Dr. Ir. Agus Wibowo, M.Kom, M.Si, MM.

TATA KELOLA TEKNOLOGI DI BIDANG HUKUM DAN REGULASI

YAYASAN PRIMA AGUS TEKNIK
UNIVERSITAS SAINS & TEKNOLOGI KOMPUTER
UNIVERSITAS STEKOM

TATA KELOLA TEKNOLOGI DI BIDANG HUKUM DAN REGULASI

Dr. Ir. Agus Wibowo, M.Kom, M.Si, MM.

YAYASAN PRIMA AGUS TEKNIK

PENERBIT :
YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

TATA KELOLA TEKNOLOGI DI BIDANG HUKUM DAN REGULASI

Penulis :
Dr. Ir. Agus Wibowo, M.Kom, M.Si, MM.

ISBN :

Editor :
Dr. Joseph Teguh Santoso, S.Kom., M.Kom.

Penyunting :
Dr. Mars Caroline Wibowo. S.T., M.Mm.Tech

Desain Sampul dan Tata Letak :
Irdha Yunianto, S.Ds., M.Kom

Penebit :
Yayasan Prima Agus Teknik Bekerja sama dengan
Universitas Sains & Teknologi Komputer (Universitas STEKOM)

Anggota IKAPI No: 279 / ALB / JTE / 2023

Redaksi :
Jl. Majapahit no 605 Semarang
Telp. 08122925000
Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id

Distributor Tunggal :
Universitas STEKOM
Jl. Majapahit no 605 Semarang
Telp. 08122925000
Fax. 024-6710144
Email : info@stekom.ac.id

Hak cipta dilindungi undang-undang
Dilarang memperbanyak karya tulis ini dalam bentuk dan dengan cara apapun tanpa ijin dari penulis

KATA PENGANTAR

Puji syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa, karena atas rahmat, karunia, dan izin-Nya buku yang berjudul "*Tata Kelola Teknologi di Bidang Hukum dan Regulasi"* ini akhirnya dapat diselesaikan dengan baik. Penyusunan buku ini merupakan bentuk kontribusi akademik untuk menjawab perkembangan pesat teknologi, khususnya teknologi kuantum, yang semakin memengaruhi lanskap hukum, kebijakan publik, keamanan siber, kekayaan intelektual, perdagangan internasional, serta hubungan antarnegara.

Perkembangan teknologi modern telah melahirkan peluang yang sangat besar, namun sekaligus menghadirkan tantangan baru bagi sistem hukum dan tata kelola regulasi. Dalam konteks tersebut, buku ini disusun untuk memberikan pemahaman yang lebih komprehensif mengenai hubungan timbal balik antara inovasi teknologi dan instrumen hukum yang mengaturnya. Fokus pembahasan diarahkan pada teknologi informasi kuantum, perlindungan kekayaan intelektual, lanskap paten, keamanan siber Uni Eropa, pengendalian ekspor komputasi kuantum, serta dimensi strategis teknologi kuantum dalam hukum internasional dan geopolitik global.

Buku ini terdiri atas tujuh bab yang disusun secara sistematis agar pembaca dapat mengikuti alur pemikiran dari dasar konseptual hingga implikasi praktisnya. Bab pertama membahas tata kelola teknologi kuantum dari perspektif hukum dan regulasi. Bab kedua menguraikan teknologi informasi kuantum dalam kerangka hukum, termasuk prinsip-prinsip informasi kuantum, dampak teknis, serta konsekuensi hukumnya. Bab ketiga menyoroti kekayaan intelektual pada teknologi informasi kuantum, dengan perhatian pada paten, rahasia dagang, dan inovasi terbuka. Bab keempat membahas lanskap paten teknologi kuantum dan dampak kebijakan yang menyertainya.

Selanjutnya, bab kelima mengulas regulasi keamanan siber Uni Eropa dalam menghadapi ancaman kuantum yang kian nyata. Bab keenam membahas tantangan dan peluang regulasi ekspor komputasi kuantum, terutama dalam konteks kebijakan unilateral dan multilateral. Adapun bab ketujuh mengkaji hubungan teknologi informasi kuantum dengan hukum internasional, termasuk dimensi strategis, geopolitik, penggunaan dalam masa damai, serta relevansinya dalam konflik bersenjata siber. Dengan susunan tersebut, buku ini diharapkan tidak hanya menjadi bahan bacaan akademik, tetapi juga rujukan konseptual bagi mahasiswa, dosen, peneliti, praktisi hukum, pembuat kebijakan, dan pemerhati teknologi.

Penulis menyadari bahwa penyusunan buku ini tidak terlepas dari berbagai keterbatasan, baik dalam hal keluasan referensi, kedalaman analisis, maupun dinamika perkembangan isu teknologi dan regulasi yang sangat cepat berubah. Oleh karena itu, masukan, kritik, dan saran yang membangun sangat penulis harapkan demi penyempurnaan karya ini pada masa mendatang. Harapannya, buku ini dapat memberikan manfaat, memperkaya wawasan, serta mendorong diskusi ilmiah yang lebih luas mengenai tata kelola teknologi dalam kerangka hukum dan regulasi yang adaptif, responsif, dan berbasis bukti.

Akhir kata, penulis menyampaikan terima kasih kepada semua pihak yang telah memberikan dukungan, baik secara langsung maupun tidak langsung, dalam proses penyusunan buku ini. Semoga buku ini dapat memberi sumbangan yang berarti bagi pengembangan ilmu pengetahuan, khususnya di bidang hukum teknologi, regulasi, dan tata kelola inovasi.

Semangat & Selamat Membaca.....!!!!!

Semarang, Juli 2026
Penulis

Dr. Ir. Agus Wibowo, M.Kom, M.Si, MM.

DAFTAR ISI

KATA PENGANTAR ..... **i**
DAFTAR ISI ..... **iii**
BAB 1 TATA KELOLA TEKNOLOGI KUANTUM: PERSPEKTIF HUKUM DAN REGULASI .. **1**
1.1 Pendahuluan 1
1.2 Teknologi Informasi Kuantum Dan Hukum 3
1.3 Hukum Kekayaan Intelektual: Paten, Rahasia Dagang, Dan Inovasi Terbuka 3
1.4 Tren Paten Teknologi Kuantum Global 4
1.5 Hukum Kuantum Dan Keamanan Siber 4
1.6 Hukum Kuantum Dan Pengendalian Ekspor 5
1.7 Kuantum Dan Hukum Internasional: Dimensi Strategis Dan Geopolitik 6
1.8 Tata Kelola Adaptif Teknologi Kuantum 6
1.9 Tata Kelola Kuantum Adaptif Dan Berbasis Bukti 7
BAB 2 TEKNOLOGI INFORMASI KUANTUM DAN HUKUM **9**
2.1 Teknologi Informasi Kuantum Dalam Kerangka Hukum 9
2.2 Sejarah Revolusi Kuantum 12
2.3 Hukum Dan Teknologi Kuantum 14
2.4 QIT Dan Kerangka Hukum Yang Berlaku 17
2.5 Tata Kelola QIT Berlapis 19
2.6 Kekhususan Tata Kelola QIT 21
2.7 Tumpukan Tata Kelola, Skema Tata Kelola, Dan Risiko 25
2.8 Menyatukan Teknologi Dan Hukum Melalui Informasi 29
2.9 Prinsip Informasi Kuantum 36
2.10 Ontologi Kuantum Dan Dampak Hukum 41
2.11 Komputasi Kuantum Dan Simulasi Kuantum 46
2.12 Komunikasi Kuantum Dan Kriptografi Kuantum 48
2.13 Penginderaan Kuantum Dan Metrologi Kuantum 49
2.14 Tumpukan Infrastruktur Kuantum 50
2.15 Dampak Teknis QIT 55
2.16 Konsekuensi Hukum Dari QIT 59
2.17 Tumpukan Tata Kelola QIT 65
2.18 Integrasi Tata Kelola QIT 68
2.19 Teori Pemrosesan Informasi Klasik Dan Kuantum 68
2.20 Efek Kategorikal QIT 76
BAB 3 KEKAYAAN INTELEKTUAL PADA TEKNOLOGI INFORMASI KUANTUM **81**
3.1 Kekayaan Intelektual Dan Inovasi Terbuka Teknologi Informasi Kuantum 81
3.2 Teknologi Kuantum Dan Hukum Paten 84
3.3 Kerahasiaan Strategis Dalam Pembelajaran Dan Pengembangan Kuantum 87
3.4 Mekanisme Kolaboratif Di Seluruh Tumpukan Tata Kelola 89

3.5 Pola, Insentif, Dan Logika Pengungkapan 98
3.6 Strategi IP Terkalibrasi Dalam Teknologi Informasi Kuantum 99
BAB 4 LANSKAP PATEN TEKNOLOGI KUANTUM DAN DAMPAK KEBIJAKAN 100
4.1 Kemajuan Teknologi Kuantum 2G Dan Dampak Kebijakan 100
4.2 Definisi Teknologi Kuantum 102
4.3 Strategi Pencarian Dan Kriteria Seleksi Paten 103
4.4 Hasil Pemeriksaan Lanskap Paten 105
4.5 Studi Terkini Atas Lanskap Paten Kuantum 115
4.6 Dampak Lanskap Paten Kuantum Terkini 117
4.7 Dampak Kebijakan Lanskap Paten Kuantum 120
BAB 5 REGULASI KEAMANAN SIBER UNI EROPA DI ERA KUANTUM 122
5.1 Paten, Keamanan Siber, Dan Kebijakan Kuantum 122
5.2 Ancaman Kuantum Terhadap Keamanan Siber 123
5.3 Regulasi Keamanan Siber Uni Eropa 125
5.4 Reformulasi Regulasi Keamanan Siber UE Terhadap Ancaman Kuantum 133
5.5 Kesimpulan Dan Dampak Keamanan Siber UE 140
BAB 6 TANTANGAN DAN PELUANG REGULASI EKSPOR KOMPUTASI KUANTUM 143
6.1 Kontrol Ekspor Teknologi Kuantum: Fungsi Dan Tantangan Kebijakan 143
6.2 Logika Dan Cakupan Kontrol Ekspor 145
6.3 Instrumen Pengendalian Ekspor Unilateral Dan Multilateral 147
6.4 Kontrol Ekspor Eropa Dan AS Yang Relevan Dengan Komputasi Kuantum 148
6.5 Tantangan Dan Peluang Pengendalian Ekspor 158
6.6 Risiko Dan Manfaat Pengendalian Ekspor Komputasi Kuantum 166
BAB 7 QIT DAN HUKUM INTERNASIONAL: DIMENSI STRATEGIS-GEOPOLITIK 168
7.1 QIT Dan Hukum Internasional: Kerangka Penerapan Doktrin 168
7.2 Dampak Geopolitik Teknologi Kuantum 169
7.3 Faktor Teknis Yang Mempengaruhi QIT Strategis 173
7.4 Pengaruh QIT Terhadap Perilaku Strategis 180
7.5 Skenario Geopolitik 182
7.6 Hukum Internasional Dan Teknologi Informasi Kuantum 186
7.7 Hukum Internasional Umum Dan Ruang Siber 196
7.8 QIT Dalam Masa Damai: Intervensi Dan Penggunaan Kekerasan 202
7.9 Penggunaan QIT Selama Konflik 206
7.10 QIT Dan Konflik Bersenjata Siber 208
7.11 Perbandingan Dengan Hukum Telekomunikasi 213
7.12 Integrasi QIT Dalam Hukum Internasional Publik 215
7.13 Kesimpulan 216
DAFTAR PUSTAKA 220

BAB 1
TATA KELOLA TEKNOLOGI KUANTUM: PERSPEKTIF HUKUM DAN REGULASI

Bab ini menawarkan pemantauan umum tentang Tata Kelola Teknologi Kuantum: Hukum & Regulasi, menyoroti peran fundamental teknologi informasi kuantum (QIT) dan pertimbangan hukum, regulasi, dan geopolitik yang muncul dari kemajuan terbarunya. Bagian ini memetakan bagaimana komputasi, komunikasi, dan penginderaan kuantum beririsan dengan kerangka hukum dan tata kelola yang mapan di seluruh kekayaan intelektual, keamanan siber, kontrol ekspor, dan hukum internasional. Bab ini memperkenalkan struktur analitis progresif yang dimulai dengan fondasi ontologis dan tata kelola QIT sebelum beralih ke pertimbangan regulasi khusus domain dan dampak strategis global. Bab ini mensintesis tema-tema utama yang dikembangkan di seluruh volume, termasuk interpretasi hukum adaptif; mekanisme tata kelola berlapis seperti model tumpukan tata kelola; strategi kekayaan intelektual campuran yang menggabungkan paten, rahasia dagang, dan inovasi terbuka; tren paten empiris; pendekatan Uni Eropa dan AS terhadap risiko keamanan siber yang didukung kuantum; evolusi arsitektur kontrol ekspor; dan penerapan norma berbasis efek dalam hukum internasional publik. Di seluruh domain ini, bagian ini mengidentifikasi tema berulang tentang adaptabilitas regulasi. Meskipun QIT memperkenalkan fitur non-klasik yang menguji sistem hukum dan kebijakan yang ada, kami berpendapat bahwa banyak tantangan dapat diatasi melalui fleksibilitas interpretatif, pembuatan kebijakan berbasis bukti, dan tata kelola teknologi daripada reformasi doktrin secara menyeluruh. Dengan mengintegrasikan pemeriksaan hukum, wawasan empiris, dan perspektif tata kelola internasional, bagian ini memberikan pembuat kebijakan, ahli teknologi, cendekiawan, dan praktisi peta jalan untuk tata kelola kuantum yang bertanggung jawab seiring transisi teknologi dari potensi teoretis ke penerapan praktis.

1.1 PENDAHULUAN

Teknologi kuantum mewakili pergeseran paradigma dalam komputasi, komunikasi, dan penginderaan, menjanjikan kemajuan yang belum pernah terjadi sebelumnya di berbagai bidang mulai dari kriptografi dan penemuan obat hingga ilmu material dan simulasi kuantum. Inti dari revolusi ini terletak pada teknologi informasi kuantum (QIT), yang memanfaatkan prinsip-prinsip mekanika kuantum seperti superposisi dan keterikatan untuk memproses informasi di luar kemampuan sistem klasik untuk tugas-tugas tertentu. Revolusi kuantum generasi kedua ini dibangun di atas revolusi pertama, yang melahirkan teknologi fundamental seperti transistor, laser, dan teknologi MRI, dengan secara eksplisit memanfaatkan fenomena mekanika kuantum. Misalnya, superposisi memungkinkan bit kuantum (*qubit*) untuk berada dalam banyak keadaan secara bersamaan, memungkinkan percepatan komputasi

eksponensial untuk tugas-tugas tertentu, sementara keterikatan memungkinkan korelasi yang menentang lokalitas klasik, membuka pintu bagi protokol komunikasi yang aman.

Potensi transformatif ini menghadirkan dampak kunci bagi tata kelola teknologi, hukum, regulasi, dan standar internasional. Seiring sistem kuantum berevolusi dari konstruksi teoretis menjadi aplikasi praktis yang terbukti dalam tonggak sejarah seperti demonstrasi keunggulan kuantum dengan prosesor yang dapat diprogram, hal ini menimbulkan pertanyaan tentang perlindungan kekayaan intelektual (IP), kerentanan keamanan siber, kontrol ekspor internasional, dan strategi geopolitik. Misalnya, sifat penggunaan ganda QIT yang mencakup inovasi sipil seperti simulasi farmasi dan aplikasi militer seperti dekripsi tingkat lanjut memperkuat risiko proliferasi dan ketidakseimbangan strategis, sehingga memerlukan kerangka kerja yang menyeimbangkan inovasi terbuka dengan keharusan keamanan.

Dampak ini diperparah oleh sifat dan kecepatan inovasi, yang dapat menguji kerangka hukum yang ada dan dapat menciptakan kekosongan tata kelola yang dapat memperburuk risiko seperti pelanggaran data dan bahkan ancaman terhadap keamanan global. Misalnya, ancaman kuantum terhadap keamanan siber, seperti serangan "panen sekarang, dekripsi nanti" yang mengeksploitasi algoritma Shor untuk melemahkan enkripsi asimetris, mungkin memerlukan inisiatif tata kelola teknologi antisipatif. Demikian pula, lonjakan pengajuan paten yang mencerminkan tingkat pertumbuhan tahunan gabungan sebesar 14,5% dari tahun 2001 hingga 2025 menyoroti kebutuhan akan kebijakan yang terus mendorong pengungkapan untuk memperkaya domain publik, melawan kecenderungan menuju kerahasiaan dagang di bidang yang padat modal.

Buku ini, Tata Kelola Teknologi Kuantum: Hukum & Regulasi, membahas keharusan ini dengan menyatukan perspektif interdisipliner dari hukum, kebijakan, teknologi, dan hubungan internasional. Buku ini bertujuan untuk memberikan para sarjana, pembuat kebijakan, praktisi, dan ahli teknologi peta jalan yang komprehensif untuk menavigasi lanskap hukum dan peraturan teknologi kuantum. Mengacu pada konsep-konsep seperti SEA (perlindungan, keterlibatan, kemajuan) dan model tumpukan tata kelola yang menyelaraskan instrumen peraturan dengan lapisan teknis QIT dari perangkat keras hingga algoritma, buku ini mengeksplorasi bagaimana hukum yang ada dapat diterapkan atau diadaptasi, di mana panduan atau peraturan baru mungkin diperlukan, dan dampak yang lebih luas bagi masyarakat di era keunggulan kuantum. Dengan meneliti dimensi domestik dan internasional, termasuk penerapan norma berbasis dampak dari hukum internasional publik dan kontrol ekspor, buku ini menggarisbawahi perlunya tata kelola teknologi yang bijaksana (keterlibatan) untuk memastikan bahwa teknologi kuantum terus maju dan bermanfaat bagi umat manusia (kemajuan) sambil mengurangi potensi risiko dan kerugian negatif (perlindungan). Struktur buku ini dirancang untuk membangun secara progresif dari konsep dasar hingga pertimbangan regulasi khusus dan pertimbangan global. Setelah pengantar ini, bagian-bagian selanjutnya membahas aspek-aspek kunci dari tata kelola teknologi kuantum. Berikut adalah gambaran umum struktur dan isi buku ini.

1.2 TEKNOLOGI INFORMASI KUANTUM DAN HUKUM

Bidang ini menetapkan titik temu mendasar antara teknologi informasi kuantum (QIT) dan prinsip-prinsip hukum, menekankan fitur ontologis unik kuantum dan dampak tata kelolanya. Bidang ini membedakan antara teknologi kuantum generasi pertama dan kedua, di mana inovasi generasi kedua seperti komputasi kuantum memanfaatkan superposisi dan keterikatan dengan cara yang menantang asumsi hukum klasik tentang kepastian dan reproduksibilitas, dan meneliti sejauh mana tata kelola QIT dapat diakomodasi melalui adaptasi hukum dan regulasi interpretatif daripada perombakan doktrinal. Model tumpukan tata kelola menyelaraskan alat regulasi dengan lapisan QIT dari perangkat keras hingga algoritma memungkinkan manajemen risiko yang ditargetkan dan mengklarifikasi bahwa sebagian besar QIT berada di bawah hukum komputasi yang ada, berpotensi mengurangi kebutuhan akan kerangka kerja yang sepenuhnya baru. Sifat probabilistik kuantum menimbulkan isu-isu baru di bidang seperti tanggung jawab dan kontrak, seperti mengaitkan kesalahan dalam hasil yang diinduksi kuantum, tetapi hal ini mungkin dapat diatasi melalui lensa teori informasi yang memperlakukan QIT sebagai perluasan dari sistem klasik.

Pemeriksaan ini mengungkapkan potensi dampak pada privasi dan standar bukti, di mana teorema tanpa kloning mempersulit duplikasi data, namun metode verifikasi tidak langsung membantu menjaga keberlakuan hukum. Dengan membingkai kemampuan QIT (misalnya, penginderaan ultra-presisi, dekripsi), diskusi ini menyoroti peluang untuk tata kelola etis, menganjurkan pendekatan multidisiplin untuk menyeimbangkan inovasi dengan risiko sosial tanpa membatasi pengembangan secara prematur. Bagian dasar ini menyiapkan panggung untuk bagian-bagian selanjutnya tentang hukum dan regulasi, mengilustrasikan bagaimana prinsip-prinsip inti kuantum memerlukan benang merah fleksibilitas interpretatif yang kohesif di seluruh domain hukum untuk mendorong kemajuan yang bertanggung jawab.

1.3 HUKUM KEKAYAAN INTELEKTUAL: PATEN, RAHASIA DAGANG, DAN INOVASI TERBUKA

Area ini mengeksplorasi strategi kekayaan intelektual dalam teknologi informasi kuantum, menggambarkan "superposisi" di mana paten, rahasia dagang, dan inovasi terbuka hidup berdampingan secara strategis di seluruh tumpukan kuantum. Perusahaan memadukan alat-alat ini secara kontekstual (misalnya, menggunakan rahasia dagang untuk pengetahuan tacit dalam lapisan perangkat keras seperti sistem kriogenik, sementara paten melindungi penemuan yang dapat direproduksi) memungkinkan perlindungan yang seimbang, sebagaimana dibuktikan oleh lonjakan pengajuan sejak tahun 2014. Keterbukaan melalui kerangka kerja seperti Qiskit IBM mendorong ekosistem dan efek jaringan, memberikan keunggulan kompetitif bagi perusahaan yang sudah mapan dan akses bagi peneliti dan perusahaan rintisan, menangkal kekhawatiran akan kekayaan intelektual yang eksklusif. Fitur probabilistik Quantum menguji doktrin paten seperti pengaktifan. Bagian ini memeriksa sejauh mana sistem paten mampu mengakomodasi penemuan QIS.

Peran kerahasiaan dagang tetap ada karena kontrol ekspor dan kompleksitas R&D, namun paten mendorong pengungkapan, memperkaya domain publik dan mengurangi risiko

kerumitan dalam lanskap pemilik yang beragam. Pendekatan berlapis mengkalibrasi IP pada tingkat tumpukan tertentu mengoptimalkan insentif swasta dan tujuan publik, membingkai ulang perdebatan dari kepemilikan versus keterbukaan menjadi model terintegrasi yang mendukung inovasi yang adil di tengah ketegangan geopolitik. Berdasarkan model tumpukan tata kelola yang mendasar, bagian ini mengaitkan tema alat hukum adaptif, menunjukkan bagaimana strategi IP tidak hanya melindungi inovasi kuantum tetapi juga menginformasikan tren kebijakan yang lebih luas yang diperiksa dalam pemetaan empiris selanjutnya.

1.4 TREN PATEN TEKNOLOGI KUANTUM GLOBAL

Bagian ini menyajikan pemetaan empiris terbaru tentang paten teknologi kuantum dari tahun 2001 hingga Oktober 2025, yang mengungkapkan tren yang memberikan informasi bagi kebijakan inovasi dan menangkal kekhawatiran tentang proteksi berlebihan. USPTO dan EPO sekarang memberikan sekitar 2500 paten setiap tahun di bawah klasifikasi kuantum, yang mencerminkan CAGR 14,5% dan percepatan yang didorong oleh terobosan seperti qubit yang dikoreksi kesalahan, yang menggarisbawahi investasi R&D yang berkelanjutan tanpa perlambatan.

Bagian ini melaporkan bahwa sistem paten mendorong pengungkapan awal penemuan kuantum yang jika tidak, dapat dirahasiakan. Bahkan, sekitar 54% pengungkapan terkait kuantum sudah berada di domain publik, termasuk lebih dari 6500 hibah paten yang telah kedaluwarsa, secara progresif memperkaya ruang informasi kuantum yang meningkatkan ambang batas kebaruan dan mempersempit klaim di masa mendatang, yang menguntungkan inovasi terbuka. Pemeriksaan paten-paten ini mengungkapkan struktur klaim paten yang mencerminkan paten semikonduktor, menyoroti kesinambungan dengan teknologi klasik dan memperingatkan terhadap reformasi yang tidak harmonis yang dapat mendistorsi pengajuan global.

Keragaman di antara pemilik utama (misalnya, mencakup IBM, Google, perusahaan rintisan seperti IonQ dan Rigetti, universitas, dan pemerintah) menunjukkan konsentrasi yang lebih rendah daripada di pasar TI, mendukung persaingan dan pemanfaatan kekayaan intelektual bagi UKM di bidang padat modal. Pergeseran geopolitik, seperti kepemimpinan Tiongkok dalam pengajuan, memperkuat dampak keamanan, mendesak kebijakan berbasis bukti yang menyeimbangkan insentif pengungkapan dengan pemantauan teknologi, sambil menegaskan peran paten dalam melawan kerahasiaan perdagangan di bidang-bidang strategis. Perspektif berbasis data ini memperluas narasi IP adaptif, memberikan landasan empiris untuk tantangan regulasi dalam keamanan siber dan kontrol ekspor yang mengikutinya, memastikan tata kelola tetap berdasarkan bukti di seluruh lanskap kuantum yang terus berkembang.

1.5 HUKUM KUANTUM DAN KEAMANAN SIBER

Bidang ini mengkaji kecukupan regulasi keamanan siber Uni Eropa terhadap ancaman kuantum, menganjurkan reformasi proaktif untuk ketahanan. Bidang ini mengidentifikasi dua tantangan inti: (1) serangan "panen sekarang, dekripsi nanti" dan (2) kuantum berpotensi

melampaui langkah-langkah kriptografi klasik melalui algoritma seperti algoritma Shor, mengekspos kerentanan dalam enkripsi asimetris yang menuntut transisi kriptografi pasca-kuantum (PQC) yang mendesak.

Konsep Uni Eropa seperti "kondisi terkini" dan "langkah-langkah yang tepat" berdasarkan NIS2 dan GDPR mungkin gagal mengatasi ancaman di masa depan yang muncul saat ini, sehingga memerlukan peningkatan seperti penilaian risiko kuantum untuk melindungi infrastruktur kritis dan standar keamanan informasi khusus kuantum. PQC menawarkan solusi praktis tanpa perangkat keras khusus, dengan standar NIST yang menyediakan cetak biru yang sedang berkembang, namun kompleksitas integrasi dalam sistem lama menyoroti perlunya fokus kebijakan pada interoperabilitas dan implementasi.

Tata kelola antisipatif melalui strategi berlapis-lapis (misalnya, menggabungkan hukum, peraturan, panduan peraturan, standar internasional, dan keputusan yudisial) dapat memungkinkan Uni Eropa untuk memanfaatkan kapasitas regulasinya di tengah upaya global seperti Peta Jalan PQC Komisi. Sementara distribusi kunci kuantum muncul sebagai pertahanan potensial, pemeriksaan ini menekankan pendekatan seimbang yang memperhitungkan ketidakpastian, mendesak pergeseran ke kontrol berorientasi masa depan untuk melindungi keamanan informasi dalam lanskap ancaman yang berkembang. Menghubungkan kembali ke penekanan tren paten pada pengungkapan dan inovasi, bagian ini menyoroti bagaimana adaptasi keamanan siber harus selaras dengan benang tata kelola yang lebih luas, membuka jalan bagi kontrol ekspor sebagai lapisan strategi perlindungan lain dalam konteks internasional kuantum.

1.6 HUKUM KUANTUM DAN PENGENDALIAN EKSPOR

Bidang ini memeriksa pengendalian ekspor teknologi kuantum, memetakan langkah-langkah AS dan Uni Eropa sambil mengidentifikasi peluang dan tantangan penegakan hukum. Bidang ini mencatat pergeseran ke koordinasi plurilateral di luar kerangka kerja multilateral seperti Wassenaar, yang memungkinkan pembatasan yang ditargetkan pada tumpukan kuantum dari perangkat keras hingga perangkat lunak di tengah persaingan AS-Tiongkok-UE, seperti yang terlihat pada iterasi 2022–2025.

Sifat berlapis kuantum memungkinkan kontrol granular, seperti pada sistem kriogenik atau model akses cloud, menawarkan penegakan hukum dinamis yang terkait dengan jejak fisik dan modularitas, meningkatkan efektivitas dibandingkan aset tidak berwujud. Tantangannya meliputi pengaturan pengetahuan dan menghindari fragmentasi, dengan "ekspor yang dianggap" AS dan variasi UE yang berisiko menimbulkan beban kepatuhan, namun peluang muncul dari infrastruktur terpusat untuk pembatasan yang dapat diverifikasi.

Potensi penggunaan ganda meningkatkan rasionalitas keamanan nasional, tetapi kesenjangan empiris dalam rezim multilateral menggarisbawahi perlunya strategi adaptif yang menyeimbangkan kolaborasi dengan pencegahan proliferasi. Kerangka kerja yang berorientasi ke masa depan harus memanfaatkan kemampuan khusus kuantum (misalnya, penargetan tingkat komponen) untuk menginformasikan kebijakan terkoordinasi, memastikan kontrol beradaptasi dengan difusi tanpa menghambat pembelajaran dan pengembangan global secara

berlebihan di bidang yang baru muncul ini. Fokus regulasi ini melengkapi penekanan keamanan siber pada langkah-langkah antisipatif, memperkuat benang merah tata kelola proaktif yang meluas ke hukum internasional, di mana kontrol ekspor berfungsi sebagai jembatan antara perlindungan domestik dan norma global.

1.7 KUANTUM DAN HUKUM INTERNASIONAL: DIMENSI STRATEGIS DAN GEOPOLITIK

Bidang ini menyelidiki dampak teknologi informasi kuantum terhadap hukum internasional publik, mengintegrasikan dimensi strategis dan geopolitik. Penempatan QIT dalam infrastruktur klasik memungkinkan doktrin yang ada (seperti yang terdapat dalam Manual Tallinn) untuk menerapkan norma berbasis efek pada operasi kuantum tanpa perubahan mendasar, menjaga kontinuitas kedaulatan dan uji tuntas. Ontologi kuantum dapat mempersulit atribusi dan yurisdiksi, namun definisi fungsional yang berfokus pada hasil memungkinkan penyempurnaan interpretatif, seperti dalam kausalitas probabilistik selama operasi siber. Model teori permainan mengungkapkan pola kerja sama dan persaingan, dengan dekripsi kuantum mengubah asimetri informasi dan mendorong norma baru untuk mengelola perlombaan senjata dan akses yang adil.

Kontrol ekspor penggunaan ganda menyediakan antarmuka tata kelola langsung, membatasi transfer sekaligus membentuk distribusi kemampuan, dengan seruan untuk reformasi multilateral untuk mengatasi sistem yang saling terkait. Pemeriksaan ini mengusulkan kerangka kerja strategis untuk tata kelola geopolitik, menekankan fleksibilitas hukum yang mungkin untuk mengakomodasi fitur non-klasik QIT melalui evolusi bertahap, mendorong transparansi dan akuntabilitas dalam skenario damai dan konflik. Sebagai puncak eksplorasi progresif volume pertama, bagian ini menghubungkan tema-tema adaptif dari hukum dasar, strategi IP, tren paten, keamanan siber, dan kontrol ekspor, menganjurkan pendekatan global yang saling terkait untuk memanfaatkan potensi kuantum secara bertanggung jawab.

1.8 TATA KELOLA ADAPTIF TEKNOLOGI KUANTUM

Pemeriksaan yang disajikan di seluruh volume ini mengungkapkan bahwa QIS menantang struktur tata kelola yang ada bukan dengan membuatnya usang, tetapi dengan mengungkap area di mana fleksibilitas interpretatif, landasan empiris, dan pandangan ke depan yang antisipatif paling dibutuhkan. Wawasan utama yang muncul dari kontribusi tersebut adalah bahwa potensi disruptif QIT tidak hanya terletak pada karakteristik teknisnya (misalnya, komputasi probabilistik, komunikasi yang didukung oleh keterikatan, dan penginderaan ultra-sensitif) tetapi juga pada sifat, kecepatan, dan asimetri perkembangannya di berbagai perusahaan, industri, dan yurisdiksi. Dinamika ini menciptakan tekanan tata kelola yang menguji kemampuan adaptasi sistem hukum dan peraturan sekaligus mengungkapkan peluang untuk memperkuatnya.

Pertama, buku ini menunjukkan bahwa teknologi kuantum pada dasarnya berlapis, mencakup perangkat keras, sistem kontrol, algoritma, dan aplikasi. Arsitektur berlapis ini memperkuat pentingnya pendekatan tata kelola yang menyelaraskan alat regulasi dengan

strata teknis tertentu. Penyelarasan tersebut membantu menghindari intervensi regulasi yang terlalu luas dan tindakan yang terlalu sempit yang gagal mengatasi risiko sistemik.

Kedua, kontribusi secara kolektif menunjukkan bahwa doktrin hukum dan kerangka kerja regulasi yang ada memiliki adaptabilitas laten yang signifikan. Baik dalam hukum kekayaan intelektual, regulasi keamanan siber, kontrol ekspor, atau hukum internasional publik, banyak prinsip lama seperti pemberdayaan, proporsionalitas, dan norma berbasis efek kemungkinan sudah memberikan ruang konseptual untuk mengatasi kompleksitas khusus kuantum. Alih-alih menuntut penemuan kembali hukum secara menyeluruh, teknologi kuantum lebih sering membutuhkan kalibrasi ulang, interpretasi yang diperbarui, panduan yang jelas, standar, dan suplementasi yang ditargetkan.

Ketiga, buku ini menyoroti pentingnya bukti empiris termasuk analitik paten, pemodelan ancaman keamanan siber, dan data penegakan kontrol ekspor dalam menginformasikan tata kelola kuantum. Perspektif empiris ini menerangi lintasan teknologi, mengungkapkan penyebaran atau konsentrasi kemampuan, dan membantu mengidentifikasi di mana asimetri atau kerentanan regulasi dapat muncul.

Terakhir, kami menekankan perlunya tata kelola yang secara bersamaan mengoptimalkan kemajuan dan perlindungan. Sifat ganda QIT, ekosistem pembelajaran global, dan dampak strategisnya memerlukan pendekatan yang menjaga keterbukaan untuk kemajuan ilmiah sambil mengelola risiko proliferasi, distorsi persaingan, dan ketegangan geopolitik. Seperti yang ditunjukkan dalam buku ini, koordinasi multilateral (misalnya, di seluruh badan penetapan standar, rezim kontrol ekspor, kerangka kerja keamanan siber, dan panduan interpretatif dalam hukum internasional) akan sangat penting untuk mencegah lanskap regulasi yang terfragmentasi atau tidak konsisten yang dapat menghambat inovasi atau memperburuk risiko sistemik.

Secara keseluruhan, kontribusi dalam buku ini menggambarkan bahwa tata kelola kuantum yang efektif harus didasarkan pada bukti empiris, adaptif, dan terlibat secara internasional. Saat QIT bertransisi dari pekerjaan teoretis ke penerapan praktis, sistem tata kelola harus berkembang seiring waktu, memastikan bahwa inovasi berjalan secara bertanggung jawab sambil menjunjung tinggi keamanan, transparansi, dan kepercayaan publik.

1.9 TATA KELOLA KUANTUM ADAPTIF DAN BERBASIS BUKTI

Secara kolektif, kontribusi ilmiah dalam volume pertama mengungkapkan tema berulang tentang kemampuan beradaptasi dalam tata kelola kuantum, di mana kerangka hukum yang ada (yaitu, didukung oleh fleksibilitas interpretatif dan wawasan berbasis bukti) mungkin dapat mengakomodasi tantangan unik kuantum tanpa memerlukan reformasi besar-besaran. Mulai dari model tumpukan tata kelola dasar yang melapisi alat regulasi di seluruh komponen QIT hingga "superposisi" strategi IP yang memadukan paten, rahasia, dan keterbukaan, narasi tersebut menggarisbawahi bagaimana inovasi kuantum lebih cenderung memperluas daripada sepenuhnya merusak paradigma klasik. Tren paten empiris lebih lanjut menegaskan hal ini, menunjukkan pertumbuhan yang kuat dan domain publik yang

berkembang pesat yang menangkal kekhawatiran akan proteksi berlebihan sambil menyoroti dinamika geopolitik, seperti meningkatnya dominasi Tiongkok, yang memperkuat kebutuhan akan insentif yang seimbang di bidang yang padat modal.

Alur adaptif ini meluas ke domain khusus, di mana reformasi keamanan siber menganjurkan strategi berlapis untuk mengurangi ancaman seperti dekripsi kuantum, selaras dengan standar global untuk infrastruktur yang tangguh. Kontrol ekspor, pada gilirannya, memanfaatkan sifat modular kuantum untuk penegakan hukum yang ditargetkan, menjembatani keamanan domestik dengan kolaborasi internasional di tengah pergeseran plurilateral. Berpuncak pada hukum internasional publik, pemeriksaan ini mengintegrasikan elemen-elemen ini melalui norma berbasis efek dan pemodelan teori permainan, mengusulkan kerangka kerja yang mendorong akses yang adil dan transparansi. Bersama-sama, wawasan ini membekali para pemangku kepentingan untuk menavigasi transisi kuantum dari teori ke aplikasi, menekankan kerja sama multidisiplin untuk memanfaatkan kekuatan transformatifnya secara adil dan etis.

Dengan mensintesis kontribusi-kontribusi ini, buku ini tidak hanya memetakan lanskap tata kelola kuantum saat ini dalam hal hukum dan peraturan yang ada, tetapi juga memetakan jalur untuk ketahanan di masa depan, menyerukan kebijakan proaktif yang menyeimbangkan inovasi dan keamanan. Seiring dengan kematangan teknologi kuantum, pendekatan yang saling terkait ini memastikan kemajuan masyarakat (kemajuan) sekaligus mengurangi risiko (pengamanan), memposisikan tata kelola sebagai penggerak dinamis daripada sebagai kendala.

BAB 2
TEKNOLOGI INFORMASI KUANTUM DAN HUKUM

Teknologi informasi kuantum (QIT) mencakup kumpulan inovasi baru komputasi kuantum, komunikasi kuantum, dan penginderaan kuantum yang memanfaatkan sifat unik sistem kuantum, seperti keterikatan, superposisi, dan kuantisasi, untuk memproses informasi dengan cara yang secara klasik tidak mungkin atau tidak layak. Meskipun QIT masih dalam tahap awal, potensinya untuk percepatan komputasi yang belum pernah terjadi sebelumnya, keamanan komunikasi, dan pengukuran ultra-presisi menunjukkan dampak dan risikonya di berbagai bidang ekonomi, strategis, dan sosial. Kami menempatkan QIT dalam konteks historis dan teknologinya, dengan fokus pada pertanyaan tentang apa yang *sui generis* atau unik tentang QIT sehubungan dengan detail teknis dan keharusan tata kelola. Kami mengidentifikasi bagaimana sifat ontologis unik dari sistem kuantum dapat menimbulkan dilema konseptual hukum baru dan mengusulkan model tumpukan tata kelola yang menyelaraskan instrumen regulasi potensial dengan lapisan spesifik dari tumpukan teknologi QIT, memungkinkan penilaian risiko yang tepat dan regulasi yang berfokus pada pemangku kepentingan. Dengan mengadopsi lensa teori informasi, kami memeriksa bagaimana kemampuan baru QIT mulai dari dekripsi enkripsi klasik hingga penginderaan ultra-presisi berpotensi berdampak pada ranah hukum. Kontribusi kami bertujuan untuk meletakkan dasar untuk memahami dampak hukum QIT, menawarkan kerangka kerja untuk menavigasi peluang dan risikonya.

2.1 TEKNOLOGI INFORMASI KUANTUM DALAM KERANGKA HUKUM

Teknologi informasi kuantum (QIT), serangkaian teknologi yang memanfaatkan sifat unik mekanika kuantum untuk memperoleh, menyimpan, dan memproses informasi, merupakan salah satu inovasi teknologi utama abad ke-21 dengan potensi konsekuensi yang luas bagi sistem ekonomi, strategis, dan bahkan sosial secara global. QIT mencakup serangkaian disiplin ilmu teoretis dan terapan yang luas, terutama komputasi kuantum, komunikasi kuantum, dan penginderaan kuantum. Dengan memanfaatkan sifat unik mekanika kuantum, setiap divisi QIT menawarkan janji kemampuan pemrosesan informasi yang tak tertandingi. Komputasi kuantum berpotensi, pada prinsipnya, untuk mendekripsi jenis data dan komunikasi terenkripsi klasik tertentu, yang dapat memengaruhi aspek-aspek keamanan siber dan postur pertahanan modern negara-negara. Penginderaan kuantum berpotensi berkontribusi pada upaya untuk mendeteksi aset strategis seperti kapal selam berkemampuan nuklir, yang mungkin memengaruhi kemampuan serangan balasan kedua negara-negara berkekuatan nuklir. Komunikasi kuantum dapat memungkinkan keunggulan kompetitif dalam komunikasi baik di masa damai maupun selama konflik.

Cakupan dan dampak potensial QIT secara luas dianggap signifikan. QIT (*Quantum Information Technology*) telah menjadi fokus utama investasi dan perencanaan strategis negara, dan menonjol dalam kebijakan kekuatan global. Secara ekonomi, potensi yang ditawarkan oleh simulasi kuantum dan komputasi kuantum membuka cara baru untuk

mempercepat daya pemrosesan secara cepat melampaui keterbatasan komputasi komputasi klasik, memungkinkan peningkatan skala komputasi konvensional, sekaligus membuka sejumlah solusi yang mungkin yang sebelumnya tidak dapat diatasi karena pertimbangan kompleksitas komputasi. Komunikasi kuantum, khususnya protokol mengenai jaringan kuantum dan internet kuantum menjanjikan revolusi dalam transfer informasi melintasi jarak yang sangat jauh.

Simulasi kuantum menawarkan prospek dalam hal sintesis struktur kimia dan protein dengan cara yang diharapkan dapat membuka pintu baru bagi inovasi farmasi. Perangkat titik kuantum menawarkan potensi tingkat pengukuran baru yang memungkinkan intervensi medis, diagnosis, dan pengobatan pada skala yang lebih halus di seluruh bidang kesehatan dan ilmu terkait. Kriptografi pasca-kuantum sudah dipromosikan oleh organisasi dan lembaga standar secara global sebagai respons antisipatif terhadap potensi risiko dekripsi yang ditimbulkan oleh perangkat kuantum yang dapat diskalakan dan tahan terhadap kesalahan.

Teknologi Baru dan Tata Kelola yang Ada

Seperti halnya semua teknologi baru yang muncul, detail tentang bagaimana teknologi tersebut harus diatur masih menjadi pertanyaan terbuka. Hal ini terutama karena QIT masih dalam tahap awal dan belum dikembangkan atau diterapkan dalam skala besar. Sebagian besar QIT masih berada pada tahap prototipe. Misalnya, kita belum melihat komputer kuantum yang benar-benar skalabel dan toleran terhadap kesalahan. Penginderaan kuantum sebagian besar terbatas pada aplikasi industri tertentu (seperti dalam ilmu hayati). Komunikasi kuantum melalui jaringan kuantum dan teleportasi masih berada pada tahap pembelajaran awal dan pembuktian konsep. Namun jelas bahwa jika teknologi ini direalisasikan sepenuhnya, maka QIT mungkin memiliki potensi signifikan untuk memengaruhi hak, kewajiban, dan kepentingan para pemangku kepentingan, mulai dari negara hingga individu.

QIT Memiliki Aplikasi yang Luas

Dampak QIT sangat luas karena kemampuan unik pemrosesan informasi kuantum, seperti memungkinkan dekripsi data yang dienkripsi secara klasik, penskalaan cepat ukuran dan kecepatan komputasi, serta simulasi sistem yang sangat kompleks. Dekripsi membawa konsekuensi bagi keseimbangan kekuatan geopolitik dan perilaku strategis Negara, serta privasi dan keamanan data dan informasi yang menjadi dasar masyarakat modern. Simulasi kuantum membuka pintu potensial untuk menemukan obat-obatan baru dengan cara yang dapat menawarkan manfaat besar, tetapi juga memfasilitasi tindakan jahat jika disalahgunakan. Penginderaan kuantum memungkinkan pengukuran yang lebih detail tetapi juga dapat menimbulkan dampak geopolitik dari pengungkapan aset kapal selam strategis. Komunikasi kuantum dan kriptografi pasca-kuantum dapat memfasilitasi era baru dalam infrastruktur komunikasi, namun juga mempersulit kemampuan untuk mencegat atau mendekode aktivitas musuh (termasuk aktivitas kriminal). Dan dampak strategis dari sintesis teknologi kecerdasan buatan dengan komputasi kuantum belum diteliti secara komprehensif.

Dampak QIT terhadap Hukum Masih Kurang Dipelajari

Cara instrumen dan lembaga pemerintahan, termasuk hukum, prinsip hukum, regulasi, dan interpretasi yudisial, merespons QIT masih relatif kurang dipelajari. Seperti halnya

sebagian besar teknologi tahap awal, hal ini disebabkan oleh kurangnya data untuk dijadikan dasar penilaian heuristik sekalipun. Komputasi kuantum masih merupakan prospek yang relatif jauh setidaknya jenis koreksi kesalahan yang sepenuhnya toleran terhadap kesalahan. Komunikasi kuantum belum dikembangkan sedemikian rupa sehingga memiliki aplikasi langsung dan infrastruktur yang dibutuhkan untuk mendukung jaringan kuantum pada dasarnya masih bersifat konseptual. Penginderaan kuantum, di antara sektor QIT yang lebih maju, masih terbatas dalam aplikasinya. Kurangnya data ini membuat dapat dipahami mengapa terdapat respons hukum yang terbatas terhadap munculnya QIT, baik dalam hal legislasi maupun dalam hal kuantifikasi formal risiko terkait QIT.

Rezim hukum yang secara khusus menangani QIT juga terbatas. Seperti yang kita bahas, pertanyaan tentang apa yang *sui generis* dari QIT baru saja mulai dibahas. QIT sebagian besar akan termasuk dalam kelas teknologi yang tunduk pada instrumen tata kelola yang ada, seperti teknologi komputasi atau teknologi komunikasi. Tetapi hampir semua instrumen tata kelola tersebut tidak secara khusus membahas QIT. Instrumen yang membahasnya, seperti kontrol penggunaan ganda dan ekspor, hanya menyentuh permukaan, biasanya terbatas pada klasifikasi teknologi tersebut sebagai strategis dan kewajiban yang timbul darinya. Cara QIT dan hukum berinteraksi, apa yang unik (jika ada) tentang hubungan mereka dan respons apa yang mungkin diperlukan, sebagian besar masih merupakan wilayah yang belum dipetakan. Kami bertujuan untuk mengatasi kesenjangan ini dengan menjabarkan serangkaian prinsip dasar tentang bagaimana sintesis QIT dan penalaran yurisprudensi, teknologi kuantum dan tata kelola, dapat berjalan.

Kontribusi

Bagian ini berkontribusi pada riset dengan memberikan pemeriksaan tentang isu-isu hukum dan konsekuensi yang mungkin timbul dari pengembangan, penggunaan, dan penerapan QIT. Sementara bagian-bagian lain dalam volume ini membahas isu-isu normatif dan kebijakan, fokus bagian ini adalah pada bagaimana fitur-fitur teknis QIT sesuai dengan konsep, asumsi, dan persyaratan hukum yang ada sebagaimana diatur dalam undang-undang, yurisprudensi, dan riset sekunder. Bagian ini bertujuan untuk merumuskan pertanyaan *sui generis* tentang QIT dan hukum: apa yang berubah, apa yang tetap sama. Untuk tujuan ini, kontribusi kami adalah sebagai berikut.

Pemeriksaan Yurisprudensi Teknis

Kami memeriksa kemungkinan konsekuensi dari penggunaan QIT dalam beberapa bidang hukum. Pemeriksaan kami mencakup survei rezim-rezim utama yang ada yang tunduk pada penggunaan QIT dan bagaimana hukum dapat menanggapi isu-isu hukum baru yang muncul dari penggunaan QIT.

Ontologi Kuantum Hukum

Kami memberikan pemeriksaan tentang konsekuensi ontologi kuantum bagi hukum, melampaui sekadar uraian tentang sifat-sifat kuantum seperti superposisi, keterikatan, kuantisasi, dll., untuk mempertimbangkan bagaimana sifat ontologis QIT yang pada dasarnya berbeda tersebut menimbulkan atau tidak menimbulkan masalah pada asumsi hukum yang mendasarinya.

Pemeriksaan Tumpukan Tata Kelola

Kami mengidentifikasi contoh bagaimana memetakan tumpukan teknologi QIT yang relevan ke instrumen tata kelola untuk memfasilitasi tujuan regulasi, termasuk memenuhi kepentingan pemangku kepentingan, memberlakukan kewajiban, dan mencapai tujuan kebijakan seperti realisasi QIT dalam toleransi risiko yang diinginkan. Kami berfokus pada bagaimana pilihan di mana dalam tumpukan teknologi QIT untuk diatur memengaruhi pilihan instrumen tata kelola yang tepat, mengklarifikasi secara tepat sejauh mana segala sesuatu yang bersifat kuantum itu sendiri merupakan subjek tata kelola yang berbeda dari teknologi yang merupakan bagian dari QIT. Untuk mendekati pertanyaan-pertanyaan ini, akan bermanfaat untuk mengkontekstualisasikan munculnya QIT dalam perkembangan historis yang lebih luas dari mekanika kuantum dan teknologi informasi.

2.2 SEJARAH REVOLUSI KUANTUM

Revolusi Kuantum

Kemunculan dan evolusi teknologi kuantum sering diklasifikasikan menjadi revolusi kuantum pertama dan kedua dengan teknologi generasi pertama dan kedua yang muncul sebagai hasilnya. Revolusi kuantum pertama didefinisikan sebagai permulaan dan pengembangan awal mekanika kuantum sebagai teori ilmiah utama tentang realitas itu sendiri. Revolusi ini menetapkan dasar-dasar matematika dan bukti eksperimental untuk fenomena kuantum, termasuk dualitas gelombang-partikel, prinsip ketidakpastian, dan tingkat energi terkuantisasi. Prinsip-prinsip dasar ini dimanfaatkan untuk menciptakan perangkat kadang-kadang disebut teknologi kuantum generasi pertama seperti transistor dan laser, yang secara kolektif mengubah elektronika, komputasi, dan komunikasi. Demonstrasi efek kuantum fundamental seperti penerowongan elektron memberikan dorongan bagi inovasi mulai dari jam atom hingga sirkuit terpadu berbasis semikonduktor. Secara keseluruhan, pencapaian ini mewakili puncak dari apa yang oleh sejarawan dan ahli teknologi disebut sebagai gelombang pertama penemuan yang didukung kuantum, yang memunculkan instrumentasi canggih dan revolusi mikroelektronika.

Revolusi Kuantum Kedua

Era QIT saat ini sering diposisikan sebagai apa yang disebut 'revolusi kuantum kedua'. Asal usulnya terletak pada gagasan memanfaatkan sifat-sifat mekanika kuantum secara langsung sebagai sumber daya (bukan sebagai efek insidental atau sumber kesalahan yang perlu dikurangi seperti halnya efek saluran pendek pada transistor yang digunakan dalam chip komputasi klasik canggih) untuk melakukan komputasi yang muncul sepanjang akhir tahun 1970-an dan awal 1980-an, sebagian karena minat teoretis untuk melampaui keterbatasan kompleksitas komputasi dalam ilmu komputer teoretis dan tantangan kemudahan penanganan terkait simulasi sistem fisik. Feynman terkenal mencatat bahwa mensimulasikan sistem kuantum pada mesin klasik dapat sangat mahal, menunjukkan bahwa simulator kuantum universal dapat melewati tuntutan sumber daya eksponensial ini dengan beroperasi di bawah aturan fisik yang sama yang ingin disimulasikannya. Secara paralel, Benioff dan Manin memberikan kerangka kerja matematika awal yang mengisyaratkan bahwa logika mekanika

kuantum mungkin menghasilkan mode komputasi yang fundamentally baru. Algoritma Shor dan algoritma Grover merupakan tonggak penting selanjutnya yang memicu upaya pembelajaran global dalam komputasi kuantum, yang menunjukkan peningkatan kecepatan polinomial atau eksponensial dibandingkan metode klasik untuk masalah bernilai tinggi tertentu.

Era modern ini ditandai dengan perkembangan teori sistem informasi kuantum komputasi kuantum, penginderaan kuantum, dan komunikasi kuantum bersama dengan kemajuan dalam ilmu komputasi terapan yang telah membuka potensi untuk melakukan kontrol langsung atas fenomena mekanika kuantum guna memanfaatkan sifat unik mekanika kuantum sebagai sumber daya itu sendiri. Generasi kedua teknologi kuantum ini dimungkinkan oleh kemajuan dalam infrastruktur komputasi, seperti sirkuit terintegrasi tinggi dan peralatan kontrol yang memungkinkan resolusi pengukuran yang sangat halus pada skala sub-mikron di mana efek kuantum menjadi dapat diamati. Berbeda dengan revolusi kuantum pertama, revolusi kuantum kedua melibatkan pemanfaatan superposisi kuantum, keterikatan, dan non-lokalitas secara sengaja sebagai sumber daya teknologi langsung. Alih-alih secara kebetulan bergantung pada fenomena kuantum, teknologi generasi kedua berupaya menggabungkan koherensi kuantum untuk melampaui batasan klasik dalam daya komputasi, presisi penginderaan, dan keamanan komunikasi.

Kemajuan dalam qubit superkonduktor, perangkap ion, dan sirkuit terpadu fotonik, misalnya, telah memungkinkan demonstrasi praktis bit kuantum qubit bersama dengan protokol seperti distribusi kunci kuantum dan teleportasi. Akibatnya, para peneliti modern mulai membayangkan komputer kuantum yang berfungsi penuh untuk tugas-tugas seperti faktorisasi, optimasi, dan simulasi molekuler, serta jaringan kuantum skala besar untuk komunikasi ultra-aman. Selain itu, generasi kedua teknologi kuantum memiliki fokus teoretis informasi khusus sebagai perangkat yang memanfaatkan mekanika kuantum untuk memperoleh, menyimpan, dan memproses informasi. Kami memanfaatkan karakterisasi informasional teknologi kuantum ini sebagai sarana untuk menjembatani lanskap kuantum yurisprudensial dan teknis, yang keduanya dapat diungkapkan dalam istilah yang berkaitan dengan informasi. Terobosan-terobosan ini telah mendorong ilmu informasi kuantum dari ranah keingintahuan teoretis menjadi QIT generasi berikutnya yang prospektif, dengan konsekuensi yang tidak sepele bagi regulasi, hukum, dan tata kelola, seperti yang telah kami uraikan.

Kondisi Terkini Teknologi Informasi Kuantum (QIT)

QIT telah dikembangkan selama lebih dari 40 tahun. Kondisi terkini QIT tidak homogen, dengan berbagai sub-divisi pada tingkat kematangan yang berbeda. Memahami tingkat perkembangan teknologi saat ini penting untuk pemeriksaan hukum dampak QIT. Sepanjang karya ini, kami mempertimbangkan kondisi terkini dan kondisi terkini QIT dalam waktu dekat, tetapi juga QIT dalam bentuknya yang sepenuhnya siap (terlepas dari ketidakpastian tentang, misalnya, modalitas mana fotonik, ion terperangkap, superkonduktor, dll. yang mungkin akan dominan). Secara umum, pada saat penulisan ini, kondisi masing-masing dari tiga komponen

utama QIT komputasi kuantum, penginderaan kuantum, dan komunikasi kuantum adalah sebagai berikut.

Komputasi Kuantum

Komputasi kuantum toleran kesalahan (FTQC) yang memungkinkan koreksi kesalahan hingga spesifikasi arbitrer masih belum tercapai. Secara umum, bidang ini masih berada di era kuantum skala menengah bising (NISQ) di mana perangkat komputasi kuantum terbatas pada beberapa hingga seribu qubit, meskipun sistem yang dapat diskalakan masih berada di era NISQ dengan qubit logis efektif yang terbatas. Yang penting, jenis fidelitas dan jaminan kualitas pada sistem kuantum yang diperlukan untuk hasil yang andal dan kuat seringkali terbatas pada sistem yang sangat kecil, dengan jaringan atau sistem qubit yang lebih besar biasanya dipelajari dari perspektif yang terbatas. Selain itu, hambatan mendasar untuk FTQC tetaplah kebisingan dan koreksi kesalahan.

Komunikasi Kuantum

Komunikasi kuantum masih berada pada tahap prototipe. Demonstrasi teknologi teleportasi kuantum dan jaringan kuantum telah terbukti layak dengan sejumlah kecil qubit dalam pengaturan terkontrol. Namun, sektor ini dianggap masih jauh dari jaringan skala besar. Tantangan utama tetaplah koreksi kesalahan dan kebisingan, bersama dengan implementasi infrastruktur yang dibutuhkan untuk saluran komunikasi kuantum fidelitas tinggi dalam skala besar.

Penginderaan Kuantum

Penginderaan kuantum adalah sektor QIT yang paling matang, dengan teknologi titik kuantum yang digunakan dalam prototipe perangkat medis dan aplikasi industri lainnya. Namun, jenis penskalaan perangkat penginderaan kuantum yang dibayangkan untuk aplikasi luas masih belum terjadi. Demikian pula, sementara penginderaan kuantum sering dibahas dalam konteks infrastruktur keamanan nasional dan komunikasi yang bersifat antagonis, masih terdapat hambatan yang cukup besar untuk penggunaannya dalam konteks ini. Dalam karya ini, meskipun kami tetap menyadari tahap awal inovasi QIT, kami mempertimbangkan konsekuensi hukum dari QIT yang kemungkinan besar telah sepenuhnya dikembangkan dan berfungsi. Meskipun ketidakpastian tentang QIT masih ada, terutama mengenai kemungkinan substrat komputasi yang akan mewujudkan komputasi kuantum atau komunikasi kuantum yang toleran terhadap kesalahan dan dapat diskalakan, jelas bahwa apa pun bentuk sukses yang diasumsikan oleh QIT tersebut, kemungkinan akan ada masalah hukum umum yang muncul dari ontologi dan karakteristik kuantum unik yang akan kami bahas di bawah ini.

2.3 HUKUM DAN TEKNOLOGI KUANTUM

Hukum dan Inovasi QIT

Hukum bukanlah hal asing bagi teknologi baru. Hukum juga bukan hal asing bagi teknologi yang memanfaatkan mekanika kuantum. Dan teknologi informasi khususnya memang telah menjadi pusat pengembangan yurisprudensi, dari penemuan tulisan, hingga mesin cetak hingga sistem komputasi modern. Bagaimana suatu teknologi seharusnya diatur adalah pokok bahasan pembelajaran teoritis dan terapan tentang tata kelola teknologi. Hukum

telah menunjukkan kemampuannya untuk menanggapi kemajuan teknologi seperti teknik nuklir, bioteknologi, internet, dan yang lebih baru kecerdasan buatan, dengan cara yang serupa, meskipun dengan tingkat coba-coba yang tak terhindarkan yang menyertai kedatangan cakrawala teknologi baru.

Hukum dan Ontologi Klasik

Namun seperti yang akan kita bahas di bawah ini, teknologi kuantum dapat dikatakan termasuk dalam kelas inovasi yang berbeda. Hal ini karena meskipun semua teknologi pada awalnya baru, hampir semua teknologi yang digunakan secara signifikan dan yang diatur oleh hukum adalah apa yang kita sebut sebagai klasik, berdasarkan apa yang dalam ilmu fisika sering digambarkan sebagai asumsi klasik tentang bagaimana objek dan materi pokok ada, berkembang, dan berinteraksi. Meskipun munculnya teknologi baru dapat dan secara teratur menantang lembaga hukum untuk memberikan respons, jarang sekali teknologi tersebut menantang sifat klasik mendasar dari hukum. Hukum sebagai sebuah institusi, praktik sosial, disiplin, dan seperangkat norma berakar kuat pada hal-hal klasik. Ini tidak berarti bahwa hukum tidak dapat menangani indeterminisme atau ketidakpastian. Tetapi ini untuk mengakui bahwa interpretasi hukum yang berlaku mengasumsikan ontologi klasik. Hukum mengasumsikan objek ada dengan cara tertentu bahwa objek tersebut bersifat tetap, bahwa objek tersebut pada prinsipnya biasanya dapat diamati (meskipun dalam praktiknya hal ini sulit), memiliki identitas dan keadaan yang pasti (sekali lagi, meskipun secara epistemik sulit diakses) dan tetap ada atau bergerak terus menerus sepanjang waktu. Demikian pula, logika yang mendasari hukum pada umumnya bersifat klasik: aturan, proposisi, pernyataan, dan deklarasi yang menjadi dasar hak, kewajiban, dan kepentingan para pemangku kepentingan di bawah hukum secara diskursif muncul, semuanya didasarkan pada asumsi ontologi klasik.

Sebagai contoh, proposisi hukum pernyataan tentang pokok permasalahannya diasumsikan pada dasarnya bersifat biner, di mana ketidakpastian tentang kebenaran suatu proposisi juga dibatasi sebagai epistemik. Kualitas penalaran yurisprudensi ini bersifat klasik: hal-hal, objek, orang, dan lembaga diasumsikan berperilaku secara klasik. Ontologi ini menginformasikan prinsip-prinsip dasar yurisprudensi (yang sering dianggap jelas) seperti bahwa pokok permasalahan suatu hukum dapat dipastikan, bahwa pokok permasalahan tersebut dapat diinteraksikan atau bahkan dikendalikan dengan cara tertentu sehingga dapat diatur. Lokasi pokok permasalahan orang, tempat, benda dilandaskan pada konseptualisasi ruang Euklides yang khas. Properti dapat diidentifikasi, dilokalisasi, dan dikendalikan. Daftarnya masih berlanjut.

Tantangan Ontologi Kuantum

Namun, sistem kuantum, yang menjadi dasar QIT, dapat menantang sejumlah asumsi fundamental yang mendasari konseptualisasi klasik dalam hukum fisika. Seperti yang akan kami uraikan di bawah ini, ciri-ciri pembeda kuantum secara ontologis berbeda dari fisika klasik. Beberapa sifat sistem kuantum pada dasarnya tidak pasti, seperti posisi atau momentum partikel. Partikel kuantum dapat berada dalam keadaan superposisi koheren dengan hasil pengukuran yang saling eksklusif, sesuatu yang secara fundamental berbeda dari keadaan klasik (atau superposisi gelombang klasik misalnya). Partikel kuantum dapat saling

terkait, menunjukkan korelasi jarak jauh dengan cara yang telah terbukti membutuhkan salah satu fondasi ontologi klasik bahwa objek terkurung secara lokal (non-lokalitas merupakan konsekuensi yang umumnya diterima dari keterentangan dan Teorema Bell). Sifat-sifat sistem kuantum ini merupakan inti dari potensi besarnya dalam arti teknologi, tetapi juga berakar kuat dalam ontologi yang aneh yang berbeda dari bagaimana hukum fisika biasanya mengasumsikan keberadaan objek. Ini tidak berarti bahwa dunia QIT sama sekali tidak dapat diprediksi, kacau, atau tidak terkendali. Memang, seringkali kita mengharapkan ketidakpastian yang ditimbulkan oleh sifat kuantum teknologi dapat dikelola atau tidak menimbulkan tantangan khusus dari perspektif hukum. Kita akan membahas konsep-konsep ini lebih lanjut di bagian ini.

Hukum yang Berlaku untuk QIT

QIT sudah tunduk pada instrumen hukum dan tata kelola yang ada secara tidak langsung berdasarkan klasifikasi atau kategori yang diberikan kepadanya. Teknologi komunikasi kuantum, misalnya, akan termasuk dalam definisi dan ruang lingkup hukum komunikasi tertentu. Komputasi kuantum akan termasuk dalam tata kelola sistem komputasi yang dibingkai secara abstrak sebagai penerapan pada, misalnya, segala bentuk pemrosesan komputasi atau informasi. Dan penginderaan kuantum, seperti yang digunakan dalam ilmu hayati misalnya, pada umumnya tunduk pada peraturan yang mengatur penggunaan perangkat dalam pembelajaran medis dan konteks terapan. Selain rezim tata kelola khusus sektor ini, perlu dicatat bahwa teknologi kuantum, seperti teknologi baru lainnya, juga secara tidak langsung tercakup oleh instrumen yang lebih umum. Fenomena ini tidak hanya terjadi pada QIT (Teknologi Informasi Kuantum) tetapi sering diamati di berbagai sektor teknologi yang baru muncul.

Sebagai contoh, prinsip-prinsip dasar hukum kontrak, hukum perdata, dan hukum rahasia dagang dapat diterapkan pada penggunaan, pengembangan, atau pembuatan QIT. Ini mungkin termasuk ketika, misalnya, vendor perangkat keras kuantum menyediakan komponen yang cacat atau gagal menjaga kerahasiaan dalam program pembelajaran kolaboratif. Demikian pula, hukum dan pedoman lingkungan yang mengatur zat berbahaya secara tidak langsung dapat mengatur aspek-aspek pembuatan perangkat kuantum, khususnya di mana material khusus (misalnya, paduan superkonduktor, cairan kriogenik) digunakan. Meskipun hukum tersebut mungkin tidak secara eksplisit menyebutkan kuantum sebagai pokok bahasan atau deskripsi, hukum tersebut tetap membebankan kewajiban pada para pemangku kepentingan, termasuk produsen, pengguna akhir, dan lembaga pembelajaran yang timbul dari penggunaan QIT. Ketergantungan pada kerangka kerja yang ada ini dapat menciptakan kejelasan dan kebingungan: kerangka kerja tersebut membawa penerapan hukum secara langsung tetapi cenderung kurang disesuaikan dengan atribut khas QIT di mana hal ini mungkin relevan dengan hak atau kepentingan pemangku kepentingan, seperti komunikasi berbasis keterikatan atau keluaran komputasi probabilistik. Sejarah tata kelola di bidang seperti bioteknologi atau nanoteknologi menunjukkan bahwa ketergantungan awal pada rezim yang ada sering kali dilengkapi dengan adaptasi bertahap setelah muncul kekhawatiran spesifik yang berpusat pada kuantum. Akibatnya, para pemangku kepentingan yang bekerja

dengan QIT mulai dari perusahaan telekomunikasi yang menerapkan distribusi kunci kuantum hingga produsen perangkat sensor menghadapi lingkungan tata kelola yang berpotensi terfragmentasi.

2.4 QIT DAN KERANGKA HUKUM YANG BERLAKU

Pada bagian ini, kami menyajikan ringkasan tingkat tinggi dari beberapa dampak konseptual dan struktural utama untuk QIT yang dibahas dalam sejumlah bagian selanjutnya.

Kategori Hukum yang Ada yang Berlaku untuk QIT

Kita dapat mengidentifikasi beberapa pertimbangan hukum utama yang ada yang berlaku untuk QIT sebagai berikut:

Verifikasi dan Bukti

Proses hukum bergantung pada bukti yang dapat direplikasi, proses yang transparan, dan beban pembuktian yang dapat didefinisikan. Mekanika kuantum menyuntikkan verifikasi probabilistik dan batasan tanpa kloning, berpotensi menimbulkan masalah pada konsep dan proses hukum yang bergantung pada informasi deterministik klasik seperti asumsi jejak bukti rantai pengawasan, dan pengaktifan paten.

Privasi dan Keamanan Data

Dengan memungkinkan dekripsi informasi yang dienkripsi secara klasik, QIT meningkatkan risiko privasi dan keamanan data. Seiring dengan pengumpulan kategori data sensitif potensial baru oleh sensor kuantum, pertanyaan baru tentang keamanan informasi juga dapat muncul. Akibatnya, undang-undang privasi mungkin perlu beradaptasi untuk melindungi data yang menjadi sasaran intersepsi atau pengukuran berbasis kuantum.

Keselarasan Regulasi

Pengawasan tradisional (misalnya, untuk perangkat medis, standar komunikasi, atau kontrol ekspor) sering kali mengasumsikan kemampuan replikasi dan lokalitas klasik. Dalam pengaturan komputasi jaringan, sifat QIT yang tidak berwujud dan non-lokal mungkin membuatnya lebih sulit untuk mendefinisikan transfer informasi di seluruh sumber daya bersama.

Asimetri Strategis dan Penggunaan Ganda

Seiring dengan peningkatan skala QIT, negara dan perusahaan besar dapat memanfaatkan kekuatan dekripsi atau simulasi uniknya. Asimetri yang dihasilkan menimbulkan pertanyaan geopolitik penting, mulai dari aturan perang siber hingga pembatasan ekspor penggunaan ganda. Misalnya, pembelajaran dan pengembangan ilmu hayati mungkin akan tunduk pada bentuk-bentuk baru pemantauan penggunaan ganda jika simulasi kuantum memfasilitasi bioteknologi yang dapat dijadikan senjata dengan cepat.

Hukum Khusus Kuantum

Terdapat instrumen tata kelola khusus kuantum yang terbatas yang terutama ditujukan pada teknologi yang diklasifikasikan menurut karakteristik atau sifat kuantumnya. Demikian pula, terdapat legislasi khusus kuantum yang sangat terbatas yang berlaku untuk QIT. Hal ini sekali lagi dapat dipahami mengingat keadaan prototipe awal teknologi dan kurangnya data yang dapat digunakan untuk menilai risiko QIT secara empiris. Dengan demikian, distribusi

instrumen tata kelola QIT cenderung terkonsentrasi pada instrumen yang menjadi ciri sektor inovatif tahap awal. Ini termasuk sejumlah kerangka kerja, panduan, dan standar yang muncul dalam tata kelola kuantum. Secara umum, di seluruh negara maju, instrumen hukum tata kelola khusus kuantum (legislasi, regulasi formal) mencakup tiga bidang kontrol ekspor dan penggunaan ganda, protokol kriptografi, dan pengembangan ekosistem. Instrumen hukum tersebut pada dasarnya mengatur atau berupaya mengatur lintasan pengembangan QIT, bukan sesuatu yang mendekati penggunaan QIT secara luas itu sendiri.

Kontrol Ekspor dan Penggunaan Ganda

Karena QIT merupakan teknologi yang sangat strategis, penyebaran dan distribusinya telah menjadi subjek kontrol ekspor dan undang-undang penggunaan ganda. Kontrol ekspor yang berlaku untuk komponen sirkuit terpadu dan perangkat lunak pada Daftar Kontrol Perdagangan, seperti yang tercantum dalam undang-undang kontrol sirkuit terpadu baru-baru ini juga mencakup komponen yang relevan dengan pembuatan QIT. Mineral tanah jarang, yang seringkali merupakan komponen penting dalam produksi QIT, juga telah menjadi subjek respons kebijakan untuk mengamankan rantai pasokan QIT.

Protokol Kriptografi

Ketertarikan utama pada QIT dari sudut pandang keamanan nasional adalah dampaknya terhadap data dan komunikasi terenkripsi. Akibatnya, respons kebijakan dan legislatif telah muncul untuk mencari solusi, biasanya dalam bentuk protokol kriptografi pasca-kuantum untuk mengurangi serangan siber berbasis QIT di masa mendatang. Ini termasuk program kriptografi pasca-kuantum NIST untuk mengamankan komunikasi terhadap serangan musuh QIT.

Inisiatif Ekosistem Kuantum

Terdapat sejumlah kerangka kerja dan peta jalan berorientasi kebijakan tata kelola lunak yang bertujuan untuk mendorong pertumbuhan sektor kuantum, yang biasanya merupakan produk dari sayap eksekutif daripada sayap legislatif pemerintah. Contoh legislatif spesifik termasuk Inisiatif Kuantum Nasional AS dan kebijakan pemerintah serupa lainnya secara global. Meskipun langkah-langkah hukum khusus kuantum ini terbatas, langkah-langkah tersebut mencerminkan tren umum dalam tata kelola teknologi yang sedang berkembang, di mana instrumen tata kelola lunak awal dibuat untuk mencegah risiko strategis yang diantisipasi daripada untuk secara holistik membentuk pengembangan teknologi yang bertanggung jawab. Mirip dengan inisiatif teknologi awal lainnya (seperti nanoteknologi), instrumen khusus kuantum ini telah dibingkai dalam istilah strategis, menetapkan tujuan, jangka waktu, atau mekanisme pendanaan yang luas untuk pengembangan QIT daripada menetapkan batasan peraturan yang terperinci.

Karakteristik penggunaan ganda QIT sejajar dengan domain lain, seperti bioteknologi atau AI, di mana teknologi dapat dimanfaatkan untuk tujuan sipil atau militer. Sifat penggunaan ganda ini mendorong peningkatan persaingan internasional dan langkah-langkah keamanan, termasuk pembatasan perdagangan dan kontrol transfer teknologi khusus yang telah muncul dalam beberapa tahun terakhir untuk diterapkan pada QIT dan elemen rantai pasokannya.

Selain itu, banyak pemerintah juga sedang menjajaki aturan terbatas dan terarah yang membahas area spesifik QIT seperti enkripsi yang diaktifkan kuantum atau pertukaran kunci berbasis kuantum. Misalnya, Undang-Undang Kesiapan Keamanan Siber Komputasi Kuantum AS adalah contoh instrumen legislatif awal yang ditujukan kepada lembaga-lembaga dalam mengadopsi kriptografi pasca-kuantum. Tujuannya adalah untuk membahas pembuatan peraturan khusus domain seiring evolusi komputasi kuantum. Seiring waktu, peraturan khusus kuantum yang lebih komprehensif dapat muncul, yang berfokus pada privasi data, standardisasi, tanggung jawab, atau kasus penggunaan spesifik sektor jika teknologi tersebut matang hingga titik di mana kerangka kerja yang ada menjadi tidak memadai.

Meskipun beberapa undang-undang dan peraturan yang ada menjadikan teknologi kuantum sebagai pokok bahasannya, secara yurisprudensi mereka tidak banyak bergerak melampaui sekadar menerapkan jenis rezim yang ada, seperti penggunaan ganda, pada teknologi yang memenuhi klasifikasi teknis sebagai kuantum. Sebagai contoh, rezim penggunaan ganda di AS secara historis sebagian besar tidak memperhitungkan bagaimana keterikatan jaringan kuantum yang digunakan untuk tujuan sipil dan militer dapat menimbulkan tantangan (jika ada) untuk pemantauan, verifikasi, dan audit kepatuhan terhadap aturan penggunaan ganda. Kontrol ekspor juga secara relatif tidak langsung menyebutkan kuantum dalam konteks rezim kontrol yang sudah mapan. Dan inisiatif ekosistem kuantum sebagian besar mengadopsi pendekatan yang sudah ada.

Hukum kekayaan intelektual yang menjadi dasar paten yang ada untuk teknologi kuantum (seperti perangkat keras) bergantung pada persyaratan umum seperti kecukupan pengungkapan dan persyaratan yang ada yang harus dipenuhi oleh QIT agar dapat dipatenkan. Hal ini dapat diharapkan karena sebagian besar jika bukan seluruhnya regulasi yang berlaku untuk QIT tidak perlu spesifik kuantum karena hukum tersebut tidak mengarahkan hasil pada tingkat mekanika kuantum, tidak seperti misalnya, hukum yang mungkin berupaya melarang atau menetapkan jenis komputasi kuantum tertentu (yang menurut kami bisa menjadi masalah).

2.5 TATA KELOLA QIT BERLAPIS

Tata Kelola Teknologi

Riset yang ada tentang teknologi kuantum dan QIT beragam tetapi seringkali kurang memiliki penjelasan sistematis atau rinci yang menghubungkan sifat-sifat mekanika kuantum teknis yang mendasari QIT dengan logika praktik hukum dan tata kelola. Karya awal yang menerapkan prinsip-prinsip tata kelola teknologi pada teknologi kuantum telah mencakup campuran pemeriksaan yurisprudensi, etika, dan berbasis kebijakan. Riset tersebut mencakup kerangka kerja tentang bagaimana memeriksa efek teknologi kuantum dan prinsip-prinsip untuk tata kelola.

Karya awal lainnya menempatkan tata kelola QIT prospektif dalam debat tata kelola teknologi mengenai sejauh mana inovasi tahap awal harus diatur secara ringan agar tidak menghambat perkembangannya. Studi berorientasi kebijakan telah meneliti prosedur kelembagaan di mana tata kelola teknologi kuantum harus dilakukan, dengan berargumen

untuk pendekatan partisipatif yang menumbuhkan kepercayaan pada teknologi yang muncul. Lebih luas lagi, studi tentang pertimbangan normatif teknologi kuantum telah berupaya mempertimbangkan dampak etika dan desain.

Telah ada juga sejumlah laporan industri yang tidak ditinjau oleh rekan sejawat dan inisiatif multilateral yang meneliti dampak terhadap tata kelola kuantum. Di antara pembahasan yang lebih luas tentang bagaimana lembaga tata kelola, hukum, dan kebijakan dapat menanggapi teknologi kuantum adalah Hoofnagle dkk. yang berfokus pada dampak tata kelola dari penginderaan kuantum berdasarkan bahwa hal itu mewakili bentuk QIT yang paling matang. Salah satu pendekatan untuk secara sistematis mendekati tata kelola kuantum yang telah berupaya mensintesis instrumen teknis dan tata kelola adalah model tumpukan tata kelola yang memperlakukan QIT dan tata kelolanya dalam bentuk tumpukan, memetakan hubungan di antara keduanya. Kami mengadaptasi model tersebut di bawah ini.

Pemeriksaan Geopolitik

Secara geopolitik, studi paling rinci tentang dampak penginderaan kuantum terhadap kemampuan serangan balasan dan penyingkapan aset strategis seperti kapal selam bersenjata nuklir adalah Rand. Karya ini mempertimbangkan secara rinci aspek praktis dari klaim bahwa perangkat penginderaan kuantum dapat mengganggu keseimbangan geostrategis berdasarkan kemampuan serangan balasan tenaga nuklir. Karya ini merupakan sintesis tepat waktu dari paparan teknis dan pemeriksaan strategis, yang menunjukkan hambatan besar yang perlu diatasi agar penginderaan kuantum dapat menimbulkan risiko geopolitik yang begitu tinggi.

Kekayaan Intelektual dan QIT

Dampak kekayaan intelektual dari QIT diuraikan dalam sejumlah artikel yang membahas poin-poin penting dari perspektif kekayaan intelektual, termasuk kemampuan paten dari penemuan kuantum. Di luar perlakuan teoretis, dalam sebuah studi IP empiris, Aboy dkk. memetakan lanskap paten QIT dan teknologi kuantum, menunjukkan penekanan pada paten perangkat keras dan bahwa secara umum sistem paten sebagaimana adanya tidak memberikan bukti bahwa tantangan kemampuan paten menghambat pengembangan QIT.

Sebuah pemantauan sistematis baru-baru ini tentang pelajaran dari tata kelola teknologi baru yang berlaku untuk QIT meneliti bagaimana bioteknologi, nanoteknologi, dan AI dapat memberikan informasi untuk pengawasan yang efektif. Artikel ini berfokus pada potensi kebutuhan akan panduan kuantum tahap awal yang mencerminkan model-model tersebut tanpa membebani inovasi secara berlebihan. Riset lain juga mempertimbangkan instrumen internasional dalam teknologi baru, seperti perjanjian atau instrumen lainnya, untuk menyelesaikan tantangan koordinasi jaringan kuantum lintas batas. Meskipun terbatas, kajian hukum yang ada menggarisbawahi perlunya mempertimbangkan bagaimana kerangka kerja tata kelola umum seperti yang digunakan untuk nanoteknologi atau AI dapat diadaptasi untuk mengatasi keunikan kuantum. Model tumpukan tata kelola yang diadopsi di sini mengusulkan bahwa regulasi kuantum dapat berlapis, dimulai dari perangkat keras tingkat rendah dan berpuncak pada aturan tingkat aplikasi yang spesifik untuk domain tersebut.

Perspektif berlapis ini selaras dengan gagasan yang muncul dari tata kelola AI: bahwa regulator membutuhkan struktur yang fleksibel untuk mengatasi risiko dan tanggung jawab pada setiap fase pengembangan, termasuk potensi sinergi dengan inisiatif multilateral yang ada untuk pengawasan teknologi canggih seperti kerangka kebijakan OECD atau upaya standardisasi ISO/IEC dalam QIT. Model tata kelola kuantum yang komprehensif masih dalam tahap pembentukan. Namun, dengan riset yang semakin menggabungkan pemeriksaan hukum, peta jalan kebijakan, dan pelajaran yang dipetik dari teknologi mutakhir lainnya untuk mengusulkan respons yang lebih kuat. Namun, terlepas dari karya yang muncul, hanya sedikit pembelajaran yang secara langsung menjawab secara tepat apa yang unik tentang QIT dalam hal kerangka hukum atau konsekuensinya. Pertanyaan mengenai sifat *sui generis* dari tata kelola kuantum: persyaratan tata kelola unik apa yang dihasilkannya dan ditimbulkannya, bagaimana posisinya dalam kerangka hukum yang ada, dan reformasi apa yang seharusnya dilakukan, jika ada, terhadap yurisprudensi khusus domain. Pertanyaan ini menjadi fokus pekerjaan kami. Untuk tujuan ini, kami merumuskan pertanyaan tentang QIT *sui generis* di bawah ini.

2.6 KEKHUSUSAN TATA KELOLA QIT

Seperti halnya perkembangan teknologi baru lainnya, dasar untuk mempelajari QIT dan hukum adalah memahami kebaruan inovatif QIT dan dampaknya, jika ada, dalam penerapannya. Mungkin pertanyaan panduan terpenting dan perlu dijawab untuk tata kelola kuantum dan perspektif yurisprudensi adalah mengenai apa yang, jika ada, *sui generis* tentang tata kelola QIT. Pertanyaan tentang *sui generis* memaksa kita untuk menyelidiki apakah ada sesuatu yang baru dari perspektif tata kelola baik konsekuensial, konseptual, prosedural yang muncul atau seharusnya muncul ketika teknologi berubah, termasuk teknologi pemrosesan informasi secara umum dan teknologi pemrosesan informasi kuantum secara khusus? Oleh karena itu, kita berfokus pada pertanyaan apakah penerapan QIT hanyalah bentuk lain dari teknologi pemrosesan informasi yang sudah tercakup dalam yurisprudensi luas tentang penggunaan teknologi komputasi, siber-teknologi, dan pemrosesan informasi secara umum (di mana QIT merupakan bagiannya). Pertanyaan-pertanyaan ini sering diperdebatkan dalam yurisprudensi dan tata kelola teknologi di bawah naungan ‘netralitas teknologi’ regulasi, di mana tata kelola bersifat netral terhadap teknologi sejauh sebagian besar bersifat agnostik secara teknis, lebih berfokus pada konsekuensi dari penggunaan teknologi apa pun dalam konteks tertentu. Perdebatan tentang netralitas teknologi sejauh mana hukum harus menjangkau spesifikasi teknis dari teknologi tertentu umum terjadi di seluruh yurisprudensi teknologi, termasuk kajian yang muncul tentang tata kelola dan etika QIT. Jawaban atas pertanyaan-pertanyaan ini sebagian bergantung pada teori yurisprudensi yang digunakan rasionalitasnya dan justifikasi tata kelola itu sendiri yang diadopsi.

Keunikan Kuantum

Seperti yang dibahas di bawah ini dan di seluruh karya ini, karena dasarnya pada mekanika kuantum, QIT dapat memperkenalkan perbedaan unik dalam bagaimana seharusnya ditafsirkan sebagai pokok bahasan dalam hukum. Sistem kuantum menunjukkan sifat-sifat

spesifik yang bukan sekadar perluasan atau penskalaan teknologi klasik, tetapi merupakan fenomena yang secara ontologis fundamental berbeda yang tidak memiliki kesamaan dalam fisika klasik. Ini termasuk keterikatan kuantum dan superposisi kuantum yang secara tepat memberikan teknologi kuantum yang memanfaatkannya sifat-sifat yang berbeda dari yang diasumsikan hukum dari teknologi klasik. Sistem kuantum juga secara inheren bersifat stokastik bukan hanya secara epistemik yang sudah dikenal oleh hukum dan pemerintahan, tetapi secara fisik dan ontologis. Salah satu hasil paling signifikan dari fisika abad ke-20 adalah bahwa ketidakpastian yang diamati dalam statistik pengukuran kuantum, pengukuran yang menurutnya kita menyimpulkan keberadaan objek bukanlah epistemik, bukan karena beberapa ketidaksempurnaan yang dapat diperbaiki dalam alat ukur. Sebaliknya, ketidakpastian itu bersifat fisik, nyata, ontologis dan ketidakpastian ini bukan sekadar fitur periferal dari sistem kuantum, melainkan ketidakpastian yang memengaruhi cara-cara primitif kita mendefinisikan objek dengan menentukan batas, keadaan, atau evolusinya dari waktu ke waktu.

Hal ini tidak dan ini adalah poin penting yang kami tekankan membuat fenomena kuantum yang menjadi dasar QIT menjadi 'tidak dapat diketahui' atau 'tidak dapat diatur' atau bahkan tidak dapat diprediksi dengan cara yang berarti kontrol dan pengaturannya menjadi tidak mungkin. Sistem kuantum dan QIT tidak dapat diketahui oleh hukum berdasarkan hal ini. Ketidakpastian lebih tepat dipikirkan sebagai masalah derajat dan masalah yang telah ditangani oleh hampir satu abad pembelajaran teoretis dan terapan untuk membuat sistem yang secara inheren tidak pasti ini dapat dikendalikan. Namun, tergantung pada jenis tata kelola yang diinginkan (seberapa penting kontrol spesifik atas evolusi kuantum atau keadaan bagi rezim tata kelola tertentu), hal ini berarti bahwa hukum mungkin perlu disesuaikan atau dimodifikasi dalam keadaan tertentu (misalnya, alih-alih berfokus pada hak milik 'dalam' informasi kuantum tertentu, hukum mungkin malah berfokus pada hak untuk mengendalikan sistem kuantum tersebut mengingat informasi kuantum secara teknis mungkin tidak memiliki batasan yang tepat yang biasanya diperlukan untuk objek yang mampu menjadi milik).

Koordinasi Tata Kelola Teknologi Membutuhkan Kekhususan

Kedua, studi tentang QIT dan hukum, termasuk potensi respons tata kelola khusus QIT, dapat dimotivasi berdasarkan kekhususan. Meskipun teknologi informasi kuantum sebagai teknologi informasi sudah termasuk dalam lingkup abstrak regulasi teknologi informasi, termasuk preskripsi dan larangan instrumental atau normatif yang berlaku, tujuan dan fungsi prinsip hukum, undang-undang, dan instrumen tata kelola bukanlah sekadar untuk menentukan prinsip umum yang abstrak. Sebaliknya, detail itu penting, termasuk detail tentang bagaimana, di mana, dan dalam kondisi apa teknologi akan dioperasikan, digunakan, dipantau, disimpan, dan diterapkan. Kekhususan merupakan fitur penting dari implementasi hukum itu sendiri dan merupakan inti dari penyelesaian masalah koordinasi dalam konteks ekonomi dan sosial. Memang, kekhususan adalah ciri khas logika semua sistem hukum yang bergantung pada hierarki klasifikasi untuk menentukan hak, kewajiban, dan kepentingan. Dan kekhususan sudah menjadi ciri bagaimana hampir semua teknologi diatur: legislasi, peraturan,

aturan, preseden, dan panduan secara khusus menetapkan bagaimana tata kelola teknologi sebagaimana diterapkan pada teknologi tertentu.

Teknologi Strategis Membutuhkan Kepastian

Ketiga, banyak jenis QIT dapat dianggap sebagai teknologi strategis, berbeda dari banyak teknologi lainnya karena potensi kemampuan uniknya yang mungkin tidak tersedia hanya melalui teknologi klasik. Hal ini mungkin dikatakan secara sepele untuk semua teknologi yang dapat memengaruhi perilaku. Tetapi QIT bersifat strategis dengan cara yang berbeda karena sifat dan kemampuannya yang unik yang tidak tersedia bagi pemangku kepentingan atau musuh yang terbatas hanya pada teknologi klasik. Dampak strategis QIT berarti bahwa penggunaan dan penyebarannya dapat memiliki konsekuensi yang berbeda bagi pasar ekonomi, perilaku regulasi, dan posisi geopolitik. Misalnya, seperti yang dieksplorasi dalam bagian-bagian selanjutnya, QIT dapat berdampak khusus pada perilaku strategis Negara mengingat potensinya untuk dekripsi dan simulasi (memang sudah memengaruhi perilaku Negara secara strategis karena Negara berupaya mengamankan rantai pasokan kuantum dengan keyakinan bahwa QIT akan benar-benar memiliki dampak yang signifikan). Demikian pula, kepemilikan komputer kuantum yang sepenuhnya toleran terhadap kesalahan dan dapat diskalakan oleh pelaku pasar yang memungkinkan penerapan strategi optimasi yang unggul dapat memiliki dampak mendalam terhadap asimetri informasi dalam aktivitas ekonomi (seperti halnya, misalnya, kepemilikan sistem kecerdasan buatan canggih). Konsekuensi strategis potensial dari QIT ini dapat menunjukkan nilai aturan atau prinsip umum yang secara khusus diarahkan pada fitur teknis atau penggunaan QIT untuk memberikan kepastian kepada para pemangku kepentingan. Aturan atau prinsip tersebut dapat relevan dalam konteks geopolitik di mana regulasi dan motivasi untuk mematuhi aturan oleh aktor negara seringkali bergantung pada insentif daripada penegakan hukum langsung.

Kepastian tata kelola teknologi juga penting untuk memecahkan masalah koordinasi, yang sering dipelajari dan menjadi subjek pemeriksaan teori permainan, tentang bagaimana aktor negara yang kepentingannya tidak selalu selaras dapat bertindak secara kooperatif. Kasus kanonik di sini dari konteks kedaulatan negara dan keamanan nasional adalah regulasi senjata nuklir, seperti melalui larangan uji coba, non-proliferasi, dan instrumen internasional lainnya. Rezim pemantauan dan verifikasi yang dikodekan dalam instrumen tersebut memainkan peran penting dalam memotivasi perilaku negara untuk mematuhi ketentuan instrumen tersebut. Ketika menyangkut penggunaan teknologi informasi canggih, seperti kecerdasan buatan atau komputasi kuantum, oleh Negara untuk tujuan yang berpotensi bersifat antagonis, maka wajar untuk mengharapkan persyaratan spesifik yang serupa berlaku (pertimbangkan, misalnya, usulan untuk regulasi tingkat komputasi sehubungan dengan teknologi kecerdasan buatan).

Penggunaan Ganda Teknologi Membutuhkan Kejelasan

Alasan keempat, tetapi terkait, mengapa spesifikasi teknologi mengenai tata kelola QIT dalam hukum domestik dan internasional sangat beralasan adalah karakteristik penggunaan ganda dari teknologi tersebut. Teknologi penggunaan ganda adalah teknologi yang memiliki aplikasi baik dalam konteks sipil maupun permusuhan, sehingga menimbulkan dilema tentang bagaimana mengatur penggunaan dan perdagangan teknologi tersebut untuk memberikan

manfaat di satu sisi, sementara membatasi penggunaannya untuk tujuan permusuhan atau berbahaya oleh pihak musuh di sisi lain. Kejelasan penggunaan yang diizinkan dan dilarang penting dalam kasus rezim penggunaan ganda untuk memberikan kepastian bagi para pemangku kepentingan, aktor, dan pengguna teknologi tersebut, terutama di mana transisi dari penggunaan sipil ke militer suatu teknologi relatif lancar atau mudah. Hal ini terutama berlaku ketika QIT diintegrasikan ke dalam teknologi sensitif tinggi lainnya yang tunduk pada rezim penggunaan ganda atau kontrol ekspornya sendiri, seperti teknologi terkait AI, chip komputasi, dan teknologi ilmu hayati. QIT sudah tunduk pada tingkat spesifikasi rezim penggunaan ganda di sejumlah yurisdiksi, seperti AS dan Australia, justru karena alasan-alasan ini.

Teknologi Baru Membutuhkan Fleksibilitas

Sebuah kontrapoint terhadap seruan untuk kepastian, kejelasan, dan spesifikasi dalam regulasi teknologi muncul dari fakta bahwa QIT masih merupakan teknologi baru yang sedang berkembang. Tata kelola QIT menghadapi dilema Collingridge klasik bahwa regulasi awal teknologi yang sedang berkembang dapat menghambat perkembangannya, sementara keterlambatan respons regulasi dapat menimbulkan dampak negatif. Tantangan yang dihadapi oleh penerapan prinsip-prinsip kehati-hatian ini merupakan pertimbangan penting yang berkaitan dengan respons normatif dan kebijakan lembaga hukum dan regulasi terhadap QIT. Secara kasat mata, risiko melemahkan inovasi baru dan kebutuhan akan adaptabilitas terhadap teknologi yang (seringkali) berkembang dengan cepat cenderung mengarah pada preferensi netralitas teknologi, di mana tata kelola menentukan hasil dengan tujuan yang terarah daripada menetapkan atau melarang kontrol spesifik pada teknologi (terutama pada tingkat teknis). Ini adalah kekhawatiran yang sah, tetapi sebenarnya merupakan pertimbangan mengenai bagaimana waktu dan spesifikasi tata kelola teknologi saling berkaitan. Ketika (dengan asumsi) pengembangan QIT terjadi seperti yang diharapkan dengan beroperasinya komputer kuantum yang skalabel dan toleran terhadap kesalahan, jaringan kuantum, dan penginderaan kuantum dengan fidelitas tinggi ada banyak hal yang kita ketahui sekarang tentang bagaimana teknologi tersebut harus bekerja dan kemungkinan akan digunakan.

Ada juga banyak hal yang kita ketahui tentang bagaimana sistem tersebut akan terwujud (biasanya dalam infrastruktur skala besar, dikelilingi oleh tumpukan komputasi klasik) dan, yang penting, di mana dalam tumpukan teknologi tersebut sistem tersebut dapat dikendalikan (yang pada gilirannya memberikan informasi spesifik mengenai bagaimana sistem tersebut harus diatur). Selain itu, untuk banyak bidang hukum, seperti kekayaan intelektual (di mana tingkat spesifikasi yang diperlukan untuk memenuhi standar kecukupan pengungkapan relevan) atau bahkan penggunaan QIT dalam ilmu hayati (titik kuantum misalnya, di mana keandalan dan ketahanan informasi yang diekstrak atau dihasilkan menggunakan QIT harus memenuhi aturan bioinformatika dan aturan lainnya yang menyeluruh), QIT sudah tunduk pada spesifikasi dan perubahan hukum. Oleh karena itu, ketidakpastian tahap awal dalam inovasi mungkin tidak serta merta menentang spesifisitas tata kelola teknologi pada waktu yang tepat. Sebaliknya, hal ini menunjukkan bahwa kehati-hatian dapat melibatkan pembatasan tata kelola antisipatif secara hati-hati mengingat potensi

variasi dalam konfigurasi pengembangan teknologi. Untuk mempermudah pemeriksaan kami, kami mengeksplorasi lebih detail bagaimana model tumpukan tata kelola regulasi teknologi akan diterapkan pada QIT.

2.7 TUMPUKAN TATA KELOLA, SKEMA TATA KELOLA, DAN RISIKO

Gambaran Umum

Untuk mempermudah pemeriksaan kami, di beberapa bagian dalam karya ini kami mengadopsi dan memperluas model tumpukan tata kelola regulasi teknologi. Ide inti di balik pendekatan tumpukan tata kelola adalah bahwa teknologi informasi kuantum diterapkan dan digunakan di lokasi spesifik dalam keseluruhan proses atau prosedur teknis yang digunakan dalam alur kerja di seluruh aktivitas ekonomi, sosial, dan ilmiah. Ini mungkin termasuk QIT sebagai sumber daya untuk simulasi komputasi atau pemrosesan data, di mana perangkat kuantum atau efek kuantum memungkinkan hasil yang baru atau berbeda dibandingkan dengan komputasi klasik. Atau mungkin melibatkan QIT yang digunakan untuk mencegat dan mendekripsi komunikasi selama konflik atau penegakan hukum. Keputusan tentang bagaimana mengatur QIT harus jelas tentang di mana dalam tumpukan teknis tata kelola ditargetkan: apakah prosedur kuantum itu sendiri memerlukan kontrol atau pengaruh? Atau hanya hasil atau efeknya pada bagian lain dari tumpukan? Model tumpukan tata kelola dimaksudkan untuk memungkinkan pemetaan instrumen tata kelola yang tepat ke tingkat yang tepat dalam tumpukan teknis dengan cara yang sesuai untuk tujuan regulasi, yaitu yang memfasilitasi regulasi hak, kepentingan, dan kewajiban pemangku kepentingan. Model tumpukan tata kelola yang kami adaptasi memiliki tiga komponen utama.

Tumpukan Teknologi dan Proses

Tumpukan teknologi terdiri dari komponen vertikal, yang dipahami sebagai tumpukan terintegrasi secara vertikal mulai dari sirkuit kuantum dasar yang mendasari semua QIT, melalui kerangka dan lapisan perangkat keras hingga keluaran akhir teknologi; dan komponen horizontal, yang mengacu pada alur kerja keseluruhan atau proses produksi di mana QIT membentuk satu komponen terintegrasi.

Tumpukan Tata Kelola

Tumpukan tata kelola mencakup pemeriksaan hierarki instrumen tata kelola yang berlaku untuk tumpukan teknologi yang relevan. Hierarki ini dapat dipahami sebagai perluasan dari instrumen formal berbasis negara (seperti perjanjian), hingga undang-undang nasional dan kota, peraturan, perintah eksekutif, instrumen publik, hingga organisasi layanan sipil dan organisasi standar. Instrumen tata kelola dibingkai sebagai penengah hak, kepentingan, dan kewajiban di antara para pemangku kepentingan (seperti antara negara dan penduduknya, atau antara perusahaan individu melalui kontrak dan sebagainya). Instrumen yang berbeda dapat disesuaikan dengan tujuan yang berbeda (seperti kepentingan pemangku kepentingan tertentu) dan dalam penerapannya dapat sesuai dengan lapisan yang berbeda dalam tumpukan teknologi (seringkali standar teknis lebih rinci dan spesifik daripada undang-undang atau perjanjian yang menyeluruh).

Taksonomi Informasi

Dalam model ini, kita menambahkan gagasan taksonomi informasi sebagai cara untuk mengidentifikasi bagaimana QIT dan hukum berhubungan dengan informasi. Taksonomi informasi dibahas lebih rinci di bawah ini, tetapi pada intinya menyangkut masukan (data masukan klasik), pemrosesan (komputasi, dll.), dan keluaran (data pengukuran). QIT sebagai teknologi informasi dapat terlibat dalam akuisisi data melalui pengukuran, pemrosesan, atau menghasilkan keluaran data. Pada gilirannya, setiap tahapan ini dapat menjadi subjek secara langsung atau tidak langsung dari beberapa instrumen tata kelola, yang dapat mengatur apa atau bagaimana pengukuran dilakukan (misalnya untuk memastikan kebenaran data), atau jenis pemrosesan atau keluaran.

Rincian lebih lanjut tentang pendekatan ini diuraikan dalam riset. Pada prinsipnya, aplikasi heuristik dari pendekatan ini akan melibatkan (1) mengidentifikasi elemen-elemen tumpukan teknis, (2) mengidentifikasi tumpukan tata kelola (termasuk tujuan pemangku kepentingan) dan (3) mengidentifikasi dampak epistemik QIT pada informasi yang tersedia dan kemudian bagaimana instrumen tata kelola apa pun harus mengatur proses tersebut secara langsung atau tidak langsung mengingat kepentingan pemangku kepentingan.

Pendekatan informasional adalah alat yang berguna untuk pemeriksaan hukum dampak QIT. Dengan menguraikan QIT menjadi komponen horizontal dan vertikal, kita dapat lebih mudah melihat bagaimana berbagai rezim hukum yang saling terkait menyatu. Daripada, misalnya, mencatat bahwa penggunaan QIT dapat menimbulkan masalah data, privasi, dan kekayaan intelektual, pendekatan berbasis tumpukan yang terperinci dapat memberikan pemeriksaan yang lebih rinci. Pertimbangan data, seperti mematuhi persyaratan standar data, mungkin menjadi masalah yang muncul pada tingkat memori kuantum dalam tumpukan. Masalah privasi mungkin tidak terkait dengan aspek kuantum teknologi sama sekali, tetapi lebih pada antarmuka klasik dengan QIT. Hak kekayaan intelektual mungkin hanya menimbulkan masalah pada beberapa komponen atau kumpulan dari tumpukan, bukan pada setiap bagian atau proses.

Tumpukan Teknologi dan Tumpukan Tata Kelola

Identifikasi Tumpukan Teknologi

Elemen pertama yang perlu dipastikan dalam tumpukan tata kelola adalah tumpukan teknologi, sebuah hierarki dari teknologi tertentu yang dimaksud. Kami menyajikan tumpukan QIT tipikal di bawah ini. Tujuan dari tumpukan ini adalah untuk memungkinkan identifikasi yang jelas tentang lokasi dan saling ketergantungan suatu teknologi. Misalnya, aspek kuantum dari QIT terletak pada skala terkecil di lapisan terendah dari setiap tumpukan yang menggunakannya: di dalam sirkuit. Ini adalah salah satu alasan mengapa teknologi kuantum generasi kedua pada dasarnya bersifat informasional. Salah satu ciri khas dampak suatu teknologi adalah kemampuannya untuk memengaruhi atau bertindak terhadap lingkungan. Kapasitas sistem kuantum yang terbatas dan relatif kecil untuk melakukan hal tersebut terbatas.

Penggunaan utamanya dalam teknologi adalah untuk penginderaan, pengkodean, pemrosesan, dan keluaran informasi. Output ini kemudian dapat menjadi input (tidak berbeda

dengan output informasi AI) ke dalam aktuator atau kerangka kerja interaktif. Di sekitar elemen teknologi khusus kuantum terdapat berbagai kerangka kerja teknologi, yang dapat dijelaskan dalam istilah fisik atau abstrak. Kerangka kerja untuk QIT ini bersifat klasik, termasuk sirkuit klasik, sistem operasi, dan perangkat pemrosesan sinyal. Kerangka kerja klasik tersebut bukanlah kuantum karena tidak ada dan berperilaku secara kuantum. Perbedaan jenis ini penting untuk memahami bagaimana tata kelola dapat diarahkan pada lapisan yang berbeda dalam tumpukan. Misalnya, tata kelola yang sangat teknis, misalnya tentang bagaimana reaktor nuklir harus berfungsi, biasanya bersifat preskriptif terhadap detail kecil, bahkan pada tingkat atom (mekanisme kontrol berupaya mengatur laju fisi misalnya), sementara tata kelola sosial normatif, seperti mengenai bagaimana platform komputasi dapat digunakan atau untuk tujuan apa, kurang spesifik secara teknis.

Identifikasi Tumpukan Tata Kelola

Kedua, tumpukan tata kelola membantu mengidentifikasi instrumen yang tepat, misalnya... Alih-alih berupaya mencapai hasil pada tingkat sirkuit kuantum, mungkin lebih tepat dilakukan pada tingkat lain dengan tujuan yang terarah daripada tujuan teknis. Sebaliknya, jika prosedur jaminan mewajibkan spesifikasi teknik, mungkin spesifikasi tersebut lebih tepat ditempatkan pada tingkat sirkuit atau kerangka teknis daripada hanya secara abstrak sebagai persyaratan di antara pemangku kepentingan atau tingkat lain dalam tumpukan. Pendekatan seperti itu mengakui bahwa tingkat yang berbeda dalam tumpukan teknis dapat dikendalikan hingga tingkat dan cara yang berbeda. Hal ini memengaruhi sejauh mana tata kelola dapat diimplementasikan pada tingkat tersebut. Seperti yang akan kita bahas di bawah ini, QIT dapat dikendalikan, tetapi biasanya dengan cara yang berbeda dari klasik: misalnya, seseorang tidak dapat mempertahankan karakteristik kuantum dari QIT dan entah bagaimana mengendalikan hasil pengukuran sistem secara deterministik jika ini merupakan tujuan normatif.

Integrasi dan Risiko

Ketiga, model tumpukan tata kelola membantu dalam proses penilaian risiko yang menjadi inti pengembangan dan penerapan teknologi apa pun. Untuk kasus penggunaan QIT, penting untuk menyadari bahwa QIT akan selalu terintegrasi dalam tumpukan teknologi dan alur kerja klasik yang lebih luas QIT hanya akan menjadi komponen dari infrastruktur yang lebih luas. Hal ini memengaruhi kerangka risikonya karena konteks di mana QIT digunakan memengaruhi profil risikonya, dan sebaliknya, penggunaan QIT dalam alur kerja dan proses pada prinsipnya dapat mengubah ukuran risiko total atau agregat yang digunakan untuk menentukan keberterimaan suatu aktivitas. Dalam kombinasi dengan paradigma berbasis tumpukan, kami mengadopsi pendekatan yang berpusat pada risiko khusus untuk QIT dan tata kelola. Kami tertarik pada bagaimana penggunaan QIT mengubah risiko baik dalam hal klasifikasi, kemungkinan kejadian, dan sebagainya. Karya kami tidak menetapkan alat dan teknik untuk mengukur risiko tersebut secara langsung, tetapi mengakui bahwa penilaian risiko teknologi merupakan elemen sentral bagi lembaga yang bergantung pada teknologi komputasi seperti kecerdasan buatan dan yang mungkin secara langsung atau tidak langsung menggunakan QIT.

Pendekatan yang berpusat pada risiko juga, menurut kami, sangat berguna bagi para pemangku kepentingan yang mempertimbangkan bagaimana hukum mungkin (atau mungkin tidak) perlu beradaptasi untuk menanggapi penggunaan QIT. Misalnya, penggunaan QIT mungkin memiliki sedikit atau tidak ada dampak signifikan pada jenis risiko yang ingin ditangani oleh hukum dan peraturan. Sebaliknya, integrasi QIT dalam alur kerja atau proses mungkin secara signifikan mengubah vektor atau sifat risiko, berpotensi membuka bentuk risiko baru yang perlu dipertimbangkan atau ditanggapi secara yurisprudensi (karena QIT dapat memungkinkan aktivitas tertentu yang sebelumnya tidak mungkin dilakukan secara fisik atau komputasi). Atau mungkin QIT memengaruhi dimensi risiko lainnya, seperti skala, cakupan, luas, atau tingkat keparahan dampak. Memahami variasi risiko yang ditimbulkan oleh penggunaan QIT (dalam batasan pemeriksaan risiko itu sendiri) memberikan manfaat praktis lebih lanjut untuk memahami konsekuensi QIT yang harus diperhitungkan oleh hukum dan peraturan.

Risiko dan Tata Kelola

Model tata kelola teknologi yang berpusat pada risiko dan berbasis tumpukan tata kelola saling melengkapi. Keduanya berfokus pada pemahaman bagaimana dan di mana dampak QIT muncul dalam tumpukan teknis. Hal ini memungkinkan ketelitian yang lebih rinci mengenai jenis, bentuk, dan cakupan instrumen tata kelola yang harus digunakan sebagai kontrol untuk mengelola risiko terkait QIT. Pendekatan berbasis tata kelola dan tumpukan teknis juga memungkinkan kita untuk mengakomodasi ukuran empiris penting dari dampak QIT. Dengan membingkai penggunaan QIT sebagai intervensi pada beberapa tingkat dalam tumpukan teknis alur kerja ekonomi, sosial, atau ilmiah, kita kemudian dapat mempertimbangkan bagaimana intervensi ini menimbulkan konsekuensi hukum. Ini mungkin termasuk penggunaan QIT yang memengaruhi hak, kepentingan, atau kewajiban pemangku kepentingan. Model tumpukan tata kelola membantu kita memetakan instrumen tata kelola ke tingkat yang tepat dalam tumpukan teknologi, sehingga memungkinkan kita untuk mengidentifikasi kewajiban atau hak yang relevan yang dipertaruhkan dari penggunaan QIT tersebut. Model tumpukan juga memungkinkan pertimbangan yang lebih rinci tentang apa yang ingin dicapai oleh tata kelola dan bagaimana cara mencapainya.

Sebagai contoh, ini mungkin melibatkan apakah penggunaan QIT atau tata kelolanya ditargetkan pada tingkat komputasi, menetapkan komputasi terlarang yang seharusnya tidak dilakukan (misalnya, sintesis unsur kimia terlarang untuk pembuatan senjata kimia), atau resep tentang bagaimana, misalnya, komputasi berlangsung dalam desain obat farmasi untuk memenuhi persyaratan bioinformatika tentang seberapa andal informasi dari simulasi tersebut. Atau mungkin melibatkan spesifikasi instrumen tata kelola yang berkaitan dengan penggunaan QIT dalam uji klinis yang menentukan bagaimana QIT diukur, digunakan, atau disebarluaskan. Atau mungkin saja instrumen tata kelola dalam kasus tertentu tidak berfokus pada dinamika teknis tingkat rendah spesifik dari suatu tumpukan, melainkan secara sengaja atau normatif pada penggunaan keluaran QIT.

Kegunaan Pendekatan Berbasis Risiko

Pendekatan berbasis risiko dapat membantu memfokuskan penyelidikan kita pada dampak QIT terhadap hukum dalam hal pertanyaan-pertanyaan berikut:

1. Apakah penggunaan QIT memengaruhi, dengan cara apa pun, penerapan atau tujuan instrumen tata kelola?
2. Apakah rezim tata kelola yang diusulkan yang mencakup QIT dapat memengaruhi penggunaannya dalam aktivitas ekonomi, sosial, atau ilmiah?
3. Apakah reformasi tata kelola mungkin diperlukan atau diinginkan untuk memenuhi berbagai tujuan tata kelola teknologi di bidang-bidang ini?

Mengingat kebaruan relatif dari aplikasi QIT di semua sektor, dan bahkan rezim tata kelola yang lebih baru untuk teknologi kuantum, kami mengadopsi fokus yang luas tentang di mana QIT kemungkinan akan diterapkan dan relevan. Luasnya aktivitas ekonomi sebagai kolokasi bidang interdisipliner bersama dengan nuansa kompleks ilmu informasi kuantum berarti bahwa upaya untuk memeriksa keterkaitannya harus ditangani dengan hati-hati karena perbedaan yang nyata dan halus dalam konseptualisasi, nomenklatur, dan pembingkaian fenomena. Menggabungkan (selain itu) berbagai kerangka kerja tata kelola, pedoman, yurisprudensi, dan sejenisnya menambah kompleksitas, yang membutuhkan penerjemahan dan pemetaan antara konsep, pendekatan, dan istilah teknis yang menunjukkan berbagai tingkat kesamaan.

2.8 MENYATUKAN TEKNOLOGI DAN HUKUM MELALUI INFORMASI

Informasi sebagai Konsep Titik Tumpu

Salah satu tantangan dalam mendekati tata kelola sektor yang sangat teknis dan sangat interdisipliner terletak pada menemukan seperangkat konsep umum yang menyatukan, yang dengannya hubungan konseptual dan teknis antar setiap disiplin ilmu dapat diperiksa. Menguraikan kerangka kerja terpadu yang memungkinkan penerjemahan antar konsep di berbagai bidang, atau yang menunjukkan secara jelas bagaimana tata kelola atau hukum yang berlaku di satu bidang dapat secara langsung atau tidak langsung memengaruhi sintesis dengan teknologi dari disiplin ilmu lain adalah tugas yang kompleks. Sebagian besar studi tentang QIT dan hukum membutuhkan mediasi semacam itu di antara disiplin ilmu teknis dan yurisprudensi yang berbeda. Kompleksitas dan keberagaman setiap disiplin ilmu berarti penting untuk mencari bahasa umum, konsep atau seperangkat konsep utama, yang digunakan untuk membandingkan dan membedakan setiap bidang. Dalam karya ini, pilihan konsep utama kami adalah informasi (dan teori informasi). Kami mengadopsi informasi sebagai sarana konseptual untuk mensintesis QIT dan hukum. Teori informasi menyediakan sarana untuk mengatur dan menata spektrum aplikasi QIT beserta dampaknya terhadap rezim hukum dan peraturan.

Informasi adalah landasan bagaimana lembaga hukum membuat keputusan. Dalam persidangan atau melalui prosedur pengambilan keputusan, informasi adalah sumber daya yang dimanipulasi. Identifikasi pemangku kepentingan, hak dan kepentingan mereka semuanya bergantung pada informasi. Tanggung jawab dan persyaratan normatif juga bergantung pada informasi. Informasi dan pengukuran memengaruhi persepsi kita tentang

apa adanya. Teknologi QIT seperti penginderaan kuantum memengaruhi apa yang dapat diketahui tentang fenomena dengan cara yang berbeda dari perangkat klasik.

Pemrosesan informasi melalui komputasi kuantum juga dapat memengaruhi jenis wawasan dan kesimpulan yang dapat kita buat tentang dunia dan keputusan yang didasarkan pada informasi tersebut. Komunikasi kuantum memengaruhi transfer informasi. Menjaga keamanan informasi sangat penting bagi aktivitas ekonomi dan sosial. Informasi memengaruhi penalaran dan pengambilan keputusan. Informasi sangat penting bagi fungsi QIT dan hukum. Penggunaan QIT memengaruhi bagaimana informasi diperoleh, bagaimana informasi diproses, dan bagaimana informasi disebarluaskan. Hal ini pada gilirannya memiliki konsekuensi terhadap informasi yang tersedia bagi pemangku kepentingan, peserta, regulator, dan pengadilan, antara lain, yang memengaruhi dan membentuk keputusan mereka yang bergantung pada informasi tersebut. Dekripsi komunikasi strategis yang terklasifikasi mewakili perubahan dalam keadaan informasi suatu negara, misalnya, yang dapat berarti perbedaan antara menang atau kalah dalam konflik. Informasi tentang wawasan teknologi atau perilaku pesaing dapat secara fundamental mengubah cara agen berinteraksi dan juga keseimbangan sistem. QIT dapat mengubah jenis, skala, dan sifat informasi yang tersedia, yang berpotensi memengaruhi bagaimana peserta bertindak. Hal ini juga mengubah dalam beberapa hal sifat informasi yang tersedia bagi hukum ketika penilaian harus dibuat, atau kontrak dinegosiasikan.

Informasi Sangat Penting bagi Teknologi dan Ekonomi Modern

Kami berpendapat bahwa penggunaan informasi sebagai prinsip pengorganisasian yang sesuai dengan pemeriksaan teknis dan regulasi yang dapat dilakukan adalah hal yang beralasan. Informasi sangat penting bagi ilmu pengetahuan modern, aktivitas ekonomi, hubungan sosial, dan pemerintahan. Dalam ilmu fisika, pendekatan teori informasi mewakili subdisiplin yang semakin umum, seperti dalam ilmu hayati (dalam bentuk bioinformatika). Semua ilmu pengetahuan, termasuk ilmu hayati, adalah ilmu informasi, yang terdiri dari serangkaian praktik yang berupaya memperoleh, memproses, dan memeriksa informasi. Hal ini terutama berlaku untuk ilmu pengetahuan karena cakupannya yang luas, dari skala atom dan molekul hingga skala organisme dan populasi. Demikian pula, banyak teknologi tata kelola berkaitan dengan memastikan prosedur ilmiah untuk akuisisi data, pengukuran, desain perangkat, dan penggunaannya dapat dipercaya, akurat, dan andal semua karakteristik yang pada akhirnya dapat dibingkai dalam istilah teori informasi. Prevalensi informasi sebagai jembatan konseptual di seluruh aktivitas sosial, ekonomi, dan ilmiah sesuai dengan peran informasi dalam ilmu kuantum. Seperti yang akan kita bahas di bawah ini, konsep teknologi informasi kuantum, sebagaimana tersirat dalam istilah tersebut, mengadopsi pendekatan teori informasi untuk klasifikasi dan dinamika, yang muncul secara alami dari kombinasi informasi klasik dan ilmu komputer dengan teori kuantum. Dengan demikian, memungkinkan sintesis ilmu kuantum di luar mekanika kuantum tradisional ke bidang komunikasi kuantum, penginderaan kuantum, dan komputasi kuantum. Kami mengadopsi paradigma informasi ini untuk mengeksplorasi potensi aplikasi interseksional QIT dan konsekuensinya bagi kerangka hukum dan peraturan.

Informasi Memungkinkan Perbandingan Domain yang Berbeda

Kami telah memilih informasi sebagai konsep utama dalam karya ini sebagai salah satu cara untuk menghubungkan kerangka kerja yang beragam, terutama di bidang teknis yang penting bagi bidang fokus yurisprudensi pilihan kami, yaitu tata kelola ilmu hayati, hukum kekayaan intelektual, hukum informasi, properti, hukum internasional publik, dan hukum komunikasi. Dari perspektif teknis, mengadopsi kerangka kerja teori informasi memungkinkan kita untuk memposisikan pemrosesan informasi kuantum, penggunaan komputasi dan komunikasi secara bermanfaat dalam konteks yang lebih luas dari pemrosesan informasi klasik yang menjadi dasar hukum itu sendiri. Tetapi apa sebenarnya artinya mengambil pendekatan informasional atau teori informasi terhadap tata kelola kuantum? Bagaimanapun, teori informasi itu sendiri adalah bidang yang beragam, mulai dari matematika informasi dan komunikasi yang sangat teknis di satu sisi, hingga penggunaan kualitatif konsep informasional seperti pengetahuan, kemampuan meramalkan, dan sebagainya dalam hukum itu sendiri.

Informasi sebagai Paradigma dan Metode

Informasi memainkan peran berikut dalam karya kami.

Kualitatif (Paradigmatik)

Informasi berfungsi sebagai sarana untuk membingkai QIT dan konsekuensi hukum secara paradigmatik. Dengan demikian, alih-alih mengukur informasi seperti dalam teori komunikasi formal (yang misalnya menyangkut jumlah informasi yang dapat ditransmisikan melalui saluran), di sini kita berfokus pada pemahaman kualitatif tentang peran suatu aktivitas atau alur kerja yang bergantung pada informasi, untuk secara memadai mengukur bagaimana risiko dan tata kelola berubah ketika komponen proses tersebut berubah dari klasik menjadi berbasis QIT.

Kuantitatif

Ukuran-ukuran berbasis teori informasi juga dapat digunakan dalam menilai dampak QIT. Karya kami hanya menguraikan penggunaan teknis ukuran informasi dalam pembelajaran ini, tetapi kami mencatat bahwa ukuran informasi seperti entropi, kompleksitas komputasi, kapasitas saluran komunikasi dan cara teknis lain untuk menilai informasi dapat dikatakan sangat berperan dalam mengidentifikasi secara tepat efek komparatif QIT dibandingkan dengan metode klasik. Ini mungkin termasuk ukuran kualitas, keandalan, dan ketahanan informasi yang diekstrak dari simulasi berbasis QIT, misalnya. Atau mungkin termasuk informasi teknis mengenai presisi dan tingkat kesalahan sensor kuantum yang pada gilirannya mungkin relevan dengan klasifikasinya untuk tujuan hukum di bawah regulasi ilmu hayati. Penggunaan informasi dalam pembelajaran ini difokuskan pada penggunaan paradigmatik daripada metodologis untuk secara konseptual membahas dampak *sui generis* dari QIT. Namun perlu dicatat bahwa metode-metode teori informasi teknis kemungkinan akan memiliki konsekuensi langsung terhadap tata kelola QIT.

Dengan demikian, misalnya, mengidentifikasi apakah dua keadaan kuantum sebenarnya identik adalah sesuatu yang signifikan di banyak penggunaan QIT tetapi juga banyak rezim tata kelola, seperti ketika berupaya memberikan jaminan mengenai ketahanan data kuantum atau komputasi kuantum yang diandalkan dalam ilmu hayati, kekayaan

intelektual, atau bidang lainnya. Membandingkan keadaan kuantum pada dasarnya adalah latihan informasional yang melibatkan ukuran, seperti batas Holevo-Helstrom, atau perbandingan distribusi operator kepadatan melalui entropi kuantum. Dan itu juga bergantung pada tomografi. Ukuran informasi ini walaupun teknis juga memiliki konsekuensi bagi rezim hukum yang bergantung pada informasi tersebut, seperti di mana klaim dapat diajukan mengenai pelanggaran kekayaan intelektual yang bergantung pada perbandingan keadaan, sistem, atau proses kuantum. Contoh lain adalah dampak atau pengaruh simulasi komputasi kuantum dapat ditempatkan dengan perbandingan dengan cara klasik saat ini (dan yang sedang muncul, seperti di bidang kecerdasan buatan) untuk melakukannya. Hal ini juga berlaku untuk aplikasi QIT lainnya. Dalam kasus-kasus yang saat ini terbatas di mana QIT meluas melampaui sekadar teknologi tambahan pemrosesan informasi ke ranah materi pokok ilmu hayati, seperti tertanam dalam perangkat medis (titik kuantum), lensa teori informasi membantu membedakan apa yang baru tentang penggunaan tersebut, bagaimana respons regulasi yang ada atau seharusnya mengkarakterisasi penggunaan QIT yang tertanam tersebut, dan pada akhirnya, rekomendasi apa, jika ada, untuk reformasi regulasi yang diinginkan mengingat tujuan para pemangku kepentingan.

Hukum dan Teori Informasi Klasik

Teori informasi dapat menjadi cara yang berguna untuk mengintegrasikan pemeriksaan yurisprudensi dengan teknologi yang muncul, dan sebagai sarana untuk menguraikan teori regulasi. Seperti yang akan kita bahas di bawah ini, jika dibingkai dalam istilah analog dengan ilmu fisika, hukum dapat ditafsirkan sebagai seperangkat prosedur, praktik, aturan, dan perilaku pemrosesan informasi klasik. Hukum memang berurusan dengan ketidakpastian dan memiliki cara-cara yang berkembang dengan baik, matang, dan berhasil dalam menyelesaikan ketidakpastian. Namun hukum tersebut berlandaskan pada asumsi bahwa ketidakpastian bersifat epistemik: hukum tersebut mungkin menilai berdasarkan keseimbangan probabilitas bahwa suatu skenario telah terjadi, tetapi hukum tersebut tidak menyatakan atau membenarkan bahwa semua atau kedua skenario tersebut benar-benar terjadi (atau bahwa objek-objek tersebut ada secara ontologis dalam keadaan superposisi misalnya). Dalam pengertian ini, hukum tersebut bergantung pada sesuatu seperti teori variabel tersembunyi tentang informasi: bahwa fenomena memiliki status ontologis yang berbeda, tetapi setiap ketidakpastian tentang apa yang terjadi atau apa suatu objek atau sifat-sifatnya, dll., bersifat epistemik. Sejauh mana fenomena kuantum secara praktis mempersoalkan asumsi-asumsi ini sebagian merupakan apa yang kita pertimbangkan dalam karya ini. Meskipun demikian, kami berpendapat bahwa kerangka kerja teoretis informasi semacam ini berguna justru karena memungkinkan perbedaan dan asumsi di balik hukum dan mekanika kuantum untuk saling terkait.

Berbagai usulan yang menghubungkan teori informasi dan pemrosesan informasi dengan tata kelola dan regulasi telah muncul dalam riset di beberapa disiplin ilmu. Seringkali penggunaan ide dan konsep teori informasi muncul dalam teori tata kelola dan regulasi melalui ekonomi dan teori permainan di mana teori informasi, di era modern, membentuk fondasi utama. Contoh usulan untuk pemeriksaan berbasis informasi tentang regulasi dan tata kelola

meliputi pemahaman proses legislatif dalam hal sistem kompleks, pemahaman dinamika tata kelola dalam hal asimetri informasi dalam ekonomi, dan bahkan penggunaan teori komunikasi dan pensinyalan klasik sebagai sarana untuk memahami bagaimana ekosistem regulasi berfungsi.

Dengan menjadikan informasi sebagai pedoman utama, kita dapat menerapkan cakupan yang luas dalam pekerjaan kita. Hal ini memungkinkan kita untuk memeriksa aplikasi yang ada dan potensial dari setiap pilar QIT komputasi kuantum, penginderaan kuantum, dan komunikasi kuantum pada aktivitas yang diatur oleh atau menjadi pokok bahasan hukum. Ini termasuk pembelajaran, desain produk, pengembangan sistem, uji klinis, komersialisasi, pengobatan, penggunaan, dan pemantauan teknologi serta bagaimana aktivitas-aktivitas ini diatur. QIT, jika diwujudkan secara maksimal, menawarkan prospek perubahan besar dalam aktivitas ekonomi dan sosial karena dampak informasinya, membuka pintu bagi teknik komputasi dan simulasi yang sebelumnya tidak tersedia karena ketidakmampuan komputasi atau kesulitan dalam memecahkan masalah. Penginderaan kuantum, di mana perangkat kuantum (seperti titik kuantum) digunakan untuk menyediakan alat penginderaan dan pengukuran beresolusi tinggi untuk perangkat dan laboratorium, sudah diimplementasikan dan digunakan dalam kegiatan ilmiah. Komunikasi kuantum, khususnya penggunaan metode kriptografi kuantum, memori kuantum, dan pensinyalan kuantum, menawarkan cara-cara baru untuk memberikan tingkat keamanan data yang lebih tinggi atas informasi sensitif, seperti bioinformatika dan data kesehatan, serta cara-cara baru untuk mengkomunikasikan informasi dengan cara yang aman dan lebih cepat, memfasilitasi kolaborasi dan inovasi dalam skala yang lebih besar.

Tata kelola teknologi sudah matang, sangat kompleks, preskriptif, dan terstruktur dengan pendekatan implisit dan eksplisit terhadap risiko yang tertanam dalam strukturnya. Hal ini juga mencakup beberapa area aktivitas ilmiah, teknologi, dan ekonomi yang paling diatur, mulai dari persyaratan ekstensif seputar pembuatan prototipe, pengujian, dan komersialisasi perangkat dan produk (seperti perangkat dan farmasi), hingga jaringan regulasi kompleks yang mengatur akuisisi, pemrosesan, dan penyebaran informasi, seperti dalam perawatan kesehatan dan uji klinis atau dalam bagaimana pasar ekonomi diatur. Sebaliknya, tata kelola QIT masih belum berkembang, dengan area tata kelola utama yang muncul adalah yang berfokus pada keamanan siber, kekayaan intelektual, dan pertimbangan penggunaan ganda. Bagaimana cara menyelaraskan hal yang saling bertentangan, sehingga teknologi kuantum yang eksperimental dan belum teruji dan tingkat risiko yang lebih tinggi yang ditimbulkannya dapat diterapkan secara bermanfaat pada aktivitas ekonomi dan ilmiah dengan manajemen risiko yang terperinci, sangat penting bagi kedua bidang tersebut. Mengatasi dilema ini mendorong pendekatan kami untuk memetakan serangkaian rezim regulasi yang akan dikenakan pada aplikasi QIT dan untuk memahami konsekuensi penggunaan QIT di bawah rezim tata kelola legislatif, regulasi, dan kebijakan yang ada. Demikian pula, seiring dengan semakin ketatnya regulasi QIT, pemahaman tentang bagaimana tata kelola tersebut seharusnya dibentuk untuk mewujudkan manfaatnya dalam konteks terapan sangatlah penting.

Taksonomi dan Ontologi Informasi

Seperti yang telah disebutkan di atas, untuk menghubungkan ekosistem QIT, aktivitas ekonomi, dan instrumen tata kelola (dari hukum, regulasi, kebijakan, dan bentuk lainnya), kami mendekati tata kelola kuantum melalui lensa pemrosesan informasi. Pemrosesan informasi adalah istilah luas yang mencakup akuisisi, manipulasi, dan pemanfaatan data, seperti misalnya penyematan langsung sensor dalam perangkat atau alat diagnostik eksternal. Ini juga mencakup penggunaan data dalam pembelajaran atau desain produk. QIT dapat ditempatkan dalam pemrosesan informasi sebagai sarana untuk memperoleh, menyimpan, atau memproses data dengan cara yang secara teknis berbeda dari teknologi klasik dan yang menghasilkan hasil baru yang tidak mungkin (atau tidak layak mengingat keterbatasan sumber daya) menggunakan teknologi klasik. Kami berfokus pada efek pemrosesan informasi dari QIT (dan konsekuensinya) untuk membedakan QIT dari peran umum mekanika kuantum di bidang aktivitas ekonomi lainnya. Semua proses fisik pada dasarnya didasarkan pada hukum mekanika kuantum, namun efek kuantum tertentu memiliki signifikansi khusus ketika digunakan dalam konteks QIT hanya dengan cara tertentu. Ini berlaku di seluruh tumpukan teknologi.

Misalnya, efek kuantum seperti penerowongan kuantum, struktur kimia, komposisi, dan evolusi, semuanya penting untuk fenomena fisik. Tetapi keterlibatan insidental proses kuantum tidak menjadikan penggunaannya sebagai teknologi itu sendiri. Untuk menjadi teknologi kuantum, setidaknya dalam kerangka kerja kami, diperlukan beberapa aspek teknik fenomena mekanika kuantum sebagai alat atau sumber daya yang terarah atau terkontrol. Partikel kuantum ada di sekitar kita dalam keadaan superposisi, tetapi baru ketika partikel tersebut menjadi subjek kontrol, penggunaan, atau penerapan, kita akan menganggapnya sebagai bentuk teknologi. Demikian pula, teknologi klasik memanfaatkan efek mekanika kuantum dalam berbagai cara seperti mesin MRI dan pemindai. Dan sementara teknologi kuantum generasi kedua yang diidentifikasi di atas dapat secara wajar dibingkai dalam istilah teori informasi, kita membedakannya dari QIT karena QIT berkaitan dengan rekayasa langsung sistem kuantum untuk memanfaatkan efek informasi kuantum seperti halnya ketika memproduksi sirkuit kuantum, perangkat penginderaan kuantum, atau perangkat teleportasi kuantum. Untuk tujuan ini, kami mengusulkan taksonomi informasi yang sederhana namun serbaguna yang berdasarkan pada itu fungsionalitas QIT (dan sistem informasi secara umum dapat didasarkan), yaitu input-proses-output tetapi dibingkai dalam hal akuisisi informasi (pengukuran), pemrosesan informasi, dan output informasi.

Input/Pengukuran Informasi

Elemen pertama dari pemrosesan informasi ini berkaitan dengan akuisisi data. Kami menganalogikan teori formal pengukuran yang dijelaskan di bawah ini. Pengukuran terjadi melalui interaksi perangkat dengan lingkungan dengan cara tertentu. Melalui proses pengukuran ini, data diperoleh. Hal ini dapat diterapkan pada perangkat fisik, seperti titik kuantum atau sensor kuantum, tetapi pada prinsipnya juga pada perangkat atau sarana yang digunakan untuk mengumpulkan bukti (proses tersebut secara efektif merupakan pengumpulan data). Kami menggunakan istilah masukan/pengukuran secara bergantian untuk mencakup kasus di mana data dimasukkan ke dalam suatu perangkat (yang pada prinsipnya

dapat diartikan dalam formalisme pengukuran), seperti ketika data dimasukkan ke dalam komputer kuantum, atau ke dalam perangkat komunikasi kuantum.

Pemrosesan Informasi

Pemrosesan informasi kemudian berkaitan dengan penggabungan kembali data atau pemrosesan fungsionalnya dengan cara tertentu yang mengubah data tersebut. Ini mungkin berupa transformasi identitas (sehingga data tetap berupa data pengukuran mentah), tetapi juga dapat melibatkan penyusunan statistik dari data. Komputer kuantum menerima data masukan dan memprosesnya sesuai dengan parameter komputasi (misalnya, Hamiltonian atau sirkuit kuantum). Sensor kuantum bahkan dapat mengubah data sinyal mentah yang diterimanya menjadi bentuk tertentu. Perangkat pengukuran kuantum berkaitan dengan, misalnya, eigenstate dari perangkat pengukuran. Dalam konteks hukum, pemrosesan informasi dapat secara abstrak tetapi bermanfaat dibingkai dalam hal penalaran atau cara lain di mana data masukan atau bukti diubah sebagai bagian dari prosedur informasi yang membentuk praktik kelembagaan hukum.

Keluaran Informasi

Ini berkaitan dengan keluaran dari suatu perangkat atau proses, sehingga berkaitan dengan informasi dari perangkat ke lingkungan. Hasil dari prosedur informasi klasik seringkali berbeda dari hasil padanannya dalam sistem kuantum, di mana hasilnya tampak berupa statistik pengukuran dan bukan informasi berulang yang diekstrak dari suatu sistem yang tidak terganggu oleh tindakan pengukuran itu sendiri.

Tingkat Abstraksi

Cara kita mendeskripsikan pemrosesan informasi itu penting. Tingkat abstraksi dan wacana yang digunakan untuk mendeskripsikan pemrosesan informasi memiliki konsekuensi yurisprudensi yang penting. Cara komputasi atau algoritma dideskripsikan merupakan bagian penting dari tata kelola komputasi secara lebih luas, relevan dengan pertanyaan tentang paten dalam kekayaan intelektual, atau spesifikasi teknis untuk pengungkapan produk teknologi. Misalnya, panduan Kecerdasan Buatan dan Pembelajaran Mesin dalam Perangkat Lunak sebagai Perangkat Medis dari FDA memberikan saran tentang bagaimana produsen yang menggunakan kecerdasan buatan atau pembelajaran mesin (dalam konteks perangkat medis) mendeskripsikan perubahan apa yang terjadi melalui protokol pembelajaran komputasi dan bagaimana algoritma belajar sambil tetap aman dan efektif. Mengubah sifat komputasi untuk memasukkan algoritma komputasi kuantum atau teknik komputasi kuantum akan berdampak pada bagaimana algoritma dideskripsikan dan dirinci untuk tujuan proses regulasi tersebut. Misalnya, sudah umum untuk mendeskripsikan algoritma kuantum menggunakan formalisme sirkuit kuantum yang selaras dengan ilmu komputasi, tetapi juga formalisme Hamiltonian yang lebih umum dalam fisika. Sejauh mana pilihan representasi QIT tertentu akan menimbulkan konsekuensi signifikan atau memerlukan respons baru dari perspektif regulasi, atau apakah rezim yang ada memadai untuk mengelola QIT dalam perangkat medis atau sektor teregulasi lainnya, adalah pertanyaan terbuka. Tetapi penting untuk diingat, karena detail kuantumnya sangat penting, terutama ketika menyangkut pembedaan yang tepat tentang apa yang *sui generis* atau berbeda dari QIT dan efeknya dibandingkan dengan padanannya yang klasik.

2.9 PRINSIP INFORMASI KUANTUM

Menjawab pertanyaan *sui generis* tentang tata kelola kuantum membutuhkan pemahaman tentang dampak QIT. Dampak ini dapat dipertimbangkan semata-mata sehubungan dengan sifat kuantum QIT, misalnya superposisi dan keterikatan, sifat ontologis yang berbeda dari sistem kuantum. Atau dampak QIT dapat dipertimbangkan secara tidak langsung, dalam hal bagaimana penggunaan QIT memengaruhi fungsi komponen lain dalam suatu proses atau alur kerja. Dalam setiap kasus, idealnya kita dapat mengukur dampak QIT dari perspektif risiko dengan membandingkannya dengan proses yang setara tanpa QIT, atau menemukan sesuatu yang analog dengan koefisien variasinya yang menunjukkan bagaimana beberapa output tertentu bervariasi sebagai ukuran korelasi dengan penggunaan QIT itu sendiri. Melakukannya secara kuantitatif tentu saja sulit. Namun demikian, kita masih dapat menilai dampak QIT menggunakan taksonomi QIT tipikal yang membagi QIT menjadi tiga divisi utamanya yaitu komputasi kuantum, komunikasi kuantum, dan penginderaan kuantum. Kita akan mempertimbangkan setiap aplikasi dan dampaknya dari perspektif hukum secara lebih rinci di bawah ini.

Namun, untuk memahami dampak-dampak ini, sangat penting untuk memiliki pemahaman yang baik tentang sifat mekanika kuantum dari QIT dan bagaimana karakteristik kuantumnya menimbulkan dampak tersebut. Karakteristik kuantum dari semua QIT berasal dari ketergantungan dan pemanfaatan sifat-sifat sistem mekanika kuantum. Pemantauan komprehensif tentang mekanika kuantum dan pemrosesan informasi kuantum dapat ditemukan di seluruh riset, termasuk riset tentang tata kelola kuantum. Kami menguraikan secara singkat konsep-konsep kunci di balik pemrosesan informasi kuantum di bawah ini sebelum merangkum subsektor utama QIT, yaitu komputasi kuantum, komunikasi kuantum, dan penginderaan kuantum. Kami bertujuan untuk mencapai keseimbangan antara kekhususan teknis dan cakupan yang luas.

Mekanika Kuantum

Komputasi kuantum, penginderaan kuantum, dan komunikasi kuantum adalah tiga disiplin ilmu informasi kuantum yang berbeda namun saling tumpang tindih. Gagasan pemersatu di balik ketiganya adalah studi tentang sistem pemrosesan informasi tertentu, baik dalam bentuk komputasi, penyimpanan data, pensinyalan, atau deteksi, yang memenuhi postulat mekanika kuantum. Pemrosesan informasi kuantum juga berkaitan dengan abstraksi sistem yang dibangun dari sistem kuantum komposit, seperti qubit logis, di mana representasi abstrak (seperti representasi keadaan qubit logis) mengikuti kuantum sebagai representasi yang berbeda dari representasi klasik. Formalisme abstrak pemrosesan informasi kuantum adalah sintesis elemen mekanika kuantum, teori formal komputasi (model sirkuit), dan teori informasi (seperti konsep saluran, register, dan sebagainya) untuk detail lebih lanjut). Komputasi kuantum, penginderaan kuantum, dan komunikasi kuantum adalah tiga divisi yang saling terkait dari informasi kuantum. Masing-masing disatukan oleh fakta bahwa sifat dan dinamika sistem yang bersangkutan, baik komputasional, mekanis, atau komunikatif, memenuhi postulat mekanika kuantum. Pemrosesan informasi kuantum mewakili cara

penalaran abstrak tentang sistem tersebut melalui aksioma dan teorema yang pada gilirannya memenuhi postulat mekanika kuantum. Dengan cara ini, pemrosesan informasi kuantum sebagai suatu disiplin ilmu memanfaatkan fisika, teori komputasi formal, dan teori informasi. Karakteristik utama yang mendasari semua teknologi informasi kuantum yang akan kita nilai di bawah ini, yang membedakan teknologi tersebut dari analog klasiknya, adalah bahwa teknologi tersebut memanfaatkan sifat-sifat unik mekanika kuantum. Untuk mempermudah diskusi dan pemeriksaan komparatif kita di bawah ini, kita merangkum beberapa prinsip utama pemrosesan informasi kuantum di bawah ini, menyederhanakan beberapa bagian untuk keringkasan dan kejelasan.

Keadaan Kuantum

Dalam teori kuantum, informasi dikodekan dalam keadaan kuantum, yang dilambangkan dalam notasi Dirac sebagai $ket\ |\psi\rangle$ yang mewakili abstraksi teori informasi dari fungsi gelombang kuantum. Keadaan dalam abstraksi dibangun dari kosakata atau alfabet yang mewakili konfigurasi berbeda di mana suatu sistem dapat berada. Keadaan mekanika kuantum direpresentasikan (biasanya) sebagai kuantisasi medan, di mana sistem kuantum menunjukkan keadaan energi diskrit (terkuantisasi) daripada kontinum keadaan (namun, nilai kontinu itu sendiri dapat dikodekan dalam amplitudo probabilitas yang diambil dari medan kompleks). Kuantisasi ini (pertama kali diperhatikan oleh para pelopor awal dalam fisika seperti Planck dan ditunjukkan oleh Einstein) memungkinkan sistem kuantum untuk merepresentasikan informasi dengan cara digital (memberikan batasan diskrit antara keadaan yang bernilai 0 atau 1).

Hal ini pada gilirannya membuka ruang komputasi digital. Keadaan kuantum direpresentasikan sebagai elemen dari ruang vektor matematika (Hilbert). Karakteristik pembeda utama keadaan kuantum dibandingkan dengan keadaan klasik adalah linearitas: jika $|0\rangle$ dan $|1\rangle$ adalah keadaan kuantum (basis), maka superposisi liniernya juga merupakan keadaan kuantum, yaitu $|\psi\rangle = a|0\rangle + b|1\rangle$, di mana $a, b \in \mathbb{C}$ adalah amplitudo dari kemungkinan keadaan basis yang mungkin dimiliki oleh keadaan kuantum tersebut. Linearitas ini berarti bahwa setiap kombinasi linier dari keadaan basis (yang dinormalisasi dengan tepat) juga merupakan keadaan kuantum, yang mencerminkan fenomena superposisi kuantum (di mana suatu keadaan berada dalam lebih dari satu keadaan dengan probabilitas tertentu saat pengukuran). Jika keadaan kuantum bersifat dua dimensi, maka disebut *qubit* (singkatan dari 'bit kuantum'). Sistem kuantum juga dapat berupa sistem komposit yang terdiri dari beberapa qubit, misalnya $|\psi\rangle_a, |\psi\rangle_b$. Ketika suatu sistem kuantum terdiri dari keadaan-keadaan yang terpisah, sistem tersebut dapat direpresentasikan sebagai hasil perkalian tensor $|\psi\rangle = |\psi\rangle_a \otimes |\psi\rangle_b (\text{a product state})$. Jika tidak, keadaan kuantum tersebut dapat dikatakan saling terkait sedemikian rupa sehingga tidak dapat difaktorkan menjadi (atau direpresentasikan secara terpisah sebagai) suatu keadaan hasil perkalian. Keadaan saling terkait merupakan fitur unik dari sistem mekanika kuantum dan merupakan sumber daya utama untuk QIT. Contohnya termasuk keadaan Bell dua-qubit $|\psi\rangle = (|00\rangle - |11\rangle)/\sqrt{2}$ di mana, seperti yang dapat dilihat, hasil pengukuran untuk setiap qubit berkorelasi (mengukur $|0\rangle$ pada qubit pertama berarti dipastikan bahwa qubit kedua juga berada dalam keadaan $|0\rangle$, dan demikian pula untuk $|1\rangle$).

Keadaan kuantum sering direpresentasikan dalam formalisme matriks densitas ρ dan dapat berupa keadaan murni (merepresentasikan informasi maksimal tentang keadaan tersebut) atau keadaan campuran (merepresentasikan kumpulan keadaan murni yang mencerminkan ketidakpastian epistemik tentang keadaan yang dimaksud). Matriks densitas analog dengan representasi operator dari distribusi probabilitas atas keadaan dan merupakan cara umum untuk mengekspresikan algoritma kuantum.

Pengukuran dan Pengkodean

Informasi dimasukkan ke dalam keadaan kuantum melalui protokol pengkodean (seperti melalui pengkodean dalam keadaan basis, fase relatif, atau bentuk lainnya). Informasi diekstrak dari sistem kuantum melalui pengukuran kuantum, di mana alat ukur berinteraksi dengan sistem. Pengukuran sistem kuantum terjadi melalui interaksi fisik sistem kuantum dengan alat ukur (yang berbeda dari sistem itu sendiri), kadang-kadang disebut eksperimen. Hasil pengukuran menghasilkan serangkaian data klasik yang mengikuti distribusi tertentu dari mana statistik dapat diambil, yang disebut statistik pengukuran. Secara matematis, proses pengukuran diwakili oleh operator Hermitian yang bekerja pada keadaan kuantum, yang nilai eigen sebenarnya adalah hasil pengukuran dengan probabilitas yang diberikan oleh kuadrat amplitudo setiap fase/koefisien. Untuk keadaan kuantum $|\psi\rangle = a|0\rangle + b|1\rangle$ (diukur dalam basis yang sesuai), probabilitas mengukur $|0\rangle$ adalah $|a|^2$ dan $|1\rangle$ adalah $|b|^2$ (aturan Born). Sekumpulan operator pengukuran yang sepenuhnya mengkarakterisasi hasil suatu eksperimen (dan disebut sebagai ukuran bernilai operator positif (POVM)). Pengukuran bersifat lengkap karena POVM ini menentukan sekumpulan hasil lengkap dari sistem. Pengukuran mereduksi keadaan kuantum setelah pengukuran menjadi eigenstate yang dinormalisasi dari operator pengukuran (misalnya $|0\rangle$ atau $|1\rangle$). Untuk memperoleh data tentang keadaan kuantum, seseorang harus melakukan pengukuran berulang pada keadaan kuantum yang disiapkan secara identik yang menghasilkan distribusi hasil pengukuran (statistik pengukuran). Detail tentang keadaan kuantum atau evolusinya kemudian direkonstruksi (menggunakan prosedur dari tomografi misalnya) dari kumpulan statistik pengukuran klasik ini.

Evolusi

Evolusi sistem kuantum tertutup (perubahan keadaannya) diatur oleh persamaan Schrödinger, persamaan diferensial orde pertama yang solusinya adalah fungsi gelombang yang mewakili keadaan kuantum dan yang mengkodekan simetri tertentu (seperti simetri unitari) dan sifat konservasi (seperti konservasi probabilitas atau ukuran) yang diperlukan agar karakteristik kuantum tetap ada. Sistem kuantum berinteraksi dengan lingkungan (memang harus demikian agar dapat diukur) dan hal ini memengaruhi keadaan sistem kuantum, mereduksi keadaan tersebut menjadi keadaan klasik atau tensor. Ini adalah perbedaan mendasar dengan sistem klasik di mana idealnya pengukuran tidak memengaruhi keadaan sistem dengan cara ini. Lingkungan dapat mencakup derau atau interaksi dengan sistem fisik tertentu lainnya. Formalisme di mana evolusi waktu sistem kuantum diekspresikan dapat mengambil berbagai bentuk (Heisenberg atau Schrodinger). Secara matematis, operator yang disebut Hamiltonian menggambarkan evolusi sistem kuantum. Hamiltonian H, sebagai

generator translasi waktu, adalah operator Hermitian yang biasanya dinyatakan dalam persamaan Schrodinger sebagai $\frac{d|\psi\rangle}{dt} = -iH|\psi\rangle$ di mana i adalah satuan imajiner dan mewakili perubahan $\frac{d|\psi\rangle}{dt}$ (infinitesimal) dalam keadaan kuantum seiring waktu. Hamiltonian merupakan bagian penting dari model sirkuit komputasi kuantum dan kontrol kuantum, yang memungkinkan spesifikasi abstrak dari perkembangan komputasi kuantum.

Kontrol

Penggunaan QIT bergantung seperti halnya teknologi lainnya pada kemampuan untuk mengendalikan sistem secara memadai untuk tujuan yang dimaksudkan. Kontrol sistem kuantum adalah subjek dari bidang kontrol kuantum. Jenis kontrol fisik yang dapat diterapkan pada sistem kuantum untuk mengarahkan evolusinya bergantung pada realisasi fisik sistem88 (misalnya, ion terperangkap, superkonduktor, dll.). Secara fisik, kontrol ini sering kali berbentuk pulsa elektromagnetik atau tegangan yang diterapkan untuk mengembangkan sistem dengan cara tertentu atau bahkan titik kuantum (yang juga, seperti yang akan kita bahas panjang lebar di bawah ini, merupakan teknologi utama dalam perangkat penginderaan kuantum saat ini). Secara matematis, kontrol ini dijelaskan sebagai koefisien fungsional dari suku-suku (generator) dalam Hamiltonian. Interaksi sistem kuantum dengan lingkungan, baik itu kebisingan atau peralatan pengukuran, juga diekspresikan melalui suku-suku tambahan dalam Hamiltonian.

Sistem Kuantum Terbuka dan Tertutup serta Kebisingan

Sistem kuantum dikarakteristikkan sebagai tertutup atau terbuka. Sistem kuantum tertutup adalah abstraksi ideal di mana evolusi keadaan kuantum diatur oleh persamaan Schrödinger sedemikian rupa sehingga sifat-sifat kuantum dari keadaan tersebut, seperti superposisi atau keterikatan, tetap terjaga. Lebih formalnya, sistem kuantum tertutup yang diidealkan umumnya mempertahankan koherensi kuantum, fitur penting dari informasi kuantum. Sistem kuantum terbuka adalah cara untuk memodelkan bagaimana sistem kuantum berinteraksi dengan lingkungannya. Lingkungan ini dapat bersifat klasik atau kuantum. Sistem kuantum berinteraksi dengan lingkungan (seperti alat ukur) yang dapat bersifat kuantum atau klasik dan yang dapat direpresentasikan sebagai Hamiltoniannya sendiri yang digabungkan dengan Hamiltonian sistem kuantum. Hamiltonian biasanya diuraikan menjadi Hamiltonian sistem H_s (menggambarkan evolusi sistem kuantum), Hamiltonian lingkungan H_E (menggambarkan evolusi lingkungan), dan Hamiltonian interaksi (menggambarkan bagaimana sistem dan lingkungan berinteraksi). Interaksi antara lingkungan dan sistem kuantum memengaruhi keadaan sistem kuantum. Hal ini dapat terjadi melalui lingkungan yang menyebabkan keadaan kuantum mengalami dekoherensi, atau melalui berbagai jenis derau seperti derau T_1 atau T_2. Pengukuran juga merupakan bentuk interaksi yang dapat dimodelkan dengan cara ini. Efek lingkungan seperti derau menyebabkan dekoherensi dan memengaruhi evolusi keadaan kuantum. Formalisme matematika yang banyak digunakan untuk merepresentasikan sistem kuantum terbuka, dan efek derau, adalah persamaan master stokastik yang memodelkan efek, misalnya, derau lingkungan pada sistem kuantum. Sistem kuantum sangat sensitif terhadap derau dan karenanya memerlukan koreksi kesalahan (seperti dalam bentuk kode koreksi kesalahan) untuk mencapai toleransi kesalahan

yang cukup, seperti komputasi kuantum toleran kesalahan. Representasi sirkuit kuantum dari derau juga umum dalam riset koreksi kesalahan, seperti dalam formalisme kode penstabil dan kode permukaan.

Fitur Unik Sistem Kuantum

Sifat-sifat fundamental sistem mekanika kuantum di atas membentuk dasar bagi kemampuan unik komputasi kuantum, komunikasi kuantum, dan penginderaan kuantum. Kita akan mengeksplorasi masing-masing secara lebih rinci di bawah ini dan pada bagian-bagian selanjutnya akan menghubungkan fitur-fitur unik tersebut dengan kemampuan yang relevan dengan pemeriksaan hukum. Postulat teori kuantum yang tercantum di atas juga menimbulkan sejumlah konsekuensi penting yang membedakan QIT dari pemrosesan informasi klasik. Hal ini mencakup (i) teorema tidak ada kloning (bahwa keadaan kuantum tidak dapat disalin), (ii) persyaratan mendasar untuk koreksi kesalahan kuantum agar QIT berfungsi (karena sensitivitas sistem kuantum) dengan cara yang toleran terhadap kesalahan, (iii) protokol pengukuran (membutuhkan persiapan keadaan yang identik atau beberapa salinan yang dihasilkan oleh proses kuantum yang identik untuk menghasilkan statistik pengukuran daripada memiliki satu keadaan kuantum yang diukur berulang kali), (iv) fenomena ontologis kuantum, yang termanifestasi dalam kontekstualitas (urutan pengukuran yang menimbulkan statistik yang berbeda), prinsip ketidakpastian dan aksi non-lokal dan (v) bahwa keterikatan adalah sumber daya. Meskipun kita tidak berfokus secara mendalam pada konsekuensi ini, keduanya sangat mendalam dan secara fundamental membedakan fisika kuantum dari rekan klasiknya.

Tidak jarang juga membandingkan pemrosesan informasi klasik dan kuantum dari perspektif teori informasi, termasuk perbandingan antara model komputasi klasik dan kuantum, hubungan antara teori informasi klasik dan rekan kuantumnya. Kami mengarahkan pembaca ke diskusi teknis dalam riset untuk detail lebih lanjut. Selain itu, sensitivitas ekstrem sistem kuantum dan fakta bahwa interaksi dengan sistem kuantum melalui pengukuran dapat secara efektif menghilangkan atau menghancurkan sifat kuantumnya berarti bahwa verifikasi, audit, dan kontrol sistem tersebut berbeda dari analog klasik, faktor yang relevan dengan usulan untuk kontrol teknis sistem tersebut dan rezim tata kelola (seperti standar dan protokol hukum internasional).

Perangkat kuantum jangka pendek masih rentan terhadap kesalahan, yang memengaruhi akurasi komputasinya. Mengembangkan arsitektur yang tahan terhadap noise, baik melalui kode koreksi kesalahan atau fitur perangkat keras, sangat penting untuk mencapai komputasi kuantum toleran kesalahan yang terukur yang pada gilirannya diperlukan untuk mewujudkan manfaatnya. Memenuhi ambang batas tersebut juga penting untuk memenuhi persyaratan jaminan dan integritas data yang mendasar dalam aplikasi QIT. Data yang dikodekan dalam komputer kuantum dapat berada dalam keadaan kuantum, pada akhirnya data dimasukkan dan dikeluarkan dari sistem kuantum melalui cara klasik seperti melalui pengkodean data klasik dalam keadaan kuantum atau mengekstrak data dari keadaan kuantum melalui pengukuran yang menimbulkan distribusi statistik pengukuran klasik. Pengkodean informasi dalam keadaan kuantum adalah proses yang kompleks, membutuhkan

teknik persiapan keadaan tingkat lanjut dan metode pengkodean data yang mungkin beroperasi pada skala efisiensi yang berbeda. Selain itu, seringkali terdapat overhead qubit fisik yang cukup besar yang dibutuhkan untuk qubit logis (yang mewakili aspek pemrosesan data) dengan kemajuan yang dibutuhkan baik dalam desain algoritma maupun rekayasa perangkat keras untuk mengurangi penggunaan qubit dan meningkatkan efisiensi persiapan keadaan kuantum. Sebelum merangkum sejumlah fitur teknis dari masing-masing tiga sektor komputasi kuantum, komunikasi kuantum, dan penginderaan kuantum yang relevan dengan disiplin ilmu hukum yang diidentifikasi di atas, kami akan memeriksa topik penting ontologi kuantum dan dampaknya terhadap yurisprudensi hukum.

2.10 ONTOLOGI KUANTUM DAN DAMPAK HUKUM

Non-lokalitas dan Teorema Bell

Di luar dampak teknis, sifat-sifat sistem kuantum yang disebutkan di atas memiliki dampak yang sangat mendalam tentang bagaimana objek kuantum dikarakterisasi secara ontologis. Hal ini terutama berlaku untuk sifat-sifat kuantum superposisi dan keterikatan. Salah satu hasil paling mendalam dari fisika abad ke-20 adalah hasil teoritis dan yang telah divalidasi secara empiris bahwa sistem kuantum secara ontologis pada dasarnya berbeda dari objek yang dijelaskan oleh fisika klasik. Mungkin perdebatan utama dalam fisika kuantum sejak awal adalah apakah statistik pengukuran yang muncul dari fenomena kuantum terutama hasil yang berlawanan dengan intuisi mengenai statistik pengukuran yang diambil dari pengukuran berulang partikel yang disiapkan secara identik hanyalah artefak ketidaktepatan dalam pengukuran yang berbeda dari sesuatu yang secara ontologis berbeda tentang sistem kuantum.

Pertanyaan ini terkenal diperdebatkan oleh para ahli teori fundamental terkemuka dalam teori kuantum, termasuk Einstein. Inti dari perdebatan tersebut adalah apakah teori mekanika kuantum merupakan teori variabel tersembunyi bahwa ketidakpastian statistik pengukuran (atau varians) mencerminkan ketidakpastian epistemik daripada ketidakpastian ontik; dan fakta yang tampak bahwa partikel identik tampaknya memiliki sifat-sifat, seperti spin, momentum, posisi, atau atribut lain yang berbeda ketika diukur. Di satu sisi perdebatan, yang dipimpin oleh Einstein, terdapat para pendukung variabel tersembunyi yang terkenal dengan pernyataan bahwa Tuhan tidak bermain dadu dengan alam semesta, sebuah ungkapan sehari-hari yang merujuk pada fakta bahwa ketidakpastian bersifat epistemik, bukan sifat inheren alam semesta pada skala kuantum. Di sisi lain, terdapat para teoretikus yang berpendapat bahwa statistik pengukuran dari teori kuantum yang baru muncul mencerminkan ketidakpastian mendasar di jantung realitas itu sendiri.

Perdebatan tentang validitas teori variabel tersembunyi terus berlanjut dan mereda selama bertahun-tahun, hingga serangkaian artikel penting oleh fisikawan John Bell. Dalam karya-karyanya yang mempertimbangkan perdebatan yang ada saat itu, Bell, dengan memperluas hasil dari Kochen dan Specker, menunjukkan bahwa teori variabel tersembunyi lokal yang memenuhi batasan tertentu (realisme lokal dan independensi statistik) sebagai suatu kelas tidak konsisten dengan statistik pengukuran dari partikel kuantum yang saling

terkait. Bell menunjukkan bahwa teori variabel tersembunyi lokal apa pun tidak dapat mereproduksi korelasi yang diprediksi dan diamati secara eksperimental dalam keadaan kuantum yang saling terkait. Hasil ini menyoroti konflik antara realisme lokal dan korelasi kuantum. Konsekuensi dari teorema Bell terkadang digambarkan sebagai pilihan Faustian tentang apakah akan menghindari realisme lokal, atau mengakui bahwa sistem kuantum menunjukkan dan bahwa teori mekanika kuantum pada dasarnya bersifat non-lokal. Pendekatan variabel tersembunyi biasanya mengasumsikan nilai-nilai realisme yang pasti, tetapi kemudian harus memungkinkan pengaruh non-lokal atau mengabaikan asumsi lain untuk mencocokkan prediksi kuantum. Konsekuensi dari hasil ini tidak hanya terbatas pada gagasan esoteris tentang lokalitas (yang memiliki makna teknis yang tepat), tetapi juga pada gagasan mendasar bahwa atribut-atribut tertentu dari sistem kuantum bersifat berbeda, tetap, dan tepat. Meskipun paradoks kucing Schrödinger lebih berfokus pada superposisi dan masalah pengukuran dalam satu sistem, hal itu juga menggarisbawahi bahwa pengukuran kuantum dapat secara fundamental mengubah sifat-sifat suatu sistem dengan cara yang berbeda dari fisika klasik.

Karakterisasi Epistemik dan Ontologis dari Keadaan Kuantum

Dalam perlakuan ontologis modern, hasil tersebut sering kali dibingkai dalam hal perbedaan antara model ψ-ontik (di mana keadaan kuantum merupakan bagian dari realitas) dan model ψ-epistemik (di mana keadaan kuantum secara epistemik mengkodekan informasi tentang keadaan ontik). Keadaan kuantum dibatasi menjadi keadaan murni dan representasi keadaan campuran dari sistem kuantum. Ketidakpastian epistemik tentang keadaan ontik yang mendasari suatu sistem ditangkap oleh operator kerapatan keadaan campuran, sementara keadaan murni mencerminkan informasi ontologis maksimal tentang keadaan tersebut. Operator kerapatan dapat dibangun dari hasil perkalian luar keadaan $|\psi\rangle$ sedemikian rupa sehingga $\rho = |\psi\rangle\langle\psi|$. Untuk memberikan contoh apa artinya ini, pertimbangkan keadaan energi partikel kuantum, pertimbangkan keadaan kuantum ρ' yang ditentukan sebagai:

$$\rho' = \frac{|00| + |11|}{2}$$

Keadaan ini tidak dapat diperoleh sebagai hasil perkalian luar dari satu keadaan tunggal $|\psi$, oleh karena itu keadaan ini mewakili campuran keadaan, dalam hal ini representasi operator kerapatan keadaan campuran maksimal (hanya dengan entri diagonal) yang menunjukkan bahwa partikel berada dalam keadaan basis (seperti energi) $|0\rangle$ dengan probabilitas epistemik ½ dan secara ekuivalen untuk keadaan $|1\rangle$. Untuk setiap pengukuran proyektif dua hasil (basis ortonormal apa pun), hasilnya adalah 50–50. Oleh karena itu, tidak ada basis pengukuran yang menghasilkan hasil tertentu, artinya ketidakpastian tidak dapat direduksi dengan perubahan basis. Sebaliknya, keadaan:

$$\rho = \frac{1}{2}(|00| + |11| + |01| + |1\rangle\langle 0|)$$

berbeda dari ρ' karena adanya suku-suku di luar diagonal $|0\rangle\ \langle 1|$ dan $|1\rangle\ \langle 0|$ yang mencerminkan koherensi kuantum. Ini mewakili hasil perkalian luar dari keadaan $|\psi\rangle = \frac{1}{\sqrt{2}}(|110\rangle + |111\rangle)$. Dalam keadaan campuran maksimal, tidak ada pilihan basis pengukuran yang menghasilkan hasil yang pasti. Sebaliknya, dalam keadaan superposisi murni, seseorang dapat memilih basis (yaitu basis $|+\rangle$, $|-\rangle$) yang menghasilkan hasil pengukuran yang pasti untuk observabel tersebut, meskipun observabel non-komutatif lainnya akan tetap tidak pasti. Meskipun merupakan contoh yang disederhanakan, kami menggunakannya untuk mengilustrasikan dampak ontologis dari QIT.

Dampak ini muncul dari ontologi unik sistem kuantum yang telah disebutkan sebelumnya sebagaimana ditetapkan oleh Teorema Bell, teori keterikatan, dan hasil eksperimen. Dengan dampak ontologis, kami mengadopsi pendekatan yurisprudensi untuk mempertimbangkan jenis ontologi yang diadopsi oleh hukum. Dalam filsafat, ontologi secara tradisional merupakan deskripsi atau pernyataan tentang apa adanya, tentang keberadaan, dan hubungan antar keberadaan. Dalam ilmu komputasi, ontologi memiliki makna yang terkait tetapi spesifik dalam hal taksonomi, kelas, dan hubungan yang ada di antara objek, dan merupakan pusat untuk membangun IDE pemrograman, basis data, dan interoperabilitas fungsional sistem terdistribusi.

Identifikasi QIT

Salah satu ciri khas sistem kuantum yang membedakannya dari sistem klasik terletak pada bagaimana sistem tersebut diidentifikasi dan diindividualisasikan. Secara klasik, objek biasanya diamati melalui pengukuran yang menentukan sifat-sifatnya. Pengukuran memungkinkan kita untuk membentuk representasi dari objek tersebut. Objek kuantum juga dibangun melalui statistik pengukuran. Namun, berbeda dengan kasus klasik di mana objek dianggap tetap dalam keadaannya dan informasi tentangnya diperoleh melalui pengukuran dengan cara yang tidak secara fundamental mengubah objek tersebut, pengukuran kuantum berbeda. Semua pengukuran dengan cara tertentu mengganggu sistem melalui penerapan gaya, tetapi pengukuran kuantum memiliki karakteristik tambahan di mana pengukuran pada dasarnya meruntuhkan keadaan kuantum menjadi keadaan klasik (interpretasi 'keruntuhan fungsi gelombang' Kopenhagen yang dibahas di atas). Dalam sistem multi-qubit, seluruh keadaan kuantum mungkin tetap ada tetapi qubit yang diukur didekoherensikan menjadi keadaan klasik. Ini terkadang digambarkan sebagai pengukuran penghancuran. Dan meskipun ada formalisme mengenai pengukuran lemah atau yang disebut pengukuran non-demolisi, pada kenyataannya, setelah pengukuran, keadaan kuantum itu sendiri runtuh, tidak lagi ada sebagai sistem kuantum (kecuali jika dipengaruhi oleh operator kuantum untuk membuatnya kembali ke keadaan kuantum, misalnya gerbang Hadamard).

Ini berarti bahwa sementara untuk objek klasik, pengukuran berulang menyiratkan bahwa objek yang sama diukur berulang kali, untuk sistem kuantum, ini tidak demikian. Kita tidak dapat mengukur ulang informasi kuantum yang sama dari qubit yang sama. Sebaliknya, informasi tentang sistem kuantum bergantung pada pembuatan banyak salinan identik dari sistem kuantum tersebut (melalui prosedur persiapan keadaan yang identik). Kita tidak bergantung pada satu sistem kuantum untuk memperoleh informasi seperti yang diasumsikan

oleh ontologi klasik yang mirip dengan identitas numerik ketika menentukan dan mengindividualkan objek. Sebaliknya, kita pada dasarnya bergantung pada keberadaan banyak salinan identik dari keadaan kuantum yang pengukurannya menghasilkan data sampel yang darinya statistik (statistik pengukuran) dihitung. Dan dari statistik pengukuran ini, representasi keadaan kuantum dalam formalisme yang dipilih kemudian diperoleh, seperti melalui tomografi keadaan kuantum atau proses. Apa yang diprediksi dari keadaan kuantum atau sistem kuantum kemudian bergantung pada statistik pengukuran ini. Ini tidak berarti bahwa semua sifat sistem kuantum tunduk pada ketidakpastian yang tidak dapat direduksi. Operator-operator itulah yang tidak saling komutatif. Misalnya, massa elektron adalah parameter dalam teori kuantum, sedangkan posisi dan momentum bukan.

Konsekuensi Ontologi Kuantum

Hukum bergantung pada konsep ontologis klasik dalam beberapa cara. Isu-isu konseptual yang luas ini relevan dengan berbagai tingkat asumsi yang menjadi dasar banyak prinsip hukum dan banyak penalaran. Kami akan menguraikannya secara singkat di sini.

Kausalitas

Mekanika kuantum menantang asumsi klasik tentang kausalitas linier dan berurutan waktu dengan mengizinkan korelasi, seperti yang diamati dalam keadaan saling terkait, yang tampaknya melampaui struktur kausal lokal. Pada tingkat teknis, teorema Bell menunjukkan bahwa tidak ada teori variabel tersembunyi lokal yang dapat mereproduksi prediksi statistik sistem kuantum saling terkait, yang menyiratkan bahwa hasil pengukuran dapat menunjukkan korelasi yang lebih kuat daripada korelasi klasik. Non-lokalitas ini tidak memungkinkan pensinyalan lebih cepat dari cahaya tetapi mengganggu pandangan klasik tentang kausalitas karena hasil yang diukur pada satu partikel saling terkait dapat secara instan berkorelasi dengan hasil pada partikel lain yang terpisah secara spasial. Akibatnya, dalam protokol informasi kuantum (seperti teleportasi kuantum), hubungan kausal menjadi lebih bernuansa, membutuhkan kerangka kerja kausalitas kuantum tingkat lanjut (misalnya, matriks proses dalam pemodelan kausal kuantum) untuk menangkap bagaimana operasi pada satu node dapat memengaruhi evolusi keadaan pada node lain tanpa melanggar batasan relativistik.

Keterpastian dan Verifikasi

Keterpastian dan verifikasi informasi dalam konteks kuantum diperumit oleh superposisi dan postulat pengukuran. Tidak seperti sistem klasik, yang dapat diperiksa secara bebas tanpa mengubah keadaannya secara fundamental, pengukuran kuantum meruntuhkan sistem menjadi salah satu eigenstate yang terkait dengan besaran yang diukur. Ini berarti bahwa informasi tertentu tentang keadaan kuantum (misalnya, hubungan fase dalam superposisi) secara inheren hilang saat pengukuran, membatasi sejauh mana "konfigurasi sebenarnya" suatu keadaan dapat dipastikan sepenuhnya. Teknik seperti tomografi keadaan kuantum mengatasi tantangan ini dengan mengumpulkan statistik dari beberapa keadaan kuantum identik, namun bahkan metode ini menghasilkan perkiraan yang tunduk pada kesalahan pengambilan sampel, kebisingan, dan kendala sumber daya. Akibatnya, verifikasi dalam sistem kuantum bersifat probabilistik dan parsial, bergantung pada protokol pengukuran dan skema koreksi kesalahan yang dirancang dengan cermat.

Reproduksibilitas

Reproduksibilitas dalam eksperimen kuantum menghadapi hambatan teknis unik karena teorema tanpa kloning. Secara klasik, reproduksibilitas ilmiah sering kali mengasumsikan kemampuan untuk menduplikasi sampel dan menjalankan kembali pengujian dalam kondisi yang identik. Dalam mekanika kuantum, setiap upaya untuk mengukur atau menduplikasi suatu keadaan pasti akan mengganggunya. Para peneliti bergantung pada persiapan beberapa keadaan yang diinisialisasi secara identik bukan mengukur keadaan yang sama berulang kali untuk mengumpulkan hasil statistik yang dibutuhkan untuk verifikasi. Kode koreksi kesalahan kuantum (misalnya, kode permukaan) dapat mengurangi dekoherensi dan sumber kebisingan lainnya, tetapi reproduksibilitas sempurna tetap sulit dicapai, dengan setiap eksperimen menghasilkan distribusi hasil daripada pembacaan definitif dari realitas mendasar yang stabil.

Interpretasi

Interpretasi keadaan dan proses kuantum secara teknis dibatasi oleh representasi matematisnya (misalnya, vektor keadaan dalam ruang Hilbert atau matriks densitas). Sementara sistem klasik memungkinkan interpretasi langsung, seringkali intuitif seperti melacak posisi atau lintasan yang pasti sistem kuantum mengkodekan informasi dalam amplitudo probabilitas dan dapat menunjukkan hubungan keterikatan di beberapa qubit. Oleh karena itu, menginterpretasikan hasil pengukuran membutuhkan pemahaman tentang efek interferensi, hubungan fase, dan struktur keterikatan, yang semuanya tidak memiliki analog klasik langsung. Alat komputasi canggih, seperti simulator sirkuit kuantum dan operasi jejak parsial, membantu memvisualisasikan dan memeriksa algoritma kuantum skala kecil, tetapi pertumbuhan eksponensial dimensi ruang Hilbert membatasi interpretasi langsung untuk sistem yang lebih besar. Akibatnya, interpretasi kuantum sangat bergantung pada model matematika abstrak, visualisasi perkiraan, dan basis pengukuran yang dirancang dengan cermat, yang masing-masing membawa potensi kesalahan interpretasi jika intuisi klasik diterapkan terlalu kaku.

Hukum

Dari sudut pandang hukum, dasar ontologis unik dari sistem kuantum korelasi non-lokal, kolaps yang diinduksi pengukuran, ketidakpastian yang tidak dapat direduksi, dan tidak adanya kloning berbeda dari landasan banyak doktrin yang dibangun di atas asumsi klasik determinisme dan bukti yang dapat direplikasi. Misalnya, keterikatan menantang pandangan konvensional bahwa informasi terlokalisasi secara jelas, sehingga memunculkan pertanyaan dalam hukum publik dan privat tentang bagaimana kepemilikan data atau qubit yang terikat dapat didefinisikan atau dialihkan. Demikian pula, rezim bukti yang didasarkan pada rantai pengawasan dan metode forensik yang dapat direproduksi mungkin perlu beradaptasi dengan pengukuran kuantum, yang tentu saja mengubah keadaan asli yang diamati (meskipun jejak audit klasik mungkin masih tersedia). Perlindungan kekayaan intelektual juga menghadapi hambatan: algoritma kuantum dan kode koreksi kesalahan, yang sangat probabilistik dan resisten terhadap pengungkapan langsung, dapat memotivasi adaptasi persyaratan pengaktifan dan kepastian klasik (misalnya, pengaktifan dipenuhi dengan mendeskripsikan

urutan kontrol). Terakhir, bidang-bidang seperti kontrol ekspor, privasi, dan kotak pasir regulasi harus mengatasi fakta bahwa keadaan kuantum pada umumnya tidak dapat dikloning yang dapat memengaruhi bagaimana mereka diaudit. Singkatnya, fitur-fitur yang menjadikan teknologi kuantum sebagai alat yang ampuh juga mengungkap celah dan ketegangan dalam hukum yang dirancang untuk dunia di mana objek dan informasi berperilaku secara klasik. Dengan konsep-konsep ini dalam pikiran, kita sekarang memeriksa detail khusus dari setiap sektor QIT komputasi kuantum, penginderaan kuantum, dan komunikasi kuantum. Bagian-bagian selanjutnya akan membahas dan memperluas aplikasi ini secara lebih detail. Kita mulai dengan komputasi kuantum dan simulasi kuantum.

2.11 KOMPUTASI KUANTUM DAN SIMULASI KUANTUM

Komputasi Kuantum

Komputasi kuantum adalah jenis komputasi dan pemrosesan informasi yang memanfaatkan dan dibatasi oleh mekanika kuantum. Komputasi kuantum dibedakan dari rekan klasiknya melalui keberadaan sifat-sifat tertentu seperti superposisi, keterikatan, dan kuantisasi yang disebutkan di atas. Algoritma yang memanfaatkan karakteristik tersebut, yang disebut algoritma kuantum, menghasilkan prosedur komputasi yang secara efektif unik dan berbeda dari komputasi klasik (atau lebih formalnya, yang dapat disimulasikan oleh komputasi klasik tetapi hanya dengan biaya sumber daya super-polinomial). Algoritma kuantum sangat bervariasi tetapi sering diklasifikasikan menjadi tiga jenis utama berdasarkan sub-rutin kuantum yang mendasarinya. Ini termasuk (i) transformasi Fourier kuantum, kelas algoritma yang menerapkan versi kuantum dari transformasi Fourier klasik, yang digunakan oleh algoritma Shor; (ii) algoritma pencarian kuantum seperti algoritma Grover untuk peningkatan kecepatan pencarian $\sqrt{n}$ berdasarkan amplifikasi amplitudo dan (iii) simulasi kuantum yang akan kita bahas lebih detail di bawah ini, dan yang terkadang diklasifikasikan sebagai kasus penggunaan efektif dari sistem kuantum daripada subkelas spesifik dari metode komputasi kuantum. Efek dari subrutin dan metode algoritmik kuantum ini adalah untuk memfasilitasi proses komputasi yang lebih efisien, seperti pencarian yang lebih cepat atau lebih akurat dan optimasi yang lebih cepat.

Simulasi Kuantum

Simulasi kuantum mewakili penggunaan prospektif utama dari sistem informasi dan komputasi kuantum. Ini melibatkan pemanfaatan sistem kuantum yang dapat dikendalikan untuk meniru dan mempelajari perilaku sistem kuantum lain, yang seringkali kurang mudah diakses atau sangat kompleks. Pendekatan ini sangat berharga di bidang-bidang seperti fisika materi terkondensasi, fisika energi tinggi, fisika atom, kimia kuantum, dan kosmologi, di mana pemahaman interaksi kuantum yang kompleks sangat penting. Bagi perusahaan, simulasi sistem dinamis yang kompleks seperti perilaku pasar dapat memberi mereka keunggulan komparatif dibandingkan pesaing. Bagi negara, potensi sintesis bahan kimia dan material menggunakan simulasi QIT atau bahkan mensimulasikan skenario permusuhan yang kompleks dapat memberi mereka keunggulan strategis baik di masa damai maupun konflik.

Pembelajaran Mesin Kuantum

Pembelajaran mesin kuantum (QML) adalah disiplin ilmu lintas disiplin lain yang menerapkan prinsip-prinsip pembelajaran mesin dengan algoritma kuantum yang menawarkan potensi untuk secara signifikan meningkatkan kemampuan pembelajaran mesin dengan memanfaatkan fitur algoritma kuantum. QML berpotensi untuk secara signifikan meningkatkan pembelajaran berbasis data, khususnya untuk tugas-tugas di mana data secara intrinsik bersifat mekanika kuantum (misalnya, material kuantum, biokimia, dan fisika energi tinggi). Contoh algoritma QML meliputi mesin vektor pendukung kuantum dan jaringan saraf konvolusional kuantum (QCNN) dan algoritma variasi kuantum. Seperti halnya penggunaan mekanika kuantum lainnya, aspek kuantum dari algoritma QML biasanya melibatkan beberapa versi dari kelas algoritma kuantum yang dijelaskan di atas. Terdapat juga analog khusus kuantum dari algoritma pembelajaran mesin klasik, seperti serangkaian algoritma pembelajaran mendalam kuantum dan berbagai algoritma hibrida (klasik-kuantum) yang mengintegrasikan informasi klasik atau informasi sebelumnya yang diketahui dengan varian kuantum. Contoh yang terakhir termasuk pembelajaran mesin geometris kuantum, jaringan saraf kuantum ekuivarian bersama dengan analog jaringan saraf kuantum.

QML menghadirkan disiplin ilmu lintas bidang yang penting antara pembelajaran mesin dan AI di satu sisi dan sistem kuantum di sisi lain. Meskipun QIT dan pembelajaran mesin klasik berbeda, pada akhirnya kemungkinan besar QIT akan tertanam dalam sistem komputasi klasik yang melibatkan atau berlabuh dalam sistem pembelajaran mesin. Lebih lanjut, mengingat kompleksitas tugas dan parameterisasi yang kemungkinan akan digunakan QIT seperti simulasi kuantum kemungkinan penggunaan QIT yang sebenarnya akan melibatkan arsitektur komputasi dan informasi adaptif yang strategi optimasi atau eksekusi tugasnya tidak sepenuhnya ditentukan pada saat runtime tetapi dipelajari selama eksekusi. QML pada akhirnya mungkin akan menjadi paradigma utama di mana komputasi kuantum benar-benar berlangsung.

Terlepas dari janji QML, kegunaannya menghadapi sejumlah tantangan selain ketergantungannya pada keberadaan komputasi kuantum yang toleran terhadap kesalahan yang dapat diskalakan. Dataran tinggi yang tandus dapat menyebabkan gradien menghilang secara eksponensial dalam jumlah qubit, mempersulit pelatihan sirkuit QML yang lebih dalam. Kebisingan pada perangkat kuantum juga dapat memengaruhi lanskap kerugian, yang membutuhkan sumber daya tambahan untuk optimasi. Penyematan data juga tetap menjadi masalah yang belum terselesaikan sementara data klasik dapat dipetakan ke keadaan kuantum, memastikan bahwa pengkodean tersebut mempertahankan struktur yang relevan untuk pembelajaran bukanlah hal yang sepele. Tanggapan teknis mencakup perancangan algoritma yang mengurangi kebisingan, memanfaatkan simetri atau prioritas spesifik masalah, dan merancang arsitektur sirkuit yang lebih dangkal atau lebih khusus untuk mencapai hasil pembelajaran yang stabil dan terukur.

2.12 KOMUNIKASI KUANTUM DAN KRIPTOGRAFI KUANTUM

Komunikasi Kuantum

Komunikasi kuantum memanfaatkan prinsip-prinsip mekanika kuantum untuk memungkinkan transfer informasi yang aman dan efisien. Secara fundamental berbeda dari komunikasi klasik karena menggunakan keadaan kuantum, seperti qubit, untuk mengkodekan dan mengirimkan data. Teknologi utama dalam komunikasi kuantum meliputi distribusi kunci kuantum (QKD), jaringan kuantum, dan protokol komunikasi berbasis keterikatan, yang masing-masing menangani tantangan dan peluang spesifik dalam komunikasi dan berbagi informasi yang aman. QKD menyediakan protokol untuk pertukaran kunci kriptografi yang aman dengan memanfaatkan fitur-fitur sistem kuantum, khususnya teorema tanpa kloning dan prinsip ketidakpastian Heisenberg untuk mendeteksi upaya penyadapan. Protokol seperti BB84 (persiapan dan pengukuran) dan E91 (keterikatan) menggunakan keadaan kuantum diskrit (misalnya, foton terpolarisasi) atau partikel saling terkait untuk menghasilkan kunci bersama secara aman antara dua pihak, bahkan dalam pengaturan yang tidak ideal. Setiap intersepsi saluran kuantum mengubah keadaan kuantum partikel yang ditransmisikan, sehingga penyadapan dapat dideteksi. Kunci yang dipertukarkan digunakan dalam skema enkripsi simetris, seperti AES, untuk komunikasi yang aman. Rezim berbasis keterikatan untuk komunikasi melalui teleportasi kuantum sangat penting untuk sistem kuantum terdistribusi yang relevan dengan kepentingan strategis. Teleportasi kuantum memungkinkan komunikasi tanpa pengukuran keadaan kuantum yang tidak diketahui dari satu sistem kuantum ke sistem kuantum lainnya melalui penggunaan keterikatan, pengukuran keadaan Bell, dan saluran EPR.

Jaringan Kuantum

Jaringan kuantum adalah aplikasi prospektif utama dari teknologi komunikasi kuantum yang memanfaatkan teleportasi kuantum untuk memungkinkan komunikasi antar banyak pengguna jarak jauh tanpa memerlukan jaringan lokal perantara (walaupun pengulang kuantum biasanya merupakan fitur dari sistem tersebut). Jaringan kuantum dan teleportasi kuantum memiliki dampak strategis tertentu sebagai hasil dari prospek internet kuantum, yang mewakili jaringan perangkat komputasi dan komunikasi kuantum (dan bahkan penginderaan) yang terhubung dan terintegrasi yang memungkinkan, dalam konteks komunikasi, distribusi informasi bervolume tinggi dan cepat melalui keadaan kuantum yang ditransmisikan secara aman dan kuat. Proposal internet kuantum tersebut diharapkan dapat memberikan cara yang lebih baik untuk menggunakan teknologi kuantum yang relevan dengan aktivitas ekonomi dan geopolitik yang tunduk pada berbagai rezim hukum, termasuk melakukan QKD, komunikasi langsung aman kuantum (memungkinkan informasi rahasia didistribusikan tanpa distribusi kunci terpisah), didistribusikan dan digunakan untuk komputasi kuantum terdistribusi, sinkronisasi jam, dan komunikasi yang ditingkatkan kuantum.

Kriptografi Pasca-Kuantum

Kriptografi pasca-kuantum (PQC) adalah seperangkat protokol kriptografi yang dimaksudkan untuk aman terhadap serangan musuh dan dekripsi oleh musuh yang dilengkapi dengan komputer kuantum toleransi kesalahan yang dapat diskalakan. PQC dimotivasi sebagai cara untuk mengatasi ancaman strategis yang dihadapi oleh para pemangku kepentingan yang

timbul dari kemampuan dekripsi komputer kuantum yang diidentifikasi di atas, yang pada prinsipnya dapat mendekripsi sistem kunci publik seperti RSA, Diffie-Hellman, dan kriptografi kurva eliptik. Skema enkripsi klasik seringkali bergantung pada algoritma kelas standar, seperti faktorisasi bilangan bulat atau algoritma logaritma diskrit. Algoritma PQC, sebaliknya, memanfaatkan algoritma dan pengkodean yang dekripsinya berada dalam kelas kompleksitas yang lebih tinggi, yaitu sulit atau tidak dapat diatasi bahkan oleh komputer kuantum, termasuk metode berbasis kisi, metode berbasis kesalahan pembelajaran, sistem polinomial multivariat, atau masalah isogeni pada kurva eliptik. Secara umum, algoritma PQC biasanya menghasilkan kunci dan sandi yang lebih besar yang melebihi sumber daya yang secara layak dapat didekode.

2.13 PENGINDERAAN KUANTUM DAN METROLOGI KUANTUM

Penginderaan Kuantum dan Titik Kuantum

Penginderaan kuantum dalam bentuk teoritis dan terapannya meneliti bagaimana sifat-sifat mekanika kuantum tertentu dari sistem memunculkan cara-cara baru dan sangat sensitif untuk mengukur lingkungan, mengumpulkan data. Dengan demikian, hal ini menghasilkan informasi yang lebih rinci tentang statistik pengukuran dan distribusi probabilitas sistem lingkungan. Penginderaan kuantum juga telah terbukti meningkatkan metrologi kuantum, seringkali memanfaatkan sifat-sifat spesifik kuantum dari superposisi dan keterikatan, memungkinkan estimasi parameter yang lebih tepat (metrologi kuantum). Salah satu bentuk teknologi penginderaan kuantum yang lebih canggih adalah titik kuantum, jenis sirkuit kuantum yang direkayasa untuk membatasi elektron (atau rongga) dalam lingkungan terbatas tertentu. Titik kuantum memiliki berbagai aplikasi dan memang merupakan komponen kandidat teknologi untuk substrat komputasi kuantum itu sendiri.

Konsep dasar titik kuantum adalah pengurungan elektron tunggal dalam potensial elektromagnetik sedemikian rupa sehingga keadaan mekanika kuantumnya dapat disetel atau disesuaikan secara efektif, misalnya melalui arsitektur kontrol yang melibatkan pulsa gelombang mikro, resonansi magnetik, atau metode lainnya. Dengan demikian, titik kuantum mewakili subsistem yang dapat dikontrol yang dapat dihubungkan ke lingkungan dengan cara yang memungkinkan kontrol halus terhadap keadaan kuantum (misalnya, memungkinkan implementasi gerbang sirkuit kuantum) tetapi juga memungkinkan penggunaannya sebagai instrumen (atau alat) pengukuran. Secara intuitif, ini karena pengukuran dan kontrol keduanya merupakan interaksi dengan sistem kuantum: pengukuran sistem kuantum membutuhkan agar eigenstate dan eigenvalue tertentu dari perangkat pengukuran cukup terdefinisi dengan baik sehingga hasil pengukuran dapat dibedakan dan dipahami.

Prosedur Penginderaan Kuantum

Perangkat penginderaan kuantum yang ada memanfaatkan sensitivitas sistem kuantum yang diwujudkan melalui sistem atom, ion, fotonik, atau padat untuk pengukuran presisi. Perangkat ini cenderung diklasifikasikan berdasarkan sistem kuantum atau target pengukuran, dengan berbagai karakteristik fisik seperti sensitivitas, berat, ukuran, daya, dan biaya yang menjadi faktor penggunaannya. Teknologi sensor kuantum mengikuti protokol di mana sensor (i) diinisialisasi, (2) diubah menjadi keadaan kuantum (misalnya superposisi), (3) berinteraksi

dengan lingkungan melalui evolusi yang terkopel, (4) transformasi menjadi keadaan yang dapat diukur (misalnya eigenstate), (5) diukur. Proses ini kemudian diulang secukupnya agar statistik pengukuran dapat dikumpulkan. Sensor kuantum adalah salah satu bentuk QIT yang lebih canggih dengan berbagai aplikasi yang akan kami sebutkan di bagian-bagian selanjutnya di bawah ini. Studi tentang penggunaannya dalam konteks seperti ilmu hayati, teknologi keamanan nasional, dan teknologi komunikasi memberikan detail tentang bagaimana integrasi QIT telah berjalan dalam rezim hukum yang ada.

2.14 TUMPUKAN INFRASTRUKTUR KUANTUM

Teknologi informasi kuantum dapat dipertimbangkan secara abstrak, sebagai bentuk teknologi komputasi dengan efek unik yang tidak tersedia untuk teknologi klasik, atau bahkan lebih abstrak lagi, sebagai suatu kemampuan yang efeknya, daripada spesifikasi teknisnya, adalah yang penting untuk pertimbangan normatif dan yurisprudensial. Namun pemeriksaan kasar semacam itu mengabaikan detail teknis penting mengenai bagaimana tumpukan infrastruktur kuantum, di mana sistem informasi kuantum berada dan akan tertanam, memengaruhi faktor strategis dan yurisprudensial. Seperti yang telah diisyaratkan di atas, akan bermanfaat untuk menilai tumpukan ini secara vertikal, dalam hal bagaimana lapisan arsitektur klasik dan kuantum diintegrasikan; Secara horizontal, dalam hal bagaimana infrastruktur kuantum dan klasik didistribusikan dan dihubungkan. Memahami fitur teknis dari tumpukan infrastruktur kuantum dapat memberikan kejelasan yang lebih besar tentang bagaimana dan di mana para pemangku kepentingan dapat bertindak (di mana lokasi atau pusat tindakan mereka, pada lapisan mana dalam tumpukan, tingkat keterhubungannya, dan sebagainya) dan, sebagai hasilnya, konsekuensi bagi penerapan prinsip-prinsip hukum internasional. Dua contoh yang kami gunakan untuk mengilustrasikan pertimbangan teknis ini adalah (i) sebuah komputer kuantum tunggal dan (ii) sebuah internet kuantum, yang terdiri dari node komputasi kuantum yang dihubungkan oleh saluran informasi klasik atau kuantum (yang mungkin misalnya merupakan arsitektur internet kuantum yang potensial).

Tumpukan Komputasi Kuantum

Tumpukan komputasi kuantum berbasis qubit yang khas dapat direpresentasikan melalui lapisan fitur seperti yang tercantum dalam Tabel 2.1. Pada dasar setiap perangkat komputasi kuantum terdapat lapisan fisik tempat substrat komputasi kuantum dibentuk, seperti sistem fotonik, superkonduktor, ion terperangkap, topologi, dan sistem lainnya. Di atas lapisan fisik terdapat lapisan pengukuran dan kontrol yang terdiri dari infrastruktur fisik untuk melakukan kontrol yang lebih detail terhadap sistem kuantum, termasuk yang diperlukan untuk pengukuran, seperti dalam bentuk pulsa gelombang mikro dan sinyal laser. Lapisan berikutnya adalah lapisan koreksi kesalahan yang mengkodekan protokol koreksi kesalahan kuantum, seperti kode permukaan.

Lapisan qubit logis adalah cara untuk mengabstraksi qubit logis yang dibentuk melalui kluster dan interaksi qubit fisik (dimediasi melalui protokol koreksi kesalahan) dan dapat mencakup struktur memori kuantum. Qubit logis merupakan elemen dari lapisan logis infrastruktur kuantum. Dari lapisan qubit logis, kemudian terdapat lapisan bahasa dan

pemrograman yang efektif, seperti (i) lapisan perakitan kuantum, analog dengan lapisan kode perakitan pada komputer klasik; (ii) kompiler kuantum yang memungkinkan kompilasi lingkungan pengembangan dan program; (iii) representasi perantara kuantum yang merupakan representasi ontologis yang menjadi perantara antara kompiler dan bahasa pemrograman; (iv) bahasa pemrograman kuantum yang merupakan bahasa interpretatif tingkat tinggi dengan kapasitas ekspresif yang cukup besar; (v) lapisan aplikasi untuk aplikasi dan antarmuka pengguna dan di mana secara praktis, misalnya, antarmuka manusia untuk penerapan komputasi kuantum akan berlaku. Selain itu, kita juga dapat menentukan lapisan antarmuka klasik seperti di mana sistem kuantum dienkapsulasi dalam komponen klasik, seperti register klasik atau basis data untuk menyimpan statistik pengukuran, spesifikasi algoritma klasik, dan sejenisnya.

Tabel 2.1 Susunan komputasi kuantum tipikal, dari substrat komputasi kuantum fisik hingga bahasa pemrograman, kompiler, dan aplikasi.

Lapisan	**Deskripsi**
Lapisan sirkuit kuantum	Substrat sirkuit komputasi kuantum, yang mencakup qubit fisik yang diwujudkan menggunakan teknologi seperti sistem fotonik, sirkuit superkonduktor, ion terperangkap, atau qubit topologi. Lapisan ini melibatkan perwujudan fisik keadaan kuantum dan manipulasinya.
Lapisan pengukuran dan kontrol	Sistem kontrol perangkat keras yang bertanggung jawab untuk berinteraksi dengan lapisan kuantum fisik yang menghasilkan sinyal presisi untuk memanipulasi qubit, seperti pulsa gelombang mikro atau sistem laser. Sistem-sistem ini memastikan implementasi gerbang kuantum dan operasi pembacaan
Lapisan koreksi kesalahan	Protokol koreksi kesalahan kuantum, seperti kode permukaan atau kode gabungan, yang mendeteksi dan mengoreksi kesalahan yang timbul dari dekoherensi dan kebisingan dalam sistem kuantum
Lapisan qubit logis	Qubit logis yang dibentuk dari qubit fisik melalui koreksi kesalahan, memungkinkan komputasi kuantum yang lebih kuat dengan mengabstraksi kebisingan pada lapisan fisik
Bahasa assembly kuantum	Bahasa pemrograman tingkat rendah yang dirancang untuk komputer kuantum, yang menentukan operasi dan sirkuit kuantum secara spesifik untuk perangkat keras (misalnya, OpenQASM (Wesley (2024)))
Kompiler kuantum	Alat perangkat lunak yang menerjemahkan algoritma kuantum tingkat tinggi menjadi instruksi yang dapat dieksekusi untuk perangkat keras kuantum, mengoptimalkan untuk batasan perangkat keras tertentu dan meminimalkan tingkat kesalahan
Representasi perantara kuantum	Representasi perantara yang digunakan oleh kompiler untuk menjembatani kode tingkat tinggi dan instruksi perakitan spesifik perangkat keras, memungkinkan optimasi di berbagai platform perangkat keras

Bahasa pemrograman kuantum	Bahasa tingkat tinggi yang digunakan untuk menulis algoritma kuantum, seperti Qiskit dan Cirq. Ini menyediakan abstraksi yang menyederhanakan pemrograman kuantum untuk peneliti dan pengembang.
Lapisan aplikasi	Aplikasi pengguna akhir yang memanfaatkan algoritma kuantum, seperti kriptografi kuantum, optimasi, pembelajaran mesin, dan simulasi sistem kuantum. Lapisan ini berfokus pada masalah spesifik domain yang diatasi menggunakan komputasi kuantum.
Lapisan antarmuka klasik	Antarmuka antara sistem klasik dan kuantum, mengelola komputasi hibrida, input/output data, dan pra- dan pasca-pemrosesan hasil. Ini termasuk perangkat keras dan perangkat lunak klasik yang terintegrasi dengan prosesor kuantum.

Tumpukan Jaringan Kuantum

Jaringan kuantum, di mana sistem QIT membentuk sistem terdistribusi, merupakan kasus penggunaan QIT prospektif yang penting. Jaringan kuantum secara sederhana melibatkan komputer kuantum sebagai node dengan saluran pengiriman pesan dan karenanya dapat direpresentasikan sebagai grafik. Persyaratan infrastruktur untuk jaringan kuantum sangat besar: termasuk semua infrastruktur yang dibutuhkan untuk satu perangkat komputasi kuantum, di samping infrastruktur kompleks yang dibutuhkan untuk mendukung komputasi dan pengiriman pesan terdistribusi. Pada Tabel 2.2, kami menguraikan sejumlah fitur utama dari tumpukan jaringan kuantum. Melakukan hal ini membantu pemeriksaan kami di bagian selanjutnya mengenai di mana dan bagaimana State dapat berinteraksi (secara kooperatif dan antagonis). Taksonomi kami bersifat generik tetapi didasarkan pada proposal untuk internet kuantum. Jaringan kuantum terdiri dari node kuantum, yaitu komputer atau prosesor kuantum yang melakukan pemrosesan informasi dan menyimpan informasi kuantum.

Node-node tersebut terhubung melalui saluran kuantum yang menghubungkan setiap node dan memungkinkan transfer informasi di antara mereka. Meskipun saluran-saluran ini mungkin klasik, untuk memanfaatkan manfaat sistem kuantum yang terhubung jaringan, saluran-saluran tersebut adalah saluran kuantum. Di atas arsitektur inti ini terdapat mekanisme untuk distribusi keterikatan. Ini mungkin termasuk lapisan pengulang kuantum yang memperluas jangkauan komunikasi kuantum melalui koreksi kesalahan dan penguatan keterikatan. Jaringan kuantum juga memerlukan lapisan kontrol klasik tersendiri untuk mengelola elemen jaringan sistem (berbeda dari yang ada di tingkat node), bersama dengan memori kuantum khusus jaringan untuk buffering dan operasi tertunda.

Protokol jaringan mewakili lapisan abstraksi di atas jaringan kuantum yang menetapkan bagaimana QKD, teleportasi kuantum, dan keterikatan dikelola. Mungkin juga ada node klasik itu sendiri dan lapisan aplikasi kuantum jaringan terpisah untuk implementasi aplikasi di tingkat jaringan (seperti untuk penginderaan kuantum terdistribusi) bersama dengan infrastruktur keamanan tambahan untuk mengamankan infrastruktur fisik terdistribusi, manajemen perutean dan topologi, dan proses optimasi sistem terdistribusi lainnya, dan tentu saja koreksi kesalahan.

Tabel 2.2 Elemen-elemen jaringan kuantum terdistribusi yang merinci komponen dan fitur internet kuantum, di mana komputer kuantum bertindak sebagai node jaringan.

Komponen	**Deskripsi**
Node kuantum	Komputer kuantum atau prosesor kuantum yang berfungsi sebagai unit komputasi dalam jaringan. Node ini melakukan komputasi kuantum dan menyimpan informasi kuantum menggunakan qubit.
Saluran kuantum	Tautan komunikasi yang memungkinkan transfer keadaan kuantum antar node. Biasanya diimplementasikan menggunakan serat optik, fotonika ruang bebas, atau sistem berbasis satelit untuk menjaga keterikatan kuantum.
Distribusi keterikatan	Mekanisme untuk menghasilkan dan mendistribusikan keadaan saling terkait di seluruh jaringan, membentuk tulang punggung protokol komunikasi kuantum. Contohnya termasuk pertukaran keterikatan dan pengulang kuantum.
Repeater kuantum	Perangkat yang memperluas jangkauan komunikasi kuantum dengan mengoreksi kesalahan dan memperkuat keterikatan di jarak jauh. Ini penting untuk jaringan kuantum skala besar.
Lapisan kontrol klasik	Lapisan komunikasi dan sinkronisasi klasik untuk mengoordinasikan operasi kuantum, mengirimkan hasil pengukuran, dan memungkinkan protokol koreksi kesalahan.
Memori kuantum	Unit penyimpanan untuk menjaga keadaan kuantum selama komunikasi atau komputasi. Memori kuantum sangat penting untuk menyangga keterikatan dan mendukung operasi kuantum yang tertunda.
Protokol jaringan	Protokol yang mengatur pengoperasian jaringan kuantum, termasuk distribusi kunci kuantum (QKD), teleportasi kuantum, dan protokol distribusi keterikatan. Ini juga mencakup protokol hibrida kuantum-klasik
Node klasik	Sistem klasik yang berinteraksi dengan node kuantum untuk mengelola tugas kontrol, melakukan pra- dan pasca-pemrosesan, dan menangani tugas komputasi non-kuantum
Aplikasi kuantum	Aplikasi tingkat tinggi yang berjalan di jaringan, seperti komunikasi aman, komputasi kuantum terdistribusi, sinkronisasi jam, dan penginderaan yang ditingkatkan kuantum
Infrastruktur keamanan	Mekanisme yang memastikan keamanan komunikasi kuantum, termasuk sistem QKD, deteksi penyadapan, dan dukungan kriptografi klasik untuk protokol hibrida
Manajemen perutean dan topologi	Sistem manajemen yang menentukan jalur optimal untuk informasi kuantum dan klasik, dengan mempertimbangkan kendala unik komunikasi kuantum seperti tidak adanya kloning dan dekoherensi
Lapisan koreksi kesalahan	Protokol koreksi kesalahan kuantum untuk mengurangi kebisingan dan dekoherensi di saluran kuantum, memastikan transmisi dan penyimpanan keadaan kuantum yang andal

Seperti yang dibahas di atas, QIT tak pelak lagi berada dalam infrastruktur klasik yang merupakan bagian integral dari pengoperasian dan dukungan QIT. Kami menyertakan taksonomi infrastruktur tersebut dalam Tabel 2.3. Elemen utama dan penting adalah sistem kontrol klasik, termasuk generator sinyal dan pengontrol urutan pulsa, yang penting untuk memanipulasi qubit dan mengeksekusi operasi kuantum, seperti pengukuran, pengkodean informasi dalam sistem kuantum, dan protokol hibrida klasik-kuantum, seperti banyak sistem pembelajaran mesin kuantum.

Antarmuka komputasi klasik juga penting untuk menangani pemrosesan data, menetapkan spesifikasi inisialisasi, dan manajemen keseluruhan QIT. Dalam komunikasi kuantum, peralatan jaringan seperti router dan switch klasik sangat penting agar perangkat kuantum dapat diintegrasikan ke dalam arsitektur jaringan yang lebih besar, memungkinkan komunikasi lintas saluran kuantum-ke-klasik dan klasik-ke-kuantum untuk tetap berlangsung. Basis data dan register klasik sangat penting untuk menyimpan hasil eksperimen kuantum, statistik pengukuran, dan kumpulan data komputasi. Sistem catu daya dan mekanisme pendinginan merupakan persyaratan penting dari semua kandidat realisasi fisik sistem kuantum, termasuk lemari pendingin kriogenik, untuk memastikan pengoperasian perangkat keras kuantum yang stabil dalam kondisi lingkungan yang presisi dan rendah kebisingan.

Tabel 2.3 Kerangka Infrastruktur Klasik di sekitar QIT

Jenis Infrastruktur Klasik	**Deskripsi**
Sistem kontrol	Perangkat keras dan perangkat lunak kontrol klasik yang digunakan untuk memanipulasi qubit, seperti generator sinyal, sistem kontrol gelombang mikro, dan pengontrol urutan pulsa
Antarmuka komputasi klasik	Komputer dan server klasik yang berinteraksi dengan komputer kuantum, mengelola pemrosesan data, inisialisasi, dan interaksi dengan sistem kuantum
Sistem penyimpanan data	Solusi penyimpanan klasik untuk menyimpan hasil eksperimen kuantum, perhitungan perantara, dan kumpulan data besar yang diperlukan untuk komputasi kuantum-klasik hibrida
Peralatan jaringan	Perangkat jaringan klasik seperti router, switch, dan hub yang membentuk tulang punggung untuk mengintegrasikan sistem kuantum ke dalam jaringan yang lebih luas, termasuk jaringan kuantum
Sistem koreksi kesalahan	Prosesor klasik yang mengimplementasikan algoritma deteksi dan koreksi kesalahan untuk menstabilkan komputasi dan komunikasi kuantum
Sistem pendingin	Sistem kriogenik yang diperlukan untuk mempertahankan lingkungan operasional untuk perangkat keras kuantum, seperti lemari pendingin pengenceran untuk qubit superkonduktor
Sistem catu daya	Infrastruktur daya yang andal yang memastikan operasi subsistem kuantum dan klasik yang stabil dan tanpa gangguan

Alat pemantauan dan diagnostik	Sistem klasik untuk memantau status sistem kuantum, termasuk alat diagnostik untuk pemeriksaan kebisingan, stabilitas, dan kinerja
Sistem keamanan	Firewall, sistem deteksi intrusi, dan langkah-langkah keamanan siber klasik lainnya untuk melindungi infrastruktur kuantum dari akses yang tidak sah
Antarmuka Klasik-Kuantum	Middleware yang menerjemahkan data klasik Perintah diubah menjadi instruksi kuantum dan sebaliknya, memungkinkan pengoperasian yang lancar antara sistem klasik dan kuantum.

Tumpukan Infrastruktur Kuantum

Selain infrastruktur fisik di sekitarnya, prosesor klasik merupakan komponen penting dalam koreksi kesalahan kuantum, mengimplementasikan pengukuran sindrom untuk mendeteksi dan mengurangi kesalahan yang muncul selama komputasi kuantum. Sistem klasik juga penting untuk arsitektur keamanan QIT, melindungi infrastruktur kuantum melalui firewall dan deteksi intrusi, serta menjaga operasi kuantum yang sensitif. Sistem ini sangat penting untuk alat pemantauan dan diagnostik yang digunakan untuk mengevaluasi kinerja sistem kuantum, memberikan wawasan waktu nyata tentang tingkat kebisingan, stabilitas, dan efisiensi. Antarmuka klasik-kuantum bertindak sebagai middleware, menerjemahkan instruksi klasik ke dalam perintah kuantum dan memproses hasil kuantum untuk interpretasi klasik. Bersama-sama, komponen-komponen ini membentuk infrastruktur klasik komprehensif yang mendukung dan meningkatkan fungsionalitas QIT.

2.15 DAMPAK TEKNIS QIT

Dampak Informasi

Sekarang kita mempertimbangkan ringkasan tingkat tinggi tentang dampak informasi teknis utama QIT yang relevan dengan tata kelola. Kita mengadopsi fokus khusus mengenai bagaimana QIT memengaruhi akuisisi, transfer, dan penggunaan data. Pada bagian selanjutnya, kita akan mempertimbangkan bagaimana dampak teknis secara keseluruhan ini memiliki konsekuensi bagi rezim hukum tertentu. Seperti yang akan kita bahas di bawah ini, transisi dari model deterministik klasik ke model stokastik kuantum informasi memengaruhi berbagai bidang hukum, termasuk tetapi tidak terbatas pada bukti, kekayaan intelektual, kontrol ekspor, perlindungan data, kebijakan persaingan, dan regulasi ilmu hayati. Kita dapat mengelompokkan konsekuensi informasi utama QIT ke dalam beberapa kategori. Setiap kategori mencerminkan pergeseran atau perluasan dalam cara data diproduksi dan diproses, yang secara langsung terkait dengan potensi masalah hukum dan regulasi. Kategori-kategori ini tidak saling eksklusif bahkan, seringkali tumpang tindih tetapi menawarkan lensa terstruktur untuk memahami dampak luas QIT. Gagasan tentang tumpukan tata kelola sengaja dikaitkan dengan ontologi dan taksonomi yang dikenal dalam ilmu komputasi dan teknik untuk secara tepat dan spesifik mengidentifikasi di mana dalam tumpukan teknologi QIT kemungkinan akan berdampak.

Ini adalah poin yang sangat penting di setiap subdivisi QIT: komputasi kuantum, penginderaan kuantum, dan simulasi kuantum pada dasarnya adalah bentuk pemrosesan informasi, meskipun dengan signifikansi khusus. Dengan tetap fokus pada karakterisasi terkait informasi dari QIT dan regulasi ilmu hayati, kami kemudian mengadopsi kerangka kategoris berikut tentang dampak informasional QIT dalam hal: (i) pengaruhnya terhadap informasi, yaitu jenis, kuantitas, kualitas, skala, dan properti lainnya, termasuk bagaimana informasi tersebut diperoleh dan informasi apa yang diperoleh; (ii) pengaruhnya terhadap pemrosesan informasi, seperti dengan memungkinkan komputasi yang jika tidak akan sulit dilakukan, atau bahkan hanya memungkinkan komputasi yang meskipun secara teknis dapat dilakukan (dalam kelas kompleksitas yang dapat ditentukan) namun, dari perspektif skala waktu manusia, secara efektif sulit dilakukan; (iii) kontrol, QIT menawarkan cara untuk berinteraksi dengan sistem dan dengan demikian melakukan kontrol (pada tingkat yang lebih besar atau lebih kecil) atas sistem tersebut. Dampak informasi dari QIT sangat luas tetapi dapat diklasifikasikan tergantung pada tahap atau proses akuisisi, penyimpanan, atau pemrosesan informasi.

Dampak Efisiensi Pemrosesan Informasi

Dengan memungkinkan pemrosesan informasi yang lebih cepat, lebih akurat, atau lebih baik, QIT dapat memiliki dampak signifikan terhadap efisiensi informasi.

Dampak Orakular

QIT dapat berdampak melalui memungkinkan pengetahuan (dan produk) baru yang tidak dapat (karena kendala komputasi atau ketidakmampuan komputasi) dihasilkan melalui cara pemrosesan informasi yang ada atau klasik.

Efek Asimetri Informasi

QIT dapat memfasilitasi distribusi kekuatan pemrosesan informasi yang asimetris (seperti melalui beberapa pelaku pasar yang memiliki akses ke QIT sementara yang lain tidak) dengan cara yang dapat berdampak pada stabilitas pasar dan pengawasan regulasi.

Dampak Pengukuran

QIT sudah memengaruhi protokol pengukuran. Hal ini terutama terjadi dalam penginderaan kuantum di mana teknologi titik kuantum yang memungkinkan pengukuran resolusi dan sensitivitas yang lebih tinggi telah jauh lebih maju dari tahap teoretis hingga pengembangan prototipe. Kami menguraikan pemeriksaan yang lebih rinci tentang poin-poin ini di Lampiran. Di bawah ini kami menguraikan dampak hukum dari penggunaan QIT di berbagai domain yurisprudensi yang dipertimbangkan dalam berbagai tingkat di bagian-bagian selanjutnya.

Peningkatan Daya Komputasi

Algoritma kuantum (seperti algoritma Shor atau Grover yang disebutkan di atas) menjanjikan peningkatan kecepatan eksponensial atau polinomial untuk kelas masalah tertentu. Hal ini dapat menghasilkan peningkatan dramatis dalam pemrosesan tugas yang sebelumnya dianggap tidak layak secara komputasi di bawah perangkat keras klasik misalnya, memfaktorkan bilangan bulat besar (mengancam enkripsi berbasis RSA) atau mensimulasikan interaksi molekuler kompleks dengan cepat dalam penemuan obat. Pada tingkat yang lebih bertahap, komputer kuantum jangka pendek (perangkat NISQ) masih dapat memberikan

peningkatan kecepatan yang berarti untuk tugas-tugas khusus, meskipun dengan tingkat kesalahan yang lebih tinggi dan jumlah qubit yang terbatas. Masalah hukum dan peraturan dapat mencakup hal-hal berikut.

Perlindungan dan Keamanan Data

Dekripsi yang lebih cepat dari mekanisme enkripsi klasik membutuhkan revisi mendesak dalam standar kriptografi. Pemerintah dan entitas swasta harus mempertimbangkan migrasi kriptografi pasca-kuantum, karena protokol keamanan yang ada dapat menjadi usang.

Kekayaan Intelektual dan Persaingan

Entitas dengan kapasitas komputasi kuantum yang substansial dapat menyelesaikan tugas optimasi atau tugas intensif pembelajaran jauh lebih cepat daripada pesaing, sehingga menimbulkan pertanyaan tentang kekuatan pasar dan keadilan dalam persaingan paten.

Penyelesaian Masalah Orakular dan Ketidakmampuan untuk Dipecahkan

Selain peningkatan kecepatan, komputer kuantum dapat bertindak sebagai perangkat orakular untuk masalah yang tidak hanya sulit tetapi juga secara efektif tidak dapat dipecahkan pada perangkat keras klasik. Ini termasuk mensimulasikan sistem kuantum tertentu, memecahkan tugas optimasi berdimensi tinggi, dan mengeksplorasi fungsi jebakan kriptografi. Ciri khas QIT orakular adalah menghasilkan jawaban yang tidak selalu dapat direplikasi atau divalidasi sepenuhnya oleh verifikasi klasik, pada dasarnya menghasilkan keluaran dari proses kotak hitam. Masalah hukum dan peraturan dapat mencakup hal-hal berikut.

Bukti dan Verifikasi

Sistem pengadilan yang bergantung pada kemampuan replikasi dan verifikasi transparan dapat ditantang oleh keluaran QIT kotak hitam. Misalnya, jika algoritma kuantum menyarankan desain obat baru, akan ada pertanyaan nyata tentang bagaimana regulator atau penggugat mengkonfirmasi hasilnya (terutama di mana verifikasi itu sendiri mungkin terlalu kompleks untuk verifikator klasik).

Tanggung Jawab dan Akuntabilitas

Untuk kasus penggunaan berisiko tinggi (misalnya, farmasi, keputusan berbasis AI), kurangnya penjelasan yang transparan dapat mempersulit penetapan tanggung jawab jika beberapa agen berinteraksi melalui komputer kuantum yang terhubung jaringan untuk membuat keputusan. Keamanan Nasional. Kemampuan QIT orakular dapat menghasilkan keuntungan asimetris dalam pemecahan kode atau pemeriksaan intelijen, meningkatkan pengawasan kontrol ekspor atau memerlukan kontrol yang lebih ketat.

Pengukuran dan Penginderaan Ultra-Halus

Penginderaan kuantum yang memungkinkan pengukuran besaran fisik misalnya, medan magnet, struktur molekuler pada resolusi yang belum pernah terjadi sebelumnya dapat menimbulkan dampak hukum atau tantangan prosedural. Perangkat seperti titik kuantum memungkinkan sensitivitas ekstrem dalam diagnostik, pemantauan lingkungan, dan karakterisasi material. Tidak seperti sensor klasik, sensor kuantum dapat mengumpulkan data yang sama sekali tidak dapat dikumpulkan oleh peralatan klasik atau hanya diukur pada resolusi yang lebih kasar. Masalah hukum dan peraturan dapat mencakup hal-hal berikut.

Ilmu Hayati dan Perangkat Medis

Data diagnostik kuantum yang presisi dapat mempercepat penemuan obat atau perawatan spesifik pasien. Namun, regulator mungkin memerlukan cara baru untuk menilai keandalan, kalibrasi, dan klasifikasi risiko untuk instrumen berbasis kuantum yang baru.

Privasi dan Pengawasan

Pengukuran dengan fidelitas tinggi dapat memfasilitasi bentuk-bentuk baru pengumpulan data invasif misalnya, berpotensi memetakan aktivitas saraf di lingkungan terkontrol atau mendekode sinyal sensitif. Hukum perlindungan data mungkin perlu menyesuaikan definisi data pribadi jika penginderaan kuantum mengungkapkan detail intim yang tidak dapat diukur melalui instrumen klasik.

Kekhawatiran Strategis dan Keamanan

Sensor kuantum yang mendeteksi pesawat atau kapal selam siluman dapat (jika dikembangkan secara memadai) mengganggu keseimbangan militer, memicu pertanyaan hukum internasional baru seputar penggunaan QIT untuk aktivitas siber dan bahkan pertimbangan pengendalian senjata.

Ketidakmampuan untuk Dikloning dan Verifikasi Probabilistik

Seperti yang disebutkan di atas, keadaan kuantum tunduk pada teorema tidak dapat dikloning, yaitu seseorang tidak dapat membuat salinan identik dari keadaan kuantum yang tidak diketahui secara sembarang. Selain itu, pengukuran akan meruntuhkan keadaan tersebut, sehingga pemeriksaan forensik berulang terhadap keadaan kuantum yang sama menjadi tidak mungkin (perhatikan bahwa sistem fisik yang sama dapat diinisialisasi ulang, tetapi secara teknis ini adalah keadaan kuantum baru). Sebaliknya, verifikasi bergantung pada pengambilan sampel probabilistik dari beberapa keadaan yang disiapkan secara identik. Protokol koreksi kesalahan lebih lanjut memperumit bagaimana data asli didefinisikan, karena koreksi kesalahan kuantum biasanya merekonstruksi keadaan logis dari beberapa qubit yang saling terkait. Masalah hukum dan peraturan dapat mencakup hal-hal berikut.

Rantai Bukti-Kepemilikan

Sistem hukum klasik mengasumsikan bahwa data (misalnya, data forensik dari audit) dapat direplikasi untuk diperiksa ulang. Data kuantum tidak dapat disalin atau diukur berulang kali tanpa mengubah keadaan dasar dari setiap contoh. Verifikasi secara umum tidak dapat terjadi tanpa mengganggu keadaan kuantum itu sendiri. Hal ini mungkin memerlukan pertimbangan tentang bagaimana verifikasi dapat atau seharusnya terjadi di mana verifikasi komputasi atau komunikasi teknis, atau penginderaan, diperlukan.

Kekayaan Intelektual dan Rahasia Dagang

Paten seringkali memerlukan deskripsi tertulis lengkap dan pengaktifan. Namun, proses kuantum yang tidak dapat dikloning atau diukur sepenuhnya, sehingga persyaratan pengungkapan klasik mengenai kecukupan mungkin difokuskan pada rezim kontrol sebagai gantinya. Demikian pula, menunjukkan penyalahgunaan rahasia dagang yang disimpan atau digunakan dalam QIT mungkin terbukti lebih sulit jika keadaan tersebut tidak dapat disalin dengan mudah.

Kontrol Ekspor dan Penggunaan Ganda

Pemantauan aliran informasi kuantum lintas batas menjadi lebih menantang ketika keterikatan kuantum tak berwujud dapat terbentuk di berbagai yurisdiksi dan data tidak dapat direproduksi secara bermakna untuk diperiksa.

Asimetri Informasi dan Konsentrasi Pasar

Infrastruktur kuantum skala besar baik itu laboratorium kriogenik kelas atas untuk qubit superkonduktor atau jaringan fotonik khusus membutuhkan sumber daya yang cukup besar. Akibatnya, sejumlah kecil pemerintah atau perusahaan dapat mendominasi kemampuan QIT. Hal ini menimbulkan pertimbangan asimetri informasi di mana hanya aktor tertentu yang dapat mendekripsi data, mengoptimalkan sistem kompleks, atau berinovasi dalam skala besar dengan algoritma kuantum. Pada gilirannya, ini menimbulkan pertimbangan asimetri informasi di mana hanya aktor tertentu yang dapat mendekripsi data, mengoptimalkan sistem kompleks, atau berinovasi dalam skala besar dengan algoritma kuantum. Masalah hukum dan peraturan dapat mencakup hal-hal berikut.

Hukum Persaingan

Jika hanya segelintir perusahaan (atau Negara) yang memiliki komputasi kuantum yang kuat, definisi pasar standar atau kerangka kerja anti-kolusi mungkin perlu dipertimbangkan kembali. Ada potensi struktur oligopoli di sekitar rantai pasokan perangkat keras kuantum atau layanan cloud kuantum khusus.

Hukum Internasional Publik dan Geopolitik

Asimetri strategis dapat memotivasi dinamika persaingan. Negara-negara dengan dekripsi kuantum canggih mungkin akan memperoleh keuntungan intelijen yang tidak proporsional, yang berdampak pada lanskap keamanan siber global dan berpotensi memotivasi tindakan antisipatif (seperti serangan preventif) oleh Negara-negara sebelum keuntungan kuantum lawan mereka terwujud.

Perlindungan Data dan Akses yang Adil

Sumber daya kuantum yang terkonsentrasi dapat menghambat akses luas terhadap terobosan dalam desain obat atau pemodelan iklim. Hal ini dapat menimbulkan pertimbangan mengenai bagaimana mengatur akses ke platform QIT penting untuk menghindari ketidakseimbangan ekonomi dalam informasi dan kekuasaan.

2.16 KONSEKUENSI HUKUM DARI QIT

Mengingat pemeriksaan ekstensif sebelumnya tentang bagaimana sifat mekanika kuantum yang unik dari QIT memengaruhi pemrosesan informasi dan cara sistem fisik berevolusi, pertanyaan dari perspektif hukum adalah apakah dan bagaimana kita dapat mengkarakterisasi dampak QIT dari perspektif hukum dan tata kelola. Kami menguraikan sejumlah tema utama yang akan diuraikan lebih lanjut di bagian-bagian selanjutnya.

Yurisprudensi dan Interpretasi

Dalam yurisdiksi hukum umum, prinsip-prinsip yurisprudensi terutama berasal dari campuran preseden hukum dan sumber konstitusional. Interpretasi dampak teknologi baru biasanya dilakukan dengan latar belakang doktrin yang telah lama ada yang mengasumsikan

pandangan klasik dan deterministik tentang objek dan fakta yang diajukan ke pengadilan. Teknologi informasi kuantum, sebaliknya, bertumpu pada fenomena seperti superposisi dan keterikatan, yang menantang asumsi klasik bahwa fakta hukum hanyalah ketidakpastian epistemik. Sifat probabilistik yang melekat pada mekanika kuantum, yang dibuktikan oleh Teorema Bell dan prinsip tanpa kloning, menunjukkan bahwa beberapa konsep hukum seperti mengaitkan keadaan tertentu dengan satu penyebab yang pasti mungkin perlu dievaluasi ulang. Meskipun pengadilan masih dapat menerapkan kerangka kerja prosedural yang ada, debat yurisprudensi di masa depan mungkin akan mengeksplorasi bagaimana non-lokalitas atau stokastisitas yang tidak dapat direduksi mengubah penentuan sebagian akibat, tanggung jawab, atau bukti faktual. Untuk mempersiapkan diri, para pembuat undang-undang dan badan peradilan dapat mengeluarkan panduan interpretatif, menekankan bahwa fenomena kuantum tetap dapat diadili tetapi mungkin memerlukan pendekatan pembuktian atau konseptual yang disesuaikan ketika proses yang saling terkait menjadi masalah.

Hukum Pembuktian

Bukti kuantum secara inheren lebih rapuh karena kolaps yang diinduksi pengukuran dan teorema tanpa kloning, yang berarti protokol rantai pengawasan dan otentikasi standar yang dirancang untuk data digital klasik mungkin tidak berlaku. Untuk memvalidasi atau mereplikasi hasil yang dihasilkan kuantum, seseorang harus bergantung pada persiapan keadaan berulang dan pemeriksaan keluaran probabilistik, sehingga pendekatan sampel yang sama secara konvensional menjadi tidak mungkin. Pengadilan dapat mensyaratkan prosedur khusus misalnya, log tomografi kuantum, catatan koreksi kesalahan untuk menetapkan keaslian berdasarkan aturan yang mirip dengan aturan pembuktian. Seiring waktu, reformasi mungkin mencakup metode atau pedoman forensik kuantum dan akreditasi khusus untuk saksi ahli kuantum untuk mengatasi efek, jika ada, dari stokastisitas yang tidak dapat direduksi dan keandalan pengukuran kuantum yang digunakan sebagai bukti dalam proses perdata dan pidana.

Di Amerika Serikat, aturan untuk menerima dan mengautentikasi bukti terutama terdapat dalam Aturan Bukti Federal 28 U.S.C. Ketentuan utama yang mungkin dipengaruhi oleh QIT meliputi bagaimana data diautentikasi Aturan 901 (autentikasi) dan bagaimana informasi diberikan secara pembuktian Aturan 1001–1008 (tulisan asli, rekaman, dan foto). Terdapat juga pertanyaan terbuka mengenai bagaimana QIT diterapkan pada standar keandalan yang telah ditetapkan untuk bukti ilmiah. Di Uni Eropa dan Inggris, aturan bukti sebagian besar tetap berada dalam kode prosedur perdata atau pidana nasional (misalnya, Undang-Undang Bukti Perdata 1995 di Inggris), tetapi dibentuk oleh prinsip-prinsip keadilan dan keandalan yang menyeluruh. Dalam setiap kasus, bagaimana penggunaan QIT dapat memengaruhi atau memiliki konsekuensi bagi proses pembuktian masih belum dipelajari.

Kekayaan Intelektual

Inovasi khusus kuantum seperti arsitektur qubit yang tahan terhadap kesalahan atau protokol berbasis keterikatan dapat mempersulit doktrin kekayaan intelektual klasik, khususnya berdasarkan Pasal 35 U.S.C. seperti spesifikasi dan pengaktifan (35 U.S.C. § 112) dan kemampuan paten inventif (35 U.S.C. §§ 101–103), karena sistem kuantum bersifat

probabilistik dan dalam kasus tertentu sulit untuk direplikasi atau dijelaskan dalam istilah klasik yang stabil. Meskipun demikian, fakta bahwa sejumlah besar paten QIT telah diberikan menunjukkan bahwa dalam praktiknya kesulitan tersebut mungkin tidak menjadi hambatan yang signifikan.

Prinsip larangan kloning dapat menimbulkan masalah pada asumsi umum tentang penyalinan dan pengungkapan, terutama dalam konteks rahasia dagang di mana pengadilan biasanya memerlukan bukti bahwa informasi kepemilikan telah disalin atau diperoleh secara tidak sah. Pemeriksa paten dan pengadilan mungkin memerlukan pedoman khusus untuk menentukan bagaimana algoritma dan perangkat keras kuantum memenuhi persyaratan pengungkapan, kepastian, dan kegunaan. Seiring waktu, standar pengungkapan eksplisit untuk fenomena mekanika kuantum mungkin perlu dipertimbangkan untuk memastikan penerapan hukum yang konsisten.

Kasus hukum yang mengatur apakah klaim yang diimplementasikan komputer atau algoritmik dianggap sebagai ide abstrak belum mempertimbangkan pertanyaan tentang algoritma kuantum itu sendiri, meskipun pada prinsipnya kita seharusnya mengharapkan prinsip yang sama atau serupa untuk diterapkan. Hukum relevan lainnya yang dampaknya mungkin memerlukan pertimbangan dalam hal QIT termasuk rahasia dagang yang dilindungi berdasarkan 18 U.S.C. §§ 1831–1839 (terkait dengan spionase ekonomi) dan undang-undang serupa. Di Uni Eropa, kemampuan dipatenkan diatur dalam Konvensi Paten Eropa (Pasal 52–57), sementara rahasia dagang diselaraskan oleh Direktif (UE) 2016/943. Inggris juga mengikuti Undang-Undang Paten 1977 dan hukum umum tentang pelanggaran kerahasiaan.

Privasi dan Kerahasiaan

Komunikasi kuantum dan penyimpanan data kuantum menghadirkan isu-isu baru bagi rezim perlindungan data, khususnya karena keadaan saling terkait dan tidak adanya kloning dapat mencegah proses replikasi dan pencadangan standar yang diasumsikan oleh peraturan. Aturan lokalisasi data juga rumit jika data kuantum terdelokalisasi atau tersebar di berbagai node saling terkait di yurisdiksi yang berbeda. Regulator mungkin perlu mengklarifikasi bagaimana informasi kuantum yang tidak terukur (disimpan dalam qubit) diklasifikasikan misalnya, apakah itu harus dianggap sebagai data pribadi sebelum pengukuran? Seiring perkembangan QIT, para legislator mungkin menetapkan jangka waktu migrasi untuk enkripsi pasca-kuantum dan mengembangkan definisi atau kerangka hukum untuk menangani keadaan kuantum yang tidak berwujud berdasarkan undang-undang privasi. Undang-undang privasi dan perlindungan data di Amerika Serikat sebagian besar bersifat sektoral. Seiring QIT meluas ke bidang-bidang seperti keuangan dan sektor konsumen (misalnya, sejumlah lembaga keuangan saat ini memiliki divisi pembelajaran komputasi kuantum), undang-undang yang ada mungkin berlaku untuk penggunaan QIT. Contohnya termasuk Undang-Undang Portabilitas dan Akuntabilitas Asuransi Kesehatan (HIPAA), Undang-Undang Gramm-Leach-Bliley untuk data keuangan, dan undang-undang tingkat negara bagian seperti Undang-Undang Privasi Konsumen California. Di Uni Eropa, perlindungan data diatur oleh Peraturan Perlindungan Data Umum (GDPR), Peraturan (UE) 2016/679, sementara Inggris mengikuti Undang-Undang Perlindungan Data 2018 dan Peraturan Perlindungan Data Umum Inggris. Konsekuensi

penggunaan QIT berdasarkan undang-undang ini belum sepenuhnya dipelajari, termasuk dalam kaitannya dengan kewajiban keamanan siber. Demikian pula, Undang-Undang AI Uni Eropa juga memiliki dampak terhadap penggunaan QIT, terutama dalam konteks pembelajaran mesin dan optimasi yang dilakukan menggunakan sistem kuantum.

Hukum Persaingan

Potensi percepatan eksponensial komputasi kuantum dan hambatan modal yang signifikan terhadap pengembangannya dapat memungkinkan segelintir entitas yang didanai dengan baik untuk mendominasi infrastruktur QIT yang penting, sehingga menimbulkan kekhawatiran akan konsentrasi kekuatan pasar. Otoritas persaingan mungkin menghadapi tantangan dalam mendefinisikan pasar yang relevan untuk perangkat keras kuantum atau perangkat lunak kuantum di mana hanya sedikit substitusi yang ada. Komunikasi yang diamankan secara kuantum juga dapat membatasi kemampuan regulator untuk mendeteksi pertukaran kolusif jika enkripsi kebal terhadap pemantauan standar. Reformasi di masa mendatang mungkin melibatkan pedoman merger khusus yang mencakup akuisisi R&D kuantum atau pendekatan baru untuk mendefinisikan pasar inovasi di QIT. Kerja sama internasional antar otoritas persaingan dapat membantu mencegah konsolidasi anti-persaingan kekayaan intelektual kuantum, terutama di mana keterikatan lintas batas atau aliran data membingungkan aturan yurisdiksi tradisional. Hal ini dapat menimbulkan dampak berdasarkan hukum antimonopoli AS seperti Undang-Undang Sherman, Undang-Undang Clayton, dan Undang-Undang Komisi Perdagangan Federal. Di Uni Eropa, aturan persaingan berasal dari Pasal 101 dan 102 TFEU, yang mengatur kartel dan penyalahgunaan dominasi, dilengkapi dengan Peraturan Penggabungan Uni Eropa (Peraturan Dewan (EC) No 139/2004). Undang-Undang Persaingan Inggris 1998 dan Undang-Undang Perusahaan 2002 mengatur isu-isu paralel pasca-Brexit. Dalam setiap kasus, efek informasi dari QIT berada pada tingkat yang lebih tinggi dalam hal tumpukan tata kelola dengan regulasi yang secara tidak langsung berdampak pada penggunaan QIT daripada diarahkan pada, misalnya, lapisan sirkuit kuantum.

Hukum Internasional Publik

Teknologi seperti dekripsi kuantum dan penginderaan kuantum dapat menggeser keseimbangan strategis, melemahkan keamanan kriptografi klasik yang digunakan oleh negara-negara. Untuk tujuan ini, praktik negara dapat berkembang untuk menafsirkan penggunaan kekuatan dan tanggung jawab negara dengan cara yang mencakup serangan siber berbasis kuantum, terutama jika alat kuantum menyebabkan gangguan di dunia nyata atau membahayakan sistem keamanan nasional. Pertanyaan yurisdiksi juga muncul jika negara-negara yang terlibat mencakup beberapa wilayah, sehingga tidak jelas otoritas hukum atau kedaulatan negara mana yang terlibat. Seiring waktu, perjanjian baru atau amandemen terhadap kerangka kerja keamanan siber atau pengendalian senjata yang ada mungkin secara eksplisit membatasi penggunaan QIT sebagai senjata. Demikian pula, versi mendatang dari Manual Tallinn dapat memasukkan pedoman tentang spionase berbasis kuantum, sabotase, atau ambang batas eskalasi konflik. Hukum internasional publik terutama berasal dari Piagam PBB (1945), praktik negara kebiasaan, dan perjanjian yang mencakup keamanan dan konflik, seperti rezim pengendalian senjata. Rezim relevan lainnya dengan konsekuensi terhadap

penggunaan QIT mungkin termasuk Konvensi Budapest tentang Kejahatan Siber yang memandu aktivitas siber transnasional tertentu, meskipun belum secara khusus membahas QIT. Masalah-masalah ini dibahas secara mendalam dalam bagian selanjutnya.

Penggunaan Ganda dan Kontrol Ekspor

Kemampuan QIT seperti keterikatan (*entanglement)* dapat mengaburkan definisi tradisional transfer, seperti halnya batasan tanpa kloning pada kuantum, yang dapat mempersulit apakah keadaan kuantum tak berwujud itu sendiri merupakan ekspor. Keterikatan lintas batas juga dapat berfungsi sebagai saluran untuk informasi kuantum tanpa pengiriman data klasik. Daftar legislatif yang ada di bawah Daftar Kontrol Perdagangan atau peraturan Uni Eropa yang setara mungkin memerlukan amandemen yang lebih spesifik untuk mencakup perangkat keras kuantum (chip superkonduktor, perangkap ion, perangkat fotonik khusus) dan perangkat lunak atau protokol enkripsi yang relevan.

Koreksi kesalahan kuantum, yang dapat menutupi atau mengompres data sensitif, juga dapat menghambat inspeksi dengan cara yang belum dipertimbangkan oleh rezim penggunaan ganda dan kontrol ekspor. Para pembuat kebijakan dapat mengembangkan rezim perizinan khusus untuk R&D kuantum, sementara badan-badan multilateral dapat mengadopsi kategori yang lebih rinci untuk QIT untuk memastikan kejelasan tentang ekspor mana yang memerlukan otorisasi sebelumnya atau tunduk pada kontrol khusus. Di Amerika Serikat, Undang-Undang Reformasi Pengendalian Ekspor (50 U.S.C. §§ 4801–4826) dan Peraturan Administrasi Ekspor (EAR) pada 15 C.F.R. §§ 730–774 mengatur ekspor komersial dan ekspor barang dwiguna. Pengendalian ekspor sudah berlaku untuk QIT di AS.152 Uni Eropa memberlakukan pengendalian barang dwiguna terutama melalui Peraturan (EU) 2021/821, dan Inggris mengikuti Undang-Undang Pengendalian Ekspor 2002 dan Peraturan Pengendalian Ekspor selanjutnya.

Ilmu Hayati

Komputasi kuantum menjanjikan jalan baru untuk pemodelan molekuler, penemuan obat, dan pengobatan presisi, tetapi menimbulkan pertanyaan tentang reproduktivitas jika hasilnya bergantung pada keluaran qubit probabilistik. Regulator dapat mensyaratkan tingkat kesalahan yang terdokumentasi, protokol mitigasi kebisingan, dan validasi silang melalui simulasi klasik atau data laboratorium. Sensor kuantum khususnya titik kuantum menawarkan diagnostik ultra-presisi atau pengiriman obat yang ditargetkan, yang memicu klasifikasi perangkat medis. Peraturan yang ada mungkin perlu memperbarui definisi untuk validitas analitik atau evaluasi klinis ketika fenomena kuantum digunakan. Seiring waktu, dokumen panduan khusus dapat membahas uji coba in silico berbasis kuantum, memastikan bahwa hasilnya selaras dengan standar Praktik Klinis yang Baik atau Praktik Manufaktur yang Baik terlepas dari kompleksitas keterikatan dan tidak adanya kloning. Di Amerika Serikat, Undang-Undang Pangan, Obat, dan Kosmetik serta peraturan FDA terkait mengatur farmasi, biologi, dan perangkat medis. Penggunaan QIT dapat menimbulkan sejumlah konsekuensi atau memotivasi respons legislatif berdasarkan undang-undang ini. Pedoman Perangkat Lunak sebagai Perangkat Medis (SaMD) menyediakan jalur untuk diagnostik berbasis algoritma, yang mungkin dapat diadaptasi untuk mencakup pembelajaran mesin kuantum, bergantung lagi

pada apakah pertanyaan *sui generis* dijawab secara afirmatif. Di Uni Eropa, instrumen kuncinya adalah Peraturan Perangkat Medis (EU) 2017/745 dan Peraturan Diagnostik In Vitro (EU) 2017/746, yang diberlakukan oleh otoritas kompeten nasional. Inggris Raya bergantung pada Undang-Undang Obat dan Perangkat Medis 2021 dan panduan MHRA, yang mencerminkan reformasi pra dan pasca-Brexit. Dalam setiap kasus, dampak QIT pada regulasi ilmu hayati masih baru dan terbatas.

Standar Internasional

Tidak seperti sistem klasik, perangkat kuantum menunjukkan stokastisitas inheren, sehingga protokol keandalan dan koreksi kesalahan memerlukan metrik yang berbeda. Standar kuantum menyediakan sarana prospektif untuk pengembangan protokol tersebut. Standardisasi definisi untuk toleransi kesalahan atau fidelitas qubit dapat membantu regulator dan pasar membandingkan perangkat keras dari vendor yang berbeda. Demikian pula, kekuatan kriptografi harus beradaptasi dengan kemampuan kuantum untuk memecahkan kunci klasik, mendorong standar seperti yang dikeluarkan oleh NIST untuk PQC dan oleh ISO/IEC untuk metode yang aman terhadap kuantum. Ke depannya, kerja sama antara ISO, IEC, IEEE, NIST, dan ETSI dapat mencegah fragmentasi atau protokol yang saling bertentangan. Dalam praktiknya, sertifikasi QIT baru atau yang direvisi dapat membahas anggaran kesalahan kuantum, proses pengukuran, dan interoperabilitas untuk jaringan kuantum, memastikan keamanan yang kuat dan kinerja yang dapat diprediksi di berbagai arsitektur kuantum. ISO dan IEC menghasilkan standar teknis internasional, banyak yang relevan dengan teknologi informasi dan komunikasi. Di bidang yang berkaitan dengan kuantum, ISO/IEC 18033–6 (kriptografi kuantum) dan standar prospektif lainnya di bawah Komite Teknis Bersama 1 (JTC 1) membahas kriptografi yang aman terhadap kuantum. Di Amerika Serikat, *National Institute of Standards and Technology* (NIST) memimpin proyek standardisasi kriptografi pasca-kuantum (seperti yang disebutkan di atas), menerbitkan draf untuk algoritma tahan kuantum. Kelompok Spesifikasi Industri ETSI (*European Telecommunications Standards Institute*) Eropa tentang Distribusi Kunci Kuantum (ISG QKD) juga mengembangkan standar komunikasi kuantum.

Kotak Pasir Regulasi

Seperti yang telah dibahas, fitur unik QIT dibandingkan dengan teknologi klasik output stokastik, tanpa kloning, keterikatan dapat mempersulit persetujuan regulasi standar, sehingga kotak pasir menjadi menarik untuk eksperimen terkontrol. Regulator dapat mengesampingkan persyaratan preskriptif tertentu untuk sementara waktu, memungkinkan pengembang kuantum untuk mendemonstrasikan kinerja dunia nyata sambil mendokumentasikan log koreksi kesalahan atau fidelitas pengukuran. Isu-isu seperti tanggung jawab atas kesalahan kuantum yang tak terduga atau pengamanan data pribadi (jika analitik kuantum digunakan untuk data kesehatan atau keuangan) dapat diuji dengan risiko publik minimal. Di masa depan, sandbox kuantum khusus mungkin mencakup pengawasan multi-regulator misalnya, melibatkan otoritas kontrol ekspor, komisioner perlindungan data, dan regulator kesehatan untuk memastikan bahwa efek kuantum yang tak terduga dipantau secara komprehensif. Melalui pengujian adaptif tersebut, para pembuat kebijakan dapat menyempurnakan definisi

hukum dan strategi penegakan hukum sebelum QIT diterapkan dalam skala besar. Sandbox regulasi biasanya muncul dari lembaga yang berorientasi pada inovasi, bukan dari satu kode legislatif tunggal. Contoh yang sebanding di Amerika Serikat yang dapat digunakan sebagai model sandboxing QIT termasuk uji coba yang dijalankan oleh Biro Perlindungan Keuangan Konsumen (CFPB) (misalnya, menguji penggunaan komputasi kuantum dengan data keuangan konsumen yang sensitif). Otoritas Pengawas Keuangan Inggris (FCA) mendirikan sandbox pada tahun 2016 untuk menguji produk keuangan inovatif dalam lingkungan terkontrol, dan Kantor Komisioner Informasi (ICO) menjalankan sandbox perlindungan data berdasarkan Undang-Undang Perlindungan Data 2018. Keduanya dapat diadaptasi dalam kasus penggunaan QIT di sektor-sektor ini.

2.17 TUMPUKAN TATA KELOLA QIT

Gambaran Umum

Pada bagian sebelum terakhir ini, kami menyajikan contoh ilustratif tentang bagaimana pendekatan tumpukan tata kelola dapat membantu memeriksa instrumen regulasi yang tepat untuk memetakan hasil pemangku kepentingan ke implementasi teknis. Seperti yang dapat dilihat, tumpukan yang terintegrasi secara vertikal (skala terkecil di atas) mewakili lapisan komponen dalam komputer kuantum yang ditopang oleh antarmuka lapisan aplikasi. Tumpukan horizontal dirancang untuk mengilustrasikan alur kerja mainan di mana QIT merupakan komponennya. Kedua konstruksi ini dapat digunakan untuk memetakan instrumen tata kelola ke tingkat yang sesuai dalam tumpukan. Idenya adalah bahwa mereka memungkinkan cara untuk memetakan instrumen tata kelola yang ada ke kemungkinan kasus penggunaan QIT. Metode ini juga dapat digunakan untuk tujuan penilaian risiko, dan oleh karena itu berguna untuk memeriksa respons regulasi baru atau inovatif yang mungkin diperlukan untuk mengatasi risiko tersebut. Contoh sederhana yang kami gunakan diambil dari ilmu hayati di mana QIT berpotensi diterapkan untuk penemuan obat kimia, penginderaan kuantum, dan bahkan komunikasi kuantum data sensitif. Dalam contoh ini, kami mengasumsikan QIT digunakan di sejumlah tempat dalam alur kerja horizontal di bawah ini.

Tumpukan Horizontal

Contoh tumpukan teknis horizontal dengan instrumen tata kelola terkait ada di bawah ini. Kami menetapkan urutan tahapan satu yang melibatkan QIT, satu yang tidak melibatkan QIT dan instrumen tata kelola yang relevan.

Untuk Tahap 1, pembuatan obat farmasi dimulai dengan proses desain yang pada prinsipnya dapat melibatkan penggunaan QIT. Pertimbangan penggunaan ganda mungkin sudah berlaku sebelum pertimbangan tata kelola ilmu hayati muncul. Untuk kasus patokan, tidak akan ada pertimbangan penggunaan ganda kuantum (meskipun mungkin masalah penggunaan ganda AI atau ilmu hayati dapat muncul).

Pada Tahap 2, komputasi kuantum QIT dapat digunakan untuk simulasi bahan kimia baru yang standar bioinformatika di bawah FDA atau pedoman terkait mungkin berlaku. Pada Tahap 3 di mana produk farmasi diproduksi, persyaratan Proses Manufaktur yang Baik (*Good*

Manufacturing Process/GMP) FDA154 mungkin berlaku dengan cara yang memerlukan adaptasi bagi operator QIT.

Untuk Tahap 4, uji klinis yang menggunakan teknologi penginderaan titik kuantum mungkin harus mematuhi aturan uji klinis dan peraturan nanoteknologi dalam ilmu hayati. Terakhir, pada Tahap 5, pemantauan dan distribusi teknologi yang relevan, seperti ke pusat manufaktur asing, mungkin memerlukan cara untuk menghubungkan data yang diperoleh dari pemantauan kembali ke proses QIT dan pertimbangan konsekuensi pengendalian ekspor. Kami menyajikan Tabel 2.4 di bawah ini yang merangkum proses alur kerja.

Tabel 2.4 Susunan horizontal yang membandingkan alur kerja dengan dan tanpa QIT

Instrumen Tata Kelola	Persyaratan penggunaan ganda	FDA Standar Bioinformatika	Prosedur manufaktur yang baik menurut FDA	Peraturan Uji Klinis FDA Peraturan Nanoteknologi	FDA Peraturan distribusi dan pemantauan Kontrol ekspor
Tahap alur kerja tanpa QIT (tolok ukur)	**Tahap 1** Desain produk farmasi menggunakan komputer klasik	**Tahap 2** Simulasi terbatas untuk sintesis kimia	**Tahap 3** Sintesis produk farmasi dengan sensor klasik	**Tahap 4** Uji klinis yang melibatkan proses data klasik	**Tahap 5** Distribusi komersial
Tahap alur kerja dengan QIT	**Tahap 1** Desain produk farmasi menggunakan QIT	**Tahap 2** Simulasi kuantum untuk sintesis kimia	**Tahap 3** Sintesis produk farmasi dengan sensor kuantum	**Tahap 4** Uji klinis yang melibatkan titik kuantum	**Tahap 5** Distribusi komersial

Pada setiap Tahap di mana QIT digunakan, kita dapat membuat susunan vertikal yang mengidentifikasi di mana dalam susunan tersebut instrumen tata kelola yang berbeda mungkin relevan. Kami menggunakan komputasi kuantum dalam alur kerja ini pada Tahap 2 sebagai contoh dan menyajikan contoh susunan tata kelola dalam Tabel 2.5 di bawah ini.

Tabel 2.5 Tumpukan tata kelola yang menunjukkan instrumen tata kelola mana yang dapat diterapkan pada tingkat mana dalam tumpukan teknologi vertikal

Lapisan	**Kepentingan/Kewajiban Pemangku Kepentingan**	**Efek Informasi**	**Tata Kelola**
Lapisan Sirkuit Kuantum	Standar rekayasa dan jaminan mutu nasional dalam bioinformatika memberlakukan persyaratan pada sirkuit	Pemrosesan informasi dengan cara baru memanfaatkan gerbang kuantum	Instrumen
Lapisan Pengukuran dan Kontrol	Pemangku kepentingan memerlukan tingkat	Cara-cara baru dalam pengkodean,	Standar teknis terkait sirkuit kuantum

	kontrol untuk memastikan algoritma kuantum diimplementasikan dengan benar dan tidak digunakan untuk tujuan yang merugikan	pengendalian, dan pengukuran data	
Lapisan Koreksi Kesalahan	Otoritas pengatur memerlukan jaminan mengenai ambang batas koreksi kesalahan untuk penggunaan QIT dalam memproses data kesehatan atau keamanan yang berisiko tinggi	Persyaratan untuk komputasi kuantum yang toleran terhadap kesalahan mungkin berarti diperlukan komputasi homomorfik yang berbeda dari komputasi klasik	Perjanjian internasional yang membatasi QIT untuk tujuan ofensif yang mensyaratkan inspeksi kerangka kerja QIT
Bahasa Pemrograman Kuantum	Pengembang dalam alur kerja terintegrasi memerlukan pipeline CI/CD yang kuat dan pengujian unit untuk memastikan sistem komputasi yang melibatkan QIT yang mungkin mencakup informasi berlisensi pihak ketiga	Bahasa pemrograman kuantum (biasanya klasik) juga dapat digunakan	Regulator yang mensyaratkan konfirmasi tingkat kesalahan dalam komputasi kuantum yang menjadi dasar simulasi
Lapisan Aplikasi	Pengguna yang menggunakan cloud kuantum, data kuantum, atau layanan serupa lainnya untuk menyimpan informasi sensitif dalam konteks kriptografi pasca-kuantum	Teknologi Informasi Kuantum (QIT) dapat membuka jalan bagi algoritma baru, misalnya instruksi untuk mensintesis bahan kimia atau obat baru	Sistem pemantauan atau instrumen hak cipta yang mengatur penggunaan dan implementasi kode seperti lisensi sumber terbuka
Lapisan Antarmuka Klasik	QIT digunakan oleh pemangku kepentingan untuk komunikasi jarak jauh untuk infrastruktur kritis	QIT memungkinkan komputasi yang dapat diskalakan dengan cara yang mengatasi keterbatasan termodinamika	Perundang-undangan yang mensyaratkan pengujian dan jaminan yang kuat terhadap sistem kriptografi pasca-kuantum

2.18 INTEGRASI TATA KELOLA QIT

Dalam bagian ini, kami telah meletakkan dasar untuk memahami persimpangan teknologi informasi kuantum (QIT) dan hukum, menekankan potensi transformatif komputasi, komunikasi, dan penginderaan kuantum sambil membahas tantangan tata kelola uniknya. Dengan mengkontekstualisasikan QIT dalam evolusi historisnya dari pemanfaatan efek kuantum secara insidental pada revolusi kuantum pertama hingga pemanfaatan superposisi, keterikatan, dan non-lokalitas yang direkayasa pada revolusi kuantum kedua kami telah menguraikan keadaan modern teknologi ini, yang sebagian besar masih berupa prototipe namun siap untuk memberikan dampak ekonomi, strategis, dan sosial yang mendalam. Kontribusi kami bertujuan untuk memajukan wacana tentang tata kelola QIT dalam beberapa cara.

Pertama, kami melakukan pemeriksaan yurisprudensi teknis, meneliti rezim hukum yang ada seperti kontrol ekspor, standar kriptografi pasca-kuantum, dan peraturan khusus sektor dan mengevaluasi bagaimana rezim tersebut beririsan dengan kemampuan baru QIT, termasuk kemampuan dekripsi dan pengukuran ultra-presisi. Kedua, kami mengeksplorasi ontologi kuantum hukum, mengungkapkan bagaimana ketidakpastian, non-lokalitas, dan sifat probabilistik yang melekat pada sistem kuantum menantang asumsi hukum klasik tentang observabilitas, identitas, dan determinisme, tanpa membuat QIT tidak dapat diatur. Ketiga, kami memperkenalkan dan mengadaptasi model tumpukan tata kelola, mengintegrasikan komponen vertikal (perangkat keras hingga keluaran) dan horizontal (alur kerja) dengan taksonomi informasi untuk memetakan instrumen peraturan secara tepat ke lapisan teknis, memfasilitasi penilaian risiko dan penyelarasan pemangku kepentingan. Pendekatan ini menggarisbawahi perlunya kekhususan dalam tata kelola, khususnya untuk teknologi strategis dan penggunaan ganda, sambil menganjurkan kerangka kerja yang berpusat pada risiko yang menyeimbangkan inovasi dengan langkah-langkah pengamanan.

Menyatukan elemen-elemen ini melalui lensa informasi (yaitu, memperlakukan QIT sebagai sistem pemrosesan informasi fundamental) menjembatani domain teknis dan yurisprudensi, memungkinkan pemeriksaan yang lebih jelas tentang dampak pada privasi, verifikasi, kekayaan intelektual, dan keseimbangan geopolitik. Meskipun QIT sebagian besar berada di bawah kerangka kerja yang ada, kualitas uniknya mungkin memerlukan adaptasi yang ditargetkan untuk memastikan akses yang adil, mengurangi ketidakseimbangan, dan mendorong penerapan yang bertanggung jawab. Seiring dengan kematangan QIT, kajian di masa mendatang tentang tata kelolanya dapat membantu para pembuat kebijakan, akademisi, dan praktisi untuk secara proaktif membentuk tata kelola yang memanfaatkan potensi QIT sekaligus melindungi dari risikonya.

2.19 TEORI PEMROSESAN INFORMASI KLASIK DAN KUANTUM

Kami secara singkat menyajikan ringkasan karakteristik teoritis dan praktis utama (termasuk pertimbangan perangkat lunak dan perangkat keras) dari teori informasi kuantum. Fokus dalam Lampiran ini adalah pada karakterisasi informasi teknologi kuantum. Seperti yang akan kami singgung, semua teknologi dapat dengan mudah dibingkai sebagai bergantung pada

mekanika kuantum karena semua fisika bergantung pada hukum mekanika kuantum. Dalam fisika, teori klasik tentang dunia adalah bagian dari teori kuantum yang lebih luas (seperti teori medan dan sejenisnya) teori klasik terkadang digambarkan sebagai kasus batas dari teori kuantum yang lebih umum. Pada tingkat yang lebih rinci, fenomena mekanika kuantum sangat penting bagi materi pelajaran ilmu hayati dan bidang terkait, seperti kimia organik, keadaan dan sintesis protein dan molekul, proses seluler dan struktur organisme, serta pensinyalan biokimia.

Sebaliknya, kami mempersempit fokus kami pada efek dan dinamika kuantum dalam istilah informasi, di mana teknologi kuantum tertentu yang diminati memenuhi beberapa peran pemrosesan informasi. Untuk komputasi kuantum, ini adalah pemrosesan data yang dikodekan dalam keadaan kuantum dan berevolusi sesuai dengan hukum mekanika kuantum, seperti dalam simulasi kimia kuantum untuk penemuan obat. Untuk komunikasi kuantum, ini adalah penggunaan sumber daya kuantum seperti keterikatan untuk memfasilitasi komunikasi atau untuk memungkinkan aktivitas kriptografi seperti distribusi kunci kuantum (penting untuk mengamankan data ilmu hayati dalam skenario pasca-kuantum) yang relevan dengan ilmu hayati. Untuk penginderaan kuantum, ini melibatkan bagaimana teknologi kuantum seperti titik kuantum digunakan, baik dengan cara tertanam dalam perangkat atau secara eksogen, untuk memperoleh informasi melalui pengukuran yang sangat detail. Memahami latar belakang teoretis pemrosesan informasi kuantum sangat penting untuk mengidentifikasi tumpukan teknologi kuantum yang relevan yang dapat diterapkan pada penggunaan setiap bentuk QIT dalam ilmu hayati. Yang penting, dengan melakukan hal tersebut, kita memperoleh kejelasan tentang apa yang berbeda dan apa yang tetap sama, dari sudut pandang teknis dan tata kelola, ketika QIT digunakan dalam kegiatan ilmu hayati. Hal ini pada gilirannya menginformasikan respons regulasi dengan mempertimbangkan tujuan yang ingin dicapai, baik itu mendorong inovasi, meningkatkan hasil ilmu hayati, atau mengelola potensi risiko negatif. Kami memulai ringkasan teoretis kami di bawah ini dengan rangkuman singkat prinsip-prinsip utama teori pemrosesan informasi klasik, diikuti dengan diskusi tentang fitur-fitur pembeda teori pemrosesan informasi kuantum.

Pemrosesan Informasi Klasik

Prinsip-prinsip Pemrosesan Informasi

Biasanya, dalam ilmu komputasi klasik, komputasi diekspresikan secara stateful, di mana fenomena yang diminati dijelaskan menggunakan state, yang secara abstrak dianggap sebagai kumpulan atau himpunan deskripsi, misalnya metrik tertentu atau bahkan proposisi, yang menggambarkan sistem yang diminati. Himpunan state diasumsikan mencakup ruang dengan state potensial di mana suatu sistem dapat berada, atau wilayah di ruang yang dapat ditempati sistem tersebut, yang disebut ruang konfigurasinya. Komputasi kemudian didefinisikan secara konseptual menggunakan mesin state terbatas atau lebih lengkap menggunakan formalisme mesin Turing untuk menjelaskan proses komputasi dan kondisi di mana suatu sistem akan berada di dalam atau mengubah state di dalam ruang state.

Representasi komputasi yang paling umum dalam formalisme ini adalah mesin Turing universal, yang mampu menghitung urutan komputasi apa pun. Terdapat representasi

komputasi lain yang dapat dibuktikan pada dasarnya setara dengan formalisme mesin Turing, seperti Proses Keputusan Markov (MDP), sebuah adaptasi dari formalisme mesin Turing dan yang dapat berfungsi sebagai model komputasi umum yang setara dengan mesin Turing. Salah satu representasi komputasi penting yang relevan langsung dengan komputasi kuantum, terutama sistem berbasis qubit, adalah model sirkuit komputasi kuantum di mana komputasi terdiri dari input dan output yang dimediasi oleh gerbang (seperti gerbang logika) yang membentuk pemetaan fungsional antara satu elemen urutan dan elemen berikutnya. Kedua metode tersebut dapat dibuktikan setara dan memiliki kegunaan tergantung pada konteksnya, namun model sirkuit komputasi kuantum cenderung lebih umum digunakan dalam banyak riset komputasi kuantum. Kami membahas kedua formalisme tersebut secara singkat untuk menghubungkannya dengan lanskap pemrosesan informasi kuantum yang lebih luas.

Formalisme mesin Turing adalah model komputasi yang memiliki keadaan. Representasi stateful dimulai dengan konsep abstrak fundamental tentang keadaan yang biasanya berupa kumpulan (n-ple) yang dijelaskan oleh elemen-elemen alfabet, yang mungkin mencakup koordinat, angka fisik yang menggambarkan fenomena, atau secara lebih luas cara merepresentasikan sistem atau objek yang diminati (seperti representasi ruang fase atau konfigurasi dalam fisika). Dalam komputasi klasik, ini adalah informasi yang dikodekan melalui string bit, yang masing-masing mewakili keadaan sistem (dengan setiap bit berupa variabel bernilai biner). Evolusi sistem informasi, bagaimana sistem tersebut berubah seiring waktu, biasanya dikarakterisasi dalam hal transisi (pemetaan atau fungsi transisi) antara keadaan atau dalam formalisme yang ketat, antara string bit (atau register yang merupakan himpunan string bit). Biasanya, dibedakan antara perangkat keras fisik (atau realisasi) pemrosesan informasi atau perangkat komputasi dan representasi abstrak data atau perangkat lunak sebagai konfigurasi dari satu atau lebih keadaan fisik. Dalam konteks komputasi kuantum, dibedakan antara qubit fisik (yang mewakili sistem fisik yang bertindak sesuai dengan aksioma komputasi kuantum) dan qubit logis (informasional) abstrak yang merupakan abstraksi dari banyak qubit, tetapi berperilaku sesuai dengan hukum kuantum.

Dalam ilmu komputasi formal, transisi keadaan dijelaskan menggunakan algoritma yang merinci bagaimana suatu keadaan berevolusi berdasarkan masukan tertentu. Algoritma mewakili prosedur yang efektif, urutan langkah-langkah (yang sifat sekuensialnya memungkinkan untuk dipetakan secara kanonik ke bilangan asli). Kami menjelaskan formalisme ini sedikit lebih detail daripada yang umum dalam konteks tata kelola untuk menggunakannya sebagai cara untuk mengkarakterisasi tata kelola lebih lanjut dalam istilah teori informasi. Formalisasi teori algoritma untuk tujuan kami dapat dibingkai dalam hal model komputasi Turing dan model komputasi sirkuit yang setara (tetapi diformalkan secara berbeda). Mesin Turing mewakili abstraksi dari proses komputasi dan secara formal direpresentasikan sebagai n-tuple $M = \langle Q, \Gamma, b, \Sigma, \delta, q_0, F \rangle$ di mana:

- $Q = \{q_i\}$ adalah himpunan keadaan yang tidak kosong dengan keadaan awal q_0 dan himpunan keadaan akhir $F \subseteq Q$

- Γ adalah himpunan simbol b yang bukan nol yang dilambangkan sebagai alfabet (perhatikan kombinasi simbol atau string membentuk kata-kata yang himpunannya terkadang digambarkan sebagai kosakata)
- $\Sigma \subset \Gamma$ adalah alfabet masukan, himpunan bagian dari alfabet
- $\delta = \frac{Q}{F} \times \Gamma \to Q \times \Gamma \times \{L, R\}$ adalah fungsi transisi (dengan L dan R masing-masing menunjukkan transisi kiri atau kanan, meskipun ini dapat diabaikan dalam bentuk umum, jangan sampai dikacaukan dengan bahasa di bawah ini)

Mesin Turing yang dijelaskan di atas adalah mesin Turing deterministik, yaitu mesin yang Transisi bersifat pasti. Mesin Turing juga dapat bersifat non-deterministik, di mana fungsi transisi bersifat probabilistik (bukan deterministik) dan sistem tersebut dikatakan stokastik. Seringkali, model komputasi lain, seperti Proses Keputusan Markov, digunakan untuk memodelkan sistem dinamis stokastik. Secara klasik, himpunan fungsi yang dapat dihitung oleh mesin Turing disamakan dengan fungsi yang dapat dihitung oleh suatu algoritma, sehingga mesin Turing mewakili formalisasi umum dari proses komputasi. Pernyataan yang menyamakan algoritma dengan mesin Turing ini pada dasarnya merupakan substansi dari *Tesis Church-Turing*.

Dalam teori bahasa formal komputasi, masalah (dan solusi algoritmiknya) dijelaskan dalam hal bahasa L di atas kumpulan simbol (alfabet masukan Σ di atas) yang merupakan himpunan bagian $\Sigma^* \subseteq$ dari simbol terbatas yang dikenal sebagai string (atau kata), misalnya. Untuk bit klasik, ini adalah $\Sigma = \{0, 1\}$ dengan L sebagai himpunan urutan 0 dan 1. Solusi untuk masalah pengambilan keputusan kemudian dapat direpresentasikan sebagai bahasa L. Dalam formalisme mesin Turing, suatu bahasa L dapat diputuskan jika mesin Turing (yaitu algoritma) memasuki keadaan yang sesuai dengan ya atau tidak dengan input x. Secara intuitif, formalisme tersebut kemudian merepresentasikan masalah pengambilan keputusan sebagai masalah klasifikasi.

Dalam ilmu informasi kuantum, lebih umum untuk mengekspresikan dinamika komputasi menggunakan model sirkuit komputasi. Model sirkuit merepresentasikan komputasi melalui gerbang dan kabel. Gerbang melakukan tugas komputasi (merepresentasikan fungsi) sementara kabel merepresentasikan saluran yang mengalirkan informasi antar gerbang. Model sirkuit terdiri dari spesifikasi himpunan input dan output serta urutan perantara kabel dan gerbang yang mungkin paralel. Gerbang logika kemudian diekspresikan secara fungsional sebagai $f: \{0,1\}^m \to \{0,1\}^n$ yang mewakili input berdimensi m bit dan output berdimensi n bit. Berbagai gerbang yang sesuai dengan operasi logika pada bit, seperti AND, OR, NAND, XOR, dan sebagainya membentuk himpunan gerbang yang beroperasi pada input (atau beberapa subsetnya).

Sirkuit biasanya juga dicirikan berdasarkan kedalamannya (seberapa 'panjang' sirkuit tersebut) dan lebarnya (berapa banyak komputasi paralel yang terjadi pada setiap langkah waktu). Kedalaman sirkuit memiliki hubungan penting dengan pertanyaan seputar kemudahan penanganan dan kompleksitas komputasi. Selain bit logis, model sirkuit juga membayangkan penggunaan bit tambahan (*ancilla bit*), yang pada dasarnya merupakan sumber daya cadangan atau tambahan yang terpisah dari sirkuit utama, yang memungkinkan misalnya komputasi

perantara untuk dilakukan atau data untuk disimpan. Qubit tambahan merupakan fitur penting dari formalisme komputasi kuantum dalam praktik dan teori, yang memungkinkan komputasi tertentu dilakukan dengan lebih efisien.

Cakupan masalah yang dapat dihitung oleh suatu model komputasi disebut ekspresibilitasnya, dengan kasus idealnya adalah seluruh himpunan gerbang yang tersedia memungkinkan komputasi arbitrer untuk dilakukan, yang disebut komputasi universal. Dalam komputasi kuantum, orang sering kali memperhatikan apakah gerbang yang dapat dilakukan memungkinkan komputasi kuantum universal, karakteristik penting dari arsitektur yang toleran terhadap kesalahan. Komputasi kuantum universal juga dapat diekspresikan dalam bahasa kontrol kuantum dalam hal menghasilkan keadaan komputasi tertentu. Yang dapat dicapai dengan diberikan serangkaian operasi kuantum, seperti gerbang unitari.

Kesesuaian antara formalisme mesin Turing dan model rangkaian pada dasarnya muncul jika ada mesin Turing yang, dengan masukan tertentu, dapat menghasilkan deskripsi rangkaian komputasi yang dimaksud. Seperti yang ditemukan Turing, beberapa masalah memang tidak dapat dihitung. Masalah yang disebut masalah berhenti (*halting problems*) menunjukkan struktur rekursif atau impredikatif tertentu sehingga tidak berhenti (pada suatu jawaban) jika diberikan input ke algoritma. Lebih lanjut, ada banyak masalah yang pada prinsipnya dapat dihitung dan bahkan dalam kelas kompleksitas tingkat rendah (seperti P di bawah), tetapi dalam praktiknya melebihi sumber daya komputasi yang tersedia atau akan memakan waktu yang sangat lama sehingga membuatnya tidak dapat dipecahkan. Perlu dicatat, seperti yang akan kita singgung di bawah ini, bahwa masalah dalam kelas kompleksitas kuantum pada prinsipnya dapat disimulasikan atau dihitung menggunakan komputer klasik, hanya saja biaya sumber dayanya mungkin eksponensial terhadap input.

Perbedaan antara komputasi klasik dan kuantum dan pembenaran untuk penggunaan komputasi kuantum dalam ilmu hayati bermuara pada efisiensi dan manfaat kemudahan pemecahan masalah yang ditawarkan oleh komputer kuantum. Tetapi apa yang kita maksud dengan istilah-istilah ini? Untuk mendekati masalah ini, mari kita pertimbangkan secara lebih detail bagaimana masalah pemrosesan informasi dikategorikan dan jenis masalah yang ingin dipecahkan oleh pemrosesan informasi. Pemrosesan informasi dalam hal komputasi dapat dibagi menjadi tiga pertanyaan berbeda:

a) *Apakah kelas masalah tersebut bersifat komputasional?* Apakah kelas masalah yang dimaksud merupakan masalah keputusan, yaitu masalah yang dapat dihitung?
b) *Kelas algoritma apa yang dapat menyelesaikan kelas masalah tersebut?* Setelah mengasumsikan suatu masalah bersifat komputasional, pertanyaan kedua menjadi apakah ada algoritma yang dapat menyelesaikan kelas masalah tersebut.
c) *Sumber daya apa yang dibutuhkan untuk menyelesaikan masalah secara optimal?* Dengan asumsi ada satu atau lebih algoritma untuk menyelesaikan masalah, pertanyaan selanjutnya menjadi apa sumber daya minimal (optimal), dalam ruang (energi) atau waktu, untuk menyelesaikan masalah tersebut.

Pertanyaan pertama membahas apakah masalah yang diminati pada prinsipnya dapat dihitung yaitu, apakah komputasi dapat menghasilkan solusi (dengan menerima bahasa solusi L).

Pertanyaan ambang batas ini pada dasarnya diarahkan pada apakah masalah tersebut menunjukkan semacam struktur impredikatif (sehingga dapat mereproduksi struktur masalah penghentian), atau apakah masalah tersebut mungkin tidak tepat atau tidak cukup terdefinisi dengan baik sehingga prosedur komputasi dapat diterapkan.

Pertanyaan kedua pada dasarnya adalah apakah algoritma ada untuk benar-benar menghitung jawabannya. Untuk banyak masalah yang menarik, keberadaan kelas algoritma yang bahkan dapat menyelesaikan masalah tersebut masih belum pasti (seperti untuk masalah Navier-Stokes yang terkenal atau solusi untuk Hipotesis Riemann). Pertanyaan ketiga, yang menyentuh sumber daya komputasi yang dibutuhkan untuk menyelesaikan masalah komputasi, adalah ranah kompleksitas komputasi, sebuah subdisiplin ilmu komputer. Bahkan jika suatu masalah dapat dihitung dan terdapat kelas algoritma untuk menyelesaikannya, biaya sumber daya mungkin sangat mahal, dan meningkat secara tidak berkelanjutan seiring dengan ukuran input. Secara umum, fokus teknologi komputasi dalam ilmu hayati hanya pada masalah yang dapat dihitung, meskipun masalah tersebut mungkin sulit dipecahkan atau kelas algoritmanya sulit ditentukan. Pertanyaan terakhir inilah yaitu kompleksitas komputasi yang memberikan dasar teknis untuk membedakan antara pemrosesan informasi klasik dan kuantum. Kami memberikan ringkasan singkat dari konsep-konsep kunci di bawah ini.

Kompleksitas Komputasi

Perbedaan mendasar antara pemrosesan informasi kuantum dan klasik terletak pada sumber daya komputasi yang berbeda yang dibutuhkan (pada prinsipnya) oleh algoritma kuantum dan klasik untuk menyelesaikan kelas masalah tertentu. Dalam praktiknya, menentukan sumber daya komputasi yang diperlukan dapat menjadi masalah yang sangat menantang. Sekilas, sumber daya dalam ruang, energi, dan waktu yang dibutuhkan untuk menyelesaikan masalah pemrosesan informasi secara komputasi sangat bergantung pada perangkat fisik yang digunakan untuk melakukan komputasi, apalagi desain algoritma dan spesifikasi masalah. Ilmu kompleksitas komputasi mengabstraksikan detail teknis ini (atau di dalam algoritma itu sendiri, misalnya dengan memilih mesin Turing multi-pita daripada tipe pita tunggal) untuk berkonsentrasi pada sifat kompleksitas esensial dari suatu algoritma.

Kompleksitas suatu algoritma direpresentasikan menggunakan notasi asimtotik (atau notasi 'O' besar) yang menggambarkan, secara abstrak, bagaimana kebutuhan sumber daya suatu algoritma dalam menyelesaikan suatu masalah meningkat seiring dengan bertambahnya input ke masalah tersebut. Persyaratan sumber daya diubah menjadi bentuk matematis, intuisinya adalah bahwa persyaratan tersebut dapat diekspresikan sebagai fungsi $f(n)$ dengan ukuran input n misalnya, diberikan n input (bit), waktu eksekusi (dinyatakan dalam satuan waktu) dapat dinyatakan sebagai fungsi $n \rightarrow f(n)$. Notasi Big-O secara klasik menggambarkan, diberikan n input (bit), batas atas waktu eksekusi untuk menerima jawaban dinyatakan sebagai $O(f(n))$. Untuk batas bawah, notasi $\Omega(f(n))$ digunakan untuk menggambarkan biaya sumber daya minimal. Algoritma (hingga faktor-faktor seperti konstanta, dll., dalam hal ini notasi $\Theta(f(n))$ digunakan) kemudian dapat difaktorkan ke dalam kelas berdasarkan bentuk fungsional dari batas kompleksitasnya, sehingga muncul konsep kelas kompleksitas dan,

sebagai hasilnya, kelas kompleksitas tempat masalah dan algoritmanya (sebagai solusi untuk masalah keputusan) dikategorikan.

Klasifikasi ini digunakan untuk menggambarkan efisiensi suatu algoritma sebagai ukuran bagaimana biaya solusi meningkat seiring dengan input. Sebagai contoh, terkadang mungkin ada pertukaran antara jumlah, misalnya, ruang dan waktu yang dibutuhkan suatu algoritma (lebih sedikit ruang tetapi lebih banyak waktu), atau energi dan waktu (seperti yang umum dalam teori kontrol). Perbedaan utama dalam ilmu kompleksitas komputasi untuk mengklasifikasikan algoritma adalah antara algoritma (masalah) yang (i) dapat diselesaikan dalam fungsi polinomial dengan ukuran input n (seiring bertambahnya n, biaya sumber daya tumbuh secara polinomial) dan (ii) hanya dapat diselesaikan dalam fungsi eksponensial (atau super-polinomial, misalnya $n^{\{\log n\}}$) dari n. Hal ini memotivasi perbedaan penting antara masalah yang dapat dipecahkan (masalah yang memiliki algoritma terbaik yang menghasilkan solusi yang membutuhkan sumber daya tidak lebih dari polinomial n) dan algoritma yang tidak dapat dipecahkan yang algoritma terbaiknya membutuhkan sumber daya supra-polinomial atau eksponensial n. Dalam riset kompleksitas komputasi, orang juga menemukan sinonim untuk dapat dipecahkan dalam hal kelayakan atau kemudahan. Kami menggunakan istilah "layak" untuk algoritma yang memecahkan masalah dalam jangka waktu yang bermanfaat bagi manusia, bukan istilah yang lebih formal yang digunakan dalam riset. Perbedaan antara biaya sumber daya polinomial dan eksponensial sangat relevan dengan salah satu proposisi dasar ilmu komputer, yaitu Tesis Church-Turing yang Diperluas yang (dalam bentuk kuatnya) menyatakan bahwa setiap model komputasi yang dapat direalisasikan secara fisik dapat disimulasikan atau direproduksi pada mesin Turing probabilistik dengan peningkatan sumber daya paling banyak polinomial (dalam n).

Dalam notasi kompleksitas formal, kelas kompleksitas sering dilambangkan dengan akronim atau singkatan yang diawali huruf kapital seperti $TIME(f(n))$ di mana, misalnya, masalah yang dapat dipecahkan dalam waktu polinomial dilambangkan TI (untuk k terbatas). Secara formal, himpunan bahasa L dalam $TIME(n^k)$ dikenal sebagai kelas kompleksitas $P = \cup_k TIME(n^k)$ untuk k tetap (sehingga kelas kompleksitas dapat dibingkai sebagai himpunan bahasa atau dalam formulasi intuitif kita, himpunan solusi untuk masalah).

Kelas kompleksitas NP (singkatan dari *non-deterministic polynomial time*) kemudian didefinisikan sebagai himpunan bahasa yang penerimaannya dapat diverifikasi dalam waktu polinomial. Alternatifnya, NP memiliki definisi sebagai himpunan masalah keputusan yang dapat diselesaikan oleh mesin Turing non-deterministik dalam waktu polinomial. Masalah NP-lengkap didefinisikan sebagai masalah dalam NP yang dapat direduksi menjadi semua masalah keputusan lain dalam NP dalam waktu polinomial. Terdapat labirin kelas kompleksitas (kadang-kadang disebut kebun binatang kompleksitas) seperti PSPACE (masalah yang dapat diselesaikan dengan jumlah bit polinomial, bukan ruang) dan EXP (keputusan yang dapat diselesaikan dalam waktu eksponensial, yaitu $O\left(2^{n^k}\right)$ untuk k konstanta) yang diyakini diurutkan dalam hierarki.

Salah satu masalah terbuka mendasar dalam ilmu komputer adalah membuktikan secara formal apakah $P \neq NP$, yaitu apakah ada masalah dalam NP yang tidak ada dalam P.

Asumsi bahwa P dan NP (dan kelas lainnya) tidak setara inilah yang memotivasi pencarian komputasi kuantum. Salah satu aspek penggunaan pemrosesan informasi (klasik atau kuantum) adalah sejauh mana masalah dapat diklasifikasikan secara teridentifikasi ke dalam satu kelas kompleksitas atau lainnya. Meskipun tidak perlu mengetahui kelas kompleksitas tempat suatu algoritma berada untuk, misalnya, mencoba menggunakannya untuk simulasi ilmu hayati, pemeriksaan kompleksitas berguna sebagai cara untuk menentukan perkiraan biaya sumber daya.

Perbedaan teknis antara komputer klasik dan kuantum umumnya dinyatakan dalam hal kelas kompleksitas probabilistik. Probabilitas bahwa mesin Turing probabilistik (non-deterministik) akan menerima atau menolak L dengan benar dan menghasilkan jawaban yang benar dengan probabilitas setidaknya 2/3 dalam waktu polinomial dilambangkan sebagai kelas kompleksitas BPP (*bounded-error probagianilistic polynomial time*). BPP dianggap sebagai klasifikasi yang lebih pragmatis dari komputasi klasik dan pemrosesan informasi klasik. Dalam pengaturan komputasi kuantum, kelas kompleksitas komparatif yang relevan adalah BQP (*bounded-error quantum polynomial time*) yang merupakan himpunan masalah keputusan yang dapat diselesaikan menggunakan algoritma kuantum dalam waktu polinomial dengan probabilitas 2/3 (atau sebaliknya dengan probabilitas kesalahan 1/3). BQP juga dapat didefinisikan dalam hal mesin Turing kuantum yang berbeda dari rekan-rekan klasiknya. Perbedaan antara komputer kuantum dan klasik dalam formulasi ini dibingkai dalam hal BPP sebagai himpunan bagian yang tepat dari BQP, yaitu bahwa $BPP \subset BQP$ meskipun ini belum terbukti secara formal. Perbedaan inilah yang sering digunakan dalam riset teknis sebagai perbedaan utama antara algoritma kuantum dan klasik. Selain itu, karena kelas kompleksitas probabilistik cenderung lebih bermanfaat secara pragmatis, kita sering melihat kelas algoritma dibingkai dalam hal kompleksitas 'kasus terburuk' atau 'rata-rata'.

Perlu diingat apa artinya suatu algoritma dikarakterisasi sebagai kuantum: proses algoritmik (prosedur efektif) harus mencakup langkah-langkah yang unik secara mekanika kuantum. Dengan demikian, meskipun semua algoritma kuantum, seperti yang disebutkan di bawah ini dalam hal pencarian, kriptografi, dan simulasi melibatkan pemrosesan informasi klasik, karakteristik pemrosesan informasi kuantum khusus dari kelas algoritma tersebut pemanfaatan dan ketergantungannya pada superposisi atau keterikatan misalnya yang menimbulkan keunggulan kuantumnya. Ini adalah poin yang berbeda tetapi terkait dengan apakah, mengingat suatu algoritma kuantum, mungkin ada algoritma klasik yang secara efisien memecahkan masalah tersebut. Kita akan membahas pentingnya spesifikasi algoritmik dalam konteks kekayaan intelektual (seperti paten) untuk QIT lebih lanjut.

Sebagai contoh, sejauh metode yang dapat dipatenkan bergantung pada klaim keunggulan kuantum, maka pada prinsipnya mungkin ada argumen normatif bahwa setiap aplikasi paten harus mensyaratkan spesifikasi fitur kuantum unik yang memungkinkan keunggulan tersebut. Kelas kompleksitas BQP pada dasarnya mewakili definisi kerja komputasi kuantum melalui formalisasi kelas kompleksitas (masalah atau bahasa, tergantung pada karakterisasi formal yang dipilih). Perlu dicatat hierarki kelas-kelas tersebut:

$$P \subseteq BPP \subseteq BQP \subseteq \cdots \subseteq PSPACE \subseteq EXP$$

dengan inklusi yang diyakini oleh banyak orang (walaupun tidak terbukti dalam kasus tertentu) sebagai himpunan bagian yang benar-benar tepat. Berdasarkan asumsi ini, hierarki tersebut secara intuitif menunjukkan bahwa meskipun diyakini komputer kuantum pada prinsipnya dapat memecahkan kelas masalah yang lebih luas daripada komputer klasik, masih ada banyak sekali masalah yang bahkan komputer kuantum pun tidak dapat selesaikan atau membuatnya dapat dipecahkan atau layak.

Perbedaan yang diyakini secara luas antara BQP dan BPP pada gilirannya memiliki dampak bagi tesis Church-Turing, yang memerlukan penyesuaian (atau bahkan membatalkannya menurut beberapa sudut pandang) dengan mengganti konsep simulasi pada komputer klasik dengan komputer kuantum. Modifikasi ini dikenal sebagai Church-Turing-Deutsche, yang berpotensi menimbulkan masalah pada rekan klasiknya jika komputer kuantum dapat memecahkan masalah yang tidak dapat dipecahkan secara efisien oleh komputer klasik. Kami menjabarkannya di bawah ini.

- *Tesis Church-Turing*. Setiap fungsi yang dapat dihitung secara efektif (algoritma) dapat dihitung oleh mesin Turing.
- *Tesis Church-Turing yang Diperluas*. Setiap algoritma dapat disimulasikan secara efisien (dengan overhead polinomial paling banyak) menggunakan mesin Turing probabilistik.
- *Tesis Church-Turing-Deutsch Kuantum*. Komputer kuantum universal dapat mensimulasikan sistem fisik terbatas apa pun, yaitu setiap sistem fisik terbatas dapat disimulasikan secara efisien oleh komputer kuantum.

Memahami perbedaan konseptual antara pemrosesan informasi klasik dan kuantum berguna untuk desain algoritma untuk memecahkan masalah dalam ilmu hayati. Hal ini juga berguna untuk menghilangkan mitos tentang pentingnya dan efek sebenarnya dari teknologi pemrosesan informasi kuantum dalam konteks ilmu hayati. Setelah membahas prinsip-prinsip dasar teori komputasi yang memotivasi penggunaan teknologi informasi kuantum, kami menyajikan ringkasan singkat tentang elemen-elemen utama mekanika kuantum dan pemrosesan informasi kuantum serta hubungannya dengan QIT.

2.20 EFEK KATEGORIKAL QIT

Efek Kategorikal

Tabel 2.6 di bawah ini menyajikan pemetaan ringkas dampak informasi utama terhadap bidang hukum dan tata kelola yang penting. Tabel ini mengulangi poin-poin yang dibuat dalam subbagian sebelumnya tetapi mengaturnya untuk referensi cepat dengan penekanan pada pemisahan QIT ke dalam konteks tertanam dan tidak tertanam. Pada prinsipnya, taksonomi di atas dapat disempurnakan secara lebih formal dengan mengadopsi ontologi pemrosesan informasi yang lebih mendasar, seperti teori pembelajaran statistik, teori pembelajaran singular (untuk aplikasi jaringan saraf dalam) atau analog kuantum.

Dalam kasus tersebut, pemrosesan informasi dicirikan oleh metrik atau properti tertentu, seperti yang terkait dengan kinerja (misalnya akurasi) dan generalisasi, waktu

eksekusi atau biaya sumber daya (misalnya dalam hal waktu dan energi), kerugian empiris, kelas kompleksitas (misalnya kelas masalah yang dapat dipecahkan) dan sebagainya. Perubahan pada pemrosesan informasi yang timbul dari penggunaan teknologi kuantum, yang berbeda dari teknologi klasik, kemudian dapat diungkapkan dalam hal perubahan pada metrik ini. Misalnya, penerapan komputer kuantum pada simulasi (misalnya protein, bahan kimia, atau sistem biologis) dapat menyebabkan simulasi dijalankan dengan cara yang lebih efisien (misalnya lebih cepat). Atau, hal itu dapat memungkinkan simulasi komputasi baru (seperti efek molekuler yang berinteraksi dan evolusi) yang saat ini berada di luar jangkauan sumber daya komputasi klasik. Dengan demikian, seseorang kemudian dapat memperkirakan efek QIT dibandingkan dengan rekan-rekan klasiknya, sehingga memungkinkan untuk mengetahui perbedaan spesifiknya.

Tabel 2.6 Efek kategorikal QIT

Efek Kategorikal QIT	
Tidak Tertanam	
Pemrosesan yang efisien	Penggunaan QIT memungkinkan peningkatan pemrosesan informasi dalam ilmu hayati berdasarkan metrik utama, seperti kecepatan, biaya, akurasi, dan sebagainya.
Efek orakel	Penggunaan QIT memungkinkan pemrosesan informasi yang saat ini tidak dapat dilakukan secara klasik (kategoris) untuk dilakukan. Secara teoritis, ini diwakili oleh penyelesaian atau penanganan masalah dalam kelas kompleksitas tingkat tinggi. Kami mengelompokkan dalam kelas ini penggunaan QIT untuk menyelesaikan tugas atau masalah yang, meskipun secara klasik dimungkinkan, secara komputasi tidak layak karena biaya sumber daya (misalnya waktu atau energi).
Asimetri informasi	Penggunaan QIT dapat menyebabkan asimetri informasi yang signifikan di antara para pemangku kepentingan yang memengaruhi keseimbangan ekonomi. Contohnya termasuk teknologi QIT yang memungkinkan keunggulan asimetris dalam kriptografi, atau optimasi, atau peningkatan teknologi.
Tertanam	
Pengukuran	Penggunaan titik kuantum sebagai perangkat penginderaan kuantum yang tertanam dalam perangkat medis atau alat diagnostik sebagai perangkat pengukuran (penghasil data atau pengumpul data)
Kontrol	Mekanisme kontrol berbeda dari mekanisme kontrol klasik mengingat sifat stokastik sistem kuantum. Kontrolabilitas bersifat probabilistik

Pemrosesan Informasi

Fokus kami terkait tata kelola aplikasi QIT di bidang ilmu hayati adalah pada aktivitas yang berkaitan dengan pemrosesan informasi, termasuk simulasi, penambangan data, pemantauan, pengukuran, dan sebagainya. Seperti yang akan kita bahas di bawah ini dan

seperti yang sudah umum diketahui, informasi, data, penyimpanan, dan metode pemrosesan merupakan fitur penting dari banyak divisi ilmu hayati. Hal ini pada gilirannya memengaruhi bagaimana dan di mana penggunaan komputasi kuantum di bidang ilmu hayati diatur. Misalnya, kerangka kerja tata kelola yang berlaku untuk tata kelola ilmu hayati memberlakukan persyaratan tertentu, baik dalam bentuk maupun substansi, pada penggunaan, penyebaran, dan karakter informasi. Ini termasuk persyaratan spesifikasi dan deskripsi berdasarkan hukum kekayaan intelektual, terutama hukum paten; spesifikasi detail teknis sebagai bagian dari prosedur persetujuan produk alat kesehatan; pengungkapan dan representasi pengujian dan pemrosesan ilmiah yang memadai sebagai bagian dari desain farmasi dan efek antisipatif obat-obatan baru, keandalan pengujian dan prosedur uji klinis, serta spesifikasi mengenai sifat, kualitas, dan keandalan informasi yang diperoleh dari pemantauan dan pengawasan aplikasi ilmu hayati. Pemanfaatan algoritma atau perangkat komputasi kuantum, misalnya dalam simulasi farmasi, simulasi efek obat, atau pemrosesan bioinformatika, mungkin menjadi jenis penggunaan yang perlu ditentukan berdasarkan rezim tata kelola yang berlaku.

Efek Orakular

Selain itu, ada yang kami sebut sebagai pertanyaan tentang tata kelola teknologi orakular yang perlu dipertimbangkan. Dalam ilmu komputasi, orakel adalah artefak, mirip dengan kotak hitam, yang dapat menjawab pertanyaan atau menyelesaikan masalah pengambilan keputusan dalam satu operasi, terlepas dari apakah jawaban tersebut dapat dihitung atau tidak. Dalam bentuknya yang paling umum, ini adalah kotak hitam yang menghasilkan solusi untuk masalah apa pun. Dengan menggunakan analogi ini, yang kami maksud dengan teknologi orakel adalah teknologi yang kemampuan pemrosesan informasinya (seperti pemrosesan informasi kuantum, pembelajaran mesin, atau kecerdasan buatan) secara kategoris melampaui kemampuan pemrosesan informasi komputasi klasik yang ada dengan dampak spesifik tertentu, pada dasarnya analog dengan orakel, pada intinya kotak hitam atau perangkat pemrosesan informasi yang sangat kompleks (dan seringkali non-linier) yang dapat memecahkan kelas masalah yang jika tidak, tidak dapat dipecahkan (dalam praktik atau prinsip).

Secara praktis, teknologi orakel memunculkan apa yang kita nilai sebagai kelas risiko terpisah, yaitu risiko orakel, yang ditimbulkan oleh misalnya generasi pengetahuan, wawasan, atau informasi yang membekali mereka yang memiliki akses ke pengetahuan tersebut dengan kapasitas yang secara kategoris berbeda. Risiko ini agak menjadi topik riset Keamanan AI dan Risiko AI, yang memeriksa skenario kontrafaktual di mana teknologi AI dapat mencapai tingkat kemajuan kognitif dengan dampak tinggi, seperti memungkinkan pembuatan senjata, sintesis bahan kimia, atau bahkan sistem robot otonom untuk menunjukkan kekuatan yang signifikan. Dalam konteks ilmu hayati, ini mungkin termasuk penggunaan AI dan QIT untuk memungkinkan sintesis bahan kimia, obat-obatan, atau protein atau desain rekayasa dengan efek dampak tinggi tertentu, seperti penyesuaian obat-obatan dengan data bioinformatika individu (dengan manfaat positif untuk pengobatan tetapi potensi bahaya negatif untuk keselamatan), atau simulasi yang sangat akurat yang memberikan keunggulan informasi yang sangat asimetris.

Selain itu, teknologi orakel juga memunculkan masalah verifikasi bagaimana keluaran orakel dapat diverifikasi dan dipercaya. Verifikasi pemrosesan informasi dan prosedur komputasi serta outputnya (dan secara tidak langsung keandalannya) merupakan elemen penting di berbagai rezim tata kelola ilmu hayati, termasuk kekayaan intelektual, pengungkapan teknis perangkat medis, pengungkapan paten, dan lainnya. Masalah verifikasi adalah masalah yang telah dipelajari dan ditangani dengan baik untuk teknologi informasi klasik, perbedaan muncul dalam kasus QIT karena fitur unik informasi kuantum, seperti fakta bahwa pengukuran memengaruhi keadaan suatu sistem dan bahwa informasi kuantum tidak dapat dikloning. Verifikasi dapat terjadi melalui tomografi, di mana, misalnya, kemampuan untuk memverifikasi keadaan suatu sistem kuantum melibatkan pengukuran berulang pada instansiasi identik dari sistem tersebut dengan cara yang memungkinkan rekonstruksi keadaannya (atau evolusinya) dari statistik pengukuran.

Ketidakmampuan untuk memverifikasi keadaan atau proses membuat sistem tersebut pada dasarnya menjadi kotak hitam. Namun, hal ini tidak selalu bermasalah: metode tata kelola dalam ilmu hayati dan bidang lainnya memiliki cara yang sudah ada dan mapan untuk mengatasi proses informasi "kotak hitam" di mana keadaan atau evolusi (proses) tetap tidak dapat diakses, atau hanya sebagian dapat diverifikasi, dalam hal ini metode lain (seperti menilai secara statistik hasil yang dapat dipastikan, atau hanya menjalankan uji coba dan mengabaikan persyaratan untuk pengetahuan spesifik tentang komputasi itu sendiri) dapat diterapkan.

Efek Asimetri Informasi

Efek asimetri informasi dari teknologi yang berpotensi bersifat ramalan, seperti AI dan QIT, belum sepenuhnya dipahami, tetapi merupakan fitur penting dari teknologi informasi tersebut. Misalnya, akses ke teknologi komputasi QIT dapat memberikan keuntungan bagi pelaku pasar, masyarakat, atau pemerintah tertentu yang timbul dari desain obat atau alat medis yang lebih baik dibandingkan pesaing dengan efek lanjutan seperti kesehatan secara keseluruhan yang lebih baik, kemungkinan umur yang lebih panjang, dan peningkatan lain dalam metrik kesehatan dan kesejahteraan.

Simulasi yang lebih baik dan lebih akurat dari QIT juga dapat menyebabkan konsentrasi inovasi dan penemuan dan kekayaan intelektual lebih lanjut pada pemangku kepentingan yang memiliki akses ke sumber daya komputasi yang canggih. Kita dapat melihat efek konsentrasi pasar muncul karena asimetri informasi yang memungkinkan teknologi komputasi bergaya orakel atau yang sangat efisien untuk menghasilkan penemuan yang menarik perlindungan kekayaan intelektual dengan lebih cepat, akurat, atau luas. Jelas meskipun agak spekulatif teknologi orakel memiliki potensi keuntungan yang sangat besar, seperti dalam menemukan obat atau strategi pencegahan terkait penyakit atau gangguan lainnya. Jelas juga bahwa, seperti yang sering terjadi dalam sejarah inovasi ilmu hayati, hanya beberapa peserta yang memiliki sumber daya yang memadai, seperti pemerintah dan perusahaan farmasi (atau, kemungkinan besar, perusahaan teknologi) yang berada di garda terdepan penemuan ilmu hayati dan penyebaran produk.

Ada situasi analogis yang ada untuk memandu tata kelola dan respons terhadap efek peningkatan konsentrasi dari pemrosesan informasi yang intensif sumber daya. Dan meskipun efek tersebut tidak terbatas pada QIT itu sendiri, seperti yang dibuktikan oleh perkembangan teknologi kecerdasan buatan, seperti berbagai model Alpha Google DeepMind untuk penemuan protein dan sejenisnya, kombinasi intensitas sumber daya yang dibutuhkan untuk komputasi QIT dan janji wawasan yang mengubah paradigma dari penggunaan teknologi tersebut berarti bahwa efek asimetris informasinya perlu mendapat perhatian dan pembelajaran.

BAB 3
KEKAYAAN INTELEKTUAL PADA TEKNOLOGI INFORMASI KUANTUM

Bab ini memeriksa strategi kekayaan intelektual (IP) yang diterapkan dalam teknologi informasi kuantum (QIT), menunjukkan bahwa perusahaan beroperasi dalam "superposisi" pendekatan: secara selektif menggabungkan paten, rahasia dagang, dan inovasi terbuka di berbagai lapisan tumpukan kuantum. Meskipun pengajuan paten telah meningkat secara signifikan, kerahasiaan dagang tetap penting karena sifat proses kunci yang tersirat dan spesifik konteks serta kendala rezim kontrol ekspor. Pada saat yang sama, keterbukaan adalah pengungkit ilmiah dan seringkali strategis, yang memungkinkan interoperabilitas, pembelajaran kumulatif, dan pembentukan ekosistem melalui mekanisme seperti kerangka kerja sumber terbuka dan platform akses cloud yang dapat menghasilkan keunggulan kompetitif melalui efek jaringan. Dengan menggunakan heuristik tata kelola yang menghubungkan instrumen hukum dengan lapisan teknis spesifik dari perangkat keras dan sistem kontrol hingga perangkat lunak dan antarmuka bagian ini memetakan bagaimana eksklusivitas, kerahasiaan, dan kolaborasi dikonfigurasi dalam praktik. Kombinasi berlapis ini, yang melibatkan superposisi dan keterkaitan antara kekayaan intelektual dan inovasi terbuka, menunjukkan bahwa strategi kompetitif QIT tidak bergantung pada pilihan antara model kepemilikan dan model terbuka, tetapi pada kalibrasi kombinasi keduanya agar sesuai dengan tujuan teknis, komersial, dan kebijakan. Bagian ini membingkai ulang perdebatan yang berlaku dalam inovasi kuantum: alih-alih bertanya apakah paten atau kerahasiaan tepat untuk teknologi kuantum, pertanyaan kuncinya menjadi kapan, di mana, dan dalam bentuk apa setiap instrumen paling baik melayani insentif swasta dan tujuan publik.

3.1 KEKAYAAN INTELEKTUAL DAN INOVASI TERBUKA TEKNOLOGI INFORMASI KUANTUM

Seiring transisi ilmu kuantum dari ranah kemungkinan teoretis menuju kelayakan komersial dalam waktu dekat, konteks hukum dan strategisnya semakin tajam. Seperti yang dijelaskan dalam Bagian. Seperti yang telah digarisbawahi, teknologi informasi kuantum (QIT) mencakup serangkaian inovasi yang muncul dalam komputasi kuantum, komunikasi kuantum, dan penginderaan kuantum, yang masing-masing memanfaatkan fitur unik mekanika kuantum seperti superposisi, keterikatan, dan non-lokalitas untuk memproses informasi dengan cara yang tidak dapat dicapai secara klasik. Meskipun sifat-sifat ini menentang asumsi lama tertentu dari ontologi klasik dan bertumpu pada fondasi probabilistik yang tidak dapat direduksi dan tidak dapat dikloning, bukti yang terkumpul menunjukkan bahwa doktrin IP yang ada menyerapnya dengan sedikit gesekan.

QIT bersifat *sui generis* dalam banyak hal, memadukan fisika fundamental dengan teknik dengan cara yang dianggap akan membebani kerangka hukum konvensional. QIT memanfaatkan fenomena mekanika kuantum seperti superposisi dan keterikatan untuk mencapai kemampuan yang tidak dapat dicapai dengan sistem klasik, termasuk peningkatan

kecepatan komputasi secara eksponensial dan komunikasi yang aman tanpa syarat. Meskipun prinsip-prinsip ini menantang asumsi klasik tentang informasi dan observabilitas, prinsip-prinsip ini belum memerlukan perubahan mendasar pada IP yang ada. Kerangka kerja. Rezim paten, rahasia dagang, dan inovasi terbuka sejauh ini telah mengakomodasi fitur-fitur spesifik kuantum tanpa memerlukan perombakan doktrin.

Data dan praktik penyusunan paten menunjukkan bahwa, meskipun teknologi itu sendiri tentu saja *sui generis*, perpaduan yang ada antara paten, rahasia dagang, dan alat inovasi terbuka terbukti cukup akomodatif. Sejak tahun 2014, Kantor Paten dan Merek Dagang Amerika Serikat (USPTO) dan Kantor Paten Eropa (EPO) telah bersama-sama memberikan lebih dari 1200 paten komputasi kuantum, dan pemberian tahunan melebihi 400, menghasilkan tingkat pertumbuhan tahunan gabungan sebesar 42% selama periode 2014–2021.

Sifat probabilistik teknologi kuantum dan teorema tanpa kloning, yang melarang penyalinan sempurna dari keadaan kuantum yang tidak diketahui, telah diangkat sebagai doktrin inti hukum paten yang berpotensi mengancam: bagaimana pemegang paten dapat "memungkinkan" orang lain untuk mempraktikkan penemuan tersebut, dan bagaimana pelanggaran dapat dibuktikan, jika pemeriksaan atau penggandaan keadaan yang dilindungi akan menyebabkan runtuhnya keadaan tersebut?

Meskipun kekhawatiran telah muncul, menurut pandangan kami, hal ini bukanlah sesuatu yang tidak dapat diatasi dalam praktiknya. Kami berpendapat bahwa persyaratan pengaktifan terpenuhi, misalnya, dengan mengungkapkan protokol persiapan keadaan yang dapat diulang bersama dengan detail teknis yang diperlukan untuk mereproduksi penemuan tersebut. Tergantung pada sifat penemuan tersebut, ini dapat mencakup spesifikasi material, arsitektur sirkuit, desain perangkat, metode fabrikasi, atau algoritma kontrol. Jika prosesor kuantum dapat didefinisikan secara memadai untuk memungkinkan konstruksi fisiknya, maka prosesor tersebut juga dapat dijelaskan dalam paten.

Demikian pula, jika algoritma kuantum dapat diimplementasikan pada perangkat keras kuantum yang tersedia, maka algoritma tersebut dapat diungkapkan dalam bentuk yang dapat dieksekusi atau skematis. Pelanggaran, meskipun tidak selalu dapat diamati secara langsung karena kendala pengukuran kuantum, seringkali dapat ditunjukkan melalui cara tidak langsung seperti pengambilan sampel statistik, pemeriksaan berkas kontrol klasik, atau pengujian mandiri yang independen dari perangkat. Pendekatan ini menunjukkan bahwa, meskipun teknologi kuantum menimbulkan tantangan epistemik, teknologi tersebut tidak menghalangi kepatuhan terhadap persyaratan inti hukum paten tentang pengungkapan, pengaktifan, dan penegakan hukum.

Awalnya, perusahaan cenderung menggunakan kerahasiaan dagang: sebelum tahun 2014, aktivitas paten dalam teknologi kuantum pada dasarnya stagnan, sebagian besar perusahaan mengandalkan kerahasiaan dagang, menjaga hasil eksperimen dan pengetahuan proses di luar sistem paten. Lanskap mulai berubah pada pertengahan tahun 2010-an, karena risiko pengucilan oleh portofolio pesaing memicu peningkatan defensif dalam pengajuan yang bertujuan untuk mengamankan kebebasan beroperasi. Meskipun demikian, kerahasiaan dagang terus memainkan peran penting dalam melindungi keahlian tacit yang mendasari R&D

kuantum sehari-hari. Menjembatani prosesor kuantum yang toleran terhadap kesalahan secara online atau menstabilkan tautan distribusi kunci kuantum membutuhkan penyetelan, penanganan material, dan rutinitas mitigasi kebisingan yang ada di buku catatan laboratorium dan memori otot daripada di artikel yang ditinjau oleh rekan sejawat. Realitas ini menguji kerja praktis dari kesepakatan pengungkapan inti sistem paten.

Hukum paten Eropa mensyaratkan bahwa suatu penemuan harus diungkapkan "dengan cara yang cukup jelas dan lengkap sehingga dapat dilakukan oleh orang yang ahli di bidangnya", namun di bidang kuantum mutakhir, memenuhi persyaratan kemampuan (atau "kecukupan pengungkapan") ini dapat menjadi tantangan. Paten, misalnya, pada metode koreksi kesalahan kuantum tertentu mungkin menjelaskan protokol teoretisnya, tetapi mereproduksi penemuan tersebut dapat membutuhkan waktu berbulan-bulan kalibrasi laboratorium atau metode rekayasa khusus yang tidak secara eksplisit tercantum dalam teks paten. Memang, telah dicatat dalam riset bahwa ambiguitas ontologis sistem kuantum misalnya, fakta bahwa keadaan qubit dijelaskan secara probabilistik dan tidak dapat diamati secara langsung tanpa kolaps memicu pertanyaan baru tentang asumsi pengungkapan klasik. Meskipun demikian, kami berpendapat bahwa ketika penemuan dapat ditentukan dengan jelas seperti desain perangkat keras yang terdefinisi dengan baik, proses fabrikasi, atau algoritma kuantum yang dapat dieksekusi tidak ada dalam fisika yang mencegahnya untuk diungkapkan sepenuhnya dengan cara yang memenuhi persyaratan hukum; tantangannya terletak kurang pada prinsip daripada pada praktik.

Karena sebagian dari pengetahuan ini sulit untuk dikodifikasi dan bahkan lebih sulit untuk direkayasa balik, perhitungan inovasi condong ke arah kerahasiaan. Perlindungan rahasia dagang tidak memerlukan detail pendukung, tidak memberlakukan batas waktu dua puluh tahun, dan, dalam model pengiriman berbasis cloud, dapat secara efektif dilindungi tanpa batas waktu dari pesaing. Bagi pengembang kuantum, rezim ini menarik: lemari pendingin pengenceran, sistem vakum perangkap ion, dan antarmuka akses cloud menciptakan penghalang alami untuk inspeksi; kerahasiaan berlangsung selama informasi tersebut dirahasiakan, sesuai dengan cakupan pengembangan yang panjang dari arsitektur toleransi kesalahan; dan doktrin tersebut mencakup segala hal mulai dari data eksperimental negatif hingga kurva kalibrasi yang tidak memenuhi ambang batas paten.

Namun, biayanya adalah penyusutan domain publik. Pertimbangkan fakta bahwa ilmu kuantum tumbuh dari budaya akademis yang kental dengan norma keterbukaan Mertonian, dan bahwa masa depannya algoritma untuk dijadikan tolok ukur, perangkat untuk dioperasikan bersama, standar untuk disepakati masih bergantung pada penyelidikan kumulatif. Termotivasi oleh perpaduan tujuan termasuk menghindari silo pengetahuan, mengamankan kebebasan untuk beroperasi, dan menumbuhkan efek jaringan platform komunitas kuantum telah mulai bereksperimen dengan tata kelola hibrida. Qiskit IBM dan PennyLane Xanadu membuka rantai alat tingkat tinggi sumber terbuka sambil mempertahankan kontrol tingkat pulsa sebagai pengetahuan eksklusif; program cloud yang dioperasikan oleh *Amazon Web Service* (AWS), Google dan inisiatif Eropa seperti Quantum Inspire memberikan waktu kepada peneliti eksternal pada perangkat keras yang biasanya tidak

transparan; pabrik pra-kompetitif seperti UK National Quantum Foundry mengumpulkan kapasitas ruang bersih; dan proposal industri untuk kumpulan paten berbasis FRAND (Adil, Wajar, dan Tidak Diskriminatif) pada koreksi kesalahan kuantum berupaya untuk mencegah kerumitan lisensi. Heuristik tumpukan tata kelola Bagian 1, yang menghubungkan instrumen hukum dengan lapisan berbeda dari tumpukan teknis, menyediakan lensa yang melaluinya eksperimen ini dapat dipetakan: kerahasiaan mendominasi pada lapisan fisik dan kontrol, paten mempertahankan nilai residual pada lapisan antarmuka, dan inovasi terbuka serta mekanisme kolaboratif berkembang di lapisan ilmiah dan di mana efek jaringan ekosistem paling kuat.

Pemeriksaan kami berlanjut dalam empat langkah. Bagian 2 memeriksa lanskap paten kuantum dan menjelaskan bagaimana praktik Eropa dan AS sejauh ini telah menyerap penemuan kuantum tanpa ketegangan doktrinal yang jelas. Bagian 3 memeriksa daya tarik yang terus-menerus dari kerahasiaan perdagangan dan negara untuk kelas pengetahuan seperti resep fabrikasi dan perangkat lunak kalibrasi dan menarik paralel dengan praktik bioteknologi dan kecerdasan buatan. Bagian 4 meninjau langkah-langkah inovasi terbuka di sektor ini: kerangka kerja sumber terbuka, platform pengujian cloud, foundry bersama, kumpulan paten FRAND, dan standardisasi ISO/IEC (Organisasi Internasional untuk Standardisasi/Komisi Elektroteknik Internasional). Pada akhirnya, kami menyimpulkan bahwa tidak ada satu instrumen pun yang menentukan; sebaliknya, setiap perusahaan menyusun superposisi paten, pengetahuan yang dijaga, dan keterbukaan selektif yang disesuaikan dengan sumber daya, model bisnis, dan ambisi platformnya.

3.2 TEKNOLOGI KUANTUM DAN HUKUM PATEN

Inovasi kuantum mencakup spektrum yang luar biasa, mulai dari fisika dasar dan desain algoritma hingga rekayasa prosesor yang dapat diskalakan dan infrastruktur kriogenik. Dengan demikian, inovasi ini melintasi wilayah konseptual yang sering dianggap sensitif secara hukum: formulasi matematika abstrak, fenomena fisik, dan prototipe eksperimental yang belum sepenuhnya terwujud dalam praktik. Oleh karena itu, orang mungkin mengharapkan teknologi kuantum untuk menguji batas-batas subjek hukum paten atau membebani doktrin pengungkapan dan pengaktifannya. Namun, yang mengejutkan, justru sebaliknya yang terjadi. Seperti banyak teknologi baru lainnya, sistem paten telah terbukti mudah beradaptasi sejauh ini, menyerap penemuan kuantum tanpa gangguan doktrinal dan setidaknya hingga saat ini tanpa memerlukan kerangka kerja *sui generis*. Bagian ini menelusuri lanskap paten yang muncul dalam QIT, menempatkan tren empiris terbaru dalam arsitektur doktrinal hukum paten kontemporer. Dengan demikian, buku ini menawarkan penjelasan yang berlandaskan empiris tentang aktivitas paten di sektor ini, dengan memberikan perhatian khusus pada pertanyaan tentang kelayakan materi pokok, perilaku strategis, dan kualitas pengungkapan, serta meletakkan dasar untuk diskusi tentang hubungan antara pematenan, kerahasiaan dagang, dan keterbukaan dalam pembelajaran kuantum.

Berdasarkan Konvensi Paten Eropa (EPC) dan hukum paten AS, kategori abstrak tertentu seperti metode matematika, algoritma, dan teori ilmiah dikecualikan dari

perlindungan kecuali jika dikaitkan dengan implementasi teknis konkret atau memberikan kontribusi teknis. Dalam pandangan ini, algoritma kuantum yang dipahami murni sebagai konstruksi matematika (misalnya, algoritma Shor untuk pemfaktoran, atau kode koreksi kesalahan kuantum) pada dasarnya tidak dapat dipatenkan. Namun, kelayakan paten tidak bergantung pada abstraksi itu sendiri, tetapi pada apakah materi pokok yang diklaim menghasilkan efek teknis atau diimplementasikan dengan cara yang memecahkan masalah teknis konkret.

Dalam praktiknya, penemuan kuantum telah melewati ambang batas ini dengan semakin mudah. Kantor paten menerapkan doktrin kelayakan konvensional: uji "karakter teknis" Eropa dan kerangka kerja *Alice/Mayo* AS. Klaim algoritma kuantum yang tertanam dalam implementasi fisik seperti integrasinya dengan prosesor kuantum atau penggunaannya dalam mengendalikan sistem kuantum fisik secara rutin dianggap dapat dipatenkan, dan memang sejumlah paten tentang algoritma dan perangkat lunak kuantum telah diberikan. Contohnya termasuk klaim yang diarahkan pada pengoperasian susunan qubit superkonduktor, protokol distribusi kunci kuantum, atau arsitektur pembelajaran mesin yang diimplementasikan pada sirkuit kuantum. Pemberian paten tersebut menunjukkan bahwa teknologi informasi kuantum tidak terlalu membebani doktrin kelayakan, melainkan menegaskan relevansinya yang berkelanjutan.

Data empiris mendukung penilaian ini. Antara tahun 2001 dan 2021, total 1892 paten terkait komputasi kuantum diberikan secara global. Dari jumlah tersebut, 1224—atau 64,7%—diberikan dalam periode tiga tahun dari tahun 2018 hingga 2021 saja. Pemeriksaan klaim yang diberikan menunjukkan bahwa lanskap paten kuantum mencakup beragam materi pokok, yang umumnya terbagi menjadi empat kelompok besar: realisasi fisik dan perangkat keras kuantum, algoritma dan metode kuantum terapan, koreksi kesalahan kuantum, dan penemuan kuantum tingkat aplikasi.

Telah diamati lebih lanjut bahwa format klaim yang digunakan dalam paten-paten ini sangat mirip dengan yang ditemukan dalam bidang komputasi klasik dan semikonduktor. Meskipun sistem kuantum didasarkan pada prinsip-prinsip non-klasik, perilaku kuantum yang beroperasi dapat disampaikan melalui artefak klasik. Diskontinuitas ontologis, sejauh ini, belum diterjemahkan menjadi hambatan epistemik. Bahkan, pengungkapan yang dibutuhkan diagram sirkuit kuantum, Hamiltonian, urutan kalibrasi cenderung melebihi ambang batas minimal kecukupan.

Hal ini sebagian karena banyak paten kuantum diajukan oleh fisikawan atau insinyur akademis dengan keahlian domain yang mendalam, yang membawa tingkat spesifikasi teknis yang tinggi pada penyusunannya. Dibandingkan dengan paten dalam kecerdasan buatan dan pembelajaran mesin, yang sering dikritik karena pengungkapan yang samar, fungsional, atau spekulatif, pengajuan paten kuantum cenderung menunjukkan tingkat ketelitian deskriptif yang jauh lebih tinggi. Salah satu klaim utama bagian ini adalah bahwa, terlepas dari kekhasan epistemik dan ontologis sistem kuantum, tidak ada ketidaksesuaian struktural antara teknologi kuantum dan persyaratan inti hukum paten khususnya pengungkapan dan pengaktifan. Dalam praktiknya, penemuan kuantum dapat dan sedang diungkapkan dengan kejelasan dan

kelengkapan yang cukup untuk memenuhi ambang batas hukum. Ketika pokok bahasannya adalah prosesor kuantum, pengaktifan dapat melibatkan penentuan material, arsitektur qubit, perangkat keras kontrol, dan proses fabrikasi yang dibutuhkan untuk mereproduksi perangkat tersebut. Jika penemuan tersebut terletak pada algoritma kuantum terapan, pengungkapan biasanya mencakup diagram sirkuit yang dapat dieksekusi, urutan gerbang, atau deskripsi matematis yang terkait dengan tugas komputasi tertentu. Bahkan fenomena yang diatur oleh teorema tanpa kloning atau kolaps yang diinduksi pengukuran tidak menghalangi kemampuan untuk dipatenkan, selama penemuan tersebut didefinisikan oleh prosedur persiapan yang dapat diulang dan parameter klasik yang dapat diverifikasi. Penegakan hukum, meskipun terkadang tidak langsung karena ketidakmampuan untuk mengamati keadaan kuantum, masih dapat dicapai melalui pengujian statistik, audit kode kontrol klasik, atau protokol verifikasi mandiri yang independen dari perangkat.

Ini bukan sekadar teori. Sejumlah besar paten yang diberikan termasuk pengungkapan Hamiltonian, rutinitas koreksi kesalahan kuantum, dan protokol kalibrasi qubit menunjukkan bahwa penemuan kuantum, jika ditentukan dengan benar, dapat diwujudkan melalui representasi klasik yang memenuhi standar hukum. Yang penting bukanlah sifat kuantum dari penemuan itu sendiri, tetapi sejauh mana penemuan tersebut telah distabilkan, diformalkan, dan dikodifikasi dengan cara yang mendukung reproduksibilitas. Dalam hal ini, untuk tujuan hukum paten, teknologi kuantum kurang berbeda dari teknologi klasik daripada yang sering diasumsikan: di mana kematangan teknis ada, pengaktifan hukum akan mengikutinya. Diskontinuitas ontologis yang diduga antara sistem kuantum dan klasik tidak sama dengan keretakan doktrinal dalam hukum kekayaan intelektual hal itu dapat, dan sudah, dijembatani melalui pengungkapan yang tepat dan kaya secara teknis.

Peningkatan ini merupakan fungsi dari kematangan ilmu pengetahuan dan cerminan dari pergeseran perilaku industri. Ketika teknologi kuantum mulai menarik modal ventura dan pendanaan publik yang signifikan, portofolio paten menjadi instrumen sinyal yang penting, terutama bagi pendatang baru. Perusahaan rintisan seperti Rigetti dan D-Wave menggunakan hibah paten awal untuk mengamankan pendanaan dan visibilitas pasar, sementara perusahaan mapan seperti IBM dan Google meningkatkan pengajuan paten untuk mengamankan kebebasan beroperasi dan melindungi diri dari gangguan.

Bukti empiris juga menunjukkan pergantian paten kuantum yang cepat. Sebuah studi menemukan bahwa sekitar 50% dari semua pengungkapan paten teknologi kuantum dari 20 tahun terakhir sudah berada di domain publik, baik yang telah kedaluwarsa atau ditinggalkan. Lebih dari 4500 paten kuantum yang diberikan telah kedaluwarsa, dan hampir 15.000 aplikasi yang dipublikasikan tidak pernah menghasilkan pemberian paten, melainkan berfungsi sebagai pengungkapan publik atas pengetahuan teknis.

Sifat sementara hak paten seringkali diangkat dalam konteks kuantum sebagai argumen potensial terhadap kesesuaiannya: masa berlaku paten terbatas biasanya 20 tahun sejak pengajuan dan berfokus pada waktu awal: aplikasi dipublikasikan 18 bulan setelah pengajuan, jauh sebelum sebagian besar teknologi kuantum akan matang secara komersial. Dalam industri

klasik yang serba cepat (seperti ponsel pintar), jangka waktu 20 tahun seringkali lebih dari cukup untuk memanfaatkan suatu penemuan.

Teknologi kuantum, sebaliknya, masih baru dan mungkin memerlukan jangka waktu pengembangan yang panjang. Banyak penemuan kuantum yang dipatenkan saat ini adalah bukti konsep atau komponen untuk sistem yang mungkin baru mencapai kegunaan penuh satu atau dua dekade mendatang (jauh di dalam atau tepat di luar jangka waktu paten). Namun, dihadapkan pada dinamika pasar yang kompetitif, kekhawatiran ini tidak memperlambat peningkatan aktivitas paten kuantum. Sebaliknya, sektor ini telah menyaksikan peningkatan yang signifikan dalam pengajuan dan pemberian paten, karena perusahaan terutama pendatang baru menggunakan paten baik sebagai sinyal strategis maupun sebagai instrumen eksklusi atau negosiasi.

Di satu sisi, masuknya pengetahuan kuantum yang cepat ke ranah publik ini menciptakan "ruang informasi kuantum bersama" yang muncul, di sisi lain, hal ini menggarisbawahi bahwa banyak paten kuantum awal belum menghasilkan keuntungan kepemilikan yang berkelanjutan bagi pemiliknya, baik karena penemuan tersebut terbukti prematur atau karena perusahaan secara strategis mempublikasikan melalui paten tanpa mengejar eksklusivitas penuh. Alih-alih mengungkap ketidaksesuaian struktural antara inovasi kuantum dan sistem paten, dinamika ini menunjukkan bahwa kendala temporal telah diimbangi atau bahkan dimanfaatkan oleh keharusan strategis dari bidang yang kompetitif dan berkembang pesat.

3.3 KERAHASIAAN STRATEGIS DALAM PEMBELAJARAN DAN PENGEMBANGAN KUANTUM

Mengingat uraian Bagian 2 tentang lanskap paten yang berkembang pesat, mungkin tidak mengherankan bahwa rahasia dagang telah menjadi penting sebagai strategi IP pelengkap dalam QIT. Rahasia dagang adalah informasi apa pun data eksperimental, teknik fabrikasi, kode sumber perangkat lunak, bahkan sirkuit kuantum yang telah dikompilasi yang memberikan keunggulan kompetitif karena tidak diketahui publik, selama pemegangnya mengambil langkah-langkah yang wajar untuk menjaga kerahasiaannya. Tidak seperti paten, rahasia dagang tidak memberikan monopoli formal terhadap penemuan independen atau rekayasa balik, tetapi juga tidak memiliki tanggal kedaluwarsa tetap. Perlindungan berlangsung selama kerahasiaan dipertahankan. Dalam praktiknya, hal ini membuatnya sangat menarik di sektor-sektor di mana nilai komersial penuh dari inovasi mungkin tidak terealisasi dengan masa berlaku paten.

Di sektor kuantum, beberapa faktor membuat rahasia dagang, dan, tergantung pada konteksnya, kerahasiaan negara, menjadi sangat menarik. Pertama, bersifat epistemik: sebagian besar pengetahuan kuantum yang paling berharga bersifat prosesual atau tacit, tertanam dalam rutinitas laboratorium, alur kerja kalibrasi, dan urutan penyetelan yang sulit jika bukan tidak mungkin untuk ditulis. Hal ini seringkali menentukan apakah suatu sistem kuantum berkinerja stabil atau runtuh di bawah gangguan.

Kedua, banyak sistem kuantum memiliki arsitektur yang kompleks dan secara fisik tidak dapat diakses oleh pihak luar. Platform komputasi kuantum berbasis cloud, seperti yang ditawarkan oleh IBM, IonQ, atau Alibagiana, menyediakan antarmuka pemrograman kuantum kepada pengguna tetapi tidak memberikan visibilitas langsung ke perangkat keras, protokol kalibrasi, atau tumpukan firmware yang mendasarinya. Model "komputasi kotak hitam" ini membuat rekayasa balik menjadi sangat sulit, terutama ketika kinerja sistem bergantung pada tumpukan terintegrasi dari kontrol kriogenik, mitigasi kesalahan, dan jalur kompilasi kepemilikan. Di mana akses fisik terbatas, kerahasiaan de facto secara struktural tertanam dalam arsitektur platform.

Ketiga, kerahasiaan dalam QIT seringkali merupakan respons strategis terhadap risiko geopolitik dan harapan investor. Teknologi kuantum secara luas dipahami memiliki aplikasi militer dan intelijen, mulai dari radar dan penginderaan kuantum hingga ketahanan kriptografi pasca-kuantum. Karakteristik penggunaan ganda ini telah menyebabkan banyak pemerintah nasional memberlakukan kontrol ekspor, rezim klasifikasi, atau firewall institusional di sekitar kelas-kelas tertentu dari R&D kuantum. Kerahasiaan, dalam konteks tersebut, diwajibkan.

Terakhir, kerahasiaan juga merupakan fungsi dari tuntutan material dan infrastruktur yang khas dari inovasi kuantum. Perangkat kuantum harus dibangun, ditempatkan, dan dioperasikan secara fisik dalam lingkungan dengan spesifikasi tinggi, seperti lemari pendingin pengenceran kriogenik, sirkuit superkonduktor, dan ruang vakum ultra-tinggi. Fasilitas ini mahal untuk dibangun, sulit diakses, dan seringkali membutuhkan material khusus dan sistem kontrol yang terintegrasi erat. Selain itu, pengetahuan yang dibutuhkan untuk mengoperasikan perangkat keras kuantum secara efektif sangat tersirat, berada di dalam tim teknik khusus dan rutinitas laboratorium yang berulang. Akibatnya, bahkan tanpa perlindungan hukum formal, QIT secara alami tahan terhadap pengamatan, duplikasi, dan rekayasa balik.

Hal ini sangat kontras dengan sektor seperti farmasi, di mana biaya pengembangan senyawa baru juga sangat tinggi, tetapi begitu produk berada di pasaran, komposisinya seringkali dapat direkayasa balik dengan relatif mudah. Asimetri tersebut mendasari ketergantungan yang kuat pada perlindungan paten dalam ilmu hayati: eksklusivitas harus dibangun secara hukum karena kerahasiaan sulit dipertahankan. Dalam QIT, kebalikannya berlaku. Hambatan tinggi terhadap inspeksi dan replikasi memungkinkan perusahaan untuk lebih bergantung pada kerahasiaan dagang, bahkan untuk inovasi yang seharusnya dapat dipatenkan. Ketidakjelasan struktural ini membuat teknologi kuantum sangat cocok untuk strategi berbasis kerahasiaan, terutama pada tahap pengembangan awal, di mana perusahaan mungkin lebih memilih untuk menunda pengungkapan atau menghindarinya sama sekali. Namun, hukum rahasia dagang juga mewujudkan pertimbangan kebijakan. Yang paling jelas, hal itu memperlambat laju ilmu pengetahuan kumulatif. Tidak seperti paten, yang dipublikasikan dan dapat diakses sehingga mendorong pengungkapan, rahasia dagang menurut definisinya menjaga informasi tetap berada di luar domain publik.

Pembelajaran dasar yang penting dalam ilmu kuantum secara historis telah dilakukan dalam lingkungan akademis terbuka dengan publikasi dan berbagi data yang cepat: beralih ke kerahasiaan perusahaan dapat memperlambat penyebaran pengetahuan ilmiah atau bahkan

menghambat pengembangan standar. Perlindungan rahasia dagang, menurut desainnya, mengarahkan upaya inventif ke dalam "penindasan informasi". Kesepakatan ini mungkin efisien ketika hanya mencegah penumpang gelap, tetapi juga merampas hasil negatif, data kalibrasi, dan rutinitas laboratorium dari sesama ilmuwan yang membentuk infrastruktur tak terlihat dari penyelidikan kumulatif. Hal ini memperburuk asimetri struktural.

Menjaga kerahasiaan tidak hanya membutuhkan kecanggihan teknis tetapi juga infrastruktur organisasi: ruang bersih yang aman, protokol akses, pemeriksaan karyawan, kepatuhan hukum. Ini adalah biaya yang meningkat seiring dengan ukuran perusahaan. Pemain utama AWS, Google, atau Alibagiana dapat mengamortisasi biaya overhead tersebut melalui anggaran pembelajaran miliaran dolar, tetapi perusahaan rintisan tahap awal tidak dapat melakukannya. Perusahaan rintisan berada di sisi yang salah dari asimetri informasi: mereka harus melisensikan akses kotak hitam ke perangkat keras yang tidak dapat mereka periksa, sementara secara bersamaan mendekati investor yang menuntut jaminan IP yang tidak dapat mereka ungkapkan. Hasilnya adalah siklus konsentrasi pasar yang saling memperkuat, yang mendinginkan daya saing yang diberikan oleh sains terbuka dalam revolusi kuantum pertama.

Ketidaktransparan dapat menghambat interoperabilitas dan pembentukan standar. Banyak metrik kinerja dalam komputasi kuantum kesetiaan gerbang, waktu dekoherensi, konektivitas qubit tidak mudah diverifikasi secara independen tanpa akses ke data mentah dan protokol. Ketika perusahaan mengklaim keunggulan teknis berdasarkan tolok ukur kepemilikan, menjadi sulit untuk menetapkan kriteria bersama untuk perbandingan. Hal ini mempersulit keputusan pengadaan, kemitraan pembelajaran akademis, dan pengawasan regulasi. Metode tersembunyi juga dapat menggagalkan verifikasi formal, sertifikasi, atau pemantauan kontrol ekspor, terutama dalam kolaborasi lintas batas yang sensitif.

Ketegangan kebijakan ini tidak dibiarkan begitu saja dalam inovasi kuantum. Sebaliknya, hal itu diatasi dengan serangkaian instrumen strategis paralel yang mencapai kolaborasi dan mendorong keterbukaan, terkadang dalam batasan strategis yang berfokus pada koalisi atau wilayah tertentu. Konfigurasi multi-modal ini mencerminkan arsitektur sistem kuantum itu sendiri: bertumpuk, saling bergantung, dan sensitif terhadap konteks. Bagian berikut ini secara langsung membahas arsitektur ini, meneliti bagaimana mekanisme kolaboratif diterapkan di berbagai lapisan teknis yang berbeda dari tumpukan kuantum.

3.4 MEKANISME KOLABORATIF DI SELURUH TUMPUKAN TATA KELOLA

Inovasi terbuka, dalam definisi penting Chesbrough, adalah pengaturan aliran pengetahuan yang disengaja di seluruh batas perusahaan sehingga ide-ide dari luar dan jalur-ke-pasar dari luar mempercepat pengembangan teknologi. Dahulu dianggap radikal, model ini sekarang menjadi paradigma yang menarik di berbagai sektor seperti otomotif (misalnya, pengembangan bersama BMW–Toyota Z4/Supra) dan bioteknologi. Uni Eropa secara khusus mendukungnya dalam wacana kebijakannya, mengembangkan program kerangka kerja yang secara eksplisit mempromosikan berbagi pengetahuan, upaya standardisasi, dan pengembangan bersama infrastruktur kuantum fundamental.

Dalam konteks QIT, terlepas dari (atau paralel dengan) momentum di balik kerahasiaan, inovasi terbuka terwujud dalam berbagai cara. Kita melihatnya dalam konsorsium pembelajaran publik-swasta (ciri khas program Unggulan Kuantum Uni Eropa) di mana lembaga akademik dan perusahaan menggabungkan keahlian dan berbagi temuan sementara, masing-masing mendapat manfaat dari dorongan kolektif ke depan. Kita melihatnya dalam proliferasi perangkat lunak dan perangkat keras kuantum sumber terbuka. Misalnya, IBM terkenal membuka kode sumber kerangka kerja pemrograman kuantum Qiskit dan menyediakan akses berbasis cloud ke prosesor kuantum nyata untuk pengembang di seluruh dunia. Strategi ini memicu komunitas global yang terdiri dari lebih dari 450.000 pengguna dan 1700 publikasi yang dibangun di atas platform IBM.

Contoh IBM menunjukkan bagaimana keterbukaan pada lapisan antarmuka dapat dipertahankan justru karena eksklusivitas dipertahankan lebih dalam di dalam tumpukan. Dengan kata lain, inovasi terbuka tidak berarti tidak adanya hak kekayaan intelektual. Sebaliknya, ia mengkonfigurasi ulang penggunaannya. Paten dalam model inovasi terbuka dapat digunakan lebih selektif: misalnya, untuk mengamankan posisi defensif perusahaan atau memungkinkan lisensi silang, daripada untuk memblokir area pembelajaran yang luas. Rahasia dagang mungkin masih melindungi proses inti yang benar-benar bersifat hak milik, tetapi perusahaan mungkin dengan sukarela berbagi wawasan lain di forum terbuka untuk menetapkan standar industri atau menarik mitra.

Janji paten komitmen publik sukarela yang dibuat oleh pemegang paten untuk menahan diri dari menggunakan sebagian atau seluruh haknya dalam satu atau lebih paten mencerminkan logika yang sama, menandakan keterbukaan terhadap kolaborasi sambil mempertahankan pengaruh atas aset yang sangat diperlukan. Meningkatnya popularitas instrumen ini di bidang teknologi tinggi lainnya48 menunjukkan bahwa instrumen ini, pada waktunya, dapat memainkan peran pengisi celah yang serupa di QIT: sebuah pilihan yang patut dipertimbangkan seiring dengan terus berkembangnya tumpukan tata kelola ini. Bagian ini mengkaji bagaimana ekosistem inovasi terbuka berlapis, yang terstruktur melalui pengaturan swasta, yaitu sistem aturan kontraktual dan konsorsium yang dirancang oleh aktor swasta untuk melengkapi hukum publik, telah mulai melengkapi dan mengimbangi kecenderungan rezim IP formal terhadap kerahasiaan kepemilikan.

Lima mekanisme inovasi terbuka utama, yang mencakup perangkat lunak hingga perangkat keras hingga tata kelola kekayaan intelektual, menggambarkan tren penyeimbang terhadap pengurungan pengetahuan kuantum. Mekanisme-mekanisme ini (1) kit pengembangan sumber terbuka, (2) platform pengujian berbasis cloud, (3) pusat fabrikasi pra-kompetitif, (4) kumpulan paten berorientasi FRAND, dan (5) kolaborasi standar diperiksa di bawah ini secara berurutan, ditempatkan dalam konteks tata kelola IP Eropa dan perkembangan fisika kuantum kontemporer. Pendekatan berlapis ini selaras dengan gagasan Bagian 1 bahwa tata kelola QIT yang efektif akan berlapis-lapis: langkah-langkah teknis dan hukum saling memperkuat di berbagai tingkatan.

Sebelum beralih ke lima mekanisme tersebut, ada baiknya untuk menyoroti tren latar belakang: persaingan geopolitik yang semakin intensif mulai membentuk apa yang secara

realistis dapat diartikan sebagai "keterbukaan" bagi pembelajaran dan pengembangan kuantum. Pengetatan jadwal kontrol ekspor dan konsorsium yang memiliki izin keamanan berisiko menghasilkan "tragedi anti-commons," di mana hak-hak yang terfragmentasi atau dibatasi memperlambat kemajuan kolektif. Akibatnya, keterbukaan semakin terbagi menjadi dua lingkaran konsentris: keterbukaan berbasis klub di antara yurisdiksi tepercaya yang berbagi perangkat dan data di bawah lisensi timbal balik, dan keterbukaan global berbasis standar di mana spesifikasi antarmuka dan kode berlisensi permisif tetap dapat diakses oleh semua orang. Yang terakhir bercita-cita untuk mencapai commons global yang sesungguhnya, di mana standar antarmuka dan lisensi OSS permisif mengundang adopsi di seluruh dunia, terlepas dari blok geopolitik.

Matriks dalam Tabel 3.1 merangkum wawasan inti dari bagian ini: keterbukaan dalam QIT bersifat spesifik lapisan dan diatur secara kontraktual. Subbagian berikut (§4.1–§4.4) menguraikan setiap mekanisme secara berurutan, menunjukkan bagaimana pilihan desain hukum mereka memperkuat keunggulan kompetitif dan koherensi ekosistem.

Tabel 3.1 Inovasi terbuka di QIT

Instrumen	**Lapisan (tumpukan)**	**Contoh**	**Fitur tata kelola**
SDK sumber terbuka (Qiskit, PennyLane)	Kompiler/aplikasi	Qiskit (IBM) (Pada tanggal 8 Mei 2025, paket Python Qiskit mencatat 519.646 unduhan pada bulan sebelumnya, menurut statistik PyPI. Lihat *https://pypistats.org/packages/Qiskit?* Diakses 22 Juli 2025), PennyLane (Xanadu)	Lisensi permisif (Apache 2.0), termasuk pemberian paten bebas royalti. Perjanjian lisensi kontributor (CLA) memastikan hak masuk; lisensi keluar memungkinkan add-on kepemilikan sambil mewajibkan pelestarian pemberitahuan. API terbuka menjadi standar sirkuit/pulsa de facto, namun menyembunyikan kekayaan intelektual kalibrasi tingkat rendah.
Tempat uji coba berbasis cloud dengan program hibah	Antarmuka klasik/lapisan akses cloud	Pengalaman kuantum IBM & tingkatan "terbuka" akademis, kredit pembelajaran Amazon Braket, hibah kuantum Microsoft Azure	Syarat dan ketentuan yang berlaku melarang peretasan, rekayasa balik, dan eksperimen yang dikontrol ekspor; penyedia dapat menangguhkan akun. Pengukuran granular (shot, prioritas antrian)

			(“Pengukuran” mengacu pada bagaimana penggunaan layanan kuantum diukur dan dikontrol. Misalnya, Amazon Braket mengenakan biaya kepada pengguna per tugas dan per “shot” (eksekusi sirkuit kuantum) dan IBM menawarkan sejumlah eksekusi tertentu secara gratis tanpa antrian, sementara pengguna premium atau anggota hub mendapatkan akses yang diprioritaskan.)
Pusat fabrikasi bersama dan perangkat keras terbuka	Perangkat keras/fabrikasi	Qu-pilot (chip UE JU)	Perjanjian kemitraan kerangka kerja mengalokasikan pendanaan Uni Eropa, mensyaratkan pembagian biaya dan slot akses terbuka. Hak kekayaan intelektual (KI) latar belakang tetap dimiliki oleh kontributor; pengetahuan proses utama dibagikan tanpa royalti di dalam konsorsium. Pemeriksaan penggunaan akhir dan perjanjian kerahasiaan (NDA) memenuhi kontrol penggunaan ganda Uni Eropa.
Kumpulan paten dan standar	Semua lapisan	Aliansi paten kuantum Tiongkok (CQPA)	Kumpulan paten komputasi kuantum khusus pertama (2023), yang menggabungkan SEP prospektif di tujuh domain (termasuk QEC)

			Ketentuan lisensi spesifik belum dipublikasikan

Kit Pengembangan Perangkat Lunak Sumber Terbuka

Lapisan pertama dari tumpukan terdiri dari serangkaian kit pengembangan perangkat lunak (SDK) dan algoritma sumber terbuka yang terus berkembang. Kerangka kerja terkemuka seperti Qiskit dari IBM dan PennyLane dari Xanadu keduanya dirilis di bawah lisensi Apache 2.0 sumber terbuka yang permisif, tersedia secara terbuka untuk siapa saja. SDK ini memungkinkan para peneliti dan pengembang di seluruh dunia untuk menulis program kuantum, mensimulasikan sirkuit kuantum, dan bahkan menjalankan kode pada prosesor kuantum yang sebenarnya. Di sini, paradigma rahasia dagang dibalik pada lapisan perangkat lunak, yang memiliki signifikansi strategis dan tata kelola. Kode terbuka menumbuhkan komunitas pengembang global dan basis pengetahuan bersama, menyelaraskan komunitas pada antarmuka dan representasi umum. Pada gilirannya, struktur data dan API (*Application Programming Interfaces*) yang tertanam dalam toolkit ini format Qiskit untuk sirkuit kuantum dan integrasi pustaka pembelajaran mesin kuantum PennyLane dapat menjadi standar *de facto*. Terlebih lagi, dengan menyediakan infrastruktur terbuka umum untuk menulis program kuantum, SDK semacam itu secara dramatis menurunkan hambatan masuk dan mempercepat difusi pengetahuan di bidang ini.

Pilihan lisensi memainkan peran penting dalam keberhasilan SDK. Lisensi Apache 2.0 yang digunakan oleh Qiskit memungkinkan integrasi kepemilikan dan terbuka, hanya memerlukan pelestarian pemberitahuan hak cipta dan memberlakukan pembatasan minimal lainnya. Lisensi ini juga mencakup pemberian paten secara eksplisit dari kontributor, yang berarti siapa pun yang menyumbangkan kode juga memberikan pengguna lisensi bebas royalti untuk klaim paten apa pun yang akan dilanggar dengan menggunakan kontribusi tersebut. Dengan demikian, perusahaan komersial dapat memasukkan SDK kuantum sumber terbuka ke dalam alur kerja atau produk mereka tanpa risiko konflik IP, dan pengembang akademis dapat membangun di atasnya dengan mengetahui bahwa karya mereka akan tetap tersedia secara terbuka dan terlindungi.

Model kontributor dan struktur tata kelola menyertai lisensi ini. Proyek kuantum sumber terbuka utama biasanya mengharuskan kontributor untuk menandatangani Perjanjian Lisensi Kontributor (CLA) atau perjanjian serupa, yang memformalkan penerimaan kontributor terhadap ketentuan lisensi dan pemberian hak atas kontribusi mereka. Misalnya, CLA IBM untuk Qiskit secara eksplisit meminta kontributor (termasuk kontributor perusahaan) untuk memberikan lisensi kepada IBM dan pengguna hilir atas hak cipta dan paten apa pun yang mencakup kode yang mereka sumbangkan. Seperti yang diamati di domain Teknologi Informasi dan Komunikasi (TIK) lainnya, implementasi sumber terbuka mendorong penyebaran standar yang luas, interoperabilitas, dan menghindari efek penguncian. Dalam konteks kuantum, adanya banyak vendor perangkat keras dan kelompok pembelajaran yang

bersatu di sekitar SDK umum berarti program yang ditulis untuk satu sistem seringkali dapat dijalankan di sistem lain dengan perubahan minimal.

Platform Uji Coba Cloud dengan Program Hibah

Menghubungkan perangkat lunak ke perangkat keras fisik adalah lapisan uji coba cloud. Karena prosesor kuantum mahal, langka, dan membutuhkan lingkungan khusus, akses langsung ke perangkat keras terbatas. Sebagai tanggapan, perusahaan seperti IBM, Amazon, dan Google telah menyediakan prosesor kuantum mereka melalui layanan cloud, seringkali dengan program akses khusus untuk akademisi dan pembelajaran publik. IBM Quantum Experience, yang diluncurkan pada tahun 2016, adalah cloud kuantum publik pertama: memungkinkan siapa pun untuk menjalankan algoritma pada perangkat superkonduktor 5-qubit melalui internet. Sejak itu, IBM telah mengembangkan jaringan prosesor kuantum yang dapat diakses melalui cloud, yang diikuti oleh pihak lain (misalnya, Amazon Braket yang menyediakan akses ke chip kuantum dari berbagai perusahaan, Microsoft Azure Quantum atau platform Quantum Inspire Eropa).

Model perangkat keras akses terbuka ini telah secara dramatis menurunkan hambatan masuk. Pada tahun 2018, IBM melaporkan bahwa 80.000 pengguna telah menjalankan lebih dari tiga juta eksperimen pada mesin kuantum cloud-nya, dan pada tahun 2020, program IBM Quantum gratis memiliki komunitas lebih dari 200.000 pengguna terdaftar yang secara kolektif menjalankan jutaan eksperimen dan menerbitkan ratusan artikel. Strategi perangkat keras terbuka mendemokratisasi akses ke sumber daya yang sebelumnya dikontrol ketat, mengatasi tujuan kesetaraan dan diseminasi.

Program-program ini sering menawarkan tingkatan gratis atau program akademik khusus (misalnya, Program Pengguna Komputasi Kuantum Laboratorium Nasional Oak Ridge AS). Hal ini mencerminkan filosofi pembagian biaya pra-kompetitif: perusahaan dan pemerintah berbagi biaya awal yang tinggi untuk mesin kuantum sehingga seluruh komunitas dapat belajar dan berinovasi, menciptakan gelombang pasang yang pada akhirnya akan mengangkat semua perahu. Dari perspektif IP, sementara pengguna menjalankan algoritma secara terbuka, desain dan pengoperasian perangkat keras seringkali tetap bersifat hak milik API cloud mengekspos antarmuka yang terkontrol (gerbang, sirkuit) tetapi bukan detail rahasia dagang tentang kalibrasi atau mitigasi kebisingan di baliknya. Adegan-adegan tersebut. Mereka merupakan bagian kunci dari tumpukan tata kelola QIT karena berfungsi sebagai mekanisme quasi-regulasi: dengan menetapkan ketentuan penggunaan dan mewajibkan pengguna untuk mematuhi kebijakan tertentu (misalnya, tidak meretas sistem atau eksperimen yang dikontrol ekspor), penyedia cloud mengisi peran tata kelola secara real-time, bahkan ketika peraturan formal untuk komputasi kuantum masih baru muncul.

Pusat Fabrikasi Bersama dan Perangkat Keras Terbuka

Pada lapisan perangkat keras, QIT menghadapi hambatan sumber daya dan pengetahuan: fabrikasi perangkat kuantum (qubit, sensor kuantum, dll.) membutuhkan ruang bersih canggih, material eksotis, dan keahlian mendalam. Untuk menghindari duplikasi upaya ini secara terpisah, komunitas kuantum telah mulai membangun pusat fabrikasi bersama dan

inisiatif perangkat keras terbuka. Ini dapat dianggap sebagai padanan kuantum dari foundry kolaboratif atau layanan wafer multi-proyek dalam pembelajaran semikonduktor klasik.

Sebagai contoh, AS telah meluncurkan foundry yang didukung akademis dan pemerintah (UCSB Quantum Foundry, LPS Qubit Collaboratory, MonArk Quantum Foundry) yang bertujuan untuk memberikan akses kepada peneliti dan perusahaan rintisan ke fabrikasi mutakhir untuk teknologi superkonduktor, fotonik, atau teknologi qubit lainnya. Eropa mengikuti jejak tersebut: program Qu-Pilot, yang diluncurkan pada tahun 2024 di bawah EU Chips Joint Undertaking, akan membiayai dua jalur percontohan lintas batas, satu berfokus pada chip superkonduktor/fotonik dengan stabilitas tinggi, dan yang lainnya pada perangkat ion terperangkap. Setiap jalur akan dicakup oleh Perjanjian Kemitraan Kerangka Kerja multi-tahun. Dana Uni Eropa mencakup peningkatan peralatan dan kualifikasi proses dasar, sementara Usaha Kecil dan Menengah (UKM), perusahaan rintisan, dan universitas yang berpartisipasi membeli "tiket wafer" dengan biaya operasional marginal, memastikan akses bagi para pelaku yang tidak akan pernah mampu membeli tumpukan ruang bersih penuh.

Pusat fabrikasi terbuka ini menggabungkan biaya tetap yang tinggi dari pembelajaran dan pengembangan perangkat kuantum dan memungkinkan banyak pemangku kepentingan untuk mendapatkan manfaat dari infrastruktur canggih yang tidak mampu dibiayai oleh satu perusahaan rintisan atau laboratorium universitas saja. Mereka beroperasi dengan model berbagi biaya yang menurunkan hambatan masuk sambil mempertahankan kekayaan intelektual strategis: kekayaan intelektual latar belakang tetap berada di setiap organisasi yang berkontribusi; peningkatan proses utama yang dihasilkan pada proses bersama dilisensikan tanpa royalti di dalam konsorsium dan dapat ditawarkan kepada pengguna eksternal dengan persyaratan yang wajar.

Pedoman sains terbuka Horizon-Europe mendorong penyimpanan data proses dan desain referensi, mengizinkan embargo jika perlu untuk melindungi kekayaan intelektual, memperkuat basis pengetahuan publik tanpa kehilangan keunggulan kompetitif secara langsung. Terakhir, langkah-langkah sensitif seperti kriogenik di bawah 10 mK atau pemesinan elektroda perangkap ion diperiksa berdasarkan Peraturan Penggunaan Ganda Uni Eropa, dengan penyaringan penggunaan akhir dan NDA yang melindungi pengetahuan yang dikendalikan ekspor.

Kumpulan Paten dan Standar

Di puncak tumpukan tata kelola (dan melintasi semua lapisan teknis) terdapat pengaturan kekayaan intelektual kolaboratif: kumpulan paten dan organisasi penetapan standar (SSO), yang anggotanya berjanji untuk melisensikan teknologi penting dengan persyaratan FRAND. Seiring dengan kematangan teknologi kuantum dan perusahaan mengumpulkan portofolio paten, ada kekhawatiran bahwa kumpulan paten atau kendali eksklusif atas teknik kuantum fundamental dapat memperlambat bidang ini. Salah satu solusi yang diusulkan, yang diambil dari industri lain, adalah pembentukan kumpulan paten kuantum. Kumpulan paten adalah konsorsium di mana beberapa pemegang paten setuju untuk saling melisensikan atau menggabungkan paten mereka, biasanya untuk memberikan akses yang lebih mudah bagi pihak ketiga dengan persyaratan standar.

Pada Maret 2023, Baidu dan Akademi Ilmu Informasi Kuantum Beijing meluncurkan Aliansi Paten Kuantum Tiongkok (CQPA) dan, bersamaan dengan itu, kumpulan paten komputasi kuantum pertama di negara tersebut, yang terbuka untuk anggota baru dan telah mengumpulkan beberapa lusin paten. Kumpulan ini secara eksplisit menargetkan tujuh area strategis termasuk koreksi kesalahan kuantum dan beroperasi di bawah kelompok kerja Standar & Kekayaan Intelektual khusus yang akan memposisikan paten penting standar di masa mendatang untuk lisensi FRAND.

Koreksi kesalahan kuantum (QEC) secara luas diakui sebagai tulang punggung komputasi kuantum yang dapat diskalakan: banyak kelompok yang menciptakan kode dan teknik kontrol untuk mendeteksi dan memperbaiki kesalahan qubit. Hal ini telah menyebabkan banyaknya pengajuan paten tentang metode QEC, mulai dari kode permukaan topologi hingga algoritma mitigasi kesalahan yang cerdik. Kepemilikan yang tersebar atas pengajuan ini berisiko menghambat interoperabilitas atau membuatnya terlalu mahal bagi siapa pun untuk membangun prosesor yang toleran terhadap kesalahan. Kumpulan paten yang berfokus pada QEC seperti yang sudah dikelola oleh CQPA akan mencegah bahaya tersebut dengan mengumpulkan paten-paten utama dan melisensikannya sebagai satu paket dengan ketentuan FRAND. Kontributor menerima royalti dan akses timbal balik ke seluruh kumpulan paten, memperluas penawaran non-diskriminatif yang sama kepada pihak luar. Model ini mencerminkan kumpulan paten nirkabel 4G dan MPEG di mana tidak ada satu perusahaan pun yang dapat memveto masuknya pasar dengan menahan kekayaan intelektual (IP) yang penting.

Risikonya adalah bahwa kumpulan paten QEC yang tersebar dapat menghambat interoperabilitas atau membuatnya terlalu mahal bagi pendatang baru untuk membangun komputer kuantum yang toleran terhadap kesalahan. Kumpulan paten ini bertujuan untuk mencegah masalah ini dengan mengumpulkan paten QEC utama dan melisensikannya sebagai satu paket berdasarkan ketentuan FRAND. Secara praktis, perusahaan yang menyumbangkan paten mereka ke kumpulan tersebut setuju untuk melisensikannya kepada semua pengimplementasi (termasuk pesaing) dengan royalti yang wajar dan juga mendapatkan akses ke paten pihak lain: suatu bentuk lisensi silang yang juga diperluas ke pihak luar dengan ketentuan yang sama. Hal ini mengikuti pendekatan yang telah lama digunakan di industri seperti telekomunikasi, di mana tidak ada satu perusahaan pun yang mengendalikan kekayaan intelektual (IP) penting dari standar tersebut.

Jika skema QEC yang dominan diadopsi sebagai standar industri, hukum Uni Eropa kemungkinan akan memperlakukan paten tersebut sebagai hal yang penting bagi standar, memicu kewajiban untuk memberikan lisensi dengan persyaratan FRAND berdasarkan aturan ETSI (*European Telecommunications Standards Institute*)/ISO. Dengan secara sukarela menggabungkan paten sekarang, industri kuantum pada dasarnya memberlakukan sendiri rezim pro-kompetitif yang didorong oleh regulator. Eropa sudah mempersiapkan landasannya: Rencana Aksi Komisi Eropa tahun 2020 tentang Kekayaan Intelektual mendesak penggabungan paten secara sukarela dan cepat di bidang teknologi tinggi untuk menghindari hasil "pemenang mengambil semua", sementara pedoman IP Quantum Flagship 2024 merekomendasikan

penggabungan dan FRAND sebagai alat standar untuk standar kuantum. Penggabungan juga memperkuat penyebaran pengetahuan: ketika paten digabungkan dan dipublikasikan, hal itu sebenarnya memperkuat domain publik pengetahuan teknis. Pengungkapan paten mengajarkan masyarakat tentang teknik QEC baru, berkontribusi pada munculnya "sumber informasi kuantum bersama" berupa ide-ide, sementara penggabungan memastikan ide-ide tersebut tetap dapat diakses untuk digunakan.

Tanpa penggabungan, perusahaan mungkin cenderung menyimpan terobosan QEC mereka sebagai pengetahuan internal (karena mengungkapkannya melalui paten dapat memungkinkan pesaing). Tetapi penggabungan menciptakan jalan tengah: mematenkan dan berbagi inovasi untuk saling menguntungkan, daripada menyembunyikannya. Sebuah kumpulan paten menggunakan fungsi pengungkapan sistem paten dan pengaturan pembagian kontraktual untuk menyeimbangkan insentif untuk berinovasi (setiap kontributor masih mendapatkan bagian dari pendapatan lisensi) dengan kebutuhan untuk menyebarluaskan teknologi penting secara luas. Jika berhasil, hal ini dapat menjadi preseden bagi subbidang kuantum lainnya (misalnya, kriptografi kuantum atau penginderaan) untuk membentuk platform IP kolaboratif serupa. Namun, pertanyaan kebijakan yang berulang adalah siapa yang boleh bergabung. Lebih tepatnya, apakah kelompok tersebut harus membatasi partisipasi (atau hak suara) pada entitas dari yurisdiksi yang memiliki standar kontrol ekspor, peninjauan keamanan, dan supremasi hukum yang sama.

Terakhir, organisasi penetapan standar (SSO) dan kelompok kerja memainkan peran penting dalam menyelaraskan industri kuantum menuju keterbukaan dan interoperabilitas. Badan-badan seperti Komite Teknis Gabungan ISO/IEC tentang Teknologi Kuantum dan Komite Teknis Gabungan CEN-CENELEC Eropa 22 tentang Teknologi Kuantum mengumpulkan para ahli dari akademisi, industri, dan pemerintah untuk mengembangkan standar umum untuk antarmuka komputasi kuantum, format data, terminologi, dan protokol. Pengembangan standar pada dasarnya adalah inovasi terbuka: peserta harus berbagi detail yang cukup tentang pendekatan mereka untuk membangun konsensus.

Ilustrasi kontemporer adalah OpenQASM, bahasa *assembly de facto* yang diadopsi oleh vendor perangkat keras dan perangkat lunak. Peta jalan Unggulan Kuantum Uni Eropa menekankan bahwa standar awal “mencegah ketergantungan pada vendor dan mendorong basis pasokan yang kompetitif”; standar tersebut juga selaras dengan kumpulan paten, karena paten yang dikumpulkan dapat ditetapkan sebagai SEP dan secara otomatis ditawarkan dengan ketentuan FRAND. Inisiatif standardisasi dalam teknologi kuantum berfungsi sebagai kerangka kerja lapisan atas yang mengikat ekosistem inovasi terbuka: inisiatif ini dibangun di atas perangkat lunak sumber terbuka (yang sering diadopsi ke dalam standar), bergantung pada IP yang dikumpulkan (dengan komitmen FRAND), dan menggabungkan masukan yang luas (melalui konsorsium dan kelompok kerja).

Koordinasi Strategis Lintas Lapisan: Arsitektur Keterbukaan Kuantum

Secara keseluruhan, kelima mekanisme ini membentuk ekosistem inovasi terbuka multi-lapisan yang diatur secara pribadi yang diperkenalkan di awal bagian ini: ekosistem yang dibangun di atas sistem aturan kontraktual dan konsorsium yang meredam kecenderungan

alami R&D kuantum menuju opasitas rahasia dagang. Setiap mekanisme menargetkan titik hambatan yang berbeda dalam jalur inovasi: SDK sumber terbuka menyuntikkan transparansi dan berbagi pada tingkat perangkat lunak dan algoritma; platform pengujian cloud memperluas akses ke perangkat keras yang sebelumnya terisolasi; foundry dan hub bersama menyebarkan pengetahuan dalam membangun tulang punggung fisik; kumpulan paten membuka ruang kekayaan intelektual; dan standar memastikan seluruh ekosistem berbicara dalam bahasa yang sama. Pendekatan multi-cabang ini mencerminkan apa yang oleh para sarjana inovasi disebut sebagai "pluralisme kebijakan inovasi": pengakuan bahwa campuran strategi kolaboratif dan kompetitif menghasilkan hasil terbaik di bidang teknologi tinggi yang baru muncul.

3.5 POLA, INSENTIF, DAN LOGIKA PENGUNGKAPAN

Secara empiris, lanskap kekayaan intelektual dalam teknologi informasi kuantum (QIT) sepenuhnya kontinu dengan pola yang lebih luas yang didokumentasikan dalam dekade terakhir. Para inovator semakin mengandalkan rahasia dagang untuk melindungi R&D tahap awal yang berisiko tinggi, terutama ketika produk secara fisik tidak dapat diakses dan sulit untuk diperiksa. Teori inovasi klasik mengantisipasi konfigurasi ini. Di mana biaya imitasi tinggi, pengeluaran modal tidak merata, dan waktu tunggu komersial terkompresi, perusahaan rasional mengandalkan kerahasiaan abadi. Pengungkapan biasanya terjadi kemudian, ketika didorong oleh tuntutan pertahanan IP dan lisensi silang, interoperabilitas, pendanaan, atau sinyal strategis.

QIT mengikuti logika ini. Di seluruh industri, kita mengamati arsitektur IP berlapis yang mencerminkan kompleksitas integrasi sistem kuantum dan opasitas epistemik operasinya. Kerahasiaan dagang dan paten sama-sama terbukti bermanfaat: yang pertama melindungi proses yang sensitif terhadap integrasi dan sulit untuk direkayasa balik, sementara yang kedua memfasilitasi investasi, interoperabilitas, dan posisi strategis. Dalam beberapa kasus, klasifikasi keamanan nasional atau kewajiban kontrak pemerintah memberlakukan lapisan keempat: rahasia negara. Pada saat yang sama, akar akademis disiplin ilmu ini, dari kuliah Dirac di Cambridge hingga budaya pracetak akses terbuka arXiv, telah menanamkan norma-norma pengungkapan yang mengimbangi naluri kepemilikan. Setiap instrumen pengaturan pribadi yang dijelaskan dalam Bagian ini menyalurkan budaya "ungkapkan dan berkolaborasi" yang telah lama ada ke dalam arsitektur IP kumpulan paten, lisensi FRAND yang dapat dengan mudah diakomodasi oleh hukum.

Perusahaan jarang berinovasi secara terisolasi. Mereka sering membutuhkan kolaborator, pengadopsi, dan standar. Kerahasiaan tidak menghasilkan ekosistem. Akibatnya, pengembang QIT semakin terlibat dalam keterbukaan selektif: menahan pengetahuan sensitif sambil mematenkan penemuan-penemuan kunci untuk mencegah pengajuan paten yang luas dari pesaing dan menarik investasi. IBM mencontohkan pendekatan ini. Meskipun IBM menjaga kerahasiaan aspek-aspek kunci dari desain prosesor kuantumnya, perusahaan ini mematenkan secara ekstensif dan menyediakan akses terbuka ke platform cloud kuantum dan alat pengembangnya. Tujuan dari strategi ini adalah untuk mengkatalisasi inovasi eksternal

pada tumpukan IBM, yang pada akhirnya memperkuat posisi pasar dan kepemimpinan perusahaan di bidang ini.

3.6 STRATEGI IP TERKALIBRASI DALAM TEKNOLOGI INFORMASI KUANTUM

Teknologi informasi kuantum tampaknya tidak memerlukan rezim IP *sui generis*. Sebaliknya, instrumen dan kerangka hukum yang ada telah terbukti cukup adaptif bila diterapkan dengan memperhatikan fitur-fitur khas bidang ini. Seperti yang telah ditunjukkan bagian ini, perusahaan terlibat dalam "superposisi" strategi IP yang bervariasi tergantung pada posisi mereka dalam tumpukan kuantum, tahap pengembangan mereka, lingkungan pendanaan, dan model bisnis. Perusahaan rintisan yang mencari modal ventura mungkin menekankan pengajuan paten untuk menarik investor, sementara perusahaan besar yang memiliki sumber daya yang memadai mungkin lebih mengandalkan kerahasiaan dagang dan keterbukaan yang terkontrol untuk melindungi kemampuan inti dan membentuk standar. Heuristik tumpukan tata kelola menawarkan kerangka kerja yang berguna untuk memahami bagaimana berbagai alat hukum selaras dengan lapisan teknis tertentu: dari perangkat keras dan sistem kontrol hingga perangkat lunak dan antarmuka pengguna. Alih-alih mengajukan biner antara model kepemilikan dan terbuka, bagian ini menekankan pentingnya kombinasi yang terkalibrasi yang bergeser dari waktu ke waktu dan di berbagai konteks. Pertanyaan kebijakan kuncinya bukanlah apakah paten atau kerahasiaan secara inheren cocok untuk inovasi kuantum, tetapi bagaimana, di mana, dan dalam kondisi apa setiap mode perlindungan berkontribusi pada insentif swasta dan nilai publik yang lebih luas. Dalam lanskap yang berlapis dan heterogen ini, interaksi antara eksklusivitas dan keterbukaan bukanlah sebuah kontradiksi, melainkan ciri khas strategi inovasi yang efektif.

BAB 4
LANSKAP PATEN TEKNOLOGI KUANTUM DAN DAMPAK KEBIJAKAN

Kemajuan terkini dalam ilmu kuantum menyoroti potensi kemampuan transformatif teknologi kuantum generasi kedua (2G), seperti komputasi kuantum, komunikasi kuantum, dan penginderaan kuantum. Tren paten dalam teknologi tersebut berfungsi sebagai indikator utama kecepatan inovasi pada tahap penemuan. Pemeriksaan empiris aktivitas paten di dunia nyata menawarkan bukti penting untuk mengevaluasi dan menginformasikan usulan kebijakan tentang hak kekayaan intelektual, inovasi, dan tata kelola dalam teknologi kuantum. Berdasarkan wawasan yang diperoleh dari studi kami sebelumnya pada tahun 2022 yang memetakan lanskap paten teknologi kuantum, bagian ini melaporkan hasil studi terbaru yang menggabungkan data hingga Oktober 2025. Kami menilai tren paten selama periode 2001 hingga 2025 untuk menentukan: (1) pertumbuhan paten teknologi kuantum, (2) rincian teknologi dan klasifikasi aktivitas paten, (3) pilihan kantor paten prioritas, (4) jenis klaim dan strategi paten, (5) pokok bahasan paten yang baru diberikan, (6) pemilik paten teratas, (7) portofolio paten dominan, dan (8) distribusi geografis aktivitas ini. Dengan menggunakan pemeriksaan lanskap ini, kami secara kritis mengevaluasi dampak paten di bidang teknologi kuantum, mulai dari signifikansinya dalam mendorong inovasi hingga efek nilai pribadinya. Temuan kami menunjukkan bagaimana pengungkapan paten berkontribusi pada munculnya informasi kuantum bersama, yang secara progresif memperkaya domain publik. Selanjutnya, kami mengeksplorasi dampak inovasi dan kebijakan dari hasil ini dalam kerangka yang lebih luas dari inisiatif inovasi kuantum, dinamika persaingan pasar, antarmuka paten-rahasia dagang, dan tata kelola teknologi kuantum, dengan menekankan peran paten dalam mendorong pengungkapan di tengah komersialisasi yang cepat dan pergeseran geopolitik.

4.1 KEMAJUAN TEKNOLOGI KUANTUM 2G DAN DAMPAK KEBIJAKAN

Kemajuan terkini dalam ilmu kuantum telah menyoroti potensi besar teknologi kuantum generasi kedua (2G), yang mencakup berbagai bidang seperti simulasi, penginderaan dan metrologi, komputasi, dan komunikasi. Tonggak penting, termasuk demonstrasi keunggulan kuantum dengan prosesor yang dapat diprogram yang menggunakan qubit superkonduktor, menggambarkan kemajuan ini. Penerapannya mencakup berbagai hal, mulai dari simulasi sistem kuantum kompleks untuk memajukan pengetahuan dasar dan penggunaan praktis (misalnya, mempercepat penemuan obat melalui pemodelan proses kimia), hingga memungkinkan presisi superior dalam pengukuran melalui penginderaan dan metrologi kuantum, mengatasi tantangan komputasi yang sulit dipecahkan dengan algoritma kuantum pada komputer kuantum, dan membangun jaringan komunikasi ultra-aman.

Perkembangan ini memikat akademisi, industri, dan pembuat kebijakan, karena dampaknya terhadap pembelajaran fundamental, berbagai sektor seperti teknologi informasi dan farmasi, serta pertimbangan keamanan nasional. Inovasi dalam teknologi kuantum biasanya muncul dari kolaborasi antara lembaga akademik, perusahaan, dan dinamika pasar,

termasuk tekanan kompetitif, pendatang baru, teknologi alternatif, dan daya tawar pemangku kepentingan. Pemerintah sangat penting, membentuk struktur insentif dan lingkungan peraturan, sementara seringkali bertindak sebagai pelanggan utama, terutama untuk aplikasi yang berkaitan dengan pertahanan.

Strategi pemerintah mencakup mekanisme pendorong seperti hibah pembelajaran yang memicu revolusi kuantum pertama dan inisiatif transfer teknologi yang mendorong revolusi kuantum kedua, yang dicontohkan oleh Program Unggulan Teknologi Kuantum Eropa dan insentif penarik seperti perlindungan paten untuk mendorong pengungkapan penemuan sebagai imbalan atas eksklusivitas terbatas. Insentif pendorong bertujuan untuk mendorong teknologi dari tahap awal pembuktian konsep (misalnya, Tingkat Kesiapan Teknologi 3) menuju validasi prototipe dalam pengaturan yang relevan (TRL 6-7), sementara mekanisme penarik, termasuk hak kekayaan intelektual (HKI), memfasilitasi komersialisasi setelah risiko dikurangi (TRL 8-9).

Sebagai antisipasi integrasi teknologi kuantum ke dalam produk praktis, para cendekiawan, pejabat, dan analis telah menyuarakan kekhawatiran dan mengajukan rekomendasi untuk tata kelola, standardisasi (misalnya, melalui ISO/IEC/IEEE), dan regulasi. Rekomendasi ini sering menargetkan insentif, HKI, dan pengawasan yang lebih luas. Untuk mengevaluasi ide-ide tersebut secara efektif, ide-ide tersebut harus didasarkan pada wawasan empiris untuk pembuatan kebijakan yang berbasis bukti. Misalnya, pembelajaran sebelumnya telah menunjukkan risiko perlindungan IP yang berlebihan di bidang kuantum dan menyarankan penyesuaian sistem paten. Namun, apakah bukti kontemporer pada tahun 2025 mendukung klaim perlindungan yang berlebihan?

Pola apa yang muncul dalam paten teknologi kuantum selama seperempat abad terakhir? Negara dan entitas mana yang mendominasi aktivitas ini? Struktur dan strategi klaim apa yang berlaku, dan di tempat mana perlindungan dicari? Tanpa pemeriksaan IP yang kuat dan berbasis data yang menjawab pertanyaan-pertanyaan ini, para pembuat kebijakan berisiko melakukan modifikasi yang tidak bijaksana terhadap rezim yang ada, terutama di bidang yang berisiko tinggi dan padat modal seperti teknologi kuantum yang menuntut untuk mengatasi hambatan ilmiah dan teknik yang berat.

Kurangnya perlindungan secara konvensional dipandang sebagai penghambat insentif di bidang-bidang yang sedang berkembang, di mana paten dan HKI lainnya sangat penting untuk mengamankan investasi untuk R&D yang berisiko. Sebaliknya, terlalu banyak perlindungan dapat menciptakan hambatan pasar, melemahkan persaingan dan inovasi terbuka. Paten menandakan dinamika inovasi pada fase penemuan, menjadikan studi paten empiris sangat berharga untuk menilai kebijakan tentang HKI, inovasi, dan regulasi. Pentingnya studi empiris di bidang-bidang ini semakin dipertegas oleh ketegangan geopolitik saat ini dan meningkatnya seruan untuk menggunakan HKI dan regulasi sebagai salah satu instrumen dalam upaya meningkatkan ketahanan dan apa yang disebut "kedaulatan teknologi" di bidang-bidang yang sangat penting secara strategis, seperti teknologi AI dan kuantum.

Namun, pemeriksaan paten yang ada di bidang ini masih terbatas: banyak yang tidak memiliki pemantauan sejawat, berkonsentrasi pada pemantauan yang sempit, atau inovasi

metodologis, atau sudah ketinggalan zaman. Bagian ini menyajikan pemetaan lanskap paten teknologi kuantum yang diperbarui, berdasarkan studi kami sebelumnya yang diterbitkan dalam *International Review of Intellectual Property and Competition Law*. Dengan menggabungkan data empat tahun tambahan hingga Oktober 2025, kami memeriksa tren dari tahun 2001 dan seterusnya untuk memastikan: (1) pertumbuhan paten dalam teknologi kuantum, (2) kategorisasi dan rincian teknologi, (3) kantor prioritas pilihan, (4) jenis dan pendekatan klaim, (5) isi pemberian paten baru-baru ini, (6) pemilik terkemuka dan profil mereka, (7) portofolio berpengaruh melalui kutipan ke depan, dan (8) pola geografis global. Temuan ini memungkinkan kami untuk meneliti pernyataan tentang perlindungan paten yang berlebihan atau kurang dalam teknologi kuantum terapan di garis depan teknologi saat ini. Kami selanjutnya memeriksa inovasi dan dampak kebijakan dalam konteks inisiatif kuantum, pasar kompetitif, hubungan paten-rahasia dagang, dan tata kelola kuantum.

4.2 DEFINISI TEKNOLOGI KUANTUM

Mendefinisikan teknologi kuantum secara akurat sangat penting, khususnya dalam konteks perlindungan kekayaan intelektual, karena hal itu menentukan batasan penemuan apa yang dianggap "kuantum" untuk dipatenkan dalam bidang yang sedang berkembang ini. Definisi yang tepat membantu menentukan klasifikasi di bawah sistem seperti Klasifikasi Paten Kooperatif (CPC), serta panduan khusus kuantum terkait kelayakan materi pokok, deskripsi tertulis dan persyaratan pengaktifan, dan ruang lingkup perlindungan, sambil menghindari campur tangan yang berlebihan terhadap teknologi klasik yang sudah mapan. Kejelasan ini penting bagi para pembuat kebijakan yang mempertimbangkan panduan atau reformasi, seperti potensi rezim *sui generis* untuk kekayaan intelektual kuantum, untuk mencegah distorsi dalam insentif inovasi dan menjaga keselarasan dengan standar internasional seperti TRIPS, yang mewajibkan ketersediaan paten yang netral terhadap teknologi. Kesalahan definisi dapat menyebabkan kurangnya perlindungan, yang menghambat investasi dalam R&D berisiko tinggi, atau perlindungan yang berlebihan, yang menciptakan hambatan masuk dan menghambat kemajuan kolaboratif dalam domain yang semakin terkait erat dengan keamanan nasional dan persaingan global.

Seperti yang telah kami catat sebelumnya, tampaknya wajar untuk mendefinisikan teknologi kuantum sebagai teknologi yang operasinya diatur oleh hukum mekanika kuantum. Namun, definisi tersebut bermasalah karena secara teknis hukum mekanika kuantum mengatur perilaku semua fenomena fisik pada tingkat partikel fundamental. Bahkan definisi yang lebih sempit seperti teknologi yang operasinya memanfaatkan prinsip-prinsip mekanika kuantum akan mencakup perangkat semikonduktor yang digunakan dalam prosesor klasik terbaru, karena panjang kanal transistor yang digunakan saat ini berada pada skala 2 nm yang berarti bahwa efek mekanika kuantum harus dipertimbangkan dalam desain dan pengembangan perangkat elektronik ini. Dengan demikian, teknologi kuantum sering diklasifikasikan menjadi dua generasi, dan istilah tersebut biasanya dikhususkan untuk teknologi yang termasuk dalam generasi kedua (2G).

Teknologi generasi pertama (1G) meliputi transistor, laser, dan perangkat lain yang desain dan operasinya didasarkan pada prinsip-prinsip mekanika kuantum (yaitu, perangkat yang secara langsung memanfaatkan penemuan ilmiah dari revolusi kuantum pertama). Perangkat 1G ini telah menghasilkan teknologi komputasi dan komunikasi yang telah mengubah seluruh industri dan masyarakat sejak diperkenalkannya sirkuit terpadu semikonduktor (IC) pertama. Paten awal tentang IC (Paten AS No. US3138743A, diajukan pada tahun 1959 dan diberikan pada tahun 1964) menyatakan:

> [...] tujuan utama dari penemuan ini adalah untuk menyediakan sirkuit elektronik mini baru yang dibuat dari bahan semikonduktor [...] di mana semua komponen sirkuit elektronik sepenuhnya terintegrasi ke dalam bahan semikonduktor.

Miniaturisasi melalui IC menyebabkan revolusi komputer dan teknologi informasi. Sebagai ilustrasi, prosesor Intel 8008 yang diperkenalkan pada tahun 1974 berisi 2500 transistor dan menggunakan proses MOS 10.000 nm, Intel Pentium 4 tahun 2005 berisi 169 juta transistor (90 nm), Intel Xeon tahun 2017 berisi 8 miliar transistor (14 nm), Apple M1 Max tahun 2021 memiliki 57 miliar transistor (5 nm), dan NVIDIA Blackwell B200 tahun 2025 memiliki 208 miliar transistor (4 nm), dengan proses 2 nm yang mulai diproduksi pada akhir tahun 2025.

Miniaturisasi ini memungkinkan industri untuk meningkatkan jumlah transistor dalam sebuah chip (yaitu, meningkatkan daya komputasi dan fungsionalitas IC) dan kecepatannya, sekaligus mengurangi biaya produksi. Konsekuensi dari penskalaan ini adalah bahwa perangkat klasik yang digunakan dalam "komputer klasik" menunjukkan efek mekanika kuantum yang perlu diperhitungkan sebagai bagian dari desain dan pengembangan prosesor (CPU) dan unit pemrosesan grafis (GPU) untuk perangkat komputasi kita saat ini (misalnya, telepon, tablet, laptop, komputer). Dengan kata lain, fenomena fisika kuantum menjadi tak terhindarkan pada skala nanometer. Misalnya, pada skala submikron dan nanometer yang sangat kecil, MOSFET menunjukkan penerowongan mekanika kuantum dari sumber ke oksida gerbang karena ketebalan lapisan oksida (sekitar 2 nm), penerowongan mekanika kuantum dari sumber ke drain ketika panjang saluran kurang dari 10 nm, dan kuantisasi energi.

Teknologi kuantum generasi kedua (2G) adalah teknologi yang saat ini sedang dikembangkan yang secara langsung memanfaatkan fenomena mekanika kuantum yang unik seperti superposisi, keterikatan, penerowongan, dan kuantisasi sebagai prinsip operasi dasarnya (yaitu, perangkat yang operasinya secara langsung memanfaatkan fenomena kuantum) untuk mencapai keunggulan dibandingkan teknologi canggih kita saat ini. Ini termasuk komputasi kuantum, komunikasi kuantum, dan penginderaan kuantum.

4.3 STRATEGI PENCARIAN DAN KRITERIA SELEKSI PATEN

Untuk menjawab pertanyaan pembelajaran yang diuraikan di atas, kami menggunakan strategi pencarian yang disempurnakan yang mendorong konsistensi dan transparansi dalam pemetaan lanskap paten, sambil tetap mematuhi pedoman yang telah ditetapkan untuk kualitas dan reproduksibilitas dalam laporan lanskap paten. Pendekatan ini dirancang khusus

untuk tujuan studi kami daripada menawarkan gambaran umum yang komprehensif. Metode yang sebanding sebelumnya telah diterapkan untuk memetakan lanskap paten di bidang-bidang seperti paten gen, penggunaan kembali obat, dan AI medis.

Strategi kami mencakup pencarian yang luas dan sangat sensitif (Tabel 4.1, ID Pencarian: S1) hingga kueri yang lebih terarah dan sangat spesifik yang bertujuan untuk mengurangi kesalahan positif (Tabel 4.1, ID Pencarian: S4). Secara spesifik, kriteria ini mencakup: 1) semua dokumen paten yang secara longgar terkait dengan konsep "kuantum" (S1), 2) paten teknologi kuantum esensial (S2), 3) paten yang menampilkan klaim yang berfokus pada penemuan terkait "kuantum" (S3), dan 4) paten di mana klaim independen berkaitan dengan teknologi kuantum (S4). S1 memprioritaskan inklusivitas, mencakup dokumen apa pun dengan kata kunci seperti "kuantum" atau istilah terkait (misalnya, qubit, keterikatan) untuk menetapkan batas atas untuk paten terkait kuantum yang didefinisikan secara luas. Sebaliknya, S2-S4 meningkatkan presisi dengan membatasi hasil pada kasus di mana kata kunci muncul dalam judul, abstrak, atau klaim (TAC) untuk S2, hanya dalam klaim untuk S3, dan dalam klaim independen untuk S4.

Untuk lebih meningkatkan spesifisitas, kami membatasi hasil pada kategori Klasifikasi Paten Kooperatif (CPC) yang ditetapkan oleh USPTO dan EPO untuk penemuan khusus kuantum. Metode ini memanfaatkan klasifikasi manual ahli oleh pemeriksa paten di kantor-kantor tersebut, menggabungkan pencarian otomatis dengan pengawasan manusia. CPC, perluasan dari Klasifikasi Paten Internasional (IPC) WIPO, dikelola bersama oleh USPTO dan EPO untuk menstandarisasi klasifikasi dan meningkatkan efisiensi pencarian di berbagai yurisdiksi.

Kami menggunakan kelas CPC untuk mengelompokkan paten ke dalam area kuantum utama: perangkat kuantum (S5), optik kuantum (S6), pemrosesan informasi kuantum (S7), komputasi kuantum (S8), kriptografi kuantum (S9), dan komunikasi kuantum (S10). Pemeriksaan selanjutnya dari dokumen-dokumen ini meneliti pertumbuhan tahunan dalam pematenan teknologi kuantum, status hukum paten, kantor prioritas pilihan, aktivitas berdasarkan kelas CPC, bahasa klaim dan konsep inventif, pemilik terkemuka dalam komputasi kuantum, metrik kutipan ke depan, dan distribusi geografis di seluruh dunia. Pencarian mencakup aplikasi dan pemberian paten yang diterbitkan dari 1 Januari 2001 hingga 15 Oktober 2025 (dilakukan pada 15 Oktober 2025).

Tabel 4.1 Teknologi kuantum yang dipatenkan di AS (USPTO) dan Eropa (EPO)

ID	Konsep Pencarian	Istilah Pencarian	Aplikasi	Diberikan
S1	Paten terkait kuantum	"kuantum" (& kata kunci QT)	344.541	238.303
S2	Paten kuantum (TAC)	S1 & TAC:Kuantum	49.894	29.701
S3	Klaim kuantum	ACLM: Kuantum	43.704	27.131
S4	Klaim independen Q.	ICLM: Kuantum	22.546	15.448
S5	Komputasi kuantum	CPC: G06N10	6685	2879

Sumber: Data aplikasi dan pemberian paten USPTO & EPO dari 1 Januari 2001 hingga 15 Oktober 2025 (pencarian dilakukan oleh MA pada 15 Oktober 2025). Kelas CPC G06N10 dikhususkan untuk

"Komputasi kuantum, yaitu pemrosesan informasi berdasarkan fenomena mekanika kuantum" (dengan total 2879 paten yang diberikan oleh USPTO dan EPO di semua tanggal).

4.4 HASIL PEMERIKSAAN LANSKAP PATEN

Setelah menjabarkan strategi pencarian, bagian ini menyajikan hasil empiris dari pemeriksaan lanskap paten. Pertama, kami menjelaskan ukuran dan komposisi dataset di seluruh set pencarian kami (S1–S5) dan kelas CPC utama, sebelum memeriksa aktivitas paten tahunan, status hukum, spesialisasi teknologi, preferensi kantor, struktur klaim, pola kepemilikan, dinamika sitasi, dan distribusi geografis. Sepanjang pembahasan, penekanan khusus diberikan pada paten komputasi kuantum, yang memberikan lensa fokus pada perkembangan di subbidang yang penting secara strategis.

Hasil Pencarian Paten

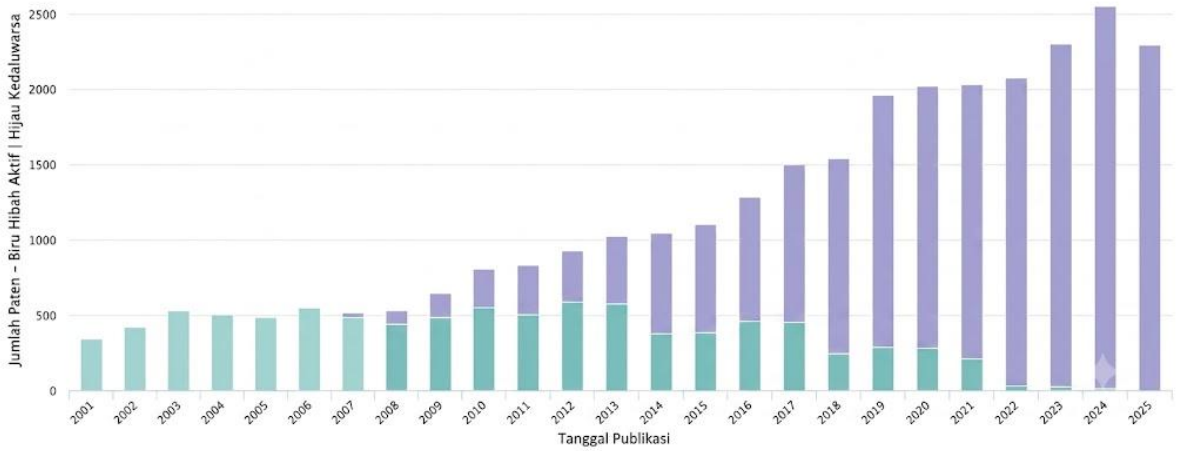
Tabel 4.1 menyajikan hasil pencarian kami untuk aplikasi paten dan paten yang diberikan terkait teknologi kuantum, yang diterbitkan antara tahun 2001 dan 2025 di USPTO dan EPO. Metodologi bervariasi dari pencarian sensitivitas tinggi (S1) hingga pencarian spesifisitas tinggi (S2–S5) untuk mengurangi kesalahan positif. Temuan kami mengungkapkan 344.541 aplikasi paten terkait kuantum dan 238.303 pemberian paten sejak tahun 2001 (S1). Namun, sebagian besar hanya terkait secara periferal dengan teknologi kuantum, menjadikan S1 sebagai batas atas yang luas untuk paten terkait kuantum yang didefinisikan secara inklusif.

Pencarian S2–S5 mempersempit fokus untuk menentukan paten teknologi kuantum inti dan mengkategorikannya berdasarkan subbidang. Kami mengidentifikasi 29.701 paten yang diberikan di mana "kuantum" menjadi pusat, muncul dalam judul, abstrak, atau klaim (TAC) (S2). Di antara paten-paten ini, 27.131 mencakup setidaknya satu klaim dengan "kuantum" sebagai batasan (S3), dan 15.448 memiliki klaim independen yang diarahkan pada penemuan terkait kuantum (S4). Studi kami akan secara khusus berfokus pada paten yang terkait dengan komputasi kuantum (yaitu, yang termasuk dalam kelas CPC G06N10), yang totalnya ada 2879 paten yang diberikan sejak tahun 2001.

Aktivitas Paten Teknologi Kuantum Tahunan dan Status Hukum

Gambar 4.1 menunjukkan aktivitas paten tahunan untuk teknologi kuantum di USPTO dan EPO (S2). Gambar tersebut menunjukkan status hukum saat ini (aktif atau kedaluwarsa) dari paten yang diberikan yang diterbitkan setiap tahun sejak tahun 2001. Hasilnya menunjukkan peningkatan lima kali lipat dalam jumlah paten yang diberikan per tahun dalam 10 tahun terakhir, dari sekitar 500 pada tahun 2004 menjadi lebih dari 2500 pada tahun 2024, yang sesuai dengan tingkat pertumbuhan tahunan majemuk (CAGR) sebesar 17,5%. Pertumbuhan ini tidak terjadi dengan laju konstan selama seluruh periode, melainkan grafik menunjukkan periode stabilitas relatif (misalnya, hampir tidak ada peningkatan jumlah paten yang diberikan per tahun) antara tahun 2003 dan 2008, diikuti oleh periode peningkatan pesat selama 10 tahun hingga 2019, dan kemudian periode stagnasi pertumbuhan lainnya dari tahun 2019 hingga 2022 (mungkin dipengaruhi oleh pembatasan selama pandemi COVID-19) sebelum periode pertumbuhan pesat lainnya dimulai pada tahun 2023. Grafik tersebut juga menunjukkan bahwa sekitar 25% dari paten yang diberikan sejak tahun 2001 telah

kedaluwarsa dan dengan demikian memasuki domain publik. Angka ini tidak termasuk aplikasi yang mungkin telah ditolak atau ditinggalkan, yang juga berkontribusi pada volume pengungkapan publik di bidang teknologi kuantum.



Gambar 4.1 Aktivitas paten tahunan untuk teknologi kuantum di USPTO dan EPO (ID Pencarian: S2) dan status hukum saat ini (aktif atau kedaluwarsa) diurutkan berdasarkan tanggal publikasi paten (2001-01-01 hingga 2025-09-30)

Rincian Teknologi

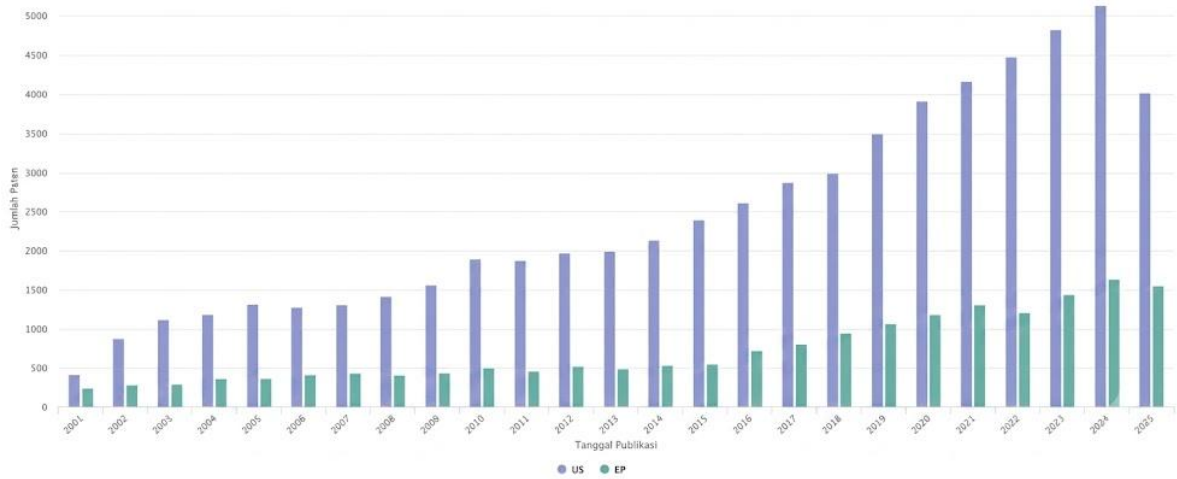
Tabel 4.2 menunjukkan kelas CPC teratas berdasarkan jumlah paten yang diberikan, deskripsinya, dan paten yang diberikan untuk setiap kelas oleh USPTO dan EPO. Hasil kami menunjukkan bahwa kelas B82Y* yang terkait dengan nanostruktur dan aplikasinya (misalnya, optik kuantum, komputasi kuantum, logika elektron tunggal) memiliki jumlah paten tertinggi $(n > 6000)$, diikuti oleh komputasi kuantum G06N10 $(n = 3295)$ dan kriptografi $(n = 1742)$.

Aktivitas Paten Teknologi Kuantum USPTO vs EPO

Gambar 4.2 menunjukkan jumlah dokumen paten yang dipublikasikan (aplikasi paten yang dipublikasikan dan paten yang diberikan) tentang teknologi kuantum yang dipisahkan berdasarkan kantor paten (USPTO versus EPO). Hasil pembelajaran kami menunjukkan bahwa USPTO telah menjadi kantor paten pilihan selama 25 tahun terakhir, dengan jumlah paten yang diberikan oleh USPTO secara konsisten melebihi 75% dari total jumlah paten yang diberikan oleh USPTO dan EPO secara gabungan. Meskipun jumlah total paten untuk kedua kantor tersebut terus meningkat selama 10 tahun terakhir, proporsi paten yang diberikan oleh masing-masing kantor tetap relatif stabil dari waktu ke waktu. Pada tahun 2024, dari total 6823 paten USPTO/EPO, 5172 (75,8%) diberikan oleh USPTO dan 1651 (24,2%) oleh EPO.

Tabel 4.2 Paten terkait kuantum USPTO dan EPO yang diklasifikasikan berdasarkan kelas CPC

CPC	Deskripsi Kelas Klasifikasi Paten Kooperatif (CPC)	Paten
B82Y20	PENGGUNAAN ATAU APLIKASI SPESIFIK DARI NANOSTRUKTUR; PENGUKURAN ATAU ANALISIS NANOSTRUKTUR; MANUFAKTUR ATAU PERLAKUAN NANOSTRUKTUR > Nanooptik, msl. **optika kuantum atau kristal fotonik**	4047
G06N10	PENGATURAN KOMPUTASI BERDASARKAN MODEL KOMPUTASI SPESIFIK > **Komputasi kuantum, yaitu pemrosesan informasi berdasarkan fenomena mekanika kuantum**	3295
B82Y10	PENGGUNAAN ATAU APLIKASI SPESIFIK DARI NANOSTRUKTUR; PENGUKURAN ATAU ANALISIS NANOSTRUKTUR; MANUFAKTUR ATAU PERLAKUAN NANOSTRUKTUR > Nanoteknologi untuk pemrosesan, penyimpanan, atau transmisi informasi, msl. **komputasi kuantum atau logika elektron tunggal**	2724
H04L9	TRANSMISI INFORMASI DIGITAL, msl. KOMUNIKASI TELEGRAF > Mekanisme kriptografi atau pengaturan kriptografi untuk komunikasi rahasia atau aman; Protokol keamanan jaringan	1742



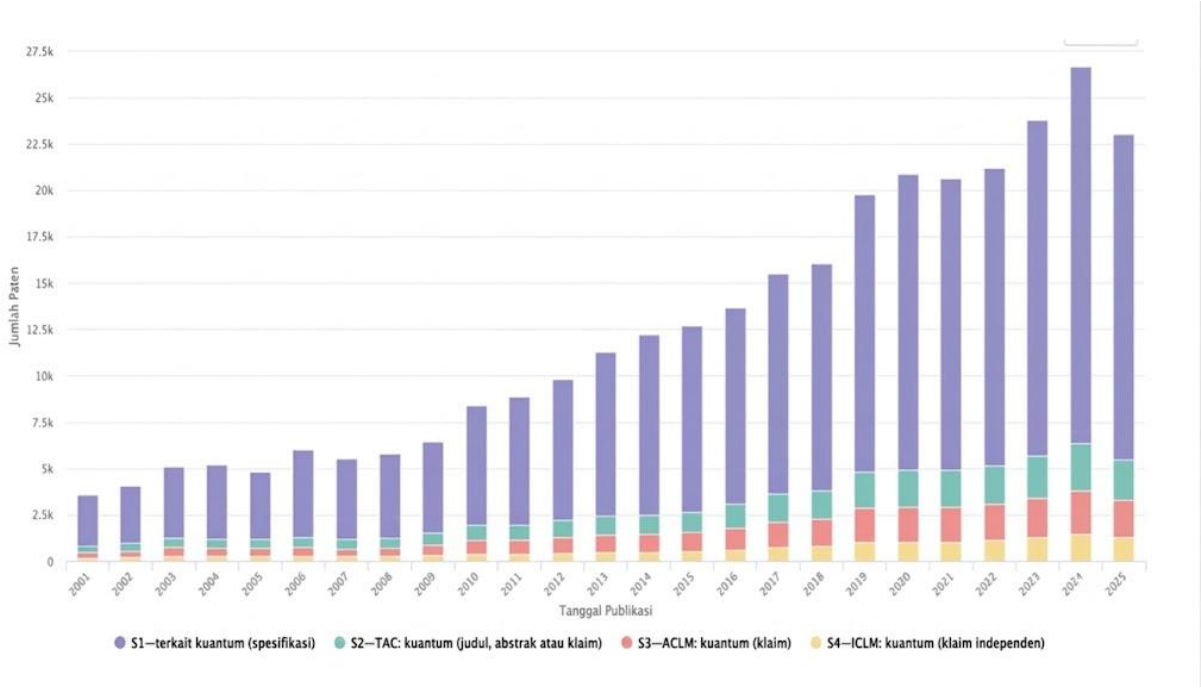
Gambar 4.2 Pilihan kantor paten (USPTO vs. EPO) untuk teknologi kuantum (ID Pencarian: S2)

Paten yang Mengklaim Teknologi Kuantum

Gambar 4.3 menunjukkan prevalensi (a) paten yang secara luas terkait dengan teknologi kuantum (S1), (b) paten kuantum inti (S2), (c) paten dengan klaim yang diarahkan pada konsep kuantum (S3), dan (d) paten dengan klaim independen (klaim terluas) yang diarahkan pada konsep kuantum (S4). Karena pencarian S1 mencakup setiap paten yang menyertakan kata kunci "kuantum" dan konsep terkait (misalnya, qubit, entangl* dan super-posit*) di mana pun dalam dokumen paten, maka pencarian ini sangat sensitif tetapi tidak spesifik (yaitu, selain paten teknologi kuantum inti, pencarian ini juga mencakup aplikasi terkait yang menyebutkan "kuantum" atau istilah terkait di mana pun dalam spesifikasi). Oleh karena itu, hasil lanskap kami didasarkan pada pencarian yang lebih spesifik di mana teknologi kuantum merupakan inti dari paten dan karenanya kata kunci kuantum digunakan dalam TAC

(S2), klaim (S3) dan klaim independen (S4). Kami juga lebih fokus pada paten yang termasuk dalam kelas CPC G06N10, yang berkaitan dengan komputasi kuantum (S5).

Gambar 4.3 menunjukkan bahwa lebih dari 90% paten yang menggunakan kata kunci "kuantum" dalam judul atau abstrak (S2) juga memiliki klaim yang diarahkan pada konsep penemuan "kuantum" (S3). Selain itu, dalam lebih dari 50% paten S2, konsep penemuan kuantum diklaim dalam klaim terluas dari paten tersebut (yaitu, klaim independen). Sejak tahun 2020 telah ada lebih dari 2000 publikasi paten per tahun (S2), dengan lebih dari 1800 publikasi paten per tahun yang berisi klaim yang diarahkan pada konsep kuantum (S3) dan lebih dari 1000 publikasi paten tahunan dengan klaim terluas yang mencakup fitur atau batasan kuantum (S4).

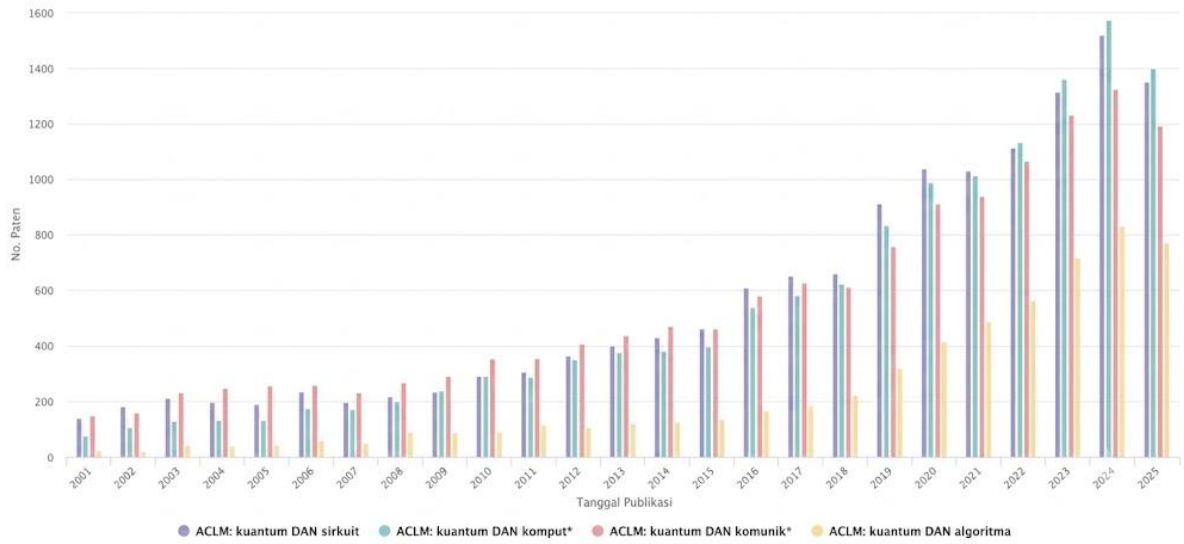


Gambar 4.3 Prevalensi relatif dari (a) paten yang secara luas terkait dengan teknologi kuantum (S1), (b) paten kuantum inti (S2), (c) paten dengan klaim yang diarahkan pada konsep kuantum (S3), dan (d) paten dengan klaim independen yang terkait dengan konsep kuantum (S4)

Gambar 4.4 menunjukkan prevalensi relatif paten teknologi kuantum USPTO dan EPO dengan klaim yang terkait dengan (a) sirkuit kuantum, (b) komputasi kuantum, (c) komunikasi kuantum, dan (d) algoritma kuantum. Selama 25 tahun terakhir, paten yang mencakup batasan klaim terkait dengan sirkuit kuantum (ACLM: kuantum dan sirkuit*) dan komunikasi kuantum (ACLM: kuantum dan komunikasi*) telah menjadi yang paling umum, dengan kesamaan yang erat antara jumlah paten di masing-masing dari dua kategori tersebut. Namun, dalam 5 tahun terakhir, paten komputasi kuantum telah mengambil alih sebagai jenis yang paling umum.

Paten yang berisi batasan klaim yang diarahkan pada "algoritma" kuantum telah tertinggal secara signifikan di belakang tiga jenis lainnya. Pengacara paten mungkin sengaja menghindari penggunaan kata "algoritma" dalam klaim untuk mengatasi pembatasan

kelayakan materi pokok yang terkait dengan ketidaklayakan paten dari "ide abstrak" (Bilsky dan Alice). Meskipun demikian, Gambar 4.4 menunjukkan peningkatan yang signifikan dan konsisten dalam paten yang terkait dengan algoritma kuantum (ACLM: kuantum dan algoritma) dalam 5 tahun terakhir.



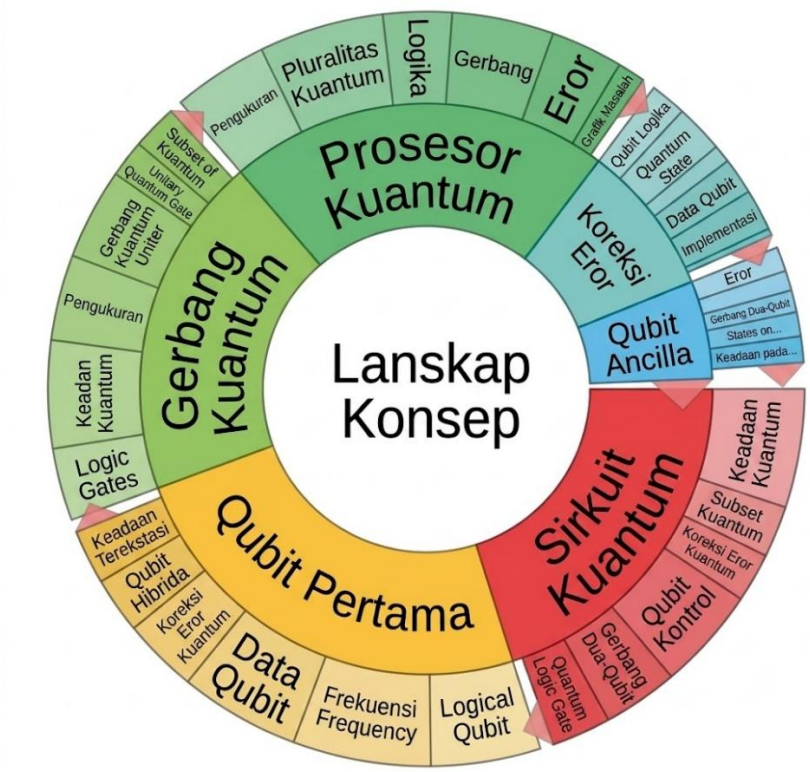
Gambar 4.4 Prevalensi relatif paten teknologi kuantum USPTO dan EPO dengan klaim yang diarahkan pada (a) sirkuit kuantum, (b) komputasi kuantum, (c) komunikasi kuantum, dan (c) algoritma kuantum.

Gambar 4.5 menunjukkan lanskap konsep untuk paten komputasi kuantum (S5). Grafik ini dihasilkan menggunakan pemeriksaan teks otomatis dari abstrak, judul, dan klaim untuk mengidentifikasi istilah yang sering digunakan dan mengelompokkannya berdasarkan kategori. Hasil kami menunjukkan bahwa paten dikelompokkan dalam enam area utama, yaitu, (1) sirkuit kuantum, (2) prosesor kuantum, (3) gerbang kuantum, (4) modalitas qubit, dan (5) koreksi kesalahan. Lapisan kedua mencakup detail tambahan mengenai istilah yang digunakan untuk menggambarkan dan mengklaim konsep inventif masing-masing. Beberapa di antaranya tumpang tindih di seluruh kelompok utama. Misalnya, "bit kuantum" (qubit) terdapat dalam paten yang terkait dengan "keadaan kuantum" dan "komputasi kuantum". Demikian pula, istilah "prosesor kuantum" dan "kontrol kuantum" merupakan bagian dari kelompok "sirkuit kuantum" dan "komputasi kuantum" dari paten S2.

Gambar 4.5 dapat dianggap sebagai ringkasan istilah teknis yang digunakan dalam judul, abstrak, dan klaim dari 3732 paten komputasi kuantum (CPC G06N10) yang telah diberikan di semua tanggal. Meskipun demikian, informasi ini sangat ringkas dan bukan pengganti pemeriksaan langsung terhadap bahasa klaim sebenarnya untuk memeriksa strategi penyusunan klaim dan ruang lingkup perlindungan.

Pemantauan terhadap pemberian paten di G06N10 (yaitu, kelas CPC untuk komputasi kuantum) mengungkapkan bahwa klaim paten diarahkan pada: (1) realisasi fisik blok bangunan

untuk komputer kuantum (misalnya, prosesor kuantum dan komponen untuk memanipulasi qubit seperti kontrol qubit), (2) koreksi kesalahan kuantum (misalnya, deteksi dan pencegahan kesalahan menggunakan kode permukaan, distilasi keadaan ajaib, dll.), (3) model sirkuit kuantum dan komputer kuantum universal, (4) aplikasi algoritma kuantum (misalnya, optimasi kuantum, transformasi Fourier atau Hadamard kuantum terapan, dll.), dan (5) platform untuk mengakses, mensimulasikan, dan memprogram komputer kuantum (misalnya, komputasi berbasis awan, platform untuk mensimulasikan sistem kuantum, antarmuka pemrograman kuantum).



Gambar 4.5 Lanskap konsep untuk paten komputasi kuantum (CPC: G06N10)

Secara khusus, subkelas teratas dalam kelas komputasi kuantum CPC G06N10 dalam hal paten yang diberikan oleh USPTO dan EPO adalah:

- G06N10/40-"Realisasi fisik atau arsitektur prosesor kuantum atau komponen untuk memanipulasi qubit, misalnya kopling qubit atau kontrol qubit" dengan 2312 paten yang diberikan.
- G06N10/20-"Model komputasi kuantum, misalnya sirkuit kuantum atau komputer kuantum universal" dengan 1408 paten yang diberikan.
- G06N10/60-"Algoritma kuantum, misalnya berdasarkan optimasi kuantum, transformasi Fourier atau Hadamard kuantum" dengan 993 paten yang diberikan.
- G06N10/70-"Koreksi, deteksi, atau pencegahan kesalahan kuantum, misalnya kode permukaan" dengan 828 paten yang diberikan.
- G06N10/80-"Pemrograman kuantum, misalnya antarmuka, bahasa, atau kit pengembangan perangkat lunak untuk membuat atau menangani program yang

mampu berjalan di komputer kuantum; Platform untuk mensimulasikan atau mengakses komputer kuantum, misalnya komputasi kuantum berbasis cloud" dengan 535 paten yang diberikan.

Paten Komputasi Kuantum yang Baru Diberikan

Tabel 4.3 mencantumkan judul-judul paten komputasi kuantum terbaru yang diberikan pada bulan sebelum tanggal pencarian dan masing-masing penerima patennya. Menurut 37 CFR 1.72, "Judul penemuan tidak boleh melebihi 500 karakter[...]" dan sesuai dengan MPEP 606.01, jika "judul tersebut tidak menggambarkan penemuan yang diklaim, pemeriksa harus meminta penggantian dengan judul baru yang jelas menunjukkan penemuan yang menjadi sasaran klaim". Oleh karena itu, judul-judul tersebut dapat dianggap sebagai ringkasan singkat (<500 karakter) dari penemuan yang diklaim. Paten-paten ini, yang diberikan antara September dan Oktober 2025, membantu menggambarkan fokus dan cakupan materi pokok paten-paten terbaru dalam komputasi kuantum.

Tabel 4.3 Judul dari 40 paten komputasi kuantum terbaru (CPC: G06N10) yang diberikan dan dipublikasikan oleh USPTO dan masing-masing pemilik paten utamanya

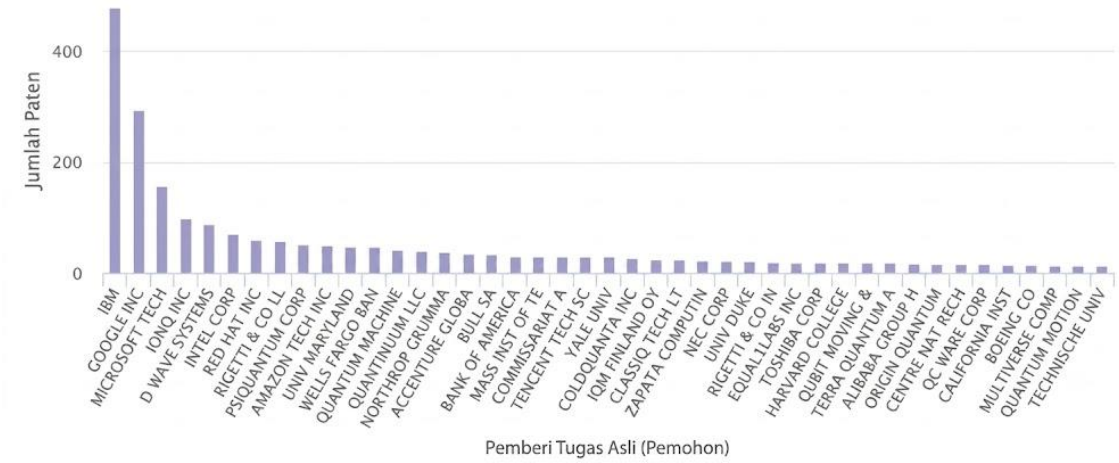
Judul	**Penerima Paten Akhir**	**Tanggal Pemberian**
Metode untuk mengeksekusi program kuantum dan metode untuk mengompilasi program kuantum	SHENZHEN TENCENT COMPUTER SYSTEMS CO; INST OF SOFTWARE CHINESE ACADEMY OF SCIENCE	2025-10-07
Amplifikasi dan atenuasi probabilistik dari kesalahan kuantum menggunakan dataset tunggal	IBM	2025-10-07
Analisis kinerja program kuantum	CLASSIQ TECH LTD	2025-10-07
Metode, sistem, dan aparatus untuk mengaktifkan dan mengelola jaringan kuantum	INTERDIGITAL TECH CORP	2025-10-07
Filter transisi termal untuk sistem sirkuit superkonduktor	NORTHROP GRUMMAN CORP	2025-10-07
Evaluasi prediktor klasik/kuantum gabungan	IBM	2025-10-07
Transduksi kuantum elektro-optomekanis	IBM	2025-10-07
Mengidentifikasi kesalahan kait parah pada saluran penstabil	MICROSOFT CORP	2025-10-07
Metode dan aparatus untuk mitigasi *crosstalk* AOD	IONQ INC	2025-10-07
Evaluasi prediktor klasik/kuantum gabungan dengan penyesuaian akurasi model	IBM	2025-10-07
Pengukuran GHZ berkode optik-linear dan komputasi serta komunikasi kuantum toleran-kesalahan	ORCA COMPUTING LTD	2025-10-07
Filter *baseband* untuk jalur sinyal mode-arus	IBM	2025-10-07
Generasi sinyal kendali komputasi-kuantum yang akurat secara fase	ZURICH INSTRUMENTS AG	2025-10-07

Sistem dan metode untuk menyediakan alur klasifikasi tetangga terdekat dengan pengurangan dimensionalitas otomatis	CAPITAL ONE FINANCIAL CORP	2025-10-07
Aparatus pemrosesan informasi, perangkat aritmetika, dan metode pemrosesan informasi	HITACHI VANTARA LTD	2025-10-07
Sirkuit tereduksi derau untuk komputer kuantum ion terperangkap	IONQ INC	2025-10-07
Metode dan sistem untuk menyediakan antarmuka komputer kuantum	CALIFORNIA INST OF TECH UNIV	2025-10-07
Sistem dan metode untuk sistem komputasi kuantum berwarta fotonik yang efisien	SOUTHERN METHODIST UNIV INC	2025-10-07
Sistem dan metode untuk menggunakan simulator komputasi kuantum terdistribusi	JPMORGAN CHASE BANK NA	2025-10-07
Dekoder komputasi kuantum dan metode terkait	RIVER LANE RES LTD	2025-10-07
Metode simulasi dinamika molekuler dipercepat pada sistem komputasi	UNIV SYSTEM OF MARYLAND	2025-09-30
Menghasilkan *offset* DC pada transmon yang dapat ditala fluks dengan loop arus persisten	IBM	2025-09-30
Sistem komputasi kuantum dengan antarmuka pemrograman aplikasi cloud multi-sumber yang aman	BANK OF AMERICA	2025-09-30
Metode dan aparatus untuk pendinginan doppler	IONQ INC	2025-09-30
Metode dan aparatus untuk pemuatan pintu perangkap	IONQ INC	2025-09-30
Sistem dan metode untuk tomografi kuantum menggunakan ancilla	ALPHABET INC	2025-09-30
Penginderaan dan komputasi kuantum menggunakan fase bertingkat	UNIV COLORADO	2025-09-30
Penalaan perangkat penyimpanan	PURE STORAGE INC	2025-09-30
Prosesor klasik untuk kendali kuantum	QM TECH LTD	2025-09-30
Konfigurasi mode gerakan untuk implementasi gerbang keterikatan pada komputer kuantum perangkap ion	IONQ INC	2025-09-30
Layanan komputasi kuantum dengan penegakan kualitas layanan (QoS) melalui prioritisasi tugas kuantum di luar pita	AMAZON TECH INC	2025-09-30
Mitigasi kesalahan dalam program kuantum	IBM	2025-09-30
Pemilihan string Pauli untuk *variational quantum eigensolver*	IBM	2025-09-30
Dekode kemungkinan maksimum dari kode kuantum	IBM	2025-09-23

Perangkat komputasi model Ising	NIPPON TELEGRAPH & TELEPHONE	2025-09-23
Estimasi fase kuantum terverifikasi	ALPHABET INC	2025-09-23
Antarmuka pelindung radiasi termal tanpa kontak	IBM	2025-09-23
Mengelola beban kerja dalam sistem orkestrasi kontainer	IBM	2025-09-23
Fabrikasi elektroda dan pembentukan cetakan (*die*) untuk perangkap ion logam-di-atas-kaca	IONQ INC	2025-09-23

Pemilik Paten Komputasi Kuantum Teratas

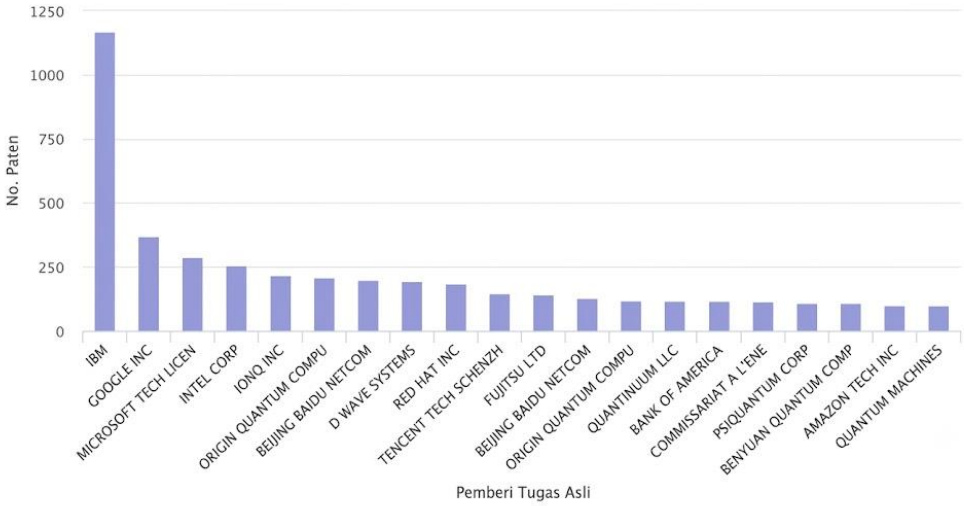
Gambar 4.6 mencantumkan pemilik paten komputasi kuantum teratas dalam 25 tahun terakhir. Di antara 10 perusahaan teratas dengan lebih dari 25 paten komputasi kuantum, kita menemukan perusahaan teknologi global AS yang berfokus pada platform perangkat keras dan perangkat lunak (IBM, Google, Microsoft, Intel), perusahaan teknologi pertahanan AS (Northrop Grumman), dan perusahaan khusus kuantum (IonQ, Rigetti, D-Wave). Di antara portofolio universitas teratas dalam komputasi kuantum adalah U. Maryland, MIT, Yale, Duke, Harvard, Caltech, dan Tech. Univ. Delft.



Gambar 4.6 Pemilik paten teratas untuk paten komputasi kuantum (G06N10) di USPTO dan EPO

Pemeriksaan Sitasi dan Portofolio Paten Dominan

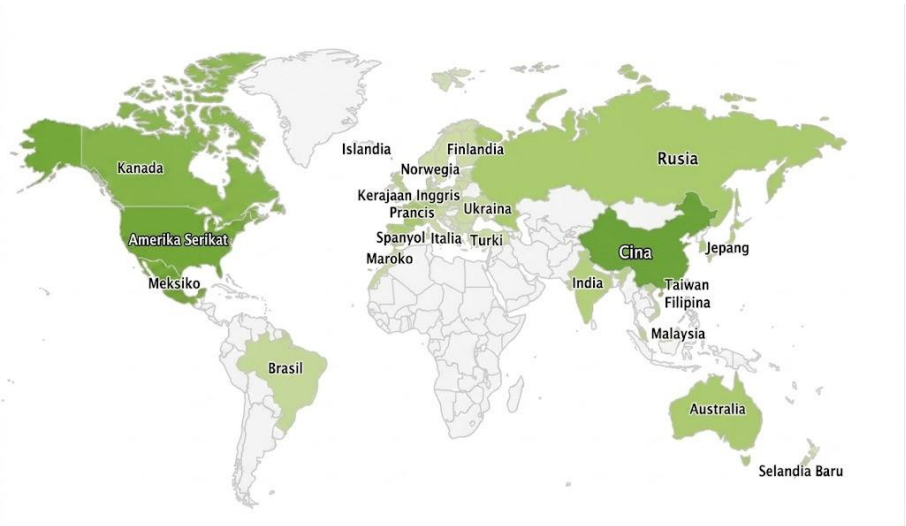
Gambar 4.7 menunjukkan pemeriksaan sitasi ke depan dari portofolio paten tentang komputasi kuantum berdasarkan penerima hak (pemilik paten utama). Sitasi ke depan merupakan ukuran nilai pribadi dan proksi untuk potensi nilai sosial dari penemuan. Paten tanpa nilai pasar yang mapan (misalnya, tanpa perjanjian lisensi dengan tarif royalti yang dinegosiasikan) sering dinilai berdasarkan kutipan ke depan dan metrik penilaian terkait. Portofolio paten dengan jumlah kutipan ke depan tertinggi adalah IBM, Google, Microsoft, dan IonQ (Gambar 4.7).



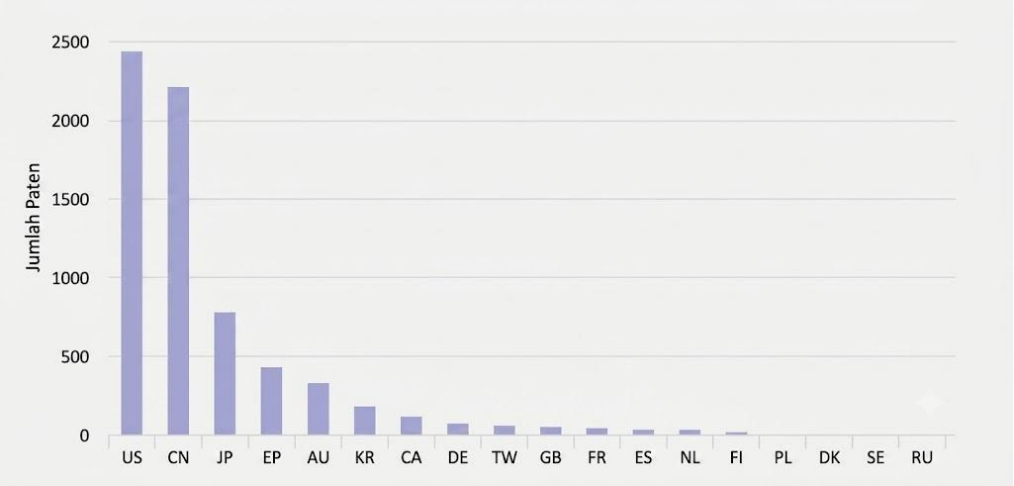
Gambar 4.7 Pemeriksaan kutipan maju portofolio paten tentang komputasi kuantum (S8) berdasarkan penerima hak paten

Distribusi Geografis Global

Gambar 4.8 dan 4.9 menunjukkan kantor paten teratas yang menerbitkan paten teknologi kuantum (ID Pencarian: S2). AS dan Tiongkok adalah negara penerbit teratas, diikuti oleh Jepang, EPO, Australia, Korea Selatan, dan Kanada. Sementara AS terus memimpin bidang komputasi kuantum, Tiongkok dapat dikatakan menjadi pemimpin dalam komunikasi kuantum. Ini luar biasa karena sebagian besar pertumbuhan Tiongkok dalam komunikasi kuantum yang aman telah terjadi dalam 5 tahun terakhir. Dengan demikian, diharapkan perangkat jaringan dan komunikasi kuantum Tiongkok akan segera hadir di pasar global. Per tahun 2021, China kini berada di urutan kedua setelah AS, dengan jumlah paten hampir 3 kali lipat dari Jepang, dan lebih dari 5 kali lipat dari EPO (Gambar. 4.9).



Gambar 4.8 Negara-negara penerbit paten teratas untuk paten teknologi kuantum (ID Pencarian: S2) di seluruh yurisdiksi dalam PCT



Gambar 4.9 Negara-negara teratas yang mematenkan komputasi kuantum (CPC G08N10). Hingga tahun 2021, Tiongkok berada di urutan kedua, di atas Jepang, Eropa, dan Australia.

4.5 STUDI TERKINI ATAS LANSKAP PATEN KUANTUM

Berdasarkan pemeriksaan kami tahun 2022 dalam *International Review of Intellectual Property and Competition Law*, yang meneliti tren paten kuantum hingga tahun 2021 dan menekankan peran paten dalam mendorong pengungkapan di tengah kekhawatiran akan perlindungan yang berlebihan, pemeriksaan terbaru hingga Oktober 2025 ini menegaskan kelanjutan pola-pola utama sambil menyoroti pertumbuhan yang diperkuat. Percepatan aktivitas pematenan pasca-2014 terus berlanjut tanpa penyimpangan, didorong oleh peningkatan komersialisasi, investasi geopolitik (misalnya, dalam komputasi kuantum dan komunikasi aman), dan integrasi dengan teknologi baru seperti AI. Namun, data tersebut tidak mengungkapkan bukti baru tentang tumpukan paten atau hambatan; sebaliknya, perluasan domain publik dan kepemilikan yang beragam memperkuat insentif inovasi yang diidentifikasi sebelumnya, dengan dampak baru untuk antimonopoli di pasar yang semakin matang.

Pertumbuhan Paten Teknologi Kuantum

Hasil studi lanskap terbaru kami menunjukkan bahwa USPTO dan EPO kini secara bersama-sama memberikan sekitar 2500 paten terkait teknologi kuantum per tahun (S2), meningkat dari sekitar 2000 paten tahunan yang diamati dalam pemeriksaan kami sebelumnya untuk tahun 2021. Sebanyak 29.701 paten diberikan dari tahun 2001 hingga 2025, mencerminkan tingkat pertumbuhan tahunan majemuk (CAGR) keseluruhan sekitar 14,5% selama 24 tahun terakhir sedikit penyesuaian dari CAGR 15,23% hingga tahun 2021, tetapi menunjukkan momentum yang berkelanjutan. Perlu dicatat, lebih dari 40% dari pemberian paten ini terjadi dalam 4 tahun terakhir, memperpanjang tren ekspansi cepat pasca-2014 setelah stagnasi relatif antara tahun 2003 dan 2013 (CAGR ≈ 4,05%) yang dicatat dalam pembelajaran kami sebelumnya. Lonjakan berkelanjutan ini sejalan dengan inisiatif kuantum global, seperti perluasan pendanaan di bawah Program Unggulan Kuantum Uni Eropa dan Inisiatif Kuantum Nasional AS, tanpa menimbulkan perubahan yang tidak terduga.

Pengungkapan Paten di Domain Publik Versus Rahasia Dagang

Dari perspektif kebijakan publik, perlu dicatat bahwa sekitar 54% dari pengungkapan paten yang dipublikasikan selama 24 tahun terakhir kini berada di domain publik, peningkatan yang moderat dari sekitar 50% yang dilaporkan dalam studi kami tahun 2022. Ini termasuk perkiraan 7697 paten yang sebelumnya diberikan dan telah kedaluwarsa (naik dari 4536), serta 21.676 aplikasi paten yang tidak menghasilkan pemberian paten (naik dari 14.830). Ajaran dalam pengungkapan publik ini tetap tersedia secara bebas untuk digunakan masyarakat, terus meningkatkan ambang batas kemampuan dipatenkan untuk aplikasi selanjutnya seperti yang telah kami soroti sebelumnya mencegah pematenan penemuan-penemuan ini dan mempersempit ruang lingkup perlindungan untuk klaim lanjutan. Tidak seperti rahasia dagang, dinamika ini terus menguntungkan inovasi terbuka, tanpa tren baru menuju peningkatan kerahasiaan meskipun bidang ini telah matang. Untuk memenuhi persyaratan kebaruan dan tidak jelas, pemohon sering mengklaim prioritas atas pengungkapan sebelumnya, yang secara efektif memperpendek jangka waktu paten (20 tahun dari tanggal prioritas). Misalnya, di antara paten teknologi kuantum yang diberikan pada tahun 2025, sebagian besar diperkirakan sekitar 80% berdasarkan pola historis memiliki tanggal prioritas mulai dari tahun 2005 hingga 2021, konsisten dengan kontinuitas yang diamati dalam temuan kami sebelumnya.

Kontinum dari Teknologi Klasik ke Teknologi Kuantum

Sebagian besar paten teknologi kuantum yang diberikan selama 24 tahun terakhir (S2) berkaitan dengan nanostruktur, perangkat solid-state, dan aplikasinya (misalnya, penginderaan dan metrologi), dengan klaim dan praktik penyusunan yang sangat mirip dengan paten semikonduktor yang mendorong revolusi teknologi informasi selama 60 tahun terakhir pola yang tidak berubah sejak pemeriksaan kami tahun 2022. Kepadatan transistor dalam sirkuit terintegrasi terus mengikuti tren hukum Moore, dengan miniaturisasi yang mendorong batas lebih jauh: Seperti yang diilustrasikan, Intel 8008 (1974) memiliki 2500 transistor pada 10.000 nm, Pentium 4 (2005) 169 juta pada 90 nm, Xeon (2017) 8 miliar pada 14 nm, Apple M1 Max (2021) 57 miliar pada 5 nm, dan NVIDIA Blackwell B200 (2025) 208 miliar pada 4 nm, dengan proses 2 nm sekarang dalam produksi. Penskalaan ini telah membuat efek kuantum semakin integral terhadap desain perangkat klasik, memperdalam kekaburan antara teknologi klasik dan kuantum yang telah disebutkan sebelumnya, tanpa menyelesaikan tantangan definisi untuk rezim IP.

Mendefinisikan Paten Teknologi Kuantum

Tumpang tindih yang semakin besar antara teknologi klasik (misalnya, transistor sub-5 nm pada CPU dan GPU saat ini) dan teknologi kuantum menimbulkan pertanyaan: Apa yang dimaksud dengan paten teknologi kuantum? Ambiguitas ini, yang pertama kali diangkat dalam studi kami tahun 2022, terus menantang proposal untuk rezim paten kuantum *sui generis*, karena mendefinisikan ruang lingkup bidang ini berisiko menimbulkan "penyusunan" klaim atau ketidaksesuaian dengan standar internasional seperti TRIPS, yang mensyaratkan paten netral teknologi dan jangka waktu paten 20 tahun. Hasil terbaru kami menunjukkan bahwa USPTO tetap menjadi kantor yang lebih disukai (mencakup ~75% dari paten S2), dan reformasi

yang tidak harmonis masih dapat mendistorsi pilihan pengajuan, tanpa perkembangan baru yang mengurangi kekhawatiran ini di tengah meningkatnya pengajuan global.

Pertumbuhan Paten Komputasi Kuantum

Pencarian kami (S5) mengidentifikasi 6685 aplikasi paten komputasi kuantum, menghasilkan 2879 paten yang diberikan dan diklasifikasikan di bawah CPC G06N10 ("komputasi kuantum berdasarkan fenomena mekanika kuantum") peningkatan substansial dari 3042 aplikasi dan 1603 pemberian paten dalam pemeriksaan kami tahun 2022. Bidang ini tetap menjadi ceruk pasar dari tahun 2001 hingga 2014 (<48 pemberian paten/tahun), tetapi sejak itu mengalami percepatan yang konsisten: Pemberian paten meningkat dari 37 pada tahun 2014 menjadi 435 pada tahun 2021 (CAGR ≈ 42,2%), dan terus tumbuh dengan kuat hingga tahun 2025, dengan perkiraan rata-rata lebih dari 300 pemberian paten setiap tahun dari tahun 2022 hingga 2025, menghasilkan CAGR yang direvisi sekitar 35% dalam beberapa tahun terakhir. Lintasan ini memperpanjang peningkatan investasi dan minat R&D yang telah disorot sebelumnya, tanpa adanya perlambatan, yang berpotensi didorong oleh kemajuan dalam qubit yang dikoreksi kesalahan dan sistem kuantum-klasik hibrida.

Pemilik Paten Komputasi Kuantum Teratas

Pemeriksaan terhadap pemilik paten teratas mengungkapkan konsentrasi yang lebih rendah daripada di pasar komputasi klasik, sebuah temuan yang tetap berlaku dari studi kami tahun 2022. Di samping perusahaan mapan (IBM, Microsoft, Alphabet/Google, Intel), universitas, dan perusahaan rintisan menonjol, dengan portofolio yang berkembang sekitar 80% secara keseluruhan sejak tahun 2021. Paten yang kuat tetap penting bagi pendatang baru dan UKM yang berfokus pada kuantum dibandingkan dengan perusahaan yang sudah mapan. Perusahaan yang sudah mapan dengan modal yang cukup mendanai R&D secara internal, sementara pendatang baru mengandalkan kekayaan intelektual untuk penggalangan dana Rigetti dan IonQ memiliki portofolio 10 besar, yang menunjukkan pengaruh kekayaan intelektual yang berkelanjutan bagi UKM yang telah disebutkan sebelumnya.

Dampak Kekayaan Intelektual dan Antimonopoli

Tren paten kuantum menimbulkan pertimbangan antimonopoli, karena konsentrasi dalam portofolio kunci dapat membatasi akses ke teknologi penting risiko potensial yang telah diidentifikasi dalam pemeriksaan kami tahun 2022 dan menjadi lebih relevan dengan gelombang komersialisasi tahun 2025 (misalnya, layanan cloud kuantum). Namun, keragaman pemilik saat ini mengurangi risiko monopoli, mendorong persaingan tanpa munculnya konsentrasi baru yang besar. Para pembuat kebijakan harus terus memantau aspek-aspek yang lebih dinamis dari persaingan (inovasi) dan keseimbangan paten-rahasia dagang untuk menghindari monopoli di bidang-bidang strategis seperti keamanan nasional, dengan data terbaru menunjukkan tidak ada pergeseran menuju dominasi tetapi peningkatan fragmentasi geopolitik (misalnya, perluasan portofolio Tiongkok).

4.6 DAMPAK LANSKAP PATEN KUANTUM TERKINI

Studi lanskap paten umum terbaru kami, yang memperluas pemeriksaan tahun 2022 kami, mengkonfirmasi keberlanjutan tren utama sambil menyoroti pertumbuhan yang

meningkat selama 4 tahun tambahan hingga Oktober 2025. Secara khusus: (1) USPTO dan EPO sekarang bersama-sama memberikan sekitar 2500 paten per tahun yang terkait dengan teknologi kuantum (S2), naik dari ~2000 pada tahun 2021; (2) CAGR keseluruhan selama 24 tahun dari tahun 2001 hingga 2025 berada di sekitar 14,5% yang mencerminkan percepatan yang berkelanjutan; (3) lebih dari 50% pengungkapan paten yang dipublikasikan dalam periode ini sudah berada di domain publik yang secara progresif memperkaya informasi kuantum bersama seperti yang diantisipasi; (4) sebagian besar paten komputasi kuantum yang diberikan berkaitan dengan realisasi fisik blok bangunan untuk komputer kuantum, koreksi kesalahan kuantum, sirkuit kuantum dan aplikasi, tanpa pergeseran dominasi; (5) sifat klaim dan praktik penyusunan tetap hampir tidak dapat dibedakan dari paten semikonduktor dan komputasi yang mendorong revolusi teknologi informasi, menggarisbawahi kesinambungan yang berkelanjutan antara teknologi klasik dan kuantum; (6) tumpang tindih yang semakin meningkat antara teknologi klasik dan kuantum tetap menjadi tantangan bagi proposal yang mengadvokasi rezim paten kuantum *sui generis*; (7) setelah aktivitas terbatas dari tahun 2001–2014 yang disebutkan sebelumnya, komputasi kuantum telah mengalami pertumbuhan substansial yang berkelanjutan, dengan paten yang diberikan meningkat; (8) konsentrasi di antara pemilik paten komputasi kuantum teratas tetap lebih rendah daripada di pasar komputasi klasik dan TI, dengan keragaman yang tetap stabil; (9) selain perusahaan besar yang terkenal, perusahaan rintisan kuantum baru yang khusus, universitas, dan entitas pemerintah termasuk di antara penerima hak teratas, dengan UKM memanfaatkan IP untuk pertumbuhan seperti sebelumnya; dan (10) USPTO terus menjadi kantor pilihan, yang menyumbang ~75% dari paten teknologi kuantum yang diberikan oleh EPO dan USPTO.

Data terbaru ini juga memperkuat kesimpulan kami tahun 2022 bahwa sistem paten terus memberikan insentif untuk pengungkapan publik di bidang komputasi kuantum dan bidang terkait, dalam situasi di mana kerahasiaan dagang mungkin diharapkan mendominasi mengingat karakter teknologi yang masih dalam tahap awal, struktur pasar, dan model bisnis seperti komputasi awan kuantum "sebagai layanan". Sepanjang periode 2001–2025, sekitar 57% pengungkapan paten terkait kuantum kini berada di domain publik (naik dari sekitar 50% pada tahun 2021) termasuk lebih dari 6000 paten yang telah diberikan dan telah kedaluwarsa. "Sumber informasi kuantum" yang berkembang ini meningkatkan standar kebaruan dan mempersempit ruang lingkup klaim dari waktu ke waktu, mengurangi kekhawatiran tentang perlindungan berlebihan atau posisi yang menghalangi. Hampir semua dari 2879 paten komputasi kuantum dalam dataset kami akan memasuki domain publik pada saat pasar komputasi kuantum mencapai skala yang sebanding dengan industri komputasi awan saat ini, menunjukkan bahwa, dari perspektif temporal, sejumlah besar pengetahuan teknis yang terkodifikasi akan tersedia secara bebas pada saat kematangan komersial yang lebih luas.

Konsisten dengan pemeriksaan kami sebelumnya, data tambahan 4 tahun menunjukkan tidak adanya munculnya tumpukan paten atau hambatan struktural baru untuk masuk. Aktivitas pematenan telah meningkat seperti yang diantisipasi, tetapi tanpa pergeseran yang terlihat menuju perlindungan berlebihan sistemik. Tingkat persetujuan tetap stabil, dan peningkatan pemberian paten yang diklasifikasikan di bawah CPC G06N10 sejak

2021 selaras dengan perkembangan teknologi terkini seperti chip Willow Google, algoritma Quantum Echoes, chip Majorana 1 Microsoft, dan kemajuan NIST dalam nanofabrikasi kuantum. Terobosan-terobosan ini tampaknya telah merangsang aktivitas pengajuan tambahan sambil tetap kompatibel dengan lanskap paten yang kompetitif dan relatif tidak terkonsentrasi.

Pada saat yang sama, pengamatan kami sebelumnya tentang interaksi antara paten, rahasia dagang, dan kerahasiaan negara tetap berlaku, meskipun dengan asimetri yang mencolok di berbagai teknologi. Beberapa inovasi penting dalam komputasi kuantum terjadi dalam kondisi kerahasiaan, khususnya dalam program R&D pemerintah yang strategis di mana kerahasiaan diperlukan karena pertimbangan keamanan nasional. Namun, tidak seperti di domain AI tertentu, data terbaru tidak menunjukkan pergeseran struktural menjauh dari paten. Khususnya dalam perangkat keras kuantum, persyaratan modal yang tinggi, fasilitas khusus, dan rantai pasokan yang kompleks membuat paten relatif lebih menarik: bagi pendatang baru dan UKM, biaya pematenan tetap kecil relatif terhadap pengeluaran R&D, dan intensitas modal kuantum memperkuat nilai paten sebagai perangkat penguasaan dan sinyal. Berbeda dengan hambatan masuk AI yang relatif rendah dan siklus inovasi yang berpusat pada kode, sektor kuantum seperti yang diamati hingga tahun 2025 terus bergantung pada paten daripada rahasia dagang atau rahasia negara sebagai saluran IP formal utamanya, meskipun kerahasiaan tetap signifikan di garis depan.

Meskipun demikian, kami menyadari bahwa dinamika geopolitik telah meningkat sejak pemeriksaan kami tahun 2022, yang menambah konteks lebih lanjut pada pola kekayaan intelektual ini. Studi terbaru seperti Laporan Indeks Kuantum MIT 2025 menunjukkan bahwa pengajuan paten kuantum Tiongkok meningkat secara signifikan dari tahun 2014 hingga 2024, menunjukkan kepemimpinan global 3 besar dalam paten teknologi kuantum (termasuk komputasi kuantum) dan mempersempit kesenjangan dengan Amerika Serikat, dengan beberapa proyeksi menunjukkan kemungkinan penyalipan pada tahun 2027.

Perkembangan ini memperluas pengamatan kami sebelumnya tentang peningkatan pesat Tiongkok dalam komunikasi kuantum menjadi penegasan kekuatan yang lebih luas di berbagai domain kuantum. Hasilnya adalah lanskap persaingan yang lebih kompleks di mana paten, rahasia dagang, dan rahasia negara digunakan sebagai instrumen kebijakan industri, kepemimpinan teknologi, dan otonomi strategis. Tren ini juga memunculkan pertanyaan-pertanyaan baru tentang hukum persaingan, karena terobosan seperti chip Willow Google dan algoritma Quantum Echoes menandai transisi dari implementasi yang terutama bersifat eksperimental menuju aplikasi yang lebih praktis dan relevan secara komersial. Interaksi yang berkembang antara terobosan teknologi, data atau infrastruktur terkonsentrasi, dan portofolio strategis paten terkait kuantum kemungkinan akan membentuk prioritas penegakan hukum dan regulasi di masa depan.

Dari perspektif kebijakan publik, catatan empiris yang diperbarui ini menyempurnakan penilaian kami sebelumnya tentang bagaimana sistem paten berinteraksi dengan inovasi kuantum. Misalnya, studi kami tahun 2022 menyoroti risiko reformasi IP yang kurang tepat di sektor padat modal dan menyoroti dimensi distribusi kebijakan paten, di mana perusahaan

besar dengan posisi pasar yang kuat mungkin secara rasional lebih memilih hak paten yang lebih lemah, sedangkan pendatang baru di bidang kuantum dan UKM biasanya mengandalkan perlindungan paten yang kuat untuk menarik investasi dan berpartisipasi secara kredibel di pasar global.

Bukti tahun 2025 konsisten dengan kerangka ini: pertumbuhan hibah yang berkelanjutan, tingkat persetujuan yang stabil, dan perluasan ruang lingkup informasi kuantum semuanya menunjukkan sistem yang terus mendorong pengungkapan dan mendukung inovasi dalam teknologi kuantum, bukan sistem yang secara sistematis menghambatnya. Namun, dimensi geopolitik dan hukum persaingan yang diperkuat yang diamati dalam data terbaru menggarisbawahi bahwa debat di masa depan tentang tata kelola kuantum dan desain kekayaan intelektual harus didasarkan pada penilaian yang diinformasikan secara empiris tentang dinamika ini, bukan pada kekhawatiran spekulatif tentang proteksi berlebihan atau kurangnya insentif.

4.7 DAMPAK KEBIJAKAN LANSKAP PATEN KUANTUM

Hasil studi lanskap paten yang diperbarui ini menegaskan kembali kesimpulan kami tahun 2022 bahwa sistem paten mendorong pengungkapan publik dalam komputasi kuantum dan bidang terkait, melayani kepentingan publik di mana rahasia dagang mungkin akan berlaku karena sifat teknologi yang masih dalam tahap awal, struktur pasar, dan model bisnis (misalnya, komputasi awan kuantum sebagai layanan). Tidak ada bukti baru tentang proteksi berlebihan yang muncul; sebaliknya, pertumbuhan yang meningkat dan perluasan domain publik mengurangi hambatan, sementara pergeseran geopolitik seperti peningkatan substansial pengajuan paten oleh Tiongkok menambah lapisan pada persaingan global. Dari perspektif kebijakan publik, perusahaan besar yang memiliki posisi terdepan mungkin lebih menyukai hak paten yang lebih lemah (karena mereka tidak memerlukan paten ini untuk mendapatkan pendanaan dan teknologi dapat dilindungi melalui rahasia dagang), sedangkan pendatang baru di bidang kuantum mendapat manfaat dari perlindungan yang lebih kuat untuk mendapatkan pendanaan investasi.

Pemeriksaan terbaru tentang lanskap paten teknologi kuantum dari tahun 2001 hingga Oktober 2025 ini mengungkapkan ekosistem inovasi yang kuat dan berkembang pesat, yang ditandai dengan tingkat pertumbuhan tahunan gabungan dua digit dalam pemberian paten, terutama di USPTO, dan beragam pemilik paten terkemuka mulai dari perusahaan teknologi seperti IBM, Google, dan Microsoft hingga perusahaan rintisan dan universitas. Dengan lebih dari 50% pengungkapan sekarang memasuki domain publik (termasuk 25% dari paten yang diberikan), sistem paten terus mendorong perluasan informasi kuantum bersama, menangkal risiko kerahasiaan dagang dan kerahasiaan negara, serta meningkatkan ambang batas kebaruan dan ketidakjelasan/langkah inventif untuk penemuan di masa depan tanpa bukti perlindungan berlebihan atau kerumitan.

Pada saat yang sama, pergeseran geopolitik seperti peningkatan pesat Tiongkok dalam komputasi kuantum dan komunikasi kuantum, serta meningkatnya seruan di seluruh dunia untuk menggunakan HKI dan regulasi untuk meningkatkan ketahanan dan apa yang disebut

"kedaulatan teknologi" di bidang-bidang yang sangat penting secara strategis, seperti teknologi AI dan kuantum, menggarisbawahi perlunya kebijakan berbasis bukti. Para pembuat kebijakan harus melihatnya sebagai tugas utama untuk menyeimbangkan insentif HKI dengan pertimbangan hukum persaingan, upaya standardisasi, dan kolaborasi global untuk mempertahankan inovasi terbuka di tengah komersialisasi dan keharusan keamanan nasional. Singkatnya, pemeriksaan terbaru tentang lanskap paten teknologi kuantum dari tahun 2001 hingga Oktober 2025 ini memperkuat temuan kami tahun 2022: paten mendorong pengungkapan dan inovasi tanpa menimbulkan masalah "perlindungan berlebihan" yang besar, tetapi pergeseran geopolitik dan potensi risiko konsentrasi memperkuat kebutuhan akan kebijakan inovasi kuantum berbasis bukti.

BAB 5
REGULASI KEAMANAN SIBER UNI EROPA DI ERA KUANTUM

Bab ini mengeksplorasi persimpangan komputasi kuantum dan hukum keamanan siber Uni Eropa (UE). Bagian ini mengkaji sejauh mana regulasi keamanan siber di UE sesuai dengan tujuan untuk mengatasi tantangan komputasi kuantum. Dua tantangan utama diidentifikasi: (i) serangan "panen sekarang, dekripsi nanti" (HNDL), dan (ii) perkembangan komputer kuantum yang dipercepat melampaui langkah-langkah keamanan siber saat ini. Bagian ini berpendapat bahwa konsep-konsep seperti "kondisi terkini" dan "langkah-langkah teknis dan organisasi yang tepat" yang menjadi ciri hukum keamanan siber UE gagal untuk cukup memperhitungkan ancaman keamanan siber yang diantisipasi akan terwujud di masa depan, tetapi berdampak pada jaringan dan sistem informasi saat ini. Solusi yang diusulkan mencakup peningkatan kejelasan yudisial mengenai persyaratan teknis keamanan siber, peningkatan fokus kebijakan pada kriptografi pasca-kuantum, penerapan persyaratan keamanan siber yang lebih tegas dalam hukum yang berlaku, dan peralihan ke istilah alternatif yang secara tepat memperhitungkan ketidakpastian keamanan siber di masa depan. Bagian ini diakhiri dengan menganjurkan pendekatan regulasi proaktif yang berlandaskan tata kelola antisipatif dan strategi berlapis untuk melindungi dari ancaman kuantum.

5.1 PATEN, KEAMANAN SIBER, DAN KEBIJAKAN KUANTUM

Komputer kuantum menjanjikan keunggulan dalam tugas-tugas yang sulit dilakukan oleh komputer tradisional, menandai pergeseran paradigma di berbagai bidang. Meskipun sifat dan cakupan tugas-tugas ini masih belum pasti, periode pengembangan saat ini yang sering disebut sebagai era "Kuantum Skala Menengah Berisik" (NISQ) mencerminkan keterbatasan aplikasi praktis teknologi ini saat ini. Namun demikian, semakin banyak pembelajaran dan pengembangan, ditambah dengan meningkatnya kepercayaan pada kemajuannya dan beberapa keberhasilan nyata baru-baru ini, menunjukkan bahwa keunggulan kuantum sudah dekat.

Sayangnya bagi para ahli keamanan siber, salah satu bidang aplikasi yang paling menjanjikan untuk komputer kuantum adalah di bidang kriptografi. Algoritma Shor berpotensi merusak prinsip-prinsip matematika yang menjadi dasar pengamanan sebagian besar infrastruktur digital kita, dengan Gartner memperkirakan bahwa “pada tahun 2029, kemajuan dalam komputasi kuantum akan membuat kriptografi asimetris tidak aman dan pada tahun 2034 sepenuhnya dapat diretas.” Meskipun prediksi tersebut terkenal terlalu optimis, banyak pihak telah bekerja secara sistematis untuk mengurangi tantangan keamanan berbasis kuantum, dengan berbagai proyek interdisipliner dalam kriptografi pasca-kuantum (PQC) pada tahap lanjut, dan PQC mulai diimplementasikan di berbagai produk dan layanan.

Meskipun Uni Eropa (UE) telah berinvestasi dalam proyek-proyek yang berkaitan dengan komputasi kuantum, dan bahkan kriptografi kuantum, upaya substansialnya baru-baru ini dalam regulasi keamanan siber melalui legislasi sekunder gagal untuk secara khusus

menyoroti ancaman kuantum. Bab ini mengkaji risiko dari kelalaian ini, dan menyarankan jalur yang mungkin untuk menutup kesenjangan legislatif.

Bab ini disusun sebagai berikut. Bagian 2 pertama-tama memberikan pengantar tentang sifat ancaman yang ditimbulkan oleh komputasi kuantum terhadap keamanan siber dan mengidentifikasi dua isu keamanan siber utama yang dapat memengaruhi organisasi saat ini dan di masa mendatang. Isu-isu ini adalah (i) serangan "*harvest now, decrypt later*" (HNDL), dan (ii) ancaman yang lebih umum dari komputer kuantum yang melampaui langkah-langkah keamanan siber saat ini. Selanjutnya, rezim regulasi keamanan siber Uni Eropa saat ini diperiksa di Bagian 3, yang mengungkapkan ketergantungan pada beberapa heuristik dan asumsi yang rentan dalam menghadapi ancaman kuantum. Bagian 4 dari bagian ini kemudian meneliti opsi kebijakan yang tersedia bagi Uni Eropa untuk diupayakan guna mengurangi potensi bahaya komputer kuantum, dan memperbaiki kekurangan pendekatan keamanan siber saat ini. Bagian 5 menyimpulkan bahwa Uni Eropa berada dalam posisi unik, sebagai aktor dengan kapasitas regulasi yang relatif tinggi, untuk mengambil peran utama dalam mengembangkan mekanisme regulasi di bidang ini.

5.2 ANCAMAN KUANTUM TERHADAP KEAMANAN SIBER

Apakah, dan sejauh mana, komputasi kuantum akan merevolusi era informasi masih harus dilihat. Di era NISQ saat ini, komputer kuantum dicirikan oleh prosesor dengan puluhan hingga ratusan bit kuantum (qubit) dengan tingkat kesalahan yang signifikan. Terlepas dari hype yang sangat besar di sekitarnya, sebagian besar, komputer kuantum sejauh ini hanya dapat memecahkan "model mainan" untuk memberikan bukti konsep, daripada menawarkan keuntungan yang berarti. Saat ini (yaitu, Juli 2025, ketika bagian ini diselesaikan), hanya ada sedikit masalah yang diyakini oleh komunitas ilmiah, dengan cukup yakin, bahwa komputer kuantum akan memiliki keunggulan signifikan dalam memecahkannya dibandingkan dengan komputer klasik.

Algoritma Shor dan Enkripsi Asimetris

Algoritma Shor adalah salah satu algoritma kuantum tertua dan paling banyak diteliti, yang pada prinsipnya memiliki "dampak yang menghancurkan" pada algoritma enkripsi asimetris yang paling banyak digunakan. Ini berarti bahwa enkripsi data dalam perjalanan, yang sebagian besar bergantung pada kriptografi asimetris untuk pertukaran kunci dan otentikasi, rentan terhadap serangan oleh komputer kuantum yang toleran terhadap kesalahan dengan jumlah qubit yang memadai. Algoritma "asimetris" ini, terutama *Rivest–Shamir–Adleman* (RSA) dan kriptografi kurva eliptik (ECC), bergantung pada masalah matematika yang mudah dipecahkan saat mengenkripsi data dengan kunci publik tetapi tidak mungkin bagi komputer klasik untuk membalikkannya saat mencoba mendekripsi data tanpa kunci pribadi. Algoritma Shor telah terbukti secara efisien memecahkan masalah matematika ini, sehingga merusak keamanan metode enkripsi ini jika komputer kuantum dengan jumlah qubit dan stabilitas yang memadai dibangun.

Dampak praktis dari algoritma Shor, jika terwujud, sangat luas. Berbagai macam infrastruktur digital di berbagai industri akan terpengaruh. Pembagian rahasia pemerintah,

informasi perbankan, data perawatan kesehatan, data transaksi terkait e-commerce, dan berbagai komunikasi sehari-hari lainnya akan jauh lebih rentan terhadap akses oleh pihak yang tidak berwenang. Jenis kriptosistem lain juga dapat melemah karena komputasi kuantum, misalnya, karena algoritma kuantum baru yang sedang dikembangkan yang menimbulkan ancaman tambahan di luar algoritma Shor. Memang, algoritma kuantum lain, seperti algoritma Grover, berpotensi memengaruhi kriptografi simetris, tetapi pembelajaran saat ini menunjukkan bahwa hal ini dapat diatasi hanya dengan meningkatkan ukuran kunci. Karena algoritma Shor memengaruhi dasar-dasar kriptografi asimetris kontemporer, pendekatan kriptografi baru sepenuhnya kemungkinan diperlukan untuk mengatasi ancaman tersebut.

Kriptografi Pasca-Kuantum (PQC)

Meskipun distribusi kunci kuantum (QKD) muncul sebagai sarana pertahanan siber, PQC menghadirkan solusi paling realistis untuk memerangi ancaman komputasi kuantum untuk sebagian besar situasi karena tidak memerlukan perangkat keras khusus. PQC mengacu pada algoritma kriptografi yang dirancang agar aman terhadap serangan kuantum. Algoritma ini sedang dikembangkan dan distandarisasi untuk menggantikan atau melengkapi metode enkripsi saat ini yang rentan terhadap komputasi kuantum. Seperti yang dikemukakan oleh Bernstein dan Lange, “tantangan utama dalam kriptografi pasca-kuantum adalah memenuhi tuntutan akan kegunaan dan fleksibilitas kriptografi tanpa mengorbankan kepercayaan.” Institut Standar dan Teknologi Nasional (NIST) yang berbasis di AS telah memimpin upaya untuk menstandarisasi PQC sejak tahun 2016 ketika mereka meminta pengajuan PQC untuk dipertimbangkan sebagai bagian dari sebuah kompetisi. Baru-baru ini mereka mengeluarkan tiga standar PQC “pemenang” yang memanfaatkan algoritma kriptografi tahan kuantum.

Namun, transisi ke PQC itu kompleks, tidak hanya melibatkan pengembangan algoritma baru tetapi juga integrasinya ke dalam sistem dan protokol yang ada. Sistem lama, misalnya, mungkin memiliki keterbatasan teknis yang membuat implementasi dan interoperabilitas PQC sulit atau tidak mungkin. Selain itu, meskipun kompetisi NIST melibatkan pengujian yang kuat terhadap algoritma PQC pemenang, algoritma tersebut tidak sekuat standar klasik yang umum seperti RSA, dan ketahanan utamanya terhadap serangan kuantum di masa depan masih belum pasti. Semua ini untuk menggarisbawahi bahwa waktu, yaitu koordinasi kronologis, sangat penting dalam mempersiapkan diri menghadapi ancaman kuantum, meskipun cakrawala peristiwa dan sifatnya yang tepat masih belum diketahui.

Ancaman Masa Depan, Risiko Saat Ini

Ancaman kuantum terhadap keamanan siber bergantung pada beberapa variabel, seperti jenis aktor yang memiliki akses ke komputasi kuantum (misalnya, publik atau swasta; sipil atau militer; negara-bangsa yang bersahabat atau tidak bersahabat). Selain itu, ancaman dapat dipahami dari berbagai perspektif termasuk dari hulu dan hilir dalam rantai nilai keamanan siber. Misalnya, kurangnya kepercayaan terhadap efektivitas enkripsi dalam mengamankan informasi di seluruh jaringan publik dapat berdampak pada pembelajaran medis yang bergantung pada transmisi informasi sensitif yang efisien dan aman. Tidak ada batasan imajinasi, dengan komputasi kuantum yang sangat cocok untuk meramalkan hari kiamat di bidang keamanan siber.

Untuk memfokuskan diskusi, dua jenis ancaman diberikan perhatian khusus dalam bagian ini. Kedua ancaman ini dipilih karena keduanya dapat dimitigasi melalui tindakan yang diambil saat ini, termasuk oleh regulator. Pertama, adalah serangan HNDL, yaitu praktik mencegat dan menyimpan data terenkripsi yang dikirim melalui jaringan publik dengan tujuan mendekripsinya setelah komputer kuantum menjadi cukup kuat untuk memecahkan metode enkripsi saat ini. Kedua, adalah risiko yang terkait dengan "ketangkasan kriptografi" yang tidak memadai, yaitu kekurangan dalam adopsi algoritma tahan kuantum, yang dapat membuat beberapa sistem rentan selama periode transisi ke PQC dan langkah-langkah mitigasi lainnya.

Dapat dikatakan, risiko-risiko ini membuat ancaman kuantum siap untuk intervensi regulasi, dan memang pekerjaan koordinasi PQC NIST yang cukup besar sebagai regulator "hukum lunak" utama di bidang ini menunjukkan pentingnya lembaga regulasi (secara luas dipahami) untuk mengurangi ancaman kuantum. Selain itu, organisasi tidak mungkin merespons risiko secara memadai tanpa insentif (atau disinsentif) regulasi yang tepat, yang menyebabkan eksternalitas negatif yang cukup besar jika dibiarkan tanpa regulasi.

Tata Kelola Keamanan Siber dan Kuantum Global

Meskipun kontribusi ini memeriksa pendekatan regulasi Uni Eropa terhadap ancaman komputer kuantum, kompleksitas masalah ini, dalam konteks tata kelola keamanan siber global, harus ditekankan sejak awal. Keamanan siber merupakan tantangan kritis bagi organisasi dari semua jenis dan ukuran, dan banyak pemangku kepentingan semakin menyadari hal ini sebagai prioritas mulai dari jajaran manajemen puncak, kepala pemerintahan, masyarakat sipil, hingga individu. Para pemangku kepentingan ini seringkali memiliki pendekatan dan kepentingan yang berbeda, dan ketidakseimbangan kekuasaan yang signifikan melekat di dalam dan di antara mereka.

Komputasi kuantum semakin menantang ruang masalah yang sudah tegang dengan memperkenalkan risiko yang belum pernah terjadi sebelumnya terhadap alat keamanan yang penting dan ada di mana-mana. Oleh karena itu, respons regulasi Uni Eropa sendiri, dan akan tetap demikian, jauh dari cukup untuk menangani secara komprehensif masalah yang ditimbulkan oleh kemungkinan komputer kuantum. Masalah potensial bersifat global, multidimensi, dan berkaitan dengan dampak teknologi mutakhir yang masih jauh dari pemahaman lengkap kita. Meskipun demikian, sejauh Uni Eropa melihat dirinya sebagai pemimpin dalam ekosistem keamanan siber global dan memang teknologi kuantum ia memang memiliki peran untuk dimainkan, meskipun sederhana. Bagian berikut menjelaskan peran apa yang saat ini dimainkannya.

5.3 REGULASI KEAMANAN SIBER UNI EROPA

Regulasi keamanan siber Uni Eropa adalah sistem aturan yang luas, kompleks, dan agak membingungkan, sehingga pernyataan umum tentang jangkauan dan (upaya) dampaknya sulit dilakukan. Selain itu, regulasi ini menghadirkan target yang bergerak karena kecepatan adopsi hukum dan kebijakan baru, dan "plastisitas" dari konsep keamanan siber itu sendiri. Meskipun demikian, terdapat semakin banyak riset yang membahas logika dan cakupan hukum dan kebijakan keamanan siber Uni Eropa yang sedang berkembang. Riset ini membuat bagian ini

tidak perlu melakukan penilaian komprehensif terhadap hukum keamanan siber Uni Eropa. Sebaliknya, bagian ini mensintesis dan menilai atribut hukum keamanan siber Uni Eropa yang sangat relevan dengan tantangan yang ditimbulkan oleh komputasi kuantum.

Bagian ini disusun sebagai berikut. Pertama, instrumen "hukum keras" keamanan siber utama diperiksa, yang mengungkapkan kecenderungan badan legislatif Uni Eropa untuk mengandalkan istilah "kondisi terkini" daripada menetapkan persyaratan keamanan teknis, operasional, dan organisasi yang spesifik. Kedua, konsep kondisi terkini dibahas, dan pentingnya hukum lunak dalam memperjelas konsep tersebut diperkenalkan. Ketiga, bagian ini memeriksa pedoman industri yang berpengaruh tentang kondisi terkini, yang mengungkapkan kurangnya pertimbangan terhadap ancaman terhadap keamanan siber yang ditimbulkan oleh komputasi kuantum.

Instrumen Keamanan Siber Uni Eropa

Uni Eropa telah mengembangkan banyak instrumen hukum sekunder untuk meningkatkan keamanan jaringan dan sistem informasi dalam berbagai konteks. Selain itu, persyaratan keamanan siber tertentu juga terkandung dalam hukum primer terutama terkait data pribadi, yang keamanannya merupakan bagian dari “esensi” hak-hak fundamental atas privasi dan perlindungan data, yang diabadikan masing-masing dalam Pasal 7 dan 8 Piagam Hak Fundamental Uni Eropa. Tidak ada instrumen omnibus yang mencakup regulasi keamanan siber di berbagai domain; agak mengecewakan, Undang-Undang Keamanan Siber hanya menetapkan mekanisme sertifikasi dan memperkuat Badan Uni Eropa untuk Keamanan Siber (ENISA) dengan mandat permanen. Sebaliknya, serangkaian instrumen khusus sektor dan domain berisi aturan mengenai langkah-langkah teknis, operasional, dan organisasi yang harus diambil oleh pihak yang diatur (yaitu, entitas yang tunduk pada instrumen tersebut) di berbagai konteks yang seringkali tumpang tindih.

Tiga instrumen tersebut patut disoroti dalam hal ini: Peraturan Perlindungan Data Umum (GDPR), Undang-Undang Ketahanan Siber (CRA), dan Arahan Sistem Jaringan dan Informasi yang diperbarui (NIS 2). Ini bukan satu-satunya instrumen dengan mandat keamanan siber, tetapi dapat dikatakan yang paling sentral karena cakupannya yang relatif luas. Masing-masing mengatur perlindungan data pribadi, produk yang terhubung ke internet (termasuk perangkat *internet of things* (IoT)) dan keamanan infrastruktur kritis. Masing-masing berisi ketentuan yang mengharuskan pihak yang diatur untuk menerapkan langkah-langkah keamanan yang "sesuai" untuk mengelola risiko keamanan siber. Langkah-langkah spesifik yang diperlukan tidak tercantum secara pasti dalam setiap instrumen dan juga tidak dapat atau tidak seharusnya demikian, mengingat jumlah dan variasi langkah-langkah yang hampir tak terbatas, dan keinginan untuk merumuskan aturan dengan tingkat netralitas teknologi yang signifikan. Lebih spesifik lagi, GDPR menyatakan dalam Pasal 32(1):

> Dengan mempertimbangkan keadaan terkini, biaya implementasi dan sifat, ruang lingkup, konteks dan tujuan pemrosesan serta risiko dengan kemungkinan dan tingkat keparahan yang berbeda-beda terhadap hak dan kebebasan individu, pengendali dan pengolah data wajib menerapkan langkah-langkah teknis dan organisasi yang sesuai

> untuk memastikan tingkat keamanan yang sesuai dengan risiko, termasuk antara lain sebagaimana mestinya:
>
> a) pseudonimisasi dan enkripsi data pribadi;

Demikian pula, CRA mewajibkan produsen produk dengan elemen digital untuk mendesain, mengembangkan, dan memproduksi produk tersebut sesuai dengan "persyaratan keamanan siber esensial", yang menuntut produsen untuk "memastikan tingkat keamanan siber yang sesuai berdasarkan risiko." Di antara persyaratan tersebut adalah bahwa produk IoT harus:

> melindungi kerahasiaan data yang disimpan, ditransmisikan, atau diproses, baik data pribadi maupun lainnya, misalnya dengan mengenkripsi data yang relevan saat disimpan atau dalam perjalanan dengan mekanisme canggih, dan dengan menggunakan cara teknis lainnya…

NIS 2 menggunakan bahasa yang serupa, yang mewajibkan apa yang disebut "entitas esensial dan penting" untuk "mengambil langkah-langkah teknis, operasional, dan organisasi yang tepat dan proporsional untuk mengelola risiko yang ditimbulkan terhadap keamanan jaringan dan sistem informasi", langkah-langkah tersebut ditentukan dengan "mempertimbangkan kondisi terkini dan, jika berlaku, standar Eropa dan internasional yang relevan, serta biaya implementasi". Instrumen tersebut merujuk pada "kebijakan dan prosedur mengenai penggunaan kriptografi dan, jika sesuai, enkripsi" sebagai salah satu hal yang diperlukan langkah-langkah yang diperlukan dari entitas penting dan esensial.

Masing-masing dari tiga instrumen Uni Eropa ini secara khusus merujuk pada enkripsi sebagai langkah yang dapat, atau harus, diimplementasikan sebagai "sesuai", meskipun tanpa panduan eksplisit mengenai skema enkripsi mana yang mungkin sesuai dalam pengaturan tertentu. Instrumen-instrumen ini bukan satu-satunya yang secara khusus menandai enkripsi. Misalnya, Kode Komunikasi Elektronik Eropa juga melakukannya. Pertanyaan yang relevan untuk bagian ini adalah apakah persyaratan keamanan dalam hukum keamanan siber Uni Eropa, mengingat kondisi hukum dan teknologi saat ini, dapat ditafsirkan dengan tepat untuk mewajibkan penggunaan PQC dalam konteks tertentu.

Dalam beberapa kasus yang dicakup oleh instrumen-instrumen ini, PQC mungkin tidak akan pernah sesuai. Misalnya, dalam kasus GDPR yang mengatur spektrum luas pemrosesan data pribadi, termasuk pada media fisik seperti kertas, mungkin ada kasus di mana segala bentuk enkripsi, apalagi PQC, tidak sesuai dengan tingkat risiko. Namun, untuk keperluan bagian ini, dipertanyakan apakah PQC dapat menjadi persyaratan hukum menurut interpretasi yang tepat dari ketentuan di atas. Dalam kasus GDPR, hal itu mungkin terjadi dalam konteks operasi pemrosesan dengan risiko tinggi terhadap hak-hak fundamental subjek data, seperti transfer data medis sensitif atau informasi keuangan yang penting.

Kriteria utama dalam menentukan pertanyaan ini adalah apakah PQC termasuk dalam "kondisi terkini". Seperti yang dikemukakan oleh Bygrave, hukum keamanan siber Uni Eropa menunjukkan "penggunaan legislatif yang luas dari persyaratan fungsional generik yang berakar pada 'kondisi terkini'". Schmitz menganggap kondisi terkini dalam keamanan siber

sebagai "tujuan perlindungan" yang diimplementasikan oleh badan legislatif Uni Eropa agar dipenuhi oleh organisasi. Setidaknya, hal itu mengharuskan pihak yang diatur untuk "mempertimbangkan kemajuan teknologi saat ini" dalam menentukan langkah-langkah keamanan siber mana, termasuk metode kriptografi mana, yang mungkin tepat. Dengan demikian, dalam konteks kemajuan dalam komputasi kuantum, konsep tersebut memerlukan pertimbangan yang cermat.

Kondisi Terkini

Seperti yang dicatat oleh Schmitz, sementara konsep kondisi terkini (*state of the art*) umum digunakan dalam instrumen Uni Eropa, termasuk dalam keamanan siber, baik legislator Uni Eropa maupun nasional belum secara formal mendefinisikannya. Selain itu, sejak kemunculannya yang tampak dalam Arahan Tanggung Jawab Produk tahun 1985, Mahkamah Keadilan Uni Eropa (CJEU) belum menemukan kesempatan untuk menguraikan apa sebenarnya arti konsep tersebut. Tanpa adanya proklamasi legislatif atau yudisial Uni Eropa, interpretasi oleh para komentator telah bergantung pada yurisprudensi Jerman tentang konsep tersebut (dirumuskan sebagai "*Stand der Technik*" dalam bahasa Jerman) dan panduan dari badan pengatur seperti Dewan Perlindungan Data Eropa (EDPB) dan ENISA.

Dalam konteks ini, organisasi Jerman TeleTrust, bekerja sama dengan ENISA, telah membuat (dan terus memperbarui) pedoman yang diterbitkan sendiri yang secara komprehensif membahas keadaan terkini berdasarkan GDPR. Publikasi ini sangat bergantung pada keputusan Mahkamah Konstitusi Federal Jerman dalam kasus Kalkar ketika mengkonseptualisasikan 'keadaan terkini', menempatkan konsep tersebut di antara "pengetahuan dan pembelajaran ilmiah yang ada" dan "aturan teknologi yang diterima secara umum". Hal ini digambarkan dalam grafik di bawah ini dari dokumen tersebut (Gambar 5.1):

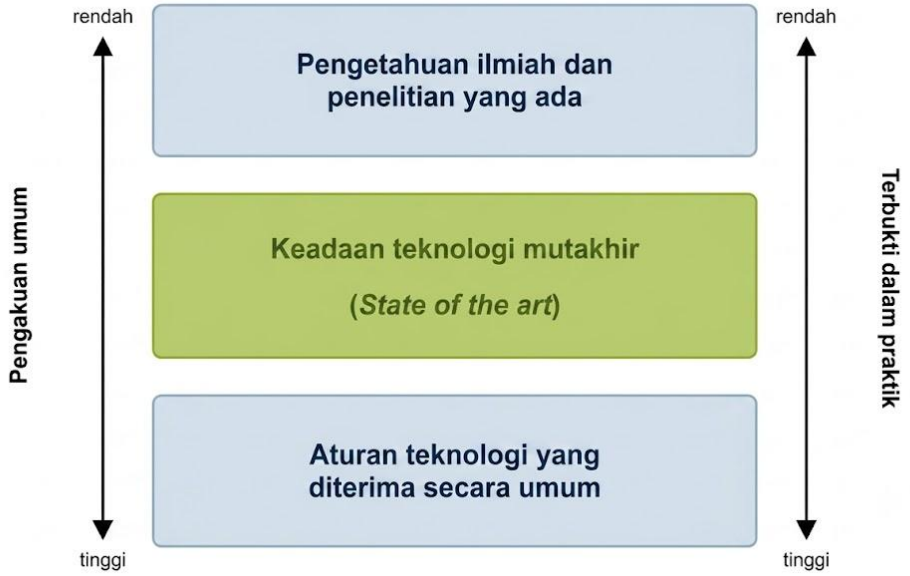
Dalam konstruksi ini, dipertanyakan apakah PQC telah mencapai status "keadaan terkini" atau saat ini berada dalam keadaan "pengetahuan dan pembelajaran ilmiah yang ada". Dokumen tersebut menyatakan bahwa:

> Langkah-langkah teknis pada tahap "pengetahuan dan pembelajaran ilmiah yang ada" sangat dinamis dalam perkembangannya dan beralih ke tahap "keadaan terkini" ketika mencapai kematangan pasar (atau setidaknya diluncurkan di pasar).

Kematangan PQC sulit untuk dinilai dalam pengertian ini. Di satu sisi, PQC baru mulai mencapai adopsi arus utama, dengan Apple dan Signal menjadi pelopor dalam menambahkan PQC ke aplikasi pesan populer mereka. Sebagai contoh lebih lanjut, upaya kolaboratif baru-baru ini oleh Banque de France dan Otoritas Moneter Singapura yang melibatkan penerapan PQC pada komunikasi email tertentu dipuji sebagai 'terobosan'. Yang perlu diperhatikan dalam setiap contoh ini adalah bahwa PQC mencakup perlindungan tambahan di atas kriptografi klasik. Pendekatan kriptografi hibrida menunjukkan awal mula PQC dan ketidakpastian manfaat perlindungannya terutama mengingat kurangnya komputer kuantum yang mampu menguji algoritma secara kuat. Pertimbangan ini memberatkan faktor "terbukti dalam praktik" dalam konseptualisasi Teletrust/ENISA dan karenanya menunjukkan bahwa PQC belum "tercanggih".

Di sisi lain, panduan TeleTrust/ENISA menunjukkan bahwa sekadar memasuki pasar berarti suatu langkah telah mencapai tahap teknologi terkini. Jelas, beberapa jenis PQC telah mencapai tingkat adopsi arus utama dan, dalam hal ini, telah memasuki pasar. Bahkan, distribusi kunci kuantum mutakhir menggunakan perangkat keras dan perangkat lunak khusus, seperti yang ditawarkan oleh perusahaan Swiss ID Quantique, saat ini tersedia. Hal ini menunjukkan bahwa, terlepas dari awal perkembangan PQC, dan cara yang hati-hati dalam penerapannya oleh organisasi tertentu, PQC seharusnya dianggap sebagai bagian dari teknologi terkini.

Namun, perlu ditekankan bahwa pendekatan Kalkar, sebagaimana diinterpretasikan dalam dokumen Teletrust/ENISA, bukanlah hal yang menentukan untuk interpretasi yang tepat dari kriteria keadaan seni dalam hukum Uni Eropa. Lebih lanjut, Bygrave dengan meyakinkan berpendapat bahwa mungkin ada lebih banyak faktor yang relevan untuk dipertimbangkan: "kriteria tersebut kemungkinan mensyaratkan langkah-langkah keamanan untuk sesuai tidak hanya dengan keadaan kemajuan teknologi saat ini, tetapi juga dengan praktik, standar, dan norma-norma kontemporer lainnya untuk manajemen teknis dan organisasi yang umumnya dianggap menawarkan tingkat keamanan terbaik pada saat itu." Dengan demikian, sekadar masuk ke pasar tidak berarti bahwa suatu langkah tersebut secara otomatis mencapai keadaan seni untuk tujuan hukum Uni Eropa.



Gambar 5.1 Gambaran "kondisi terkini" menurut hukum Jerman (Diadaptasi dari: Teletrust/ENISA 2023)

Bygrave menunjukkan peran standar hukum lunak dalam memperjelas gagasan tersebut, dengan Badan Perlindungan Data (DPA) merujuk pada hasil dari ISO, NIST, dan ENISA dalam keputusan yang melibatkan pelanggaran keamanan siber. Pemeriksaan Bygrave dan juga Teletrust/ENISA terbatas pada makna dari kondisi terkini berdasarkan GDPR. Jika dilihat dari sudut pandang hukum keamanan siber Uni Eropa secara lebih umum, argumen bahwa

standar sangat penting dalam menentukan langkah-langkah keamanan yang tepat menjadi lebih mudah dipahami.

Sebagaimana telah disebutkan sebelumnya, NIS 2 secara eksplisit merujuk pada "standar terkini dan, jika berlaku, standar Eropa dan internasional yang relevan". CRA, sebagai hukum keselamatan produk berdasarkan Kerangka Legislatif Baru, memungkinkan pihak yang diatur untuk mengandalkan standar yang harmonis untuk secara presumtif menunjukkan kesesuaian dengan aturan. Pekerjaan sedang berlangsung oleh Pusat Pembelajaran Bersama (JRC) Komisi Eropa dan ENISA untuk memetakan standar yang ada ke persyaratan penting di bawah CRA, termasuk yang berkaitan dengan kriptografi. Oleh karena itu, jelas bahwa standar dari organisasi seperti ISO, NIST, dan ENISA (termasuk dokumen Teletrust/ENISA) sangat penting untuk menentukan standar terkini dan yang lebih mendasar lagi, langkah-langkah keamanan yang "tepat" di bawah hukum keamanan siber Uni Eropa. Dengan demikian, perlakuan PQC saat ini dalam hukum lunak yang diumumkan oleh entitas-entitas ini perlu dipertimbangkan.

PQC dalam Hukum Lunak

Saat ini, tidak ada prioritas normatif yang jelas antara berbagai instrumen standar dalam regulasi keamanan siber Uni Eropa. Hal ini dapat berubah setelah standar yang harmonis diadopsi, misalnya, berdasarkan CRA (lihat khususnya Pasal 13(14) dan 27 dari CRA). Standar yang harmonis merupakan hibrida khusus antara 'hukum lunak' dan 'hukum keras'. Standar ini dirancang oleh tiga organisasi standar resmi Eropa: Institut Standar Telekomunikasi Eropa (ETSI), Komite Standardisasi Eropa (CEN), dan Komite Standardisasi Elektroteknik Eropa (CENELEC) atas permintaan Komisi Eropa dan sesuai dengan prosedur yang ditetapkan dalam Peraturan (EU) 1025/2012. Ketika dipublikasikan dalam Jurnal Resmi, standar tersebut secara resmi menjadi bagian dari hukum Uni Eropa. Namun, karena belum ada standar tersebut yang diadopsi di bidang keamanan siber, kita menemukan badan pengatur merujuk pada berbagai standar relevan lainnya.

Hal ini dibuktikan baik dalam perlakuan standar keamanan siber oleh Otoritas Perlindungan Data (DPA) berdasarkan GDPR maupun latihan pemetaan keamanan siber yang dilakukan oleh JRC dan ENISA, yang mempertimbangkan beberapa organisasi standar. Logis untuk menyatakan bahwa standar Eropa memiliki kekuatan normatif yang lebih besar daripada standar internasional, yang pada gilirannya memiliki kekuatan normatif yang lebih besar daripada standar domestik non-Eropa. Memang, ini tampaknya merupakan pendekatan yang diambil oleh JRC dan ENISA dalam latihan pemetaan mereka, dengan publikasi yang "memberikan prioritas kepada organisasi standardisasi Eropa dan internasional." Meskipun NIST yang berbasis di AS tidak secara formal diidentifikasi sebagai organisasi standar yang "relevan", hasil kerjanya dirujuk beberapa kali di seluruh dokumen, menunjukkan pengaruhnya yang kuat terhadap standar keamanan siber secara global. Dalam ranah kriptografi PQC, jelas bahwa NIST memimpin upaya standardisasi, sebuah fakta yang diakui oleh organisasi-organisasi utama Eropa seperti ENISA dan ETSI. Oleh karena itu, pekerjaan organisasi standar Eropa tentang PQC dan 'kondisi terkini' dipertimbangkan, sebelum memeriksa hasil dari organisasi standar internasional dan kemudian NIST.

Pedoman dan Standar Eropa

Pekerjaan standardisasi pasca-kuantum di Eropa paling tepat digambarkan sebagai persiapan. ETSI telah menghasilkan Laporan Teknis (TR) untuk berkontribusi pada proses PQC NIST, selain TR yang meletakkan dasar untuk migrasi ke PQC. Namun, TR ETSI hanya berisi "materi penjelasan" dan berbeda dari (dan seringkali merupakan pendahulu) Standar dan Spesifikasi Teknis Eropa yang secara lebih konkret menentukan persyaratan. Yang menarik, keluaran CEN-CENELEC mencatat "kurangnya standar untuk manajemen kunci kuantum dan integrasi kunci kuantum dengan teknologi enkripsi seperti PQC."

Pekerjaan ENISA juga bersifat pendahuluan. Sebuah laporan tahun 2022 menunjuk pada pekerjaan badan negara anggota Uni Eropa, termasuk *Agence nationale de la sécurité des systèmes d'information* (ANSSI) Prancis, yang "memperingatkan tentang ketidakmatangan algoritma pasca-kuantum, dengan mengatakan bahwa algoritma tersebut masih dalam tahap pembelajaran." Dokumen ENISA/Teletrust tentang keadaan terkini di bawah GDPR tampaknya menyarankan bahwa organisasi yang menyimpan data di cloud, saat ini, harus siap untuk beralih ke PQC di masa mendatang yang tidak ditentukan, tetapi tidak menjadikan ini sebagai persyaratan:

> Dengan mempertimbangkan masa depan, gerbang enkripsi harus dipilih yang memungkinkan organisasi pengguna untuk secara bebas bertukar algoritma enkripsi yang digunakan (Crypto Agility). Dengan perkembangan progresif komputer kuantum yang sangat canggih, prosedur yang diklasifikasikan sebagai aman saat ini mungkin akan menjadi usang dalam waktu dekat. Oleh karena itu, solusi yang sudah kompatibel dengan algoritma kriptografi pasca-kuantum (PQC) adalah ideal.

Hal ini menunjukkan bahwa implementasi PQC saat ini tidak dianggap sebagai langkah teknis dan organisasi mutakhir yang diperlukan dalam banyak konteks yang dibahas dalam dokumen ini.

Standar Internasional

Upaya badan standar internasional dalam PQC berada pada posisi yang serupa dengan organisasi-organisasi Eropa. ISO telah merilis standar yang berkaitan dengan distribusi kunci kuantum, dan telah membuat amandemen pada standarnya tentang kartu identitas untuk memungkinkan interoperabilitas untuk pertukaran operasi keamanan menggunakan PQC. Saat ini, ISO sedang mempertimbangkan amandemen terkait PQC pada ISO/IEC 18033–2 tentang algoritma enkripsi asimetris. Menariknya, algoritma yang dipilih untuk kartu identitas, dan saat ini sedang dipertimbangkan untuk aplikasi kriptografi asimetris yang lebih umum, termasuk algoritma yang dipilih pada babak final kontes PQC NIST, tetapi pada akhirnya tidak dipilih.

Pada Januari 2023, *Internet Engineering Task Force* (IETF) membentuk kelompok kerja *Post-Quantum Use In Protocols* (PQUIP), yang diposisikan untuk mendukung pekerjaan organisasi lain seperti NIST dan memiliki berbagai dokumen terkait PQC dalam tahap draf. Uni Telekomunikasi Internasional (ITU), yang pekerjaannya berfokus pada infrastruktur telekomunikasi, mungkin tidak mengherankan telah memfokuskan upayanya pada QKD (Distribusi Kunci Kuantum) daripada PQC.

NIST

Seperti yang telah disebutkan sebelumnya, NIST jelas merupakan organisasi yang memimpin upaya penetapan standar protokol kriptografi pasca-kuantum. Ini merupakan perluasan dari peran historisnya dalam menetapkan standar algoritma kriptografi klasik, peran yang tidak lepas dari kontroversi karena dugaan keterlibatan badan keamanan nasional.

Antara Desember 2016 dan Maret 2025, NIST mengadakan kompetisi yang dirancang untuk menemukan algoritma PQC yang paling sesuai untuk enkripsi asimetris umum dan tanda tangan digital untuk otentikasi. Pada Agustus 2024, Standar Pemrosesan Informasi Federal (FIPS) 203 ditetapkan, menggunakan Mekanisme Enkapsulasi Kunci Berbasis Modul-Kisi (ML-KEM), yang berasal dari pengajuan CRYSTALS-KYBER. FIPS 204 dan 205 berkaitan dengan algoritma tanda tangan digital pasca-kuantum untuk otentikasi yang aman. Pada Maret 2025, algoritma PQC tambahan diidentifikasi sebagai algoritma terpilih lebih lanjut, termasuk HQC sebagai mekanisme enkapsulasi kunci tambahan.

Secara resmi, standar keamanan siber dan kriptografi NIST bersifat wajib bagi lembaga federal AS dalam konteks tertentu, di mana hanya algoritma kriptografi yang disetujui yang dapat digunakan oleh lembaga-lembaga ini. Namun, standar NIST berpengaruh di industri AS dan global, dengan lembaga-lembaga AS seperti FTC dan lembaga-lembaga Eropa seperti EDPB atau DPA nasional sering merujuk pada standar NIST sebagai indikator praktik industri atau langkah-langkah keamanan yang tepat. Yang mencerminkan pentingnya kompetisi PQC NIST yang lebih luas adalah keragaman negara dan lembaga tempat para perancang finalis berasal.

Terlepas dari pengakuan resmi algoritma PQC sebagai FIPS, perlu ditekankan bahwa NIST memperkirakan migrasi ke PQC akan memakan waktu. Dalam hal ini, fakta bahwa terdapat algoritma PQC yang diakui oleh NIST (atau badan standar lainnya) tidak secara otomatis berarti bahwa penggunaannya diwajibkan oleh lembaga federal AS. Masih ada pekerjaan signifikan dalam menentukan protokol lebih lanjut untuk implementasi PQC ke dalam berbagai pengaturan. NIST saat ini menargetkan tahun 2030 agar algoritma klasik "dihapus" (yaitu, diizinkan, tetapi perlu diwaspadai) dan tahun 2035 agar penggunaannya "dilarang". Tampak jelas pula bahwa organisasi standar Eropa dan internasional menunggu hasil kompetisi PQC NIST sebelum memutuskan pendekatan mereka sendiri terhadap standardisasi dan pemetaan jalan migrasi ke PQC. Dengan demikian, pengakuan itu sendiri merupakan langkah penting namun tidak cukup untuk adopsi PQC yang lebih holistik. Sejauh standar hukum lunak NIST mampu 'diperkuat' di bawah peraturan keamanan siber Uni Eropa, ini menunjukkan bahwa standar PQC yang dipilih belum termasuk dalam 'kondisi terkini'.

Apakah Regulasi Keamanan Siber Uni Eropa Sesuai dengan Tujuannya?

Karena tidak adanya referensi eksplisit terhadap ancaman kuantum dalam hukum sekunder Uni Eropa, kita harus mengandalkan interpretasi yang cukup rumit untuk menyimpulkan bahwa, saat ini, hukum keamanan siber Uni Eropa mungkin tidak mewajibkan penggunaan PQC. Hal ini disebabkan oleh kurangnya pengakuan PQC dalam standar Eropa, munculnya algoritma PQC NIST, dan pekerjaan besar yang harus dilakukan untuk memastikan PQC dapat diimplementasikan secara kuat di berbagai produk.

Dalam konteks diskusi di atas, dua pengamatan sangat mencolok. Pertama, benar atau salah, hukum keamanan siber Uni Eropa sangat bergantung pada pekerjaan organisasi standar, suatu proses yang mungkin tidak memiliki pengaruh sama sekali. Hal ini menimbulkan kekhawatiran seperti legitimasi yang dijelaskan lebih rinci di tempat lain dalam volume ini dan kurangnya kontrol oleh regulator Uni Eropa. Meskipun demikian, organisasi standar merupakan aktor penting dalam tata kelola keamanan siber global. Uni Eropa sebaiknya bekerja sama dan dalam kerangka ini, daripada melawannya.

Kedua, dan terkait, adalah bahwa "penggunaan legislatif yang luas dari persyaratan fungsional generik yang berakar pada 'kondisi terkini'" oleh Uni Eropa memerlukan fokus yang tajam pada kondisi teknologi saat ini. Pendekatan presentistis yang diambil oleh legislator Uni Eropa di sini mungkin mencerminkan asal usul hukum perdata dari gagasan kondisi terkini berdasarkan premis bahwa seseorang tidak dapat diharapkan untuk memperhitungkan, dan membela diri terhadap, cacat atau hasil yang tidak diketahui. Tentu saja, konsep kondisi terkini adalah "kriteria dinamis dan cair yang memerlukan peninjauan kembali praktik keamanan secara berkala". Ini berarti, pada prinsipnya, bahwa organisasi harus dapat beradaptasi dengan ancaman yang muncul seperti komputasi kuantum. Namun, konsep tersebut mengasumsikan bahwa mengadopsi langkah-langkah kondisi terkini adalah semua yang dapat diminta dari organisasi yang berupaya melindungi jaringan dan sistem informasi. Tidak ada persyaratan eksplisit (meskipun dapat dikatakan laten dalam konsep tersebut) bagi organisasi untuk melihat melampaui keadaan terkini dan menuju masa depan. Yang penting, ini sepenuhnya mengabaikan ancaman HNDL sistem saat ini rentan terhadap ancaman yang tidak dapat diatasi dengan langkah-langkah terkini. Selain itu, diragukan apakah hukum keamanan siber Uni Eropa mengharuskan organisasi untuk siap, jika ancaman kuantum segera terwujud, untuk beralih ke sistem PQC. Kita dapat bertanya apakah hal ini perlu diperjelas oleh regulator Uni Eropa. Dalam hal ini, hukum keamanan siber Uni Eropa saat ini tidak memperhitungkan kemungkinan pergeseran paradigma dalam keamanan siber, seperti yang mungkin ditimbulkan oleh komputasi kuantum.

5.4 REFORMULASI REGULASI KEAMANAN SIBER UE TERHADAP ANCAMAN KUANTUM

Pertanyaan selanjutnya adalah apakah regulasi keamanan siber Uni Eropa perlu diubah, dan jika ya, bagaimana caranya? Hukum keamanan siber Uni Eropa dibenarkan berdasarkan alasan bahwa hukum tersebut melindungi pasar internal, dan/atau hak-hak fundamental, tergantung pada instrumennya. Sejauh komputasi kuantum menghadirkan ancaman eksistensial terhadap kepentingan dan hak-hak ini, respons yang memadai diperlukan. Mengingat Uni Eropa, dan Negara-negara Anggotanya, berinvestasi besar-besaran dalam komputasi kuantum karena peluang signifikan yang diberikan oleh teknologi tersebut, logis bahwa risikonya juga harus diperhitungkan.

Dari perspektif strategis tingkat tinggi, ancaman kuantum datang pada saat tantangan kebijakan signifikan lainnya yang dihadapi Uni Eropa terutama dalam domain teknologi. Dahulu sebagai pemimpin global dalam teknologi, Eropa kini semakin bergantung pada teknologi eksternal yang berkembang pesat, yang membahayakan kekuatan ekonomi,

koherensi politik, dan pengaruh globalnya. Kajian terbaru menekankan bahwa Uni Eropa harus melampaui strategi nasional yang terfragmentasi untuk membentuk kerangka kerja jangka panjang yang koheren yang meningkatkan otonomi digital Eropa. Dengan demikian, strategi PQC Uni Eropa tidak boleh diperlakukan secara terpisah, tetapi sebagai komponen dari strategi kuantum dan keamanan siber yang lebih luas. Era kuantum bukan hanya tantangan teknis dan peluang ekonomi, tetapi juga ujian kapasitas Uni Eropa untuk bertindak sebagai kekuatan digital yang koheren dan berdaulat. Menghadapi tantangan tersebut dapat semakin mengamankan posisinya sebagai kekuatan digital yang berdaulat.

Dari perspektif yang lebih konkret, jika hukum keamanan siber Uni Eropa tidak sesuai untuk mengatasi ancaman kuantum, berbagai cara tersedia bagi regulator untuk bertindak. Tanggung jawab untuk menghadapi ancaman kuantum juga dapat dibebankan kepada berbagai aktor dalam kerangka peraturan keamanan siber Uni Eropa, mulai dari industri hingga organisasi standar, pembuat undang-undang, dan lembaga peradilan. Kemungkinan besar, kombinasi dari berbagai perangkat regulasi yang dibahas dalam bagian ini merupakan respons yang paling tepat, daripada pendekatan tunggal. Perangkat regulasi ini secara kasar diurutkan dari yang paling ringan hingga yang paling keras, mulai dari pendekatan yang ringan dan berbasis pasar hingga peninjauan ulang sepenuhnya terhadap norma-norma keamanan siber sebagaimana yang diatur dalam peraturan keamanan siber Uni Eropa.

Laissez-Faire: Pendekatan yang Dipimpin Industri

Terdapat beberapa bukti yang menunjukkan bahwa industri swasta bergerak maju dengan transisi PQC meskipun tidak ada persyaratan hukum formal untuk melakukannya. Seperti yang telah disebutkan di bagian sebelumnya, PQC sudah ditawarkan secara mulus dan secara default dalam banyak produk dan protokol kriptografi populer seperti pesan instan dan perbankan. Hal ini menunjukkan adanya insentif pasar untuk segera beralih ke PQC misalnya, karena kekhawatiran yang muncul dari komputasi kuantum atau untuk memberikan kesan berada di garis depan keamanan siber.

Namun, menyerahkan transisi PQC kepada industri dan kekuatan pasar akan menjadi tindakan yang gegabah. Keamanan siber dapat dikatakan sebagai "pasar barang cacat" mengingat insentif yang menghambat investasi pada alat dan personel yang tangguh (dan mahal) yang muncul sebagai biaya dalam neraca keuangan, dan mengingat banyaknya pelanggaran keamanan pada sistem sektor swasta. Mengingat ancaman komputasi kuantum yang tidak pasti dan sebagian besar bersifat teoretis, mengharapkan perusahaan secara massal untuk menghabiskan sumber daya yang langka pada PQC yang baru muncul dan kompleks adalah tidak realistis. Selain itu, insentif pasar tidak berlaku secara langsung untuk entitas publik, yang mengendalikan (walaupun seringkali bersamaan dengan industri swasta) beberapa sistem yang paling penting dan rentan bagi masyarakat. Terakhir, sementara adopsi PQC oleh industri mungkin meningkat untuk produk dan layanan saat ini dan di masa mendatang, insentif untuk melindungi sistem yang lebih tua atau sistem lama menjadi berkurang.

Pada akhirnya, sebagian besar pekerjaan dalam mengimplementasikan PQC berada di pundak industri swasta, yang bertanggung jawab atas infrastruktur digital utama, termasuk

yang berada di balik barang dan jasa publik. Namun, tidak realistis dan tidak bertanggung jawab untuk menyerahkan tugas migrasi PQC kepada keinginan pasar. Migrasi ke PQC seharusnya didorong lebih kuat.

Tindakan Kebijakan: Pendekatan yang Dipimpin Eksekutif

Meskipun belum ada pengakuan hukum yang tegas dan eksplisit mengenai ancaman kuantum terhadap keamanan siber, terdapat peningkatan pengakuan di tingkat eksekutif. Komisi Eropa mencatat dalam Kertas Putih baru-baru ini bahwa "penting untuk mendorong Negara Anggota untuk mengembangkan pendekatan yang terkoordinasi dan harmonis, memastikan konsistensi dalam pengembangan dan adopsi standar PQC Uni Eropa di seluruh Negara Anggota." Komisi juga telah merilis Rekomendasi mengenai peta jalan menuju PQC yang menemukan hal serupa, seperti halnya Strategi Quantum Europe baru-baru ini, yang diterbitkan pada 7 Juli 2025. Pentingnya pendekatan yang harmonis sangat penting mengingat badan-badan keamanan siber Negara Anggota menerbitkan laporan mereka sendiri mengenai transisi PQC. Instrumen-instrumen ini menggarisbawahi pengakuan, meskipun kurangnya tindakan afirmatif dalam menanggapi ancaman kuantum terhadap keamanan siber. Untuk tujuan ini, Rodríguez berpendapat bahwa Komisi harus mengambil peran yang lebih aktif dalam mengoordinasikan tanggapan oleh Negara Anggota dan portofolio utama seperti DG CONNECT dan ENISA. Sebuah pengarahan kepada Parlemen Eropa menunjukkan bahwa tindakan Uni Eropa dan Negara Anggota terfragmentasi, dengan perhatian yang signifikan pada hasil NIST. Kompetisi standar PQC.

Terkait dengan upaya dalam lembaga standardisasi, lembaga seperti ENISA dan EDPB memiliki peran penting dalam menghasilkan hukum lunak yang relevan dengan interpretasi dan praktik hukum keamanan siber Uni Eropa. Rodríguez juga menunjuk pada sertifikasi berdasarkan Undang-Undang Keamanan Siber sebagai jalan potensial untuk mendorong adopsi PQC. Salah satu keuntungan dari pendekatan "kotak abu-abu" Uni Eropa saat ini terhadap regulasi keamanan siber, di mana konsep-konsep kunci seperti "kondisi terkini" kurang ditentukan, adalah bahwa hal itu memberikan ruang yang cukup besar bagi lembaga-lembaga eksekutif ini untuk menafsirkan dan menegakkan hukum dengan cara yang responsif terhadap ancaman keamanan siber baru. Dengan demikian, interpretasi yang mungkin bersifat presentistis terhadap "kondisi terkini" dapat diperluas melalui panduan administratif untuk mencakup ancaman di masa depan yang terkait dengan komputasi kuantum.

Sebagai contoh, ENISA, berbeda dengan publikasi bersama dengan TeleTrust, dapat memandu entitas dengan lebih kuat dan cepat menuju PQC, atau setidaknya mendorong organisasi untuk mempertimbangkan risiko terkait kuantum. EDPB juga dapat mengeluarkan pedoman yang menguraikan kapan PQC mungkin tepat untuk diterapkan misalnya, dalam operasi pemrosesan berisiko tinggi, atau transfer internasional. Lebih lanjut, mengingat ancaman yang ditimbulkan oleh HNDL, panduan dapat mengharuskan pihak yang diatur untuk mempertimbangkan apakah data sensitif atau berisiko tinggi pantas untuk ditransfer melalui jaringan publik sama sekali, dan mencari alternatif untuk enkripsi asimetris. Pendekatan ini, pada prinsipnya, akan meniadakan kebutuhan akan amandemen hukum keras yang lebih

lengkap terhadap peraturan keamanan siber Uni Eropa dan memungkinkan Uni Eropa untuk merespons ancaman PQC lebih cepat dibandingkan dengan alternatif lain.

Pendekatan yang Dipimpin Organisasi Standar

Berkaitan dengan, tetapi berbeda dari dokumen panduan dari organisasi seperti ENISA dan EDPB adalah hasil dari organisasi standar. Pendekatan yang ringan terhadap regulasi akan menyerahkan pembentukan norma mengenai PQC kepada organisasi standar. Dapat dikatakan, ini adalah pendekatan yang sebagian besar diambil oleh Uni Eropa sejauh ini dengan menyerahkan sebagian besar penetapan standar algoritma PQC kepada NIST, meskipun dengan beberapa dukungan dari lembaga-lembaganya.

Terlepas dari apakah tepat bagi regulator dan organisasi standar Eropa untuk sangat bergantung pada proses standardisasi yang dipimpin oleh entitas AS dalam memutuskan pemilihan algoritma PQC, kesimpulan dari kompetisi NIST memberi Uni Eropa kesempatan untuk menciptakan jalur yang selaras dengan kepentingannya sendiri. Dalam hal ini, perlu ditekankan bahwa Uni Eropa memiliki hubungan yang berbeda dengan, dan tingkat pengaruh yang berbeda terhadap, organisasi standar internasional dan Eropa utama. Standar mulai memainkan peran yang lebih signifikan dalam regulasi teknologi, khususnya melalui pendekatan Kerangka Legislatif Baru di bawah CRA dan Undang-Undang Kecerdasan Buatan (*AI Act*). Mengingat bahwa pekerjaan organisasi standar Eropa pada PQC masih dalam tahap awal, Uni Eropa dapat mengarahkan badan-badan standar untuk memprioritaskan pekerjaan pada transisi PQC. Misalnya, dalam konteks CRA (atau undang-undang harmonisasi Uni Eropa lainnya seperti AI Act), Komisi Eropa dapat meminta CEN, CENELEC, atau ETSI untuk menyusun standar Eropa yang berkaitan dengan PQC. AI Act memberikan preseden Komisi Uni Eropa yang mempercepat proses pembuatan standar di bidang-bidang yang dianggap penting.

Ada beberapa kekurangan dalam mengandalkan pendekatan ini, dan memang dalam mendorong standardisasi Eropa untuk implementasi PQC yang baru muncul. Pertama, dibutuhkan waktu yang signifikan untuk menyusun standar yang sesuai. Ancaman dari komputer kuantum mungkin akan segera terwujud. Kedua, masih diragukan apakah keterlibatan Uni Eropa akan memberikan dampak positif yang signifikan terhadap upaya global saat ini seputar standardisasi PQC, mengingat sifat pembelajaran keamanan siber dan PQC yang sangat kompleks dan khusus. Ketiga, dan terkait dengan hal ini, mengingat interoperabilitas global jaringan dan sistem informasi, upaya Uni Eropa untuk mengambil peran yang lebih aktif dalam standardisasi mungkin secara tidak diinginkan akan memecah belah atau bahkan melemahkan keamanan infrastruktur digital global. Dengan demikian, meskipun transisi PQC sangat penting dari segi waktu, jalur saat ini menuju standardisasi dan adopsi PQC mungkin optimal mengingat apa yang saat ini diketahui tentang ancaman kuantum.

Kejelasan Persyaratan Hukum yang Mutlak: Pendekatan yang Dipimpin oleh Lembaga Peradilan

Hukum keamanan siber Uni Eropa sangat kekurangan keputusan peradilan mengenai instrumen-instrumen kuncinya. Bygrave menjelaskan bahwa:

> Kurangnya yurisprudensi yang menafsirkan persyaratan hukum keamanan siber dengan tingkat ketelitian yang wajar juga berarti bahwa persyaratan tersebut tetap menjadi kotak abu-abu dalam arti lain yaitu, sebagai norma yang buram dan kurang terdefinisi, terutama ketika bergantung pada kriteria yang sulit dipahami, seperti kewajaran, kesesuaian, proporsionalitas, dan 'kondisi terkini'. Kriteria tersebut tidak hanya kabur secara kasat mata; kriteria tersebut cenderung menghasilkan keputusan yang tidak jelas yang didasarkan pada gagasan kepatutan yang relatif subjektif.

Kejelasan peradilan atas konsep-konsep kunci seperti kondisi terkini akan diinginkan dalam lebih banyak konteks daripada kuantum. Pada prinsipnya, pernyataan oleh CJEU mengenai jenis-jenis tindakan teknis, operasional, dan organisasi apa yang mungkin tepat dalam kasus-kasus tertentu dapat memberikan konteks yang berharga tentang bagaimana menafsirkan hukum keamanan siber Uni Eropa dalam konteks ancaman kuantum. Hukum keamanan siber Uni Eropa saat ini kurang siap untuk menghadapi ancaman di masa depan seperti HNDL. Kriteria "licin" yang digunakan oleh pembuat undang-undang Eropa dapat ditafsirkan sedemikian rupa sehingga ancaman di masa depan harus dipertimbangkan secara cermat oleh pihak yang diatur. Melakukan hal itu akan menggeser pendekatan presentistis dari hukum keamanan siber Uni Eropa saat ini, seperti yang telah dibahas di sini.

Namun, harapan ini mungkin tidak realistis mengingat masih barunya banyak instrumen keamanan siber utama (misalnya, CRA, NIS 2) dan kurangnya yurisprudensi yang ada pada instrumen yang relatif mapan (misalnya, GDPR). Peluang munculnya kasus yang tepat yang memberi kesempatan kepada CJEU untuk memberikan pendapat tentang langkah-langkah keamanan yang tepat atau mutakhir, dan CJEU mengambil kesempatan itu, sangat kecil. Dalam satu-satunya kasus yang telah ditangani sejauh ini yang melibatkan interpretasi Pasal 32 GDPR (tentang langkah-langkah keamanan), Mahkamah Eropa (CJEU) hanya memberikan "sedikit sekali detail tentang langkah-langkah keamanan aktual yang dipersyaratkan oleh Pasal 32". Pada saat yang sama, tidaklah masuk akal untuk mengharapkan lembaga peradilan memberikan banyak detail tersebut mengingat mereka bukanlah ahli di bidang tersebut. Hakim kemungkinan besar (dan memang seharusnya) akan menghormati pandangan para spesialis keamanan siber, dan ketika pandangan-pandangan ini belum berkembang, putusan pengadilan akan (dan seharusnya) cenderung bersifat umum. Dengan demikian, yurisprudensi kemungkinan besar tidak akan memberikan klarifikasi yang tepat waktu kepada pengacara, insinyur, dan praktisi lainnya mengenai persyaratan era PQC.

Persyaratan Keamanan Siber yang Lebih Tegas dalam Hukum yang Keras: Pendekatan yang Dipimpin oleh Legislator

Respons regulasi yang lebih tegas akan melibatkan amandemen terhadap peraturan keamanan siber Uni Eropa untuk lebih mempertimbangkan sifat ancaman keamanan siber yang terus berkembang seperti PQC. Dalam tulisannya pada tahun 2016 tentang hukum Uni Eropa mengenai keamanan komunikasi, Arnbak mengkritik cara pembuat undang-undang Uni Eropa secara tidak kreatif menggunakan kembali istilah-istilah dari instrumen lain yang berkaitan dengan keamanan siber:

> Kerangka peraturan Uni Eropa, secara ringkas, memuat sejumlah besar pengaturan legislatif tentang keamanan komunikasi, tetapi baik visi yang koheren dari pembuat undang-undang maupun pandangan yang jelas tentang hukum apa yang ada dan bagaimana menerapkannya masih kurang. Ketidakpastian hukum merasuki hukum keamanan komunikasi Uni Eropa […]. Tampaknya ada kebiasaan legislatif di mana konseptualisasi "keamanan" disalin dari dokumen-dokumen sebelumnya, dengan sedikit argumentasi dan elaborasi tentang dampak konsepsi "keamanan" tertentu terhadap kebijakan aktual yang diusulkan dalam instrumen-instrumen ini.

Pemeriksaan di atas terhadap instrumen Uni Eropa yang lebih baru (yaitu, NIS 2 dan CRA) menunjukkan bahwa "kebiasaan legislatif" ini masih hidup dan berkembang, meskipun persyaratannya lebih rinci dan preskriptif daripada instrumen sebelumnya (misalnya, GDPR). Dapat dikatakan, seperti yang disarankan oleh Arnbak, kecenderungan untuk mendaur ulang ketentuan di berbagai instrumen berarti bahwa para pembuat undang-undang tidak berpikir kritis tentang risiko dan ancaman apa yang harus diperhatikan oleh pihak yang diatur.

Seperti yang disarankan oleh kontribusi lain dalam buku ini, dinamika unik teknologi kuantum dapat memicu gangguan hukum yang lebih luas daripada hanya di bidang keamanan siber. Jika gangguan ini terjadi, dapat diperkirakan bahwa lebih banyak instrumen hukum daripada yang dibahas di sini perlu ditinjau kembali oleh para legislator. Namun, dalam kasus keamanan siber, hal itu mungkin sudah terlambat. Potensi masalahnya agak berbeda karena tindakan yang diambil hari ini dapat membantu mengurangi dampak ancaman di masa depan. Dalam hal ini, pengakuan legislatif eksplisit bahwa organisasi tidak selalu dapat mengandalkan langkah-langkah 'tercanggih' yang tersedia saat ini untuk melindungi jaringan dan sistem informasi mungkin layak ditambahkan di samping persyaratan fungsional yang ada. Pendekatan seperti itu, pada prinsipnya, akan mengharuskan organisasi untuk mempertimbangkan serangan HNDL. Selain itu, legislasi (bukan, seperti yang dibahas di atas, lembaga eksekutif atau pengadilan) dapat secara lebih eksplisit (bukan, seperti saat ini, secara laten) mengharuskan organisasi untuk lebih gesit dalam menanggapi ancaman yang muncul seperti komputasi kuantum.

Secara realistis, instrumen digital Uni Eropa jarang diubah secara parsial. Ini akan membutuhkan amandemen di berbagai instrumen yang membutuhkan persyaratan keamanan siber. Modal politik tersebut mungkin lebih baik dihabiskan di tempat lain, terutama mengingat sifat ancaman yang tidak diketahui. Perubahan legislatif mungkin bagus, tetapi mungkin merupakan harapan yang tidak realistis dan berpotensi tidak berdampak dalam praktik setidaknya secara sendirinya.

Rekonseptualisasi Norma Keamanan Siber: Pendekatan Seluruh Pihak

Pada dasarnya, keamanan siber berkaitan dengan menjaga kerahasiaan, integritas, dan ketersediaan jaringan dan sistem informasi (yaitu, “triad CIA”). Hukum keamanan siber Uni Eropa sering kali mengacu pada model dasar ini. Misalnya, NIS 2 mendefinisikan “keamanan jaringan dan sistem informasi” sebagai “kemampuan jaringan dan sistem informasi untuk menahan, pada tingkat kepercayaan tertentu, setiap peristiwa yang dapat membahayakan ketersediaan, keaslian, integritas, atau kerahasiaan data yang disimpan, ditransmisikan, atau

diproses, atau layanan yang ditawarkan oleh, atau dapat diakses melalui, jaringan dan sistem informasi tersebut".

Berbagai prinsip, strategi, dan konsep ada yang melengkapi dan mendukung triad CIA, beberapa di antaranya tercermin dalam hukum Uni Eropa. Misalnya, keamanan berdasarkan desain melibatkan penanaman prinsip-prinsip keamanan ke dalam proses pengembangan produk dan layanan sejak awal, bukan sebagai pertimbangan belakangan. Hal ini disebut dalam Undang-Undang Keamanan Siber dan diwujudkan dalam GDPR sebagai perlindungan data berdasarkan desain. Ketahanan siber, yang mengacu pada kemampuan organisasi untuk mencegah, menahan, dan pulih dari insiden keamanan siber, adalah konsep lain yang sangat terlihat dalam CRA.

Tidak satu pun dari hal-hal ini secara langsung menuntut atau bahkan mendorong pihak yang diatur oleh peraturan keamanan siber Uni Eropa untuk memikirkan ancaman baru yang muncul seperti komputasi kuantum. Hal ini menimbulkan pertanyaan apakah konsep-konsep baru harus dikembangkan dan akhirnya muncul dalam peraturan keamanan siber Uni Eropa yang secara memadai mencakup ancaman tersebut. Konsep ketangkasan kriptografi semakin mendapat tempat dalam wacana keamanan siber, dengan salah satu definisi yang ditawarkan sebagai "kemampuan untuk bermigrasi ke algoritma dan standar kriptografi baru secara berkelanjutan." Terdapat referensi terhadap konsep ini dalam publikasi ENISA/Teletrust tentang keadaan terkini, yang menunjukkan adanya pengakuan regulasi. Konsep ini tentu dapat bermanfaat dalam mempersiapkan organisasi untuk bermigrasi ke PQC tepat waktu. Namun, seperti yang disebutkan oleh Ott dkk., konsep ini masih baru:

> …ada kebutuhan penting untuk mengembangkan ilmu ketangkasan kriptografi yang berprinsip; ilmu yang memperluas dan mengembangkan ruang lingkup ketangkasan hingga pengembangan kerangka kerja yang aman yang memungkinkan kemajuan kriptografi berkelanjutan dalam berbagai konteks sistem, protokol, dan aplikasi.

Hanya menempatkan persyaratan tersebut dalam hukum keras atau lunak saja tidak cukup untuk mewujudkannya; diperlukan pendekatan interdisipliner yang melibatkan semua pihak. Mengintegrasikan persyaratan bagi organisasi untuk mempertahankan "ketangkasan kriptografi" secara prematur, saat ini, akan sama dengan slogan kosong yang tidak memiliki nilai regulasi konkret. Terlebih lagi, ketangkasan kriptografi tidak cukup mengurangi ancaman serangan HNDL. Dapat dikatakan, agar serangan HNDL tercakup dalam regulasi dan praktik keamanan siber, diperlukan pemikiran ulang tentang keamanan siber yang mendorong atau mewajibkan organisasi untuk berpikir melampaui masa kini atau jangka pendek.

Salah satu kemungkinannya adalah pengintegrasian tata kelola antisipatif yang lebih besar dalam rezim keamanan siber Uni Eropa. Tata kelola antisipatif mengacu pada kapasitas lembaga untuk meramalkan, mempersiapkan, dan membentuk perkembangan masa depan secara proaktif dan inklusif. Hal ini menjadi terkenal dalam kajian STS tentang nanoteknologi. Dalam konteks tersebut, tata kelola antisipatif memperlakukan "prospek" nanoteknologi sebagai "pada dasarnya tidak pasti". Pendekatan seperti itu sangat cocok untuk

menginformasikan (penataan ulang) rezim keamanan siber Uni Eropa saat menghadapi tantangan komputasi kuantum.

Seperti yang dijelaskan dalam diskusi di atas, rezim ini tidak boleh terkunci dalam pandangan dunia yang puas diri yang gagal memperhitungkan kemungkinan perubahan peristiwa yang cepat dan tidak terduga. Sebaliknya, rezim ini perlu didasarkan pada pandangan yang menghargai karakter perubahan teknologi yang seringkali belum sempurna, tidak dapat diprediksi, dan "muncul". Pihak yang diatur harus didorong untuk mengembangkan pola pikir yang mampu terus-menerus menilai kembali asumsi tentang lanskap teknologi-organisasi, termasuk ancaman yang muncul di cakrawala. Sebagaimana dikemukakan oleh Mandel,

> Sistem hukum yang menyadari ketidakpastian isu-isu baru, yang fleksibel dan mudah beradaptasi, dan yang mengakui bahwa isu-isu baru yang dihasilkan oleh kemajuan teknologi mungkin tidak sesuai dengan konstruksi hukum yang sudah ada, akan beroperasi jauh lebih baik dalam mengelola inovasi teknologi daripada sistem yang gagal mempelajari pelajaran ini.

Berlandaskan pada kebutuhan akan tata kelola antisipatif, perkembangan terkini dalam lanskap keamanan siber Uni Eropa menunjukkan pengakuan yang semakin meningkat meskipun masih dalam tahap awal tentang pentingnya kerangka kerja regulasi yang berwawasan ke depan. Wacana tingkat Uni Eropa yang lebih umum baru-baru ini mengidentifikasi tata kelola antisipatif sebagai hal yang semakin penting untuk menavigasi risiko dan peluang yang ditimbulkan oleh teknologi disruptif. Meskipun tidak secara eksplisit merujuk pada tata kelola antisipatif, Laporan ENISA baru-baru ini tentang Keadaan Keamanan Siber di Uni Eropa mempromosikan "pendekatan legislatif yang berwawasan ke depan yang dapat membawa manfaat tambahan bagi Uni Eropa" mengingat ancaman siber baru seperti AI dan komputasi kuantum.

Meskipun pengakuan ini menjanjikan, masih banyak pekerjaan yang harus dilakukan untuk menerjemahkan pengakuan ini ke dalam mekanisme hukum dan kelembagaan yang konkret. Terdapat tantangan signifikan dalam menumbuhkan budaya regulasi yang gesit, reflektif, dan mampu berkembang seiring dengan teknologi yang ingin diaturnya. Hal ini membutuhkan masukan dan dukungan dari banyak aktor dalam rantai nilai keamanan siber, mulai dari mereka yang berada di garis depan, hingga akademisi, pakar keamanan, dan sektor swasta. Waktu akan membuktikan apakah hal ini dapat dicapai sebelum teknik enkripsi asimetris saat ini terancam. Namun, mengingat industri keamanan siber pasti akan menghadapi ancaman eksistensial lainnya di masa mendatang, hal ini tetap merupakan upaya yang layak.

5.5 KESIMPULAN DAN DAMPAK KEAMANAN SIBER UE

Bagian ini telah mengeksplorasi sejauh mana kerangka peraturan keamanan siber Uni Eropa siap untuk mengatasi tantangan transformatif yang ditimbulkan oleh komputasi kuantum. Meskipun Uni Eropa telah membuat kemajuan signifikan dalam mengembangkan kerangka hukum keamanan siber yang komprehensif termasuk instrumen seperti GDPR,

Direktif NIS 2, dan Undang-Undang Ketahanan Siber pemeriksaan ini menunjukkan bahwa masih terdapat kesenjangan penting dalam kemampuan kerangka kerja ini untuk mengantisipasi dan menanggapi ancaman terkait kuantum.

Inti dari masalah ini terletak pada ketergantungan pada konsep hukum seperti "kondisi terkini" dan "langkah-langkah teknis dan organisasi yang tepat." Meskipun istilah-istilah ini menawarkan fleksibilitas dan netralitas teknologi, istilah-istilah ini juga berisiko terlalu berfokus pada kondisi saat ini dan mungkin tidak cukup mendorong manajemen risiko yang berorientasi ke masa depan. Hal ini sangat relevan dalam konteks ancaman yang muncul seperti serangan "panen sekarang, dekripsi nanti", yang menciptakan kerentanan saat ini berdasarkan kemampuan komputer kuantum yang diantisipasi di masa depan.

Meskipun PQC telah muncul sebagai solusi teknis terkemuka, penggabungannya ke dalam harapan regulasi masih terbatas. Instrumen Uni Eropa saat ini tidak secara eksplisit mensyaratkan penggunaan PQC, sebagian karena status standar yang relevan masih baru dan tidak adanya panduan yang jelas dari badan pengatur Eropa. Selain itu, Uni Eropa hingga saat ini memainkan peran yang lebih observasional dalam proses standardisasi global, khususnya bergantung pada hasil inisiatif PQC NIST yang berbasis di AS. Hal ini mencerminkan tantangan yang lebih luas bagi Uni Eropa dalam menegaskan kepemimpinan normatif di bidang di mana saat ini Uni Eropa tidak mendominasi batas teknologi.

Pada saat yang sama, Uni Eropa memiliki berbagai alat yang dapat digunakan secara lebih tegas untuk mengatasi tantangan ini. Lembaga-lembaga seperti ENISA dan EDPB berada pada posisi yang tepat untuk mengembangkan instrumen hukum lunak seperti panduan interpretatif atau skema sertifikasi yang mendorong respons proaktif terhadap ancaman kuantum. Namun, upaya-upaya ini masih belum berkembang dan agak terfragmentasi. Lembaga peradilan dan legislatif juga memainkan peran kunci, meskipun keterlibatan peradilan dengan persyaratan keamanan siber sejauh ini masih minimal, dan proses legislatif seringkali berlangsung dengan kecepatan yang sulit untuk mengimbangi perubahan teknologi yang pesat.

Di luar instrumen hukum spesifik, bagian ini telah mengidentifikasi isu konseptual yang lebih luas. Sebagian besar regulasi keamanan siber Uni Eropa masih berakar pada model keamanan tradisional, seperti triad CIA. Namun, lanskap ancaman yang terus berkembang menuntut pola pikir regulasi yang lebih antisipatif dan adaptif yang mencakup konsep seperti ketangkasan kriptografi dan mampu menanggapi risiko yang tidak pasti tetapi berpotensi sistemik. Meskipun ide-ide ini mulai muncul dalam wacana tingkat Uni Eropa, ide-ide tersebut belum dioperasionalkan secara bermakna.

Tabel 5.1 Ringkasan temuan utama

Temuan Utama	**Ringkasan**
Hukum Keamanan Siber Uni Eropa Tidak Siap Menghadapi Ancaman Kuantum	Hukum yang ada bergantung pada istilah-istilah yang samar seperti "kondisi terkini" yang tidak memperhitungkan risiko di masa depan seperti komputasi kuantum.

Adopsi Kriptografi Pasca-Kuantum (PQC) Tertinggal	Hukum Uni Eropa tidak secara jelas mewajibkan PQC, karena statusnya yang tidak jelas dalam standar dan dorongan regulasi yang terbatas.
Badan Standar Mendorong Regulasi, tetapi Uni Eropa Kurang Memiliki Kendali	Uni Eropa bergantung pada standar eksternal (terutama NIST), yang membatasi kemampuannya untuk memimpin secara global.
Instrumen Hukum Lunak Kurang Dimanfaatkan	Lembaga-lembaga seperti ENISA dan EDPB dapat mendorong adopsi PQC tetapi belum melakukannya secara tegas.
Jalur Peradilan dan Legislatif Menawarkan Bantuan yang Terbatas	Pengadilan belum mengklarifikasi ekspektasi keamanan siber; perubahan legislatif berjalan lambat dan penuh tantangan politik.
Terdapat Kesenjangan Konseptual dalam Kerangka Kerja Saat Ini	Hukum keamanan siber saat ini kurang memiliki konsep-konsep yang berwawasan ke depan seperti ketangkasan kriptografi dan tata kelola antisipatif.
Kebutuhan Mendesak akan Respons Proaktif dan Terkoordinasi	Pendekatan gabungan yang melibatkan hukum, standar, kebijakan, dan tata kelola diperlukan untuk mengatasi ancaman kuantum.

Mengingat temuan-temuan ini, bagian ini menyimpulkan bahwa meskipun kerangka kerja keamanan siber Uni Eropa memberikan fondasi yang berharga, evolusi lebih lanjut diperlukan untuk memastikan ketahanan di era kuantum. Pengembangan panduan yang lebih eksplisit, standar yang lebih jelas, dan perangkat hukum yang berorientasi masa depan ditambah dengan peningkatan koordinasi antar aktor institusional akan membantu memposisikan Uni Eropa untuk mengatasi tantangan kuantum secara lebih efektif. Sebagai titik acuan regulasi global, Uni Eropa berada pada posisi yang tepat untuk memimpin dalam membentuk respons terhadap teknologi yang muncul, tetapi untuk melakukannya akan membutuhkan keterlibatan yang lebih cermat dengan ketidakpastian dan kompleksitas yang ada di depan.

BAB 6
TANTANGAN DAN PELUANG REGULASI EKSPOR KOMPUTASI KUANTUM

Teknologi kuantum muncul sebagai aset strategis dengan potensi untuk memberikan keuntungan ekonomi, teknologi, dan keamanan yang signifikan bagi pemerintah dan perusahaan yang mencapai kepemimpinan awal. Seiring inovasi kuantum menjadi sangat penting secara strategis, pengendalian ekspor pada teknologi ini menimbulkan dilema hukum dan kebijakan yang kompleks, termasuk ketegangan antara inovasi, kolaborasi, dan keamanan nasional. Komputasi kuantum, khususnya, menghadirkan tantangan regulasi yang unik karena tumpukan teknologi berlapis dan potensi penggunaan ganda. Bab ini menawarkan pemeriksaan mendalam tentang langkah-langkah pengendalian ekspor baru-baru ini pada komputasi kuantum yang diadopsi oleh Amerika Serikat dan beberapa Negara Anggota Uni Eropa. Bagian ini memetakan ruang lingkup dan struktur pengendalian ini, memeriksa bagaimana pengendalian tersebut menargetkan elemen spesifik dari rantai pasokan kuantum, dan menyoroti pergeseran menuju pendekatan regulasi plurilateral di luar kerangka kerja multilateral tradisional. Lebih lanjut, bagian ini mengidentifikasi tantangan tata kelola utama seperti mengatur aset tak berwujud, menghindari fragmentasi, dan beradaptasi dengan paradigma kuantum baru dan menyediakan kerangka kerja yang berwawasan ke depan bagi regulator untuk merancang strategi pengendalian ekspor yang lebih terkoordinasi dan adaptif.

Selain memeriksa kendala, bagian ini mengidentifikasi berbagai peluang penegakan hukum khusus kuantum yang secara unik terkait dengan karakteristik fisik, arsitektur, dan lapisan akses teknologi tersebut. Ini termasuk jejak fisik dan sentralisasi infrastruktur skala besar, potensi model akses berbasis cloud untuk kontrol dinamis dan terdiferensiasi, dan sifat modular perangkat keras yang memungkinkan pembatasan tingkat komponen yang terperinci. Alih-alih menawarkan penilaian normatif, bagian ini menyaring pola-pola yang muncul dan pertimbangan strategis yang kemungkinan akan membentuk masa depan tata kelola teknologi kuantum. Bagian ini menilai bahwa ada peluang dan tantangan tertentu dalam pengendalian ekspor terkait komputer kuantum yang dapat memberikan informasi kepada regulator tentang strategi di bidang ini dan membantu memandu desain pendekatan regulasi yang adaptif dan kompatibel ke depan.

6.1 KONTROL EKSPOR TEKNOLOGI KUANTUM: FUNGSI DAN TANTANGAN KEBIJAKAN

Kontrol ekspor berfungsi sebagai instrumen hukum dan kebijakan yang digunakan oleh pemerintah untuk membatasi akses musuh terhadap teknologi canggih. Persaingan yang semakin ketat antara Tiongkok, AS, dan Uni Eropa telah menyoroti regulasi teknologi baru dan terobosan. Sejak tahun 2022, berbagai yurisdiksi di berbagai wilayah telah meningkatkan pembatasan ekspor teknologi yang secara langsung dan tidak langsung terkait dengan

pembelajaran dan produksi komputer kuantum, di antara teknologi tinggi lainnya dengan dampak "yang diketahui namun tidak pasti" terhadap keamanan ekonomi dan nasional.

Dasar pemikiran dan efektivitas kontrol ekspor sebagai alat regulasi, secara luas, bergantung pada beberapa faktor. Ini termasuk tingkat kerja sama internasional, ketangguhan mekanisme penegakan hukum, kejelasan peraturan, dan kemampuan regulator untuk beradaptasi dengan kemajuan teknologi. Namun, yang mungkin kurang diteliti dalam riset, adalah efek bahwa subjek kontrol ekspor mungkin lebih atau kurang mudah dibatasi tergantung pada sifat teknologi, jalur pembelajaran dan pengembangannya, dan rantai pasokannya.

Komputer kuantum mewakili teknologi mutakhir yang didukung oleh rantai pasokan yang sangat kompleks dan saling bergantung. Pengembangan dan penerapannya tidak hanya membutuhkan perangkat keras dan perangkat lunak kuantum khusus, tetapi juga infrastruktur pendukung yang canggih seperti sistem kriogenik, fasilitas ruang bersih, dan alat fabrikasi presisi serta keahlian yang sangat khusus di berbagai disiplin ilmu sains dan teknik. Teknologi ini juga saat ini kurang memiliki tata kelola eksplisit di bawah kontrol ekspor multilateral, menjadikan komputer kuantum sebagai contoh ideal untuk meneliti peluang dan keterbatasan kontrol ekspor pada teknologi canggih.

Bagian ini memberikan empat kontribusi utama pada wacana ilmiah dan kebijakan tentang kontrol ekspor teknologi kuantum. Pertama, bagian ini memberikan pemetaan hukum dan peraturan komparatif yang terperinci tentang kontrol ekspor AS dan beberapa Negara Anggota Uni Eropa yang spesifik untuk komputasi kuantum menyoroti cakupan teknisnya, variasi nasional, dan pendorong geopolitik yang mendasarinya. Kedua, bagian ini menyajikan uraian terstruktur dari 'tumpukan' komputasi kuantum dari perangkat keras dan material hingga perangkat lunak dan infrastruktur pendukung sehingga menawarkan kerangka kerja untuk memahami bagaimana kontrol ekspor berinteraksi dengan sifat berlapis dan modular dari teknologi mutakhir ini. Ketiga, bagian ini mengidentifikasi dan memeriksa secara kritis tren peraturan yang muncul, seperti pergeseran menuju koordinasi plurilateral di luar kerangka kerja multilateral tradisional seperti Perjanjian Wassenaar, dan dampaknya terhadap harmonisasi, penegakan hukum, dan kepatuhan. Keempat, bagian ini merinci serangkaian tantangan tata kelola yang bernuansa termasuk ambiguitas definisi, difusi teknologi, dan kesulitan mengatur aset tidak berwujud seperti pengetahuan dan perangkat lunak mengingat ekosistem kuantum yang berkembang pesat dan tersebar secara internasional.

Selain kontribusi inti tersebut, bagian ini menyoroti peluang penegakan hukum strategis yang muncul dari karakteristik fisik dan arsitektur komputasi kuantum. Ini termasuk jejak fisik infrastruktur perangkat keras kuantum, kontrol terpusat yang diberikan oleh model akses berbasis cloud, dan potensi pembatasan yang ditargetkan pada komponen pendukung dalam sistem kuantum. Secara keseluruhan, fitur-fitur ini menciptakan lanskap regulasi di mana langkah-langkah selektif yang berlandaskan teknis dapat menjadi layak dan berdampak terutama pada tahap awal komersialisasi bidang ini.

Dengan demikian, bagian ini memberikan kejelasan konseptual dan wawasan praktis pada bidang di mana kebijakan berkembang lebih cepat daripada konsensus hukum atau

akademis, dan memberikan dasar untuk respons regulasi yang lebih terkoordinasi, adaptif, dan efektif. Bagian ini menggarisbawahi pentingnya menyelaraskan desain kontrol ekspor tidak hanya dengan masalah keamanan nasional tetapi juga dengan kemampuan teknologi spesifik dan kemungkinan tata kelola yang dihadirkan oleh domain komputasi kuantum.

Taruhannya tinggi, dan risikonya nyata. Secara optimis, kontrol ekspor dapat mendorong dan memfasilitasi kolaborasi strategis dan regional di antara sekutu geopolitik. Namun, kontrol ekspor dapat (jika belum) menghambat kolaborasi internasional yang sah, legal, dan diinginkan pada komputer kuantum, sekaligus tidak efektif dalam mencapai hasil yang diinginkan. Oleh karena itu, sangat penting bagi para pembuat kebijakan untuk memahami tantangan yang terkait dengan penerapan kontrol ekspor pada jenis teknologi tertentu.

Sebelum melanjutkan, perlu dibuat pernyataan mengenai ruang lingkup bagian ini. Politik dan kebijakan seputar kontrol ekspor kompleks dan tidak transparan, serta kurang diteliti dalam riset akademis. Bagian ini tidak bertujuan untuk memberikan pemeriksaan kebijakan komprehensif atau evaluasi normatif tentang kontrol ekspor. Sebaliknya, bagian ini meneliti kerangka kerja kontrol ekspor saat ini yang mengatur teknologi komputasi kuantum di AS dan sekutu strategisnya di Uni Eropa dan mengidentifikasi peluang dan tantangan tertentu mengingat "tumpukan" komputasi kuantum dan rantai pasokan yang lebih luas. Terakhir, pemeriksaan bagian ini terbatas pada komputasi kuantum, bukan teknologi kuantum lainnya seperti komunikasi kuantum atau penginderaan (kecuali sejauh aplikasi tersebut tumpang tindih dengan komputasi).

6.2 LOGIKA DAN CAKUPAN KONTROL EKSPOR

Kontrol ekspor dapat diterapkan karena berbagai alasan, mulai dari respons krisis dan pengelolaan sumber daya hingga perlindungan lingkungan dan perlindungan hak asasi manusia. Dalam kasus teknologi baru seperti komputer kuantum, kontrol ini sering dibenarkan atas dasar keamanan nasional atau regional, bahkan jika mempertahankan keunggulan teknologi atas pesaing ekonomi adalah perhatian utama. Selain itu, kontrol ekspor juga dapat dianggap sebagai prasyarat untuk memungkinkan, mendukung, dan membenarkan kolaborasi regional strategis dan untuk melindungi rantai pasokan. Tentu saja, kemakmuran ekonomi dan keamanan semakin menjadi konsep yang saling terkait. Namun, dalam kasus kontrol terhadap teknologi baru, pembenaran hukum sering kali terkait langsung dengan pertahanan, dengan banyak yurisdiksi menempatkan komputer kuantum pada daftar teknologi "penggunaan ganda" dengan aplikasi militer dan sipil.

Oleh karena itu, komputer kuantum muncul bersamaan dengan perangkat keras nuklir, bioteknologi, dan satelit sebagai hal yang memerlukan pembatasan dan pengawasan pemerintah karena potensi penggunaannya untuk keperluan militer oleh musuh geopolitik. Pendekatan ini didasarkan pada berbagai “ketidakpastian yang diketahui” yang mungkin ditimbulkan oleh komputer kuantum, mulai dari risiko terhadap keamanan siber global hingga penggunaan dalam sistem senjata terkomputerisasi. Meskipun risiko-risiko ini signifikan dan memerlukan mitigasi, risiko tersebut tidak boleh menutupi motivasi lain untuk membatasi

ekspor komputer kuantum, seperti proteksionisme ekonomi. Mengingat tahap awal komputasi kuantum dan potensinya yang substansial, menjadi pelopor menawarkan keuntungan yang cukup besar bagi perusahaan swasta dan negara tempat mereka beroperasi. Yang terpenting, ada risiko kerugian yang signifikan bagi mereka yang gagal memantapkan diri di arena komputasi kuantum. Industri komputasi kuantum dapat menjadi sangat berpengaruh, dengan dampak yang luas pada sektor hilir seperti pembelajaran biomedis, kecerdasan buatan, logistik, dan keuangan. Benteng ekonomi yang dibangun di industri teknologi perbatasan lainnya seperti semikonduktor dan unit pemrosesan grafis (GPU) mungkin juga muncul di sektor komputasi kuantum, di mana satu atau beberapa perusahaan atau wilayah dominan mendapat manfaat yang tidak proporsional dari teknologi tersebut.

Tujuan utama dari kontrol ekspor sulit untuk disimpulkan, sehingga mengukur keberhasilannya hampir mustahil. Dalam kasus teknologi baru, wajar untuk berasumsi bahwa salah satu tujuan utamanya adalah untuk memperlambat, jika bukan menghentikan sepenuhnya, para pesaing geopolitik dari menikmati kemajuan teknologi di bidang yang diatur. Misalnya, pembatasan AS terhadap akses Tiongkok ke semikonduktor canggih pada 7 Oktober 2022 secara eksplisit bertujuan untuk “membatasi kemampuan RRT untuk memperoleh chip komputasi canggih, mengembangkan dan memelihara superkomputer, dan memproduksi semikonduktor canggih.” Pengumuman Biro Industri dan Keamanan AS menguraikan beberapa dampak hilir yang diharapkan dari kontrol ini sebagai rasionalisasi kebijakan. Hal ini mencakup dampak militer (seperti sistem senjata otonom), dampak ekonomi (seperti industri AI China yang berkembang pesat yang bergantung pada chip canggih), dan kekhawatiran hak asasi manusia (seperti peran AI dalam meningkatkan kemampuan pengawasan warga negara China).

Kontrol-kontrol ini dilaporkan berhasil membatasi akses China ke GPU canggih yang digunakan dalam pelatihan AI. Namun, hal ini juga mendorong China untuk mengintensifkan upayanya dalam produksi semikonduktor domestik. Bahkan, beberapa analis teknologi berpendapat bahwa kontrol semacam itu mungkin hanya menawarkan keuntungan sementara, karena dapat mempercepat R&D dalam negeri, mendorong pemisahan rantai pasokan, dan memotivasi munculnya ekosistem alternatif di luar jangkauan yurisdiksi AS atau sekutunya. Misalnya, kemajuan pesat AI perusahaan China seperti DeepSeek, yang baru-baru ini mengembangkan dan merilis model bahasa besar (LLM) domestik yang dilaporkan dilatih tanpa akses ke chip NVIDIA kelas atas, menyoroti bagaimana kendala dapat merangsang pengembangan paralel, inovasi algoritma, dan mempercepat kemandirian. Dapat dikatakan bahwa mengizinkan akses berkelanjutan tetapi terbatas ke platform AS seperti infrastruktur GPU NVIDIA atau sistem yang diterapkan di cloud AS dapat mengunci pesaing ke dalam ekosistem yang dikendalikan AS, di mana penggunaan dapat dipantau, dibatasi, dan diatur secara strategis dari waktu ke waktu.

Oleh karena itu, sulit untuk menentukan apakah perkembangan ini merupakan "kemenangan" atau kegagalan kebijakan secara keseluruhan. Ketika dikombinasikan dengan ketidakpastian yang melekat pada komputasi kuantum, hal ini menggarisbawahi tantangan dalam mengantisipasi dampak jangka panjang dari kontrol ekspor. Selain itu, keberhasilan,

daya saing, dan keberlanjutan ekosistem inovasi juga bergantung pada kolaborasi ilmiah dan inovasi terbuka yang diatur dengan baik pada tahap pra-kompetitif. Hal ini menyoroti perlunya menavigasi pertimbangan yang rumit antara nilai dan kepentingan yang terkadang saling bertentangan. Mencapai keseimbangan yang tepat seperti antara "sebisa mungkin terbuka dan sebisa mungkin tertutup" dan kebalikannya bukanlah tugas yang mudah. Bersama dengan faktor-faktor seperti timbal balik, nilai-nilai politik, kepercayaan, dan tingkat risiko penggunaan ganda, kontrol ekspor dan impor memainkan peran penting dalam mengkalibrasi keseimbangan ini dan mengidentifikasi "titik optimal" yang layak.

6.3 INSTRUMEN PENGENDALIAN EKSPOR UNILATERAL DAN MULTILATERAL

Secara internasional, pengendalian ekspor seringkali berbentuk perjanjian multilateral dan instrumen unilateral. Perjanjian multilateral dalam konteks ini adalah kerangka kerja kerja sama yang melibatkan banyak negara yang sepakat untuk menerapkan kebijakan pengendalian ekspor bersama. Tujuan utama perjanjian ini adalah untuk mencegah proliferasi senjata pemusnah massal dan teknologi lain yang terkait dengan masalah keamanan nasional. Yang paling relevan untuk teknologi baru, Kesepakatan Wassenaar berfokus pada pengendalian ekspor senjata konvensional dan barang serta teknologi penggunaan ganda, mempromosikan transparansi dan tanggung jawab yang lebih besar dalam transfer barang penggunaan ganda dengan tujuan meningkatkan keamanan regional dan internasional. Penandatangan Kesepakatan Wassenaar termasuk AS, semua negara Uni Eropa, Jepang, dan Rusia. Namun, ketentuannya bersifat sukarela dan memerlukan implementasi domestik.

Di sisi lain, instrumen unilateral adalah langkah-langkah pengendalian ekspor yang diimplementasikan oleh masing-masing negara secara independen dari perjanjian multilateral. Negara-negara dapat mengadopsi kontrol unilateral untuk mengatasi masalah keamanan nasional tertentu, melindungi kepentingan ekonomi, atau menanggapi perkembangan geopolitik yang belum tercakup oleh perjanjian multilateral. Keduanya memiliki kelebihan dan kekurangan. Mencari perjanjian multilateral bisa rumit dan lambat, dan dalam banyak kasus (termasuk Perjanjian Wassenaar yang tidak mengikat) aturan tersebut harus diimplementasikan secara domestik oleh masing-masing penandatangan. Multilateralisme juga dapat menghadapi kebuntuan; ketegangan geopolitik yang dipicu oleh invasi Rusia ke Ukraina membuat pembaruan daftar ekspor Wassenaar menjadi sulit. Di AS, kepresidenan Trump yang pertama sangat mendukung unilateralisme, dan kepresidenan keduanya tampaknya semakin condong ke arah itu.

Meskipun kontrol unilateral dapat lebih fleksibel dan responsif terhadap kepentingan nasional langsung, kontrol tersebut juga dapat menyebabkan ketegangan dengan negara lain dan memiliki dampak yang tidak dapat diprediksi pada rantai pasokan global. Kurangnya koordinasi melalui kerangka kerja multilateral dapat mengakibatkan inkonsistensi dan potensi konflik antara kebijakan nasional, dan “forum shopping” oleh entitas yang diatur yang berupaya menghindari regulasi yang memberatkan.

Seperti yang diilustrasikan di bawah ini, baru-baru ini terjadi peningkatan kontrol ekspor terhadap teknologi komputasi kuantum oleh penandatangan Wassenaar, meskipun di

luar saluran resmi Wassenaar. Beberapa upaya ini dapat digambarkan sebagai plurilateral karena jelas muncul dari kolaborasi multi-yurisdiksi, tetapi di luar kerangka kerja yang mapan seperti Perjanjian Wassenaar. Langkah-langkah ini dapat meningkatkan fragmentasi, dan berisiko mempersulit tantangan menyeimbangkan kekhawatiran keamanan nasional dengan manfaat kerja sama internasional dan rantai pasokan.

6.4 KONTROL EKSPOR EROPA DAN AS YANG RELEVAN DENGAN KOMPUTASI KUANTUM

AS, Uni Eropa, dan beberapa Negara Anggota Uni Eropa masing-masing telah menerapkan kontrol ekspor yang secara khusus atau tidak langsung memengaruhi komputasi kuantum dan rantai pasokannya. Bagian ini menjelaskan aturan yang saat ini diterapkan terkait dengan komputer kuantum. Pertama, bagian ini mengkaji Perjanjian Wassenaar, yang menjelaskan kurangnya kontrol khusus untuk komputasi kuantum. Kemudian, bagian ini meninjau kontrol AS baru-baru ini yang menargetkan komputasi kuantum, dan kontrol Eropa yang dirancang dengan istilah serupa. Perlu dicatat bahwa Uni Eropa saat ini tidak memiliki peran yang signifikan; oleh karena itu, Negara Anggota telah menerapkan "tambal sulam" kontrol di tingkat nasional yang mencerminkan aturan AS dalam berbagai tingkat.

Perjanjian Wassenaar

Perjanjian Wassenaar mencantumkan sembilan kategori barang dan teknologi penggunaan ganda, mulai dari pengolahan material hingga kedirgantaraan dan propulsi. Dalam kategori-kategori ini, kontrol diorganisasikan menjadi lima bagian, yaitu:

A—Sistem, Peralatan, dan Komponen

B—Peralatan Uji, Inspeksi, dan Produksi

C—Material

D—Perangkat Lunak E—Teknologi

Perjanjian Wassenaar tidak secara langsung membahas komputer kuantum. Satu-satunya referensi eksplisitnya terhadap teknologi kuantum adalah kriptografi terkait kuantum dan penginderaan kuantum.

Perangkat keras dan perangkat lunak komputer klasik tertentu pada prinsipnya dibatasi oleh Perjanjian Wassenaar. Pada perangkat keras, Kategori 3 dan 4, Elektronik dan Komputer, secara historis telah menerapkan berbagai macam komponen termasuk jenis "mikrosirkuit mikroprosesor" dan "elektro-optik" dan "sirkuit terpadu optik". Dapat dibayangkan bahwa beberapa di antaranya mungkin relevan dengan pembelajaran atau pengembangan komputer kuantum. Namun, sebagian besar kontrol yang berlaku umum pada komputer telah dilonggarkan atau dihapus, dan Perjanjian Wassenaar tidak berlaku untuk teknologi atau perangkat lunak di domain publik, atau untuk pembelajaran ilmiah dasar.

Perjanjian Wassenaar memang membatasi ekspor pendingin dan sistem kriogenik tertentu. Namun, ini termasuk dalam daftar amunisi dan hanya berlaku untuk sistem propulsi roket cair. Sistem pendingin kriogenik yang umum digunakan dalam komputer kuantum qubit superkonduktor tidak tercakup. Oleh karena itu, meskipun Perjanjian Wassenaar mengatur, atau secara historis telah mengatur, teknologi yang berdekatan dengan komputer kuantum dan infrastruktur pendukungnya, perjanjian ini tidak secara khusus menargetkan komputer

kuantum. Telah dilaporkan bahwa kontrol plurilateral baru-baru ini terhadap komputer kuantum yang dibahas di bawah ini muncul “di sela-sela” pertemuan tahunan Perjanjian Wassenaar pada tahun 2023. Hal ini menyiratkan bahwa beberapa negara baru-baru ini berupaya agar teknologi komputasi kuantum ditambahkan ke daftar kontrol dalam Perjanjian Wassenaar, yang jelas-jelas gagal, sehingga menyebabkan pendekatan yang terfragmentasi saat ini. Pada akhirnya, kesimpulan tersebut bersifat spekulatif mengingat kerahasiaan diskusi keamanan nasional tentang teknologi sensitif. Namun, hal ini menunjukkan adanya keinginan untuk mengatur komputer kuantum dalam kerangka kerja Wassenaar, yang akan meningkatkan legitimasi dan koordinasi kontrol.

Amerika Serikat

Pendekatan AS terhadap kontrol ekspor membedakan antara barang-barang penggunaan ganda dan barang-barang yang dirancang khusus untuk aplikasi militer. Teknologi penggunaan ganda diatur berdasarkan Peraturan Administrasi Ekspor (EAR) oleh Biro Industri dan Keamanan (BIS). Teknologi ini memiliki aplikasi komersial dan militer, dengan kontrol ekspor yang bertujuan untuk mencegah musuh meningkatkan kemampuan militer mereka sambil tetap mempromosikan inovasi dan perdagangan komersial. AS menerapkan persyaratan perizinan dan pemeriksaan penggunaan akhir untuk memastikan bahwa teknologi penggunaan ganda ini tidak jatuh ke tangan negara-negara yang dibatasi.

Rezim kontrol ekspor AS mengkategorikan negara-negara ke dalam kelompok yang berbeda (A hingga E) berdasarkan tingkat kerja sama mereka dengan kebijakan kontrol ekspor AS dan kepatuhan mereka terhadap norma-norma non-proliferasi internasional. Kategorisasi ini menentukan apakah pengecualian perizinan dapat diterapkan. Kelompok Negara A terdiri dari sekutu tradisional AS yang menikmati perlakuan paling menguntungkan. Kelompok Negara D mencakup negara-negara yang menjadi perhatian, seperti negara-negara dengan sejarah proliferasi atau negara-negara yang dikenai sanksi AS, termasuk Tiongkok dan Rusia. Ekspor ke negara-negara ini relatif dibatasi dan seringkali memerlukan lisensi khusus. Selain pembatasan ekspor ke negara-negara tertentu berdasarkan daftar barang, kontrol ekspor AS juga dapat menargetkan pengguna akhir tertentu (misalnya, perusahaan teknologi Tiongkok) dan penggunaan akhir (misalnya, untuk digunakan dalam senjata).

Pada September 2024, Departemen Perdagangan AS mengumumkan kontrol ekspor dalam bentuk Aturan Akhir Sementara tentang beberapa teknologi baru, termasuk komputer kuantum, manufaktur semikonduktor, komputasi canggih, dan barang-barang yang terkait dengan manufakturnya. Mengikuti kategori Perjanjian Wassenaar, barang-barang yang dibatasi muncul dalam Kategori 3 (Elektronik) dan Kategori 4 (Komputer). Kontrol ini didasarkan pada kontrol ekspor semikonduktor yang telah diterapkan sebelumnya pada Oktober 2022 dan Oktober 2023, dalam serangkaian manuver kebijakan yang dikenal sebagai "perang chip", yang berfokus terutama pada kekhawatiran AS bahwa mereka akan kehilangan keunggulan kompetitif dalam kecerdasan buatan (AI) dibandingkan dengan China.

Seperti yang telah dicatat, kontrol ini serupa dengan yang diterapkan oleh sekutu geopolitik seperti Belanda, Inggris, Spanyol, Prancis, Australia dan Jepang yang diