizer Domains (.ch/.swiss), wo direkte Eingriffsmöglichkeiten bestehen, und ausländischen Domains, wo die Schweiz auf internationale Kooperation angewiesen ist, klar zu unterscheiden. Angesichts der inkonsistenten nationalen Anwendung der Instrumente für Schweizer Domains gewinnt eine effektive internationale Koordination bei ausländischen Domains zusätzlich an Bedeutung.

3.5 Ergebnis der Prüfung

Die Prüfung der vom Postulat aufgeworfenen Fragen zur Zusammenarbeit und Koordination zur Bekämpfung von betrügerischen Webseiten mit Schweizer Domain-Namen zeigt, dass das bestehende Zusammenspiel zwischen dem BACS, den Polizeibehörden und den Registerbetreiberinnen im Grundsatz funktioniert, jedoch durch strukturelle und prozessuale Unterschiede sowie eine volatile Anwendungspraxis beeinträchtigt wird. Die umfassende Auswertung der Fallzahlen über acht Jahre (2017-2024) offenbart dabei sowohl die hohe Wirksamkeit der rechtlichen Instrumente bei konsequenter Anwendung als auch deren unzureichende systematische Nutzung. Auf Basis der Auswertung der Fallzahlen sowie der Analyse der Zuständigkeiten und Abläufe ergeben sich die folgenden drei zentralen Erkenntnisbereiche:

- *Optimierungsmöglichkeiten auf operativer Ebene*: Die Koordination bei der Bekämpfung von betrügerischen Webseiten funktioniert dann besonders effizient, wenn eingespielte Abläufe, klare Kommunikationswege und gegenseitiges Vertrauen zwischen den Akteuren vorhanden sind. Die Volatilität in der Anwendung der rechtlichen Instrumente unterstreicht jedoch den Bedarf nach systematischeren Strukturen. Um die Wirksamkeit zu steigern, die bestehende Zusammenarbeit zu konsolidieren und zu beschleunigen, empfiehlt sich die Umsetzung folgender operativer Verbesserungen:
    1. Standardisierung von Melde- und Rückmeldeprozessen zwischen dem BACS, den Polizeibehörden und den Registerbetreiberinnen;
    2. Förderung einheitlicher kantonaler Ansprechstrukturen im Bereich Cyberkriminalität zur Erhöhung der Reaktionsgeschwindigkeit;
    3. Verstärkung der technischen Infrastruktur beim BACS zur Automatisierung von Prüf- und Weiterleitungsprozessen;
    4. Schaffung eines regelmässigen Austauschs auf operativer Ebene (z. B. über gemeinsame Lageberichte oder Arbeitsgruppen) mit dem Ziel einer kontinuierlicheren Nutzung der verfügbaren Instrumente.
- *Rechtlicher Anpassungsbedarf der Kompetenzen des BACS trotz identifizierter Koordinationsdefizite*: Die Analyse hat keinen unmittelbaren gesetzgeberischen Handlungsbedarf für neue Anordnungsbefugnisse des BACS ergeben. Wenn die bestehenden rechtlichen Instrumente zur Anwendung kommen, zeigen sie hohe Erfolgsquoten (regelmässig über 95% bei Blockierungen). Diese belegen die Wirksamkeit der rechtlichen Instrumente, können jedoch nicht über deren unzureichende systematische Nutzung hinwegtäuschen. Die heutigen Kompetenzen ermöglichen es dem BACS entsprechend seinen Aufgaben wirksam tätig zu werden. Die identifizierten Schwachstellen liegen primär in der unzureichenden systematischen Nutzung der vorhandenen Möglichkeiten, nicht in deren rechtlicher Ausgestaltung. Falls die geplante FMG-Revision die Eingriffsmöglichkeiten – insbesondere im Hinblick auf neue Betrugsphänomene wie gefälschte Webshops oder betrügerische Investitionsplattformen – erweitern würde, so könnte dies eine weitere Verbesserung der Wirksamkeit und Geschwindigkeit der Massnahmen ermöglichen und damit auch eine Erweiterung der Kompetenzen des BACS mit sich bringen.
- *Weiterer Handlungsbedarf und Ausblick*: Die Schwankungen in der Anwendungspraxis verdeutlichen, dass die föderale Realität der Schweiz in diesem Bereich verstärkte Koordinationsanstrengungen erfordert. In der föderalen Realität der Schweiz bedarf es hierfür weder Zentralisierung noch umfassender Strukturreformen, sondern vielmehr einer klaren Rollenverteilung sowie Prozesse und einer laufenden gemeinsamen Qualitätssicherung.

