RED!SIGNAL — LESEPROBE

Das Darknet

Infrastruktur, Märkte und staatliche Kontrolle in anonymen Netzwerken

---

Die Leseprobe enthält Kapitel 1 und Kapitel 25 vollständig sowie das Inhaltsverzeichnis aller dreißig Kapitel.

DIE DREISSIG KAPITEL

Leseprobe

1. Gegenstand, Begriffe und Erkenntnisinteresse

1.1 Ein unscharfer Begriff mit harten Folgen

„Darknet“ ist kein technischer Terminus, sondern eine Sammelbezeichnung. Sie umfasst Dienste und Kommunikationsräume, die nur über besondere Software, besondere Protokolle oder besondere Zugangsvoraussetzungen erreichbar sind und deren Betrieb darauf angelegt ist, den Netzwerkstandort der Beteiligten nicht offenzulegen. Der Begriff hat sich in der öffentlichen Debatte durchgesetzt, obwohl er drei Dinge vermischt, die technisch klar auseinanderfallen: die Anonymisierungsinfrastruktur selbst, die auf ihr betriebenen Dienste und die dort stattfindenden Handlungen.

Diese Vermischung ist nicht folgenlos. Wer Infrastruktur und Handlung gleichsetzt, gelangt fast zwangsläufig zu Regulierungsvorschlägen, die die Infrastruktur adressieren, obwohl das Problem in den Handlungen liegt. Umgekehrt führt die Weigerung, den Zusammenhang überhaupt zu benennen, zu einer Verharmlosung, die weder kriminologisch noch politisch tragfähig ist. Die begriffliche Trennung ist deshalb keine akademische Vorübung, sondern die Voraussetzung dafür, überhaupt sinnvoll über Regulierung sprechen zu können.

1.2 Abgrenzungen

Vom „Deep Web“ ist das Darknet klar zu unterscheiden. Deep Web bezeichnet lediglich alle Inhalte, die von Suchmaschinen nicht indexiert werden — Datenbankinhalte hinter Formularen, Intranets, passwortgeschützte Bereiche, dynamisch erzeugte Seiten. Das ist der weitaus größte Teil des Webs und in aller Regel vollkommen unspektakulär. Anonymisierende Overlay-Netze wie Tor, I2P oder Freenet/Hyphanet sind demgegenüber durch ein aktives Schutzziel definiert: Sie sollen die Zuordnung von Kommunikationsbeziehungen zu Netzwerkstandorten erschweren.

Ebenso ist zwischen anonymer Nutzung des offenen Webs und dem Betrieb von Diensten innerhalb des Overlay-Netzes zu trennen. Wer über Tor eine gewöhnliche Website aufruft, nutzt Anonymisierung als Zugangsschutz. Wer einen Onion Service betreibt, verlagert auch den Dienst selbst in das Netz hinein. Beide Fälle haben unterschiedliche Bedrohungsmodelle, unterschiedliche Angriffsflächen und unterschiedliche rechtliche Anknüpfungspunkte.

1.3 Erkenntnisinteresse

Für dieses Buch ist das Darknet weder ausschließlich Kriminalitätsraum noch ausschließlich Schutztechnologie. Es ist ein Feld, in dem sich zwei legitime, aber schwer vereinbare Ansprüche überschneiden: der Anspruch auf vertrauliche, unbeobachtete Kommunikation und der Anspruch des Rechtsstaats auf Aufklärung schwerer Straftaten. Beide Ansprüche sind grundrechtlich fundiert. Die interessante Frage ist deshalb nicht, welcher von beiden richtig ist, sondern unter welchen institutionellen Bedingungen ihr Konflikt bearbeitbar bleibt.

Das Erkenntnisinteresse ist entsprechend dreifach. Erstens technisch: Was leistet die Infrastruktur tatsächlich, und wo liegen ihre Grenzen? Zweitens sozial und ökonomisch: Wie entstehen in einem Raum ohne staatliche Vertragsdurchsetzung dennoch stabile

Austauschbeziehungen? Drittens institutionell: Welche Formen von Kontrolle sind wirksam, welche sind bloß symbolisch, und welche erzeugen Kosten, die den Nutzen übersteigen?

1.4 Methodische Grundhaltung

Methodisch verbindet die Darstellung Technikgeschichte, Netzwerkarchitektur, Kriminologie, Plattformökonomie, Rechtsvergleichung und Regulierungsforschung. Diese Kombination ist notwendig, weil jede Einzelperspektive systematisch verzerrt. Eine rein technische Darstellung überschätzt die Steuerungskraft von Protokolldesign. Eine rein kriminologische Darstellung überschätzt den Anteil illegaler Nutzung. Eine rein juristische Darstellung unterschätzt, wie schnell sich technische Voraussetzungen unter dem Recht verändern.

Der Text arbeitet deshalb durchgehend mit einer Unterscheidung, die im weiteren Verlauf immer wiederkehrt: zwischen dem, was technisch möglich ist, dem, was praktisch geschieht, und dem, was rechtlich zurechenbar ist. Diese drei Ebenen fallen im Darknet häufiger auseinander als in fast jedem anderen digitalen Kontext. Genau das macht den Gegenstand als Prüfstein digitaler Ordnung interessant.

