Stellungnahme von Dr. Sven Herpig, Lead Cybersecurity & Emerging Threats bei interface – Tech analysis and policy ideas for Europe e.V. (ehemals: Stiftung Neue Verantwortung), im Rahmen der Beteiligung von Spitzenverbänden, Fachkreisen und Verbänden zum Referentenentwurf des Bundesministeriums des Innern (BMI) für ein "Gesetz zur Stärkung der Cybersicherheit"

Kontakt

Dr. Sven Herpig

Lead Cybersecurity & Emerging Threats

interface – Tech analysis and policy ideas for Europe e.V.

Email: sherpig@interface-eu.org

Github: https://github.com/z-edian/publications

Zusammenfassung

Der Referentenentwurf erweitert intrusive Cyberabwehrbefugnisse erheblich. Gleichzeitig bleiben zentrale strukturelle Probleme ungelöst:

- Fragmentierte Zuständigkeiten,
- Fehlende Governance für intrusive Werkzeuge,
- Unzureichende Stärkung von Resilienz.

Ohne Koordinationsmechanismen und Transparenzstandards drohen Effektivitätsverluste und rechtliche Unsicherheiten.

1. Vorbemerkung

Der vorliegende Referentenentwurf[1] behandelt das Thema „Cyberabwehr", auch bekannt als „Aktive Cyberabwehr", „Gefahrenabwehr im Cyberraum" oder „Hackback". interface versteht unter diesem Begriff Maßnahmen, bei denen ein einzelner oder mehrere Staaten gemeinsam (intrusive) technische Eingriffe anordnen oder durchführen lassen, um eine aktuelle, spezifische Cyberoperation oder -kampagne zu neutralisieren, zu mitigieren oder zuzuordnen.[2] Die im Referentenentwurf genannten Instrumente, etwa in BKAG-E § 62e, richten sich gegen die Integrität, Vertraulichkeit und Verfügbarkeit informationstechnischer Systeme zur proaktiven Abwehr maliziöser Cyberaktivitäten, inklusiver von Dritten gemäß BKAG-E §62e (3), und fallen damit unter diese Definition.

Der politische und fachliche Diskurs über diese Form der Cyberabwehr zieht sich seit fast zehn Jahren hin[3], ohne nennenswerte Fortschritte – abgesehen von BSIG § 7b und § 7c. Ursachen dafür sind sowohl oberflächlich geführte Debatten als auch bewusste Nebelkerzen, wie die Umdeutung des Begriffs „Hackback".[4] Auch frühere Initiativen – etwa der Vorstoß des Präsidenten des Bundespolizeipräsidiums, Dr. Dieter Romann, im Rahmen der Neustrukturierung des Bundespolizeigesetzes 2024[5] scheiterte. Parallel zu den vom Bundesministerium des Innern (BMI) geplanten Ausweitungen intrusiver Cyberabwehrbefugnisse für Bundeskriminalamt (BKA) und Bundespolizei (BPol) sollen ähnliche Kompetenzen künftig auch beim Bundesnachrichtendienst (BND) geschaffen werden.[6]

[1] Bundesministerium des Innern (2026): Gesetzesentwurf zur Stärkung der Cybersicherheit
[2] Sven Herpig (2023): Active Cyber Defense – Toward Operational Norms
[3] Sven Herpig et al. (2020): Aktive Cyberabwehr/ Hackback in Deutschland
[4] Sven Herpig (2022): Aktive Cyberabwehr statt Hackback?
[5] Dieter Romann (2024): Schriftliche Stellungnahme des Präsidenten des Bundespolizeipräsidiums Herrn Dr. Dieter Romann zur öffentlichen Anhörung am 22. April 2024 zum Entwurf eines Gesetzes zur Neustrukturierung des Bundespolizeigesetztes BT-Drucksache 20/10406
[6] Thorsten Wetzling (2026): Germany's Reform of Foreign & Military Intelligence

