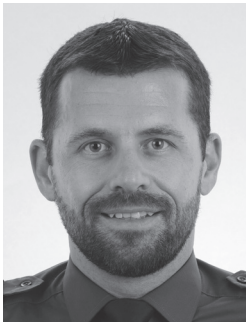
Proaktive Massnahmen zur Bekämpfung digitaler Kriminalität[1]



Damian Broger
Stv. Leiter IT-Forensik & Cybercrime (IFC)
Leiter Gruppe Cyberermittlungen / Datenanalyse (IFC1)
Kantonspolizei St. Gallen

Zusammenfassung

Bei der Bearbeitung von Fällen digitaler Kriminalität dringt seit geraumer Zeit immer mehr die Erkenntnis durch, dass der Fokus von repressiven auf proaktive Massnahmen gelenkt werden muss. Letztere zielen darauf ab, die Täterschaft über die klassische Ermittlungsarbeit hinaus vor bzw. während der Tatausführung zu stören und so weitere Straftaten zu verhindern. Die aktuelle Fokussierung auf Repression bei aus dem Ausland handelnden Kriminellen erzielt nur eine geringe Wirkung. So gelingt es den Strafverfolgungsbehörden mangels effizienter Amts- bzw. Rechtshilfe lediglich in Einzelfällen, die Täterschaft der Strafverfolgung zuzuführen. Dieser Artikel fasst die wichtigsten Erkenntnisse aus der vom Autor für die Höhere Fachprüfung Polizistin / Polizist (HFP) verfassten Diplomarbeit zusammen, stellt zweckdienliche proaktive Massnahmen vor und zeigt das Entwicklungspotenzial in diesem Bereich auf.

Delikte der digitalen Kriminalität steigen kontinuierlich an. So ergab eine repräsentative telefonische Umfrage von Dezember 2021 bei rund 1000 privaten Internetnutzenden in Deutschland, dass 79 % der Befragten innerhalb der letzten 12 Monate von kriminellen Vorfällen im Internet betroffen waren (Bitkom, 2021). Bei Unternehmen zeigt eine Befragung von 2712 Risikomanagement-Experten/-innen zu den grössten Geschäftsrisiken 2022, dass Cyber-Vorfälle und Geschäftsunterbrechungen mit je 34 % der Antworten weltweit als grösstes Risiko angesehen werden (Allianz, 2023, S. 2–17). Von den 56 befragten Unternehmen aus der Schweiz gaben sogar 57 % an, dass Cyber-Vorfälle aktuell das grösste Geschäftsrisiko darstellen (Allianz, 2023a, S. 14).

Digitale Kriminalität ist aber nicht nur in der Wahrnehmung der Internet-Nutzenden auf dem Vormarsch. Seit drei Jahren werden sämtliche Straftaten nach Strafgesetzbuch (StGB), die eines oder mehrere Cybercrime-Phänomene betreffen, in der polizeilichen Kriminalstatistik (PKS) national erhoben und als digitale Kriminalität ausgewiesen. Bei der Analyse dieser statistischen Daten wurde ersichtlich, dass es im Jahr 2021 gegenüber 2020 zu einer Zunahme von 24,3 % kam. Im Folgejahr wurde ein weiterer Zuwachs um 9,8 % ermittelt (s. Abb. 1). Der Mehrjahresvergleich zwischen den Jahren 2020 und 2022 ergab bei der digitalen Kriminalität einen

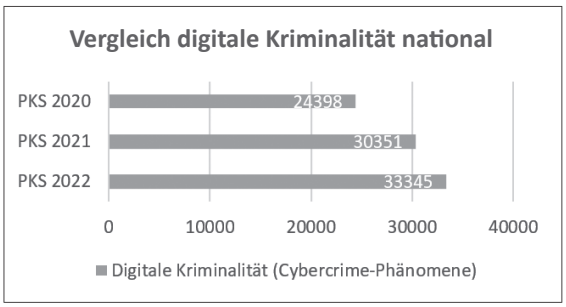


Abb. 1: Vergleich der nationalen Fallzahlen im Bereich der digitalen Kriminalität über drei Jahre (Quellen: BFS, 2021; BFS, 2022; BFS, 2023)

