

Sehr geehrter [REDACTED]

Vielen Dank für Ihr Interesse an meinem Impulsvortrag im Rahmen des parlamentarischen Frühstücks [REDACTED]. Gerne gebe ich Ihnen einen etwas tieferen Überblick über die Herausforderungen für eine sachgerechte Verfolgung von unbefugten Drohnen bzw. ihren Piloten.

Kernaussage:

Das Strafgesetzbuch kennt keine Drohnen und leider auch keine kritische Infrastruktur.

Die Herausforderungen für die Gefahrenabwehrbehörden beginnen also damit, überhaupt erst einen relevanten Verstoß erfüllt zu sehen, um einen Eingriffsgrund zu haben.

Hier ein paar **Beispiele für infrage kommende Straftatbestände und die Schwierigkeiten bei der Anwendung.**

- **Hausfriedensbruch (§ 123 StGB):** Zwar fühlt man sich im Hausfrieden gestört, der Paragraph setzt allerdings voraus, dass der Täter selbst, nicht seine Drohne, ins Objekt eingedrungen ist. Das Eindringen per Drohne kann also keinen Hausfriedensbruch darstellen, und der Hausfriedensbruch stellt keine gravierende Straftat dar, die eine Zerstörung der Drohne rechtfertigen würde.
- **Nötigung (§ 240 StGB):** Wer eine Drohne über sich selbst oder seinem Objekt sichtet, kann evtl. seine Arbeiten nicht fortsetzen und fühlt sich genötigt. Der Straftatbestand setzt jedoch physische Gewalt voraus. Die Drohne selbst übt, sofern sie nicht abstürzt oder Waffen einsetzt, aber keine physische Gewalt aus. Sie ist dennoch in der Lage, allein durch ihre Anwesenheit den Betrieb zu stören und Unterbrechungen zu provozieren.
- **Störung öffentlicher Betriebe (§ 316b StGB):** Es wäre naheliegend, diesen Straftatbestand als erfüllt anzusehen. Allerdings sieht der Wortlaut des Paragraphen Einschränkungen vor („zerstören, beschädigen, beseitigen, verändern oder unbrauchbar machen oder el. Kraft entziehen“), die durch den bloßen Drohnenflug über der Kritis nicht erfüllt sind, obwohl dennoch aus Sicherheitsgründen der Betrieb gestört werden kann.
- **Gefährlicher Eingriff in den Bahn-, Schiffs- und Luftverkehr (§ 315 StGB) / Gefährlicher Eingriff in den Straßenverkehr (§ 315b StGB):** Hier hat die Polizei einen klaren Eingriffsgrund, denn der „gefährliche Eingriff“ ist eine gravierende Straftat. Das Problem für die meisten KRITIS-Betreiber: Sie fallen nicht unter den entsprechenden Paragraphen. Einen „gefährlichen Eingriff in die kritische Infrastruktur“ gibt es leider nicht. Interessant zu wissen: Der Eingriffsgrund für die Polizei entfällt ggf. automatisch mit der proaktiven Einstellung des Flug-/Bahn-Betriebs bzw. des Straßenverkehrs. D. h. selbst hier kann die Polizei nach Einstellung des Verkehrs nicht ohne Weiteres mit Gewalt gegen Drohnen vorgehen.
- **Nachstellung/Stalking (§ 238 StGB):** Das Verfolgen von Personen mittels Drohnen kann eine Straftat darstellen. Allerdings erst dann, wenn es wiederholt erfolgt. Ferner ist dies ein Antragsdelikt, das nur die geschädigte Person, nicht durch ein Unternehmen, angezeigt werden kann.
- **Körperverletzung (§ 223 StGB), schwere Körperverletzung (§ 224 StGB), fahrlässige Körperverletzung (§ 229 StGB):** Kommt es zu Körperverletzung (oder auch nur zum Versuch), hat die Polizei unmittelbar einen Eingriffsgrund. Ein Unternehmen kann diese einfache Körperverletzung aber nicht anzeigen. Das kann nur der Geschädigte selbst tun. Ist die Tat noch nicht vollzogen, ist es für die

Polizei schwer abzuwägen, ob eine unmittelbar gegenwärtige Gefahr vorliegt. Anders als beim Drohnenflug über Menschenansammlungen kommen diese Straftatbestände in der Regel in der Industrie kaum in Betracht.

Die **Polizei kann immer im Rahmen der Gefahrenabwehr tätig werden, vorausgesetzt eine Gefahr** liegt vor. Das lässt sich bei Drohnen, die „nur“ über der kritischen Infrastruktur fliegen, aber meist nicht beurteilen. Die Frage, wann eine Drohne gefährlich ist, ist rechtlich nicht geklärt und technisch aus der Ferne nicht erkennbar. Selbst vermeintlich harmlose Ladungen wie Aluminiumschnipsel oder die im Vortrag eines anderen Teilnehmers erwähnten leitfähigen Stäube (Metallspäne oder Graphitpulver zum Beispiel) können für die Energieinfrastruktur sehr gefährlich werden. Zur Abwehr von Gefahren kann die Polizei **unmittelbare Zwang** anwenden. Hier sind aber mitunter nicht alle Hilfsmittel gleichermaßen zulässig. Je nach Landespolizeigesetz sind die Hilfsmittel des unmittelbaren Zwangs definiert. Typischerweise z. B. Schlagstöcke, Wasserwerfer oder Pferde. Auch Waffen (hier z.B. Laser oder Schusswaffen) können eingesetzt werden, aber beim Einsatz von solchen gefährlichen Wirkmitteln entsteht ein hohes Rechtfertigungs-/Verhältnismäßigkeitsrisiko, dass absehbar weiterhin regelmäßig zur Entscheidung gegen die Drohnenabwehr führen wird.