Bevor die Befugnisse für aktive Cyberabwehr erweitert werden, muss zunächst klar benannt werden, welche Risiken damit verbunden sind. Unbeabsichtigte Kollateralschäden sowie die mögliche Proliferation der eingesetzten Werkzeuge können die Lage schnell verschärfen. Fehlzuordnungen könnten zudem dazu führen, dass Maßnahmen gegen kompromittierte Drittinfrastruktur oder unbeteiligte Betreiber gerichtet werden – mit dem Risiko diplomatischer oder rechtlicher Konflikte in Drittstaaten. Unter sorgfältiger Auswahl und Abwägung sowie mit robusten Schutzmechanismen können solche Maßnahmen die nationale Cybersicherheit zwar erhöhen. Entscheidend ist jedoch, dass sie konsequent in bestehende Sicherheitskultur, IT-Architektur und strategische Konzepte eingebettet werden. Ohne diese Einbettung droht ein Ungleichgewicht zwischen operativer Handlungsmacht und tatsächlicher Sicherheitswirkung – ein Problem, das bereits in vergleichbaren Diskussionen um hochinvasive Cyberbefugnisse deutlich wurde.

Offene, differenzierte technische und politische Debatten über Anwendungsfälle, Kriterien und Schutzvorkehrungen sind dabei unerlässlich. Nur so wird das Verursachen von Kosten für Angreifende nicht zur bloßen symbolischen Demonstration staatlicher Handlungsfähigkeit. In der Praxis werden aktive Cyberabwehrmaßnahmen ohnehin nur einen kleinen Teil des Portfolios ausmachen, das die Cybersicherheit stärkt; IT-Sicherheit und Resilienz bleiben die zentralen Säulen der nationalen Sicherheit im Cyberraum.[7]

Vor diesem Hintergrund sollte die Bundesregierung intrusive Maßnahmen auf das notwendige Minimum beschränken und sich auf nicht-intrusive, bedrohungsunabhängige, skalierbare und nachhaltige Schritte zum Schutz der eigenen IT-Infrastruktur konzentrieren. Reicht dies in Einzelfällen nicht aus, erfordert eine verantwortungsvolle Durchführung die Wahl der am wenigsten intrusiven und eskalierenden Gegenmaßnahmen (z. B. Walled Garden-Anordnung statt „verdeckte[r] Eingriff in informationstechnische Systeme von Geschädigten"). Diese müssen effizient, wirksam und verhältnismäßig sein. Zugleich gilt: Der wirtschaftliche, politische, sicherheits- und gesellschaftliche Schaden des Nicht-Handelns muss größer sein als die Kosten, die eine aktive Cyberabwehr verursacht.[8]

[7] Sven Herpig (2021): Active Cyber Defense Operations – Assessment and Safeguards
[8] Sven Herpig (2023): Active Cyber Defense – Toward Operational Norms

2. Kritik

2.1 Parallelstrukturen gefährden Effektivität

Wie bereits in der Vorbemerkung hervorgehoben, ist die bestehende Sicherheitsarchitektur entscheidend für die Effektivität und Effizienz geplanter Cyberabwehrmaßnahmen. Der aktuelle Referentenentwurf plant jedoch eine Ausweitung der Befugnisse, ohne die bekannten Defizite der deutschen Cybersicherheitsarchitektur zu adressieren.[9]

Neben den bestehenden Befugnissen der Länderpolizeien im Bereich Gefahrenabwehr im Cyberraum sollen die Kompetenzen für BSI und BND (parallel durch BNDG-E) erweitert, für das BKA deutlich ausgeweitet und für die Bundespolizei neu geschaffen werden. Der Entwurf sieht jedoch weder verbindliche Einvernehmensregelungen noch Konfliktlösungsmechanismen oder abgestimmte Koordinationsprozesse vor. Selbst wenn solche Mechanismen vorgesehen wären, fehlt bislang eine operative Plattform, auf der alle relevanten Behörden vertreten sind und sich koordinieren könnten. Ohne formalisierten Abstimmungsprozess könnten künftig alle genannten Behörden parallel aktive Cyberabwehrmaßnahmen durchführen – weitgehend unabhängig voneinander oder mit nur begrenzten Koordinationsmechanismen.