1 Der vorliegende Artikel basiert auf einer vom Autor für die Höhere Fachprüfung Polizistin / Polizist eingereichten Diplomarbeit (Broger, 2022). Er wurde mit der redaktionellen Unterstützung von Barbara Angerer, Übersetzerin Deutsch am SPI, verfasst.

Anstieg um 36,7 % (BFS, 2021; BFS, 2022; BFS, 2023). Demgegenüber steht im gleichen Zeitraum bei analogen Delikten nach StGB «nur» ein Anstieg um 7 %. Somit weist die digitale Kriminalität eine über fünf Mal höhere Steigerungsrate aus.

Das «zerbrochene Web»

Ein Erklärungsansatz für diese rapide Verbreitung von Straftaten im digitalen Raum liefert die Theorie des «Broken Web». Damit beschreibt Thomas-Gabriel Rüdiger ausgehend von der Broken-Windows-Theorie von Wilson und Kelling (1982) und der Routine-Activity-Theorie von Cohen und Felson (1979) das Phänomen, dass durch offen begangene Delikte im digitalen Raum, auf die keine sichtbare normenkontrollierende Reaktion erfolgt, ein Verstärkungseffekt eintritt (Rüdiger, 2017). Im Kern geht es also darum, dass die Hemmschwelle zur Verübung von Straftaten umso niedriger ist, je geringer das Risiko eingeschätzt wird, für einen Gesetzesverstoss auch zur Verantwortung gezogen zu werden. Bei der digitalen Kriminalität ist der Repressionsdruck tatsächlich viel zu gering. Verstärkend kommt hinzu, dass die Tatausführung im digitalen Raum kein Handeln am Erfolgsort erfordert, weshalb Kriminelle wiederum von jedem Ort der Welt aus tätig werden können. Die damit verbundene fehlende physische Konfrontation zwischen Täter und Opfer erfordert von der Täterschaft auch weniger Mut zur Tatbegehung.

Geringer repressiver Effekt bei aus dem Ausland verübten Delikten

Die Ermittlungen zur Identifizierung der Täterschaft zeigen, dass ein Grossteil der Cyber-Wirtschaftskriminalität aus dem Ausland verübt wird. Mit modernen Ermittlungsmassnahmen und dank internationaler Zusammenarbeit gelingt es den Cyber-Ermittelnden zwar häufig, die jeweilige Tat in einem konkreten Land zu verorten und teilweise sogar die tathandelnden Personen oder deren Gehilfen zu identifizieren. Bei den für die Folgeermittlungen in Rechts- oder Amtshilfe angefragten Behörden der Herkunfts- und/oder Aufenthaltsländer mangelt es jedoch oftmals an Kooperationsbereitschaft und staatsvertraglichen Verpflichtungen.

Weil statistische Daten fehlen, wurde im Rahmen der HFP-Diplomarbeit eine quantitative Online-Umfrage bei den Ansprechpersonen (SPOC) der im Netzwerk Digitale Ermittlungsunterstützung Internetkriminalität (NEDIK) vertretenen Polizeikorps durchgeführt. Dabei wurde neben Informationen zu den in den entsprechenden Korps eingesetzten oder angedachten proaktiven Massnahmen insbesondere erfragt, wie gross die Erfolgsaussichten von repressiven Ermittlungshandlungen zu aus dem Ausland handelnden Täterschaften sind. Bei der Auswertung wurde nachfolgendes Bild ersichtlich:

- Bei 87 % aller Fälle von digitaler Kriminalität handelt die Täterschaft aus dem Ausland.
- In 41 % aller Fälle kann die Täterschaft einem konkreten Land zugeordnet werden.
- In lediglich 2,3 % aller Fälle kann die Täterschaft mittels internationaler Amts- oder Rechtshilfe identifiziert werden (Name, Vorname, Geburtsdatum, Wohnort).
- Nur in 0,3 % aller Fälle kann die ausländische Täterschaft der Strafverfolgung zugeführt werden.