Der Bundesrat wird über die Verwaltung die Zusammenarbeit mit den Kantonen und weiteren Akteuren weiter stärken und den bestehenden Austausch gezielter fördern. Die Ergebnisse dieses Berichts fliessen zudem in die Weiterentwicklung der Nationalen Cyberstrategie (NCS) ein mit

besonderem Fokus auf die Gewährleistung einer kontinuierlicheren Anwendung der verfügbaren Rechtsinstrumente sowie auf die Prüfung von punktuellen Erweiterungen der rechtlichen Instrumente, um neue Betrugsphänomene wirksamer und schneller bekämpfen zu können.

4 Schlussbetrachtung

Die Prüfung der vom Postulat aufgeworfenen Fragen sowie die Auswertung der Praxis zwischen 2017 und 2024 bestätigen, dass die bestehenden Bestimmungen in der VID, insbesondere die Artikel 15 ff. und Artikel 30, ein robustes, rechtlich tragfähiges und in der Praxis bewährtes Instrumentarium zur Bekämpfung von bestimmten Missbrauchsformen von Domain-Namen mit den Endungen «.ch» und «.swiss» bieten. Sie ermöglichen ein abgestuftes Vorgehen bei Missbrauch – von der technischen Sperrung bis zur Umleitung oder dem Widerruf – unter Beachtung der rechtsstaatlichen Prinzipien und mit belegten Erfolgsquoten von über 95 % bei Blockierungsmassnahmen.

Gleichzeitig macht die Analyse deutlich, dass dieses Instrumentarium gegenwärtig nicht flächendeckend und systematisch genug zur Anwendung gelangt. Die stark schwankenden Fallzahlen bei Blockierungsanträgen (zwischen 20 und 1'492 pro Jahr) weisen auf eine uneinheitliche Nutzung hin, die sich weder allein mit kantonalen Zuständigkeitsunterschieden noch mit tatsächlichen Schwankungen im Bedrohungsaufkommen erklären lässt. In der föderalen Struktur der Schweiz bestehen teils erhebliche Unterschiede bei Abläufen, Ansprechstrukturen und Reaktionsgeschwindigkeit. Diese Heterogenität beeinträchtigt sowohl die Kohärenz des nationalen Lagebilds als auch die Effektivität der Massnahmen.

Vor diesem Hintergrund ist der Bundesrat der Ansicht, dass die heutigen rechtlichen Grundlagen ausreichen, um bei konsequenter und koordinierter Anwendung rasch und wirksam auf Bedrohungen zu reagieren. Es besteht ein zentraler Handlungsbedarf auf operativer Ebene: Es gilt, bestehende Melde- und Reaktionsprozesse zwischen den involvierten Akteuren zu standardisieren, technische Automatisierungen zu fördern, kantonale Ansprechpartner zu vereinheitlichen und regelmässige operative Austausche zu institutionalisieren. Dabei sollte das BACS eine noch stärkere koordinierende Rolle übernehmen, um den Informationsfluss zu verbessern und die Nutzung der bestehenden Instrumente zwischen Bund, Kantonen und Registerbetreiberinnen gezielt zu steuern. Damit kann die Reaktionsfähigkeit auf Missbrauchsfälle signifikant erhöht werden – auch ohne zusätzliche Gesetzgebung.

Zugleich hat sich im Verlauf der Bearbeitung des Postulats gezeigt, dass punktuelle Optimierungen innerhalb des bestehenden Verordnungsrahmens sinnvoll erscheinen. Im Rahmen der geplanten FMG-Revision wird zu prüfen sein, ob insbesondere folgende Aspekte auf Verordnungsstufe präzisiert oder ergänzt werden sollten: die Validierung von Registrierungsdaten, die klare Verpflichtung der Registrare, der Zugriff auf RDDS-Daten sowie die Verbindlichkeit und zeitliche Regelung der Umsetzung von Sperranträgen. Auch die Möglichkeit zur Stellungnahmepflicht bei Halterabfragen und die Fristverkürzung bei dringlichem Missbrauchsverdacht wären mögliche zielführende Ergänzungen.

Darüber hinaus hat sich gezeigt, dass ein grosser Teil betrügerischer Webseiten ausserhalb der schweizerischen Domain-Endungen registriert und betrieben wird. Die internationale Dimension stellt eine zusätzliche Herausforderung dar, insbesondere wenn Kooperationsmechanismen mit ausländischen Registraren, Hosting-Providern oder Strafverfolgungsbehörden fehlen oder geopolitisch erschwert sind. Die Stärkung der internationalen Zusammenarbeit – durch verbindlichere Mechanismen, gemeinsame Standards und operative Netzwerke – ist deshalb ein weiterer zentraler Pfeiler für die nachhaltige Bekämpfung von Internetmissbrauch.