Erschwerend kommt hinzu, dass der Umgang des Staates mit Schwachstellen, die für bestimmte Cyberabwehroperationen erforderlich sein könnten, weiterhin ungeklärt bleibt. Deutschland verfügt bislang über kein transparentes Verfahren zur staatlichen Entscheidung über das Zurückhalten oder Offenlegen von Schwachstellen.[10] Risiken und rechtliche Grauzonen bestehen daher fort.[11] Die geplante Parallelstruktur einer aktiven Cyberabwehr durch BKA, BSI, Bundespolizei und die Länder schafft mehrere operative Säulen ohne klare Priorisierung oder Abstimmungsregeln mit dem BSI als zentraler Cybersicherheitsbehörde des Bundes. Das erinnert an ein ähnliches Vorgehen bei den Sicherheitsgesetzen Ende 2019. Damals resümierten Dr. Ulf Buermeyer und ich: “Statt weiteren Behörden weitreichende Befugnisse einzuräumen, müsste die Lösung eher darin bestehen, Zuständigkeiten klarer zu definieren und das bisherige Nebeneinander und oftmals auch Gegeneinander von

[9] Sven Herpig (2023): Stellungnahme von Dr. Sven Herpig , Leiter für Cybersicherheitspolitik und Resilienz bei der Stiftung Neue Verantwortung e. V. (SNV), für die öffentliche Anhörung des Ausschusses für Digitales des Deutschen Bundestags am 25. Januar 2023 zum Thema "Cybersicherheit - Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland" und Bundesrechnungshof (2025): Bericht nach § 88 Absatz 2 BHO zur Cybersicherheit

[10] Sven Herpig (2018): Schwachstellen-Management für mehr Sicherheit – Wie der Staat den Umgang mit Zero-Day-Schwachstellen regeln sollte

[11] Sven Herpig (2023): Stellungnahme von Dr. Sven Herpig , Leiter für Cybersicherheitspolitik und Resilienz bei der Stiftung Neue Verantwortung e. V. (SNV), für die öffentliche Anhörung des Ausschusses für Digitales des Deutschen Bundestags am 25. Januar 2023 zum Thema "Cybersicherheit - Zuständigkeiten und Instrumente in der Bundesrepublik Deutschland" und Sven Herpig (2025): Schriftliche Stellungnahme von Dr. Sven Herpig, interface vom 8. Oktober 2025 – Öffentliche Anhörung – Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Umsetzung der NIS-2-Richtlinie und zur Regelung wesentlicher Grundzüge des Informationssicherheitsmanagements in der Bundesverwaltung BT-Drucksache 21/1501

Sicherheitsbehörden zu beenden. Stattdessen wird der Ausbau der Sicherheitsgesetzgebung mit teils massiven Eingriffen in die Grundrechte der Bürgerinnen und Bürger weiter vorangetrieben [...]".[12]

Das geplante Vorgehen droht, Ressourcen zu zersplittern, Verantwortlichkeiten zu verwässern und die Gesamteffektivität der Cyberabwehr für die nationale Sicherheit erheblich zu mindern.

2.2 Befugnisse statt Resilienz

Wie in der Vorbemerkung betont, sind offene und differenzierte technische sowie politische Debatten über Anwendungsfälle, Kriterien und Schutzvorkehrungen unerlässlich. Nur so wird das Verursachen von Kosten für Angreifende nicht zu einer bloßen symbolischen Demonstration staatlicher Handlungsfähigkeit. In der Praxis werden aktive Cyberabwehrmaßnahmen ohnehin nur einen kleinen Teil der Maßnahmen ausmachen, die die Cybersicherheit insgesamt stärken; IT-Sicherheit und Resilienz bleiben die zentralen Säulen.

Diese Säulen werden unter anderem durch die erweiterten Befugnisse des BSI gestärkt. Gemäß BSIG-E § 11 Absatz 1 Satz 1 erhält das BSI die Befugnis, „zur Suche und Identifikation der Beeinträchtigung der Sicherheit und Funktionsfähigkeit [von] informationstechnischen Systemen" tätig zu werden. Von diesen sogenannten Threat-Hunting-Operationen[13] soll das BSI auf Basis der im Referentenentwurf vorgesehenen Personalstellen drei Aktivitäten pro Jahr durchführen können. Selbst wenn hierfür auch Personal aus der Vorfallsbearbeitung eingesetzt wird, ist dies zu wenig, um die Ausweitung der Befugnisse zu rechtfertigen. Der Referentenentwurf sollte deutlich mehr Stellen für die Bereiche Vorfallsbearbeitung und Threat Hunting vorsehen, um die IT-Sicherheit und Resilienz substantiell zu stärken. Gleichzeitig sollte das BSI prüfen, seine operative Handlungsfähigkeit strategisch zu erweitern und interne Stellen gezielt in operative Arbeitsbereiche zu verschieben.