Diese Ergebnisse machen deutlich, dass die aktuelle Ausgestaltung der Repression insbesondere bei international agierenden Täterschaften der digitalen Kriminalität nur einen sehr geringen Effekt erzielt.

Von Prävention und Repression hin zu proaktiven Massnahmen

Einerseits ist bei aus dem Ausland handelnder Täterschaft eine Erhöhung des Repressionsdrucks derzeit nicht möglich. Andererseits stossen Präventionsmassnahmen an ihre Grenzen, so etwa, wenn bekannte Lücken bei Exchange-Servern trotz verfügbarer Patches von den potenziell angreifbaren Unternehmen selbst nach mehrfacher Mahnung des Nationalen Zentrums für Cybersicherheit (NCSC) nicht geschlossen werden (Maron, 2022). Da also Repression und Prävention nur eine geringe Wirkung erzielen, braucht es andere Möglichkeiten, um die Ausführung solcher Taten zu ver- oder zumindest zu behindern. Hier setzen proaktive Massnahmen an.

Konkret geht es darum, den Kriminellen ihre Arbeit so schwer wie möglich zu machen.

Proaktive Massnahmen umfassen Initiativen, mit denen Straftaten verhindert werden bzw. die Täterschaft bei der Ausführung derselben gestört wird. Konkret geht es darum, den Kriminellen ihre Arbeit so schwer wie möglich zu machen. So sollen beispielsweise die polizeilich bekannten täterischen Adressierungselemente zeitnah an von der Täterschaft genutzte Dienstleister (z. B. Banken, Provider, Internet Service Provider,

Hoster) weitergeleitet werden, sodass diese die betroffenen Accounts prüfen und nötigenfalls sperren können.

Ein Einsatz von proaktiven Massnahmen ist besonders dann angezeigt, wenn seitens Polizei keine verdeckten Überwachungen laufen und die Wahrscheinlichkeit einer erfolgreichen Identifizierung und Zuführung der Täterschaft zur Strafverfolgung nur gering ist. Die Frage ist nun: Welche proaktiven Massnahmen sind geeignet, um aus dem Ausland agierende Cyberkriminelle bei der Ausübung von Delikten zu hindern, respektive sie frühzeitig zu stören?

Methodik

Im Rahmen der HFP-Diplomarbeit wurden die Anforderungen und Erwartungen hinsichtlich der proaktiven Bekämpfung digitaler Kriminalität bei der Kantonspolizei St. Gallen sondiert. Darauf folgte eine Bestandsaufnahme der in den Korps bereits bestehenden oder künftig geplanten proaktiven Massnahmen. Dazu wurden vier Massnahmen vom Autor neu entwickelt. Diese proaktiven Massnahmen wurden schliesslich mittels Nutzwertanalyse anhand von im Vorfeld festgelegten Beurteilungskriterien zur Gewichtung der geeigneten proaktiven Massnahmen bewertet. Weil gewisse proaktive Massnahmen einer vertieften Abklärung der bestehenden rechtlichen Grundlagen bedürfen, wurden zwei verschiedene Nutzwertanalysen mit abweichenden Gewichtungskriterien vorgenommen. So konnten sowohl schnell umzusetzende Massnahmen («Quick Wins») wie auch effektive Alternativen hervorgehoben werden, für die es einer vertieften rechtlichen Prüfung bzw. der Schaffung von zusätzlichen Rechtsgrundlagen bedarf.