Zusammenfassend wird der Bundesrat eine konsequente, systematische und kooperative Nutzung der bestehenden Rechtsinstrumente fördern und deren gezielte Weiterentwicklung auf Verordnungsstufe im Rahmen der bevorstehenden FMG-Revision prüfen. Zudem wird der Ausbau der operativen Koordination auf nationaler und internationaler Ebene vorangetrieben. Dies insbesondere auch, weil im Rahmen der FMG-Revision geprüft werden soll, ob neue Möglichkeiten zur Bekämpfung der Betrugsphänomene wie gefälschte Webshops und betrügerische Investitionsplattformen geschaffen und die Kompetenzen des BACS als Massnahme zur Erhöhung der Cybersicherheit gesetzlich vorgesehen werden sollen. Zudem werden die Ergebnisse dieses Berichts in die Weiterentwicklung der Nationalen Cyberstrategie (NCS) einfliessen – insbesondere mit Blick auf die Schaffung einheitlicher Mindeststandards, die Verbesserung der operativen Zusammenarbeit sowie die Sicherstellung einer kontinuierlichen und effektiven Anwendung der bestehenden Instrumente im föderalen System der Schweiz.

Glossar

Botnetz	Netzwerk von infizierten Computern oder IoT-Geräten, die durch Schadsoftware ferngesteuert werden können. Die kompromittierten Geräte (Bots) werden von Cyberkriminellen über Command-and-Control-Server koordiniert und können für verteilte Denial-of-Service-Angriffe (DDoS), Spam-Versand, Datendiebstahl oder Kryptowährungsschürfung missbraucht werden. Botnetze können aus tausenden oder sogar Millionen infizierter Geräte bestehen und sind eine zentrale Infrastruktur für verschiedene Formen der Internetkriminalität.
CERT/CERTs	Computer Emergency Response Team. Spezialisierte Organisationen, die Informationen über Cybersicherheitsbedrohungen sammeln, analysieren und verbreiten sowie bei der Bewältigung von IT-Sicherheitsvorfällen unterstützen. Sie dienen als zentrale Anlaufstelle für die Meldung und Koordination von Reaktionen auf Cybersicherheitsvorfälle.
Domain-Generation-Algorithmen (DGA)	Algorithmen, die automatisch eine grosse Anzahl von Domain-Namen erzeugen. Sie werden häufig von Malware verwendet, um Kommunikationskanäle mit Command-and-Control-Servern zu etablieren und die Erkennung durch Sicherheitssysteme zu erschweren.
Domain-Halter	Natürliche oder juristische Person, die eine Internet-Domain registriert hat und Rechte an dieser Domain besitzt. Der Domain-Halter ist in den WHOIS-Daten einer Domain eingetragen und für die Verwendung der Domain rechtlich verantwortlich.
Domain Name System (DNS)	Hierarchisches Namenssystem im Internet, das Domain-Namen in IP-Adressen übersetzt. Das DNS ermöglicht die Nutzung benutzerfreundlicher Namen (wie beispiel.de) anstelle von numerischen IP-Adressen, um Websites und andere Internetdienste zu erreichen.
E-Commerce	Elektronischer Handel oder Internethandel. Bezeichnet den Kauf und Verkauf von Waren und Dienstleistungen über das Internet, einschliesslich Online-Shops, elektronischer Zahlungssysteme und digitaler Verträge.
Fake-Shop	Betrügerischer Online-Shop, der vorgibt, legitime Waren zu verkaufen, jedoch nach Zahlungseingang keine oder minderwertige Waren liefert. Fake-Shops imitieren oft das Erscheinungsbild seriöser Online-Händler und locken mit ungewöhnlich niedrigen Preisen.
Hosting-Anbieter	Unternehmen, das Serverinfrastruktur und Dienste bereitstellt, um Websites, Anwendungen oder Daten im Internet zugänglich zu machen. Hosting-Anbieter