Vor dem Hintergrund der politischen Versprechen der Bundesregierung zu Bürokratieabbau und Ausgabendisziplin wirkt der laut Referentenentwurf bzw. begleitender Personalplanung geplante Ausbau von rund 300 Stellen bis 2030 für hochinvasive, personalintensive und nur in Einzelfällen notwendige aktive Cyberabwehrmaßnahmen bei BKA und BPol politisch und strategisch fragwürdig. Vor allem, weil unklar bleibt, welches konkrete Mehr an nachhaltiger Cybersicherheit hierdurch erzielt werden kann. Tom Uren, ehemaliger Mitarbeiter des australischen Verteidigungsministeriums schrieb hier vor Kurzem: "Even very effective takedowns and disruptive cyber operations are speed bumps rather than roadblocks. They

[12] Ulf Buermeyer und Sven Herpig (2019): Immer neue Sicherheitsgesetze helfen nicht
[13] Sven Herpig (2022): Cybersicherheitspolitik: Deutsche Ideenlosigkeit?

slow adversaries, but don't stop them."[14] Vor diesem Hintergrund steht der Ansatz des Gesetzentwurfes im Widerspruch zu den empirisch belegten Herausforderungen der IT-Infrastruktur in Deutschland: Die zentralen und dezentralen Systeme der Bundesverwaltung bezeichnete der Bundesrechnungshof im Sommer 2025 in seinem Prüfbericht als „unverändert defizitär".[15] Er empfahl, Standardmaßnahmen zur IT-Sicherheit und Resilienz zu stärken – über die Notwendigkeit aktiver Cyberabwehr verlor er kein Wort.

Die geplanten Ausweitungen aktiver Cyberabwehrbefugnisse sind angesichts begrenzter personeller Kapazitäten und fehlender Koordination unverhältnismäßig und adressieren nicht die eigentlichen Defizite in IT-Sicherheit und Resilienz. Effektiver Schutz erfordert stattdessen eine Stärkung standardisierter Sicherheitsmaßnahmen und operativ handlungsfähiger Strukturen bei den Betreibern der IT des Bundes und beim BSI.

2.3 Rechtsunsicherheit und Fragmentierung

Mit der Verortung vor allem intrusiver Cyberabwehrbefugnisse beim BKA ist in den vergangenen Jahren im politischen Prozess immer wieder eine zentrale Frage aufgetaucht: die verfassungsrechtliche Zuständigkeit. Die Gefahrenabwehr ist grundsätzlich Aufgabe der Länder, wobei der Bund nur unter bestimmten Voraussetzungen eigene Zuständigkeiten wahrnehmen kann. Vor diesem Hintergrund wurde mehrfach auf die Notwendigkeit einer Grundgesetzänderung hingewiesen, sollten dem BKA derartige Befugnisse übertragen werden.

Nach der Bundestagswahl 2025 war jedoch klar, dass die Bundesregierung die dafür erforderliche Zweidrittelmehrheit im Parlament nicht erreichen würde. Stattdessen suchte sie nach Möglichkeiten, diese Hürde zu umgehen. Ein Ansatz war die Verteilung der Befugnisse auf BPol, BSI, BND und BKA. Die geplanten Anpassungen am BPolG, BSIG und BNDG erfolgen dabei lediglich auf Ebene des einfachen Gesetzes. Diese „Strategie" führt jedoch zu einer starken Zersplitterung der Zuständigkeiten, schafft Überschneidungen und erschwert eine kohärente und effiziente Cyberabwehr auf Bundesebene.