Rechtliche Gegebenheiten

Staatliches Handeln ist nur dann legitim, wenn eine Rechtsgrundlage dafür existiert (Legalitätsprinzip, Art. 5 Abs. 1 Bundesverfassung[2]). Genau hier liegt das Problem neuer Deliktsformen der digitalen Kriminalität: Die bestehenden Gesetze sind nicht oder nur ansatzweise auf die Bekämpfung dieser Delikte ausgelegt. Der Umstand, dass eine Täterschaft zwar identifiziert, jedoch nicht geahndet werden kann, ist bei physischen Delikten eher eine Randerscheinung – ausser es handelt sich um niederschwellige analoge Delikte, bei denen die Inanspruchnahme von internationaler Rechtshilfe unverhältnismässig wäre. Entsprechend musste der Gesetzgeber bislang auch keinen Fokus auf die Schaffung konkreter Rechtsgrundlagen für diese speziellen präventiven Zwecke legen. Gerade für proaktive Massnahmen gegen verschiedene Deliktsformen der digitalen Kriminalität braucht es aber entsprechende rechtliche Grundlagen, damit die proaktive Polizeiarbeit auf einer rechtsstaatlichen Grundlage geschehen kann.

Gerade für proaktive Massnahmen gegen verschiedene Deliktsformen der digitalen Kriminalität braucht es aber entsprechende rechtliche Grundlagen, damit die proaktive Polizeiarbeit auf einer rechtsstaatlichen Grundlage geschehen kann.

Bisher bewegt sich die Polizei bei der Durchführung von proaktiven Massnahmen im Spannungsfeld zwischen dem Grundauftrag der Gefahrenabwehr (Prävention) und dem Schutz des Amtsgeheimnisses bzw. dem Datenschutz. Es ist unbedingt nötig, dass die kantonalen Polizeigesetze konkrete Massnahmen wie die polizeiliche Datenübermittlung an für Straftaten genutzte Dienstleister erlauben, um diese Spannungen zu beseitigen. Die Grundsatzfrage zu bereits bestehenden bzw. ausreichenden Rechtsgrundlagen der kantonalen Polizeigesetze (z. B. im Rahmen der polizeilichen Generalklausel) bzw. zum Datenschutzgesetz ist sowohl bei Juristen/-innen als auch Praktikern/-innen der Polizeikorps umstritten. Lediglich zwei Kantone (Graubünden und Schwyz) verfügen aktuell in ihren Polizeigesetzen über Passagen, die den Informationsaustausch mit Dritten zum Zweck der Prävention bzw. Gefahrenabwehr vorsehen: Art. 29 Abs. 1 PolG Graubünden vom 20.10.2004[3] sowie Art. 2 Abs. 2 und Art. 4 Abs. 1 lit. b PolG Schwyz vom 22.03.2000[4].

Proaktive Massnahmen: Übersicht

Proaktive Massnahmen sollten mindestens in einem der drei nachfolgend beschriebenen Bereiche eine Wirkung bei der Täterschaft erzielen. So zeichnen sich Massnahmen im Bereich Kommunikation dadurch aus, dass der Täterschaft der Zugang zu Kommunikationsdienstleistungen abgeschnitten oder zumindest erschwert wird (beispielsweise durch Sperrung der genutzten Domains oder E-Mail-Konten). Massnahmen im Bereich Finanztransaktion sollen es