	vermieten Speicherplatz und Rechenleistung auf ihren Servern an Kunden.
HTTP	Hypertext Transfer Protocol. Kommunikationsprotokoll für die Übertragung von Informationen im World Wide Web. Es definiert, wie Nachrichten formatiert und übertragen werden sowie welche Aktionen Webserver und Browser als Reaktion auf verschiedene Befehle ausführen sollen.
ICANN (Internet Corporation for Assigned Names and Numbers)	Internationale gemeinnützige Organisation, die für die Koordination der technischen Elemente des Domain Name Systems verantwortlich ist. ICANN verwaltet die Vergabe von Domain-Namen, IP-Adressen und anderen Parametern des Internets.
Internet-Domain	Eindeutiger Name, der eine Website oder andere Internetressource identifiziert (z. B. beispiel.de). Domains sind hierarchisch aufgebaut und bestehen aus mehreren durch Punkte getrennten Teilen, wobei der rechteste Teil die Top-Level-Domain darstellt.
IP-Adresse	Internet Protocol-Adresse. Numerische Kennzeichnung, die jedem mit dem Internet verbundenen Gerät zugewiesen wird. IP-Adressen dienen zur Identifikation und Lokalisierung von Geräten im Netzwerk und ermöglichen die Kommunikation zwischen diesen.
IPv4	Internet Protocol Version 4. Älteres und noch weit verbreitetes Protokoll zur Zuweisung von IP-Adressen. IPv4-Adressen bestehen aus vier durch Punkte getrennten Zahlen (z .B. 192.168.0.1) und bieten etwa 4,3 Milliarden mögliche Adressen.
IPv6	Internet Protocol Version 6. Neuere Version des Internet Protocols, entwickelt als Nachfolger von IPv4 aufgrund der Erschöpfung des IPv4-Adressraums. IPv6-Adressen sind länger (128 Bit) und werden als acht Gruppen von Hexadezimalziffern dargestellt (z. B. 2001:0db8:85a3:0000:0000:8a2e:0370:7334).
Landing Page	Spezielle Webseite, auf die Besucher nach dem Klicken auf einen Link oder eine Werbeanzeige geleitet werden. Im Kontext von Internetkriminalität werden Landing Pages oft für Phishing oder andere betrügerische Aktivitäten eingesetzt.
Login	Authentifizierungsprozess, bei dem Benutzer ihre Identität durch Eingabe von Benutzername und Passwort oder andere Methoden nachweisen, um Zugang zu geschützten Systemen, Diensten oder Konten zu erhalten.
Phishing-Seiten	Betrügerische Websites, die legitime Webseiten (wie die von Banken oder E-Mail-Anbietern) imitieren, um Benutzer zur Preisgabe sensibler Informationen wie Passwörter, Kreditkartendaten oder persönliche Informationen zu verleiten.

Privacy-Dienste	Dienste, die die Identität und persönliche Informationen von Domain-Haltern verbergen, indem sie stellvertretend als registrierte Halter auftreten. Diese Dienste ersetzen die persönlichen Kontaktdaten des eigentlichen Domain-Halters in öffentlichen WHOIS-Datenbanken.
Registration Data Directory Services (RDDS)	Dienste, die Informationen über registrierte Domain-Namen, deren Halter und technische Kontakte bereitstellen. Früher als WHOIS-Dienste bekannt, wurden diese aufgrund von Datenschutzbedenken durch strukturiertere Systeme ersetzt, die den Zugang zu persönlichen Daten einschränken.
Root-Zone	Oberste Ebene in der hierarchischen Struktur des Domain Name Systems. Die Root-Zone enthält Verweise auf alle Top-Level-Domains und wird von 13 logischen Root-Servern verwaltet, die von verschiedenen Organisationen unter Aufsicht der ICANN betrieben werden.
Sink-Server	Speziell konfigurierte Server, die im Rahmen von Sinkholing-Operationen bösartigen Datenverkehr umleiten und aufzeichnen. Diese Server analysieren die eingehende Kommunikation, um Informationen über Malware-Infektionen und Botnetze zu sammeln.
Sinkholing	Technik zur Umleitung von verdächtigem oder bösartigem Datenverkehr auf spezielle Analyse-Server (Sink-Server). Wird häufig von Sicherheitsforschern und Strafverfolgungsbehörden eingesetzt, um Botnetze zu neutralisieren und Informationen über deren Struktur und infizierte Systeme zu sammeln.
Top-Level-Domain (TLD)	Höchste Ebene im Domain Name System, dargestellt durch den letzten Teil einer Domain (z. B. .com, .org, .de, .ch). TLDs werden in generische (gTLD) wie .com und länderspezifische (ccTLD) wie .ch unterteilt und von autorisierten Registerbetreiberinnen unter Aufsicht der ICANN verwaltet.