Wie können wir das auflösen? Benötigt wird eine Schärfung des Strafrechts und ein besonderer Schutzstatus der kritischen Infrastruktur.

Einflug = Straftat, Abwehr = legitim.

1. Künftig muss der Einflug, aber auch das Eindringen am Boden eine gravierende Straftat – statt wie bisher eine bloße Ordnungswidrigkeit bzw. eine geringfügige Straftat (Hausfriedensbruch) – darstellen. Das sieht das neue LuftVG für Flugfelder ja nun auch vor, aber eben nicht für die übrige KRITIS.
2. Drohnen über Kritis sollen den Status als Luftverkehrsmittel verlieren, sodass die Neutralisierung keinen Eingriff in den Luftverkehr mehr darstellt.
3. Drohnenabwehr über Anlagen der KRITIS darf nicht als Sachbeschädigung gewertet werden. Naheliegender erscheint der Ansatz, dass der Pilot einer Drohne durch den Verstoß gegen Flugbeschränkungen sein Recht auf Eigentum an der Drohne teilweise oder vollständig verliert. In diesem Fall würde eine zerstörende Drohnenabwehr durch Zivilpersonen zumindest nicht mehr den Straftatbestand der Sachbeschädigung nach § 303 StGB erfüllen. Eine praxistaugliche Alternative ist die Beleihung von Betreibern kritischer Infrastrukturen oder von durch sie beauftragten Sicherheitsdiensten mit der hoheitlichen Aufgabe der Drohnenabwehr (vgl. entsprechende Empfehlungen des BDEW zur Schaffung einer Beleihungsgrundlage).
4. Der Einsatz von Jammern sollte zur Drohnenabwehr über Anlagen der KRITIS freigegeben werden. Derzeit ist er durch das Telekommunikationsgesetz grundsätzlich untersagt, während er in bestimmten Einrichtungen – insbesondere in Justizvollzugsanstalten – bereits zugelassen ist. Vor diesem Hintergrund stellt sich die Frage, ob eine Ausweitung des zulässigen Einsatzes von Jammern auf weitere Objekte der kritischen Infrastruktur in Betracht kommt und wie eine solche Ausnahme rechtssicher auszugestalten wäre.
5. Der Einsatz von Waffen wie Netzwerfern ist – je nach Art der Treibladung und Energiemenge – ebenfalls verboten oder zumindest waffenrechtlich stark eingeschränkt. Vor diesem Hintergrund wäre zu prüfen, inwieweit der Einsatz solcher Systeme für speziell ausgebildetes (Sicherheits-)Personal an Anlagen der KRITIS freigegeben werden kann und welche waffen- und sicherheitsrechtlichen Voraussetzungen hierfür zu schaffen wären. Parallel dazu stellt sich die Frage, wie

Polizei und andere hoheitliche Stellen technisch und rechtlich befähigt werden können, eine fernwirkte Drohnenabwehr durch fest installierte Systeme oder Interceptor-Drohnen durchzuführen.

6. Das routinemäßige Auslesen der mitgesendeten ID und das Verfolgen von Drohnen mit Kameras auch außerhalb der Einfriedung einer kritischen Infrastruktur darf kein Verstoß gegen die DSGVO darstellen. Zwar ist der Anflug an KRITIS schon jetzt außerhalb des Betriebsgeländes eine Ordnungswidrigkeit (100-m-Regel), aber eben nur eine Ordnungswidrigkeit und keine Straftat. Das überwiegende, berechnigte Interesse des KRITIS-Betreibers zur Verarbeitung dieser Daten (Art. 6 DSGVO) ist damit bisher nicht zweifelsfrei erfüllt. Das muss sich ändern.
7. Die drastische Beschränkung der Nutzung von Videoüberwachung durch die DSGVO ist im Ländervergleich (z. B. Niederlande und UK) nicht nachvollziehbar. Es sollten stattdessen zum Schutz der kritischen Infrastruktur klare Empfehlungen von Sicherheitsbehörden herausgegeben werden, die weit über die derzeitige - aus KRITIS-Sicht nicht nachvollziehbare - Empfehlung der Deutschen Datenschutzkonferenz (DE: max. 72 h) hinausgehen. Zum Vergleich: In NL/UK werden in der Regel 28–31 Tage Aufbewahrungszeit empfohlen.
8. Auch das berechnigte Interesse zur Videoüberwachung im unmittelbaren Nahbereich außerhalb von Geländeeinfriedungen sollte durch eine klare sicherheitsbehördliche Empfehlung bejaht werden. Kameras, die erst Bilder liefern dürfen, wenn ein Täter (oder die Drohne) den Zaun überwunden hat, sind nicht länger zeitgemäß.
9. Überbordende Transparenz – etwa durch Internetveröffentlichungen im Planungs- und Umweltrecht (z. B. in Genehmigungsverfahren und Umweltverträglichkeitsprüfungen) – stellt ein gravierendes Risiko für die KRITIS dar. Gerade im Zusammenhang mit AI-Tools sind ehemals schwer auffindbare Informationen über KRITIS im Internet heute viel zu leicht zugänglich. Selbst Laien, wie sogenannte „Low-Level-Agents“, können diese Informationen aufbereiten und anschließend missbrauchen. Unkontrollierte Online-Kartendienste wie OpenInfraMap.org dienen offenbar bereits jetzt der Ermittlung potenzieller Angriffsvektoren. Im Zusammenhang mit programmierten Drohnen(-schwärmen) gewinnt das Thema zusätzliche Brisanz und erfordert eine Neubewertung sowie gegebenenfalls Einschränkungen.