2 SR 101

3 BR 613.000 (Polizeigesetz [PolG] des Kantons Graubünden vom 20.10.2004)

4 SR 520.110 (Polizeigesetz [PolG] vom 22.03.2000)

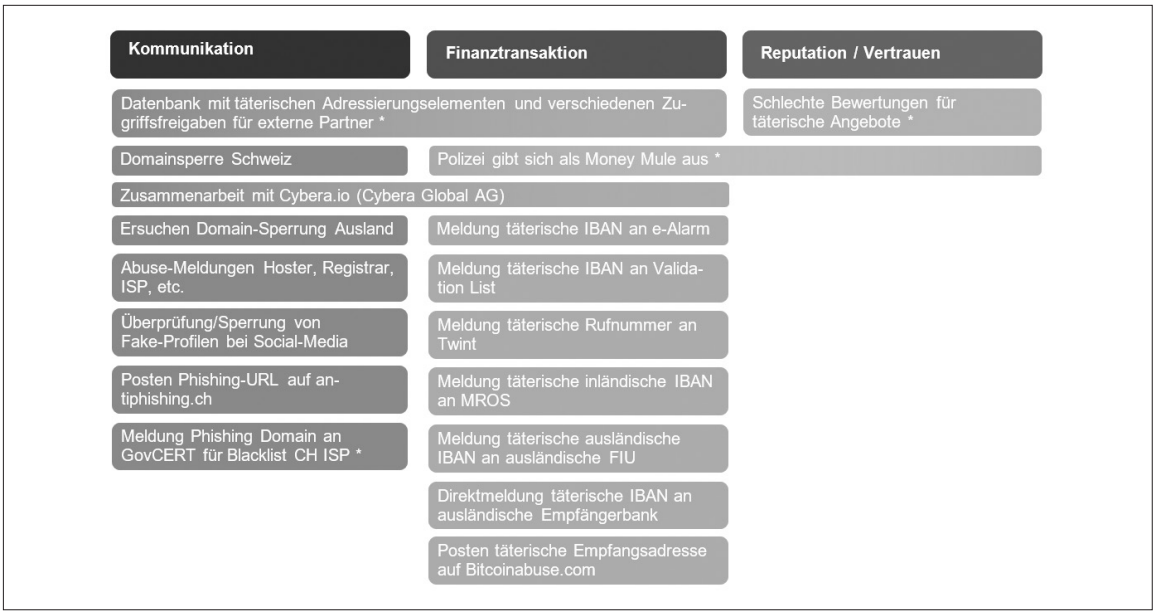


Abb. 2: Übersicht verschiedener proaktiver Massnahmen (neu erarbeitete sind mit einem Stern gekennzeichnet [*]; Quelle: eigene Darstellung)

der Täterschaft erschweren, unrechtmässig generierte finanzielle Erlöse auf andere Konten zu überweisen. Zielführend sind hier insbesondere die Zusammenarbeit mit Finanzintermediären oder Financial Intelligence Units (FIU). Zum dritten Bereich gehören Massnahmen zur Störung der Reputation oder des Vertrauens. Dies kann durch gezieltes Abwerten von täterischen Produkten oder der Erschütterung des Vertrauens in den Erfolg einer täterischen Kampagne geschehen. Abbildung 2 enthält eine Übersicht über diese drei Kategorien und die dazugehörigen proaktiven Massnahmen.

In den nachfolgenden beiden Absätzen werden zwei im Rahmen der HFP-Diplomarbeit neu erarbeitete Massnahmen detailliert vorgestellt. Zu den anderen Massnahmen finden sich die relevanten Informationen im Cyberwiki, der nationalen Wissensplattform der schweizerischen Cyber-Ermittelnden und IT-Forensiker/-innen.

Proaktive Massnahme: Polizei gibt sich als Money Mule aus

Bei digitaler Kriminalität hat die Täterschaft oftmals das Motiv, eine Verschiebung von Vermögen von den Geschädigten zur Täterschaft zu erzielen. Der Anstieg der Fallzahlen sowie die immer höher werdenden Deliktssummen führten dazu, dass Finanzintermediäre Massnahmen zur Betrugsprävention einführten. Auch potenzielle Geschädigte sehen eine Zahlung auf ein ausländisches Konto zunehmend kritisch. Auf diese Entwicklung reagierte die Täterschaft mit dem Einbau von inländischen Zwischenstellen, sogenannten Money Mules. Es sind dies Privatpersonen, die deliktisch erwirtschaftetes Geld ins Ausland transferieren sollen (Straftatbestand Geldwäscherei). Durch den Einsatz von Money Mules wird den Geschädigten eine inländische Zahlung suggeriert – und gleichzeitig die Analyse des Geldflusses erschwert.