Auch bei den Änderungen am BKAG verweist der Referentenentwurf lediglich auf Änderungen im verfassungsrechtlichen Rahmen. Die §§ 62c–62e BKAG-E eröffnen dem Bundeskriminalamt jedoch weitreichende Befugnisse: von der Untersagung des Betriebs informationstechnischer Systeme über die Umleitung und Unterbindung von Datenverkehr bis hin zu Eingriffen in Systeme durch Erheben, Löschen oder Verändern von Daten – jeweils auch ohne Wissen der Betroffenen. Diese Maßnahmen sind nicht als isolierte Ausnahmeinstrumente konzipiert,

[14] Tom Uren (2026): Srsly Risky Biz: Trump's Cyber Strategy... Great, Amazing, The Best Yet
[15] Bundesrechnungshof (2025): Bericht nach § 88 Absatz 2 BHO zur Cybersicherheit

sondern systematisch in die allgemeine Gefahrenabwehr integriert und knüpfen an vergleichsweise offene Tatbestände wie „schwerwiegende“ IT-Gefahren oder Fälle außen- und sicherheitspolitischer Bedeutung (§ 3a BKAG-E) an. Das spiegelt sich auch in dem hohen Personalbedarf von über 250 Stellen bis 2030 wieder. Auch wenn für Eingriffe in private Systeme zusätzliche gerichtliche Hürden vorgesehen sind, wird der Anwendungsbereich strukturell weit gezogen. Die Darstellung als bloße Detailkorrektur unterschätzt damit die qualitative Erweiterung staatlicher Eingriffsbefugnisse im digitalen Raum. Angesichts der Intensität der vorgesehenen Maßnahmen und ihrer potenziellen Reichweite drängt sich die Frage auf, ob hier nicht eine offene verfassungsrechtliche Grundsatzdebatte – einschließlich der Frage nach einer Grundgesetzänderung – geführt werden müsste, statt die Neuregelung als punktuelle Anpassung zu behandeln. Zudem erscheint zweifelhaft, dass die im Gesetzentwurf vorgesehenen Eingriffsschwellen den Anforderungen entsprechen, die das Bundesverfassungsgericht in seiner Rechtsprechung zu Eingriffen in informationstechnische Systeme oder den Schutz des Fernmeldegeheimnisses aufgestellt hat.

Die geplante Verlagerung intrusiver Cyberabwehrbefugnisse zum BKA und die Ausweitung von Eingriffsmöglichkeiten ohne offene verfassungsrechtliche Debatte führen zu einer Zersplitterung der Zuständigkeiten und einer erheblichen Rechtsunsicherheit. Angesichts der Reichweite und Intensität der Maßnahmen ist eine grundsätzliche Diskussion über die verfassungsrechtliche Legitimation dringend geboten.

2.4 Unklare Transparenz und Governance

Wie bereits in der Vorbemerkung betont, sind transparente und wirksame Schutzvorkehrungen unverzichtbar, wenn Sicherheitsbehörden neue intrusive Befugnisse erhalten.[16] Der vorliegende Referentenentwurf spezifiziert solche Schutzmechanismen bislang jedoch nicht explizit.

Unklar bleibt insbesondere, nach welchen Standards und aus welchen Quellen BKA und Bundespolizei Schwachstellen, Exploits oder andere technische Werkzeuge für intrusive Cyberabwehroperationen beschaffen und wie diese anschließend verwaltet werden sollen. Angesichts der erheblichen Risiken und der problematischen Marktstruktur für solche Fähigkeiten wäre hier ein deutlich höheres Maß an Transparenz und Regulierung erforderlich.[17]

Darüber hinaus fehlt eine systematische Transparenz über Anordnungen, Genehmigungen und tatsächlich durchgeführte Maßnahmen. Ein Berichtssystem analog zu den Statistiken des

[16] Sven Herpig (2018): A Framework for Government Hacking in Criminal Investigations
[17] Foreign, Commonwealth & Development Office (2025): The Pall Mall Process declaration: tackling proliferation and irresponsible use of commercial cyber intrusion capabilities und Sven Herpig (2018): A Framework for Government Hacking in Criminal Investigations

Bundesamts für Justiz zur Telekommunikationsüberwachung könnte hier Abhilfe schaffen.[18] Insbesondere für Maßnahmen gemäß BPolG-E § 41a (7) oder BKAG-E § 62f (4) wäre eine solche Dokumentation notwendig, um Anwendungshäufigkeit, Effektivität und Verhältnismäßigkeit im Nachhinein beurteilen zu können.