Ende Kapitel 1.

25. Quantencomputer, Post-Quanten-Kryptografie und die langfristige Sicherheit anonymer Netze

25.1 Das Bedrohungsmodell

Ein hinreichend leistungsfähiger Quantencomputer würde mit dem Shor-Algorithmus die derzeit verbreiteten asymmetrischen Verfahren brechen: RSA, Diffie-Hellman und Verfahren auf elliptischen Kurven. Symmetrische Verfahren sind weniger betroffen; der Grover-Algorithmus halbiert dort effektiv die Schlüssellänge, was durch längere Schlüssel ausgeglichen werden kann.

Für Anonymitätsnetze ist die praktisch relevante Bedrohung nicht der spätere Bruch einer aktuellen Verbindung, sondern das Sammeln heute und Entschlüsseln später. Aufgezeichneter Verkehr behält seinen Aussagewert über Jahrzehnte — bei politisch sensiblen Kommunikationsbeziehungen sogar besonders lange.

25.2 Die Lage bei Tor

Tor verwendet für den Circuit-Aufbau das ntor-Handshake, das auf klassischen Diffie-Hellman-Annahmen beruht und damit nicht quantenresistent ist. Die Fachliteratur hat mehrere hybride Ansätze entwickelt, die einen klassischen Schlüsselaustausch mit einem gitterbasierten Kapselungsverfahren kombinieren, sodass die Sicherheit erhalten bleibt, solange mindestens eines der beiden Verfahren hält (Ghosh und Kate 2015; Schanck et al. 2016). Neuere Arbeiten analysieren die vollständige Migration einschließlich Onion-Service-Descriptors, Introduction- und Rendezvous-Punkten sowie der Signaturverfahren der Verzeichnisinfrastruktur (Buchanan et al. 2025).

Betroffen sind dabei zwei unterschiedliche Bausteine mit unterschiedlicher Dringlichkeit. Schlüsselaustausch ist vorrangig, weil er der Sammeln-und-später-entschlüsseln-Bedrohung unmittelbar ausgesetzt ist. Signaturen sind nachrangig, weil eine Fälschung erst in dem Moment nützt, in dem der Quantencomputer existiert — sie müssen aber rechtzeitig ausgetauscht sein, weil Umstellungen im Verzeichnissystem lange Vorlaufzeiten haben.

25.3 Standardisierung und Zeitrahmen

Die Standardisierung ist weit fortgeschritten: Das NIST veröffentlichte 2024 die Standards FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) und FIPS 205 (SLH-DSA) und wählte 2025 zusätzlich HQC als zweites Kapselungsverfahren aus, um nicht ausschließlich von gitterbasierten Annahmen abzuhängen. Im breiten Web ist hybrider Schlüsselaustausch bereits verbreitet; ein erheblicher Anteil der TLS-Verbindungen großer Anbieter läuft quantenresistent.

Für Tor ist die Umstellung anspruchsvoller als für TLS. Die größeren Schlüssel und Chiffrate erhöhen die Datenmenge beim Circuit-Aufbau; bei einem mehrstufigen Aufbau summiert sich dieser Zusatzaufwand, und das Netz wird von freiwillig betriebenen, teils leistungsschwachen Relays getragen. Die veröffentlichten Abschätzungen halten die Migration für technisch machbar, benennen aber Latenz- und Bandbreitenkosten als zentrale Nebenbedingung.

Abb. 7 — Post-Quanten-Migration: Dringlichkeit nach Baustein

25.4 Was das für die Ordnungsfrage bedeutet

Politisch relevant ist ein oft übersehener Punkt: Die Post-Quanten-Umstellung nützt Schutzbedürftigen und Straftätern gleichermaßen — und sie nützt zugleich der staatlichen und wirtschaftlichen Infrastruktur, deren Absicherung dieselben Verfahren voraussetzt. Es gibt daher, anders als bei der Frage nach Zugriffsmöglichkeiten, keinen Interessengegensatz: Alle Beteiligten benötigen dieselbe Migration. Das macht diesen Bereich zu einem der wenigen, in denen sicherheitspolitischer Konsens tatsächlich besteht.

Ende Kapitel 25.

Die Vollfassung umfasst alle dreißig Kapitel in beiden Sprachen, mit Fußnotenapparat, Literaturverzeichnis, Sachregister, Glossar und acht Abbildungen. Lizenzen und Konditionen auf Anfrage.

office@entropicunit.eu

The Darknet

Infrastructure, Markets and State Control in Anonymous Networks

The sample contains chapters 1 and 25 in full, together with the table of contents of all thirty chapters.

THE THIRTY CHAPTERS

Sample

1. Subject, Terms and Purpose of Inquiry

1.1 An imprecise term with hard consequences

"Darknet" is not a technical term but a collective label. It covers services and communication spaces that are reachable only through particular software, particular protocols or particular access conditions, and whose operation is designed not to disclose the network location of those involved. The term has established itself in public debate even though it conflates three things that are technically quite distinct: the anonymising infrastructure itself, the services operated on it, and the actions taking place there.