Erkenntnisse zum täterischen Einsatz eines Money Mules liegen oftmals in einem frühen Stadium der polizeilichen Ermittlungen vor. Polizeiliche Ersuchen um sofortige Sperrung und Edition der betreffenden Konten an die Staatsanwaltschaft werden jedoch oftmals zurückhaltend oder erst mit einem erheblichen Zeitverzug bearbeitet. Häufig werden die betreffenden Konten auch lediglich ediert (Auskunft der wirtschaftlich Berechtigten), auf eine Kontosperre wird jedoch verzichtet. Dies führt dazu, dass diese Konten über einen längeren Zeitraum für weitere deliktische Zahlungen missbraucht werden können.

Als proaktive Lösung für dieses Problem empfiehlt der Autor einen verdeckten polizeilichen Einsatz auf Basis des kantonalen Polizeigesetzes. Indem die Polizei auf diverse, potenziell täterische Anzeigen zur Rekrutierung von Money Mules reagiert, sich anwerben lässt und deliktische Zahlungen auf legendierte polizeiliche Konten zulässt, erzielt sie gleichzeitig zwei gewünschte Effekte: Einerseits kann der Zahlungsfluss unterbrochen und das Geld den Geschädigten zurücktransferiert werden, andererseits kann bei den Rekrutierenden der Money Mules die

Reputation bzw. bei deren Kunden (Täterschaft) das Vertrauen vermindert werden. Daher ist es auch kein Problem, sondern sogar wünschenswert, wenn die Täterschaft von verdeckten Einsätzen der Polizei als Money Mule erfährt. So kann sie sich beim Rekrutieren von neuen Money Mules nicht mehr sicher sein, ob es sich um die Polizei oder wirklich um eine ahnungslose Privatperson handelt.

Proaktive Massnahme: Schlechte Bewertungen für täterische Angebote

Besonders im Bereich des Hightech-Crime organisiert sich die Täterschaft oftmals arbeitsteilig. Es existiert ein weitverzweigtes Netz von Partnern und Playern mit eigenen Spezialisten und klar definierten Aufgabenbereichen (Hostettler & Cornelius, 2022, S. 79). Die jeweiligen Leistungen werden vor allem im Darknet in Foren oder auf Marktplätzen angeboten. Abgesehen vom Angebot an Waren und Dienstleistungen unterscheiden sich Darknet-Marktplätze nicht von einem klassischen legalen Online-Shop (z. B. Amazon). Meist existiert für Käufer/-innen wie auch Verkäufer/-innen ein Bewertungssystem. Zudem können die Angebote oftmals nach Land der Lieferung oder Erbringung der Dienstleistung gefiltert werden. Dies eröffnet der Polizei die Möglichkeit, durch die Abgabe von schlechten Bewertungen für illegale Angebote die Reputation der Verkäufer/-innen nachhaltig anzugreifen (vgl. Sebagh et al., 2022).

Nutzwertanalyse A: «Quick Wins»

Bei der Nutzwertanalyse A liegt der Fokus auf der Rechtsgrundlage und schnellen Initialisierung. Die Quick-Win-Massnahmen «Domainsperre Schweiz», «Meldung Phishing Domain an GovCERT für Blacklist ISP» und «Posten Phishing-URL auf antiphising.ch» schnitten erwartungsgemäss am besten ab. Bei allen drei proaktiven Massnahmen geht es um die zeitnahe Blockierung täterisch genutzter Domains. Die Vorteile liegen in der klaren Rechtsgrundlage und der verhältnismässig einfachen Umsetzung. An vierter Stelle folgt die neu erarbeitete Massnahme «Polizei gibt sich als Money Mule aus», die etwas komplexer in der Umsetzung ist und einen höheren internen Ressourcenaufwand aufweist.