Da bestimmte Maßnahmen ohne Wissen der Betroffenen durchgeführt werden dürfen – etwa verdeckte Eingriffe gemäß BKAG-E § 62e –, ist ein nachträglicher individueller Rechtsschutz strukturell ausgeschlossen. Um dieses Defizit auszugleichen, sollten unabhängige Kontrollmechanismen vorgesehen werden, etwa durch die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI). Eine solche institutionelle Kontrolle ermöglicht eine effektive Überprüfung der Maßnahmen, ohne den Ermittlungserfolg durch vorzeitige Bekanntgabe an potenziell Tatbeteiligte zu gefährden.

Schließlich ist bei polizeilichen Maßnahmen die Integrität der Beweismittelkette von zentraler Bedeutung – auch im digitalen Raum. Gerade vor dem Hintergrund erweiterter Befugnisse zum Löschen oder Verändern von Daten, etwa gemäß BKAG-E § 62e, wären klare technische Standards und Governance-Mechanismen erforderlich, um die Nachvollziehbarkeit und gerichtliche Verwertbarkeit digitaler Beweise sicherzustellen. Entsprechende Regelungen fehlen im vorliegenden Referentenentwurf bislang.

Der Referentenentwurf erweitert intrusive Cyberabwehrbefugnisse, ohne gleichzeitig die notwendigen Schutz-, Transparenz- und Governance-Mechanismen zu etablieren. Insbesondere beim Umgang mit Schwachstellen, der Dokumentation operativer Maßnahmen und der Sicherung digitaler Beweismittel bestehen erhebliche Regelungs- oder Transparenzlücken. Ohne entsprechende Standards drohen sowohl rechtliche Unsicherheiten als auch Risiken für Transparenz, Kontrolle und gerichtliche Verwertbarkeit.

[18] Bundesamt für Justiz (2025): Statistiken zur Telekommunikationsüberwachung für das Jahr 2023 veröffentlicht

3. Empfehlungen

Systematische Evaluierung einführen: Jede Maßnahme der Cyberabwehr sollte messbare Sicherheitsgewinne dokumentieren. So lassen sich politische und operative Entscheidungen transparent begründen. Nur auf dieser Basis können Wirksamkeit und Bedarf realistisch bewertet werden.

Verhältnismäßige Maßnahmen: Intrusive Eingriffe sollten auf das notwendige Minimum beschränkt werden. Effizienz, Wirksamkeit und Eskalationsrisiko sind zu prüfen, Risiken von Kollateralschäden und Werkzeugproliferation zu bewerten und die Kosten aktiver Cyberabwehr gegen die Risiken des Nicht-Handelns abzuwägen.

Verfassungsrechtliche Klarheit schaffen: Zuständigkeiten zwischen Bund und Ländern müssen eindeutig geregelt werden. Eine offene Grundsatzdebatte über BKA-Befugnisse und gegebenenfalls eine Grundgesetzänderung ist dafür erforderlich.

Operative Plattform etablieren: Alle relevanten Behörden müssen auf einer gemeinsamen Ebene planen und operative Maßnahmen koordinieren können. Nur so lassen sich Doppelstrukturen vermeiden und Effizienzgewinne realisieren.

Koordination sicherstellen: Einheitliche Abstimmungs- und Konfliktlösungsmechanismen zwischen BKA, BPol, BSI, BND und den Länderpolizeien sind notwendig. Dies schafft Klarheit bei Verantwortlichkeiten und verhindert zersplitterte Vorgehensweisen.

Personelle Kapazitäten erhöhen: Die Stellen für Threat Hunting und Vorfallsbearbeitung beim BSI sollten deutlich ausgebaut werden. Gleichzeitig ist die operative Handlungsfähigkeit strategisch zu stärken, um IT-Sicherheit und Resilienz effektiv zu erhöhen.

Transparenz und Schutzmechanismen stärken: Für intrusive Cyberabwehrbefugnisse sollten klare Regeln für Beschaffung, Nutzung und Verwaltung von Schwachstellen, Exploits und technischen Werkzeugen festgelegt sowie ein regelmäßiges Berichtssystem über angeordnete, genehmigte und durchgeführte Maßnahmen eingeführt werden. Ergänzend sind verbindliche technische Standards und Governance-Mechanismen erforderlich, um die Integrität digitaler Beweismittel und die gerichtliche Verwertbarkeit sicherzustellen; sofern vorhanden, sollten entsprechende Hinweise in den Gesetzesfolgen aufgenommen werden.