This conflation is not without consequence. Anyone who equates infrastructure with conduct will almost inevitably arrive at regulatory proposals that address the infrastructure although the problem lies in the conduct. Conversely, refusing to name the connection at all leads to a trivialisation that is neither criminologically nor politically tenable. Terminological separation is therefore not an academic preliminary but the precondition for speaking meaningfully about regulation at all.

1.2 Distinctions

The darknet must be clearly distinguished from the "deep web". Deep web denotes merely all content not indexed by search engines — database content behind forms, intranets, password-protected areas, dynamically generated pages. This is by far the largest part of the web and as a rule entirely unspectacular. Anonymising overlay networks such as Tor, I2P or Freenet/Hyphanet are defined by an active protective goal: they are intended to make it difficult to attribute communication relationships to network locations.

A second distinction runs between anonymous use of the open web and the operation of services inside the overlay network. Someone who uses Tor to reach an ordinary website is using anonymisation as access protection. Someone who operates an onion service moves the service itself into the network. The two cases have different threat models, different attack surfaces and different legal points of attachment.

1.3 Purpose of inquiry

For this book the darknet is neither exclusively a space of crime nor exclusively a protective technology. It is a field in which two legitimate but hard-to-reconcile claims overlap: the claim to confidential, unobserved communication and the claim of the constitutional state to investigate serious crime. Both are grounded in fundamental rights. The interesting question is therefore not which of the two is correct, but under what institutional conditions their conflict remains manageable.

The inquiry is accordingly threefold. First, technical: what does the infrastructure actually achieve, and where are its limits? Second, social and economic: how do stable exchange relationships nevertheless arise in a space without state enforcement of contracts? Third, institutional: which forms of control are effective, which are merely symbolic, and which generate costs exceeding their benefit?

1.4 Methodological stance

Methodologically the account combines the history of technology, network architecture, criminology, platform economics, comparative law and regulatory research. This combination is necessary because every single perspective distorts systematically. A purely technical account overestimates the steering capacity of protocol design. A purely criminological account overestimates the share of illegal use. A purely legal account underestimates how quickly technical conditions change beneath the law.

The text therefore works throughout with a distinction that recurs in what follows: between what is technically possible, what actually happens, and what is legally attributable. These three levels diverge more often in the darknet than in almost any other digital context. That is precisely what makes the subject interesting as a test case for digital order.

End of Chapter 1.

Sample

25. Quantum Computers, Post-Quantum Cryptography and the Long-Term Security of Anonymous Networks

25.1 The threat model

A sufficiently powerful quantum computer would, using Shor's algorithm, break the asymmetric methods in common use: RSA, Diffie-Hellman and elliptic-curve schemes. Symmetric methods are less affected; Grover's algorithm effectively halves the key length there, which can be compensated by longer keys.

For anonymity networks the practically relevant threat is not the later breaking of a current connection but harvesting now and decrypting later. Recorded traffic retains its evidential value for decades — in politically sensitive communication relationships, particularly long.

25.2 The situation at Tor

Tor uses the ntor handshake for circuit construction, which rests on classical Diffie-Hellman assumptions and is therefore not quantum-resistant. The literature has developed several hybrid approaches combining a classical key exchange with a lattice-based encapsulation method, so that security is preserved as long as at least one of the two holds (Ghosh and Kate 2015; Schanck et al. 2016). More recent work analyses the complete migration, including onion-service descriptors, introduction and rendezvous points and the signature schemes of the directory infrastructure (Buchanan et al. 2025).

Two distinct components are affected, with differing urgency. Key exchange takes priority because it is directly exposed to the harvest-now-decrypt-later threat. Signatures rank second because forgery becomes useful only once a quantum computer exists — but they must be replaced in good time, since changes in the directory system have long lead times.

25.3 Standardisation and time frame

Standardisation is well advanced: NIST published the standards FIPS 203 (ML-KEM), FIPS 204 (ML-DSA) and FIPS 205 (SLH-DSA) in 2024 and additionally selected HQC as a second encapsulation method in 2025, in order not to depend exclusively on lattice-based assumptions. On the broad web, hybrid key exchange is already widespread; a substantial share of TLS connections to major providers is quantum-resistant.

For Tor the transition is more demanding than for TLS. Larger keys and ciphertexts increase the data volume of circuit construction; with multi-stage construction this additional cost accumulates, and the network is carried by voluntarily operated, sometimes low-capacity relays. Published assessments consider the migration technically feasible but identify latency and bandwidth costs as the central constraint.

Fig. 7 — Post-quantum migration: urgency by component

25.4 What this means for the question of order

Politically relevant is an often overlooked point: post-quantum migration benefits those in need of protection and offenders alike — and it simultaneously benefits state and economic infrastructure, whose security presupposes the same methods. Unlike the question of access

capabilities, there is therefore no conflict of interest: all parties require the same migration. That makes this one of the few areas in which security-policy consensus genuinely exists.

End of Chapter 25.

The full edition comprises all thirty chapters in both languages, with footnote apparatus, bibliography, subject index, glossary and eight figures. Licences and terms on request.

office@entropicunit.eu