Nutzwertanalyse B: Fokus auf grösstem Effekt

Bei der Nutzwertanalyse B liegt der Fokus auf dem grössten Effekt. Am besten schnitt hier die Massnahme «Zusammenarbeit mit Cybera Global AG» ab, bei der täterische Spuren der Hauptbereiche Kommunikation (E-Mail-Adressen, Telefonnummern, URLs etc.) wie auch Finanztransaktion (IBAN, Kryptowährungsadressen etc.) in einer Watchlist eingetragen werden. Der Echtzeitzugriff auf die Datenbank für alle Kunden/-innen, die mögliche Direktintegration in bestehende Bankensoftwares, die automatische Weiterleitung von missbräuchlich genutzten Domains sowie die Möglichkeit, eine Straftat mit Bezug zu digitaler Kriminalität international zu melden, sind weitere Vorteile dieser Massnahme. Insgesamt schnitten Massnahmen zur Unterbrechung des Finanzflusses an die Täterschaft am besten ab.

Fazit

Bei der Bekämpfung der digitalen Kriminalität ist bei ausländischer Täterschaft rein repressives Handeln häufig nicht zielführend. Entsprechend wird den Polizeikorps empfohlen, die Ressourcen nebst der Repression auch für proaktive Massnahmen zur Verhinderung von weiteren Delikten sowie zur Störung der Täterschaft einzusetzen. Dabei sollen insbesondere Massnahmen eingesetzt werden, welche eine grosse Reichweite (internationale Ausrichtung) haben und idealerweise in mehreren Bereichen (z. B. Geldfluss und Reputation) eine Wirkung bei der Täterschaft erzielen. Zur Umsetzung der meisten proaktiven Massnahmen bedarf es im Vorfeld öffentlich-privater Partnerschaften mit denjenigen Dienstleistern, deren Plattformen zur Ausübung der Straftaten genutzt werden. Zwecks Übermittlung von täterischen Daten an diese Dienstleister ist eine Prüfung von bestehenden bzw. das Anstossen des politischen Prozesses zur Schaffung von neuen Rechtsgrundlagen nötig.

Literaturverzeichnis

Allianz. (2023). *Allianz Risk Barometer 2023.* https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2023.pdf

Allianz. (2023a). *Allianz Risk Barometer. Results appendix 2023.* https://www.agcs.allianz.com/content/dam/onemarketing/agcs/agcs/reports/Allianz-Risk-Barometer-2023-Appendix.pdf

Bitkom. (2021). *Vertrauen und Sicherheit in der digitalen Welt.* https://www.bitkom-research.de/sites/default/files/2023-03/Bitkom_Vertrauen%26ITSicherheit2021.pdf

Bundesamt für Statistik (BFS). (2021). *Polizeiliche Kriminalstatistik (PKS). Jahresbericht 2020 der polizeilich registrierten Straftaten.* https://www.bfs.admin.ch/bfs/de/home/aktuell/neue-veroeffentlichungen.assetdetail.16464401.html

Bundesamt für Statistik (BFS). (2022). *Polizeiliche Kriminalstatistik (PKS). Jahresbericht 2021 der polizeilich registrierten Straftaten.* https://www.bfs.admin.ch/bfs/de/home/aktuell/neue-veroeffentlichungen.assetdetail.22164350.html

Bundesamt für Statistik (BFS). (2023). *Polizeiliche Kriminalstatistik (PKS). Jahresbericht 2022 der polizeilich registrierten Straftaten.* https://www.bfs.admin.ch/bfs/de/home/aktuell/neue-veroeffentlichungen.assetdetail.24545217.html

Broger, D. (2022). Proaktive Massnahmen zur Bekämpfung der Digitalen Kriminalität bei der Kantonspolizei St. Gallen. Erarbeiten von behördlichen Massnahmen zur Verhinderung von weiteren Delikten sowie Störung von international agierenden Täterschaften, welche der Strafverfolgung nicht zugeführt werden können [unveröffentlichte Diplomarbeit]. Höhere Fachprüfung Polizistin / Polizist. Kantonspolizei St. Gallen.

Cohen, L. E, & Felson, M. (1979). Social Change and Crime Rate Trends: A Routine Activity Approach. *American Sociological Review,* 44(4), 588–608.

Hostettler, O., & Cornelius, A. (2022). *Underground Economy: Wie Cyberkriminelle Wirtschaft und Staat bedrohen.* NZZ Libro.

Keller, C., Braun, F., & Roggenkamp, J. D. (2020). *Cybercrime.* Verlag Deutsche Polizeiliteratur GMBH, Buchvertrieb.

Maron, H. J. (2022, 17. Mai). NCSC ärgert sich weiterhin über ungepatchte Exchange-Server. *Inside IT.* https://www.inside-it.ch/ncsc-aergert-sich-weiterhin-ueber-ungepatchte-exchange-server-20220517

Rüdiger, T.-G. (2017). Das Broken-Web-Phänomen. *Der Wirtschaftsführer für junge Juristen,* 50–53. http://formularservice-online.de/sixcms/media.php/605/wifue-2-2017.pdf

Sebagh, L., Lusthaus, J., Gallo, E., Varese, F., & Sirur, S. (2022). Cooperation and distrust in extra-legal networks: a research note on the experimental study of marketplace disruption. *Global Crime,* 23(3). https://www.tandfonline.com/doi/full/10.1080/17440572.2022.2031152

Wilson, J., & Kelling, G. L. (1982). Broken Windows: The Police and Neighbourhood Safety. *The Atlantic Monthly, March 1982.* 29–38. https://www.theatlantic.com/magazine/archive/1982/03/broken-windows/304465/

Résumé

Mesures proactives permettant de lutter contre la cybercriminalité

Dans le traitement des cas de cybercriminalité, il est, depuis un certain temps, devenu clair que l'accent doit être mis sur des mesures proactives plutôt que répressives. Au-delà du travail d'enquête classique, ces mesures visent à perturber l'auteur·e avant ou pendant la commission de l'infraction, afin d'empêcher que d'autres infractions soient perpétrées. Se concentrer comme c'est le cas actuellement sur la répression n'a que peu d'effet sur les criminel·le·s agissant depuis l'étranger. Ainsi, faute d'une entraide administrative ou judiciaire efficace, les autorités de poursuite pénale ne parviennent que dans de rares cas à engager des poursuites contre les auteur·e·s. Cet article résume les principales conclusions du travail de diplôme rédigé par l'auteur en vue de l'obtention de l'Examen professionnel supérieur de Policière / Policier (EPS), tout en présentant des mesures proactives pertinentes et en mettant en évidence le potentiel de développement dans ce domaine.

Riassunto

Misure proattive per la lotta alla criminalità digitale

Nel trattamento dei casi di criminalità digitale, da un certo tempo si diffonde sempre più la consapevolezza che l'attenzione principale deve passare dalle misure repressive a quelle proattive. Queste ultime mirano a ostacolare gli autori, tramite il lavoro classico di indagine, prima o durante l'esecuzione dell'atto e quindi a evitare ulteriori reati. L'attenzione rivolta attualmente alla repressione di atti compiuti dall'estero porta solo a risultati limitati. Le autorità di perseguimento penale, a causa dell'assenza di assistenza giudiziaria e amministrativa efficienti, riescono solo in pochi casi a condurre in tribunale gli autori. Il presente articolo riprende i risultati principali del lavoro di diploma per l'esame professionale superiore di agente di polizia (EPS) redatto dall'autore, presenta misure proattive appropriate e mostra il potenziale di sviluppo in questo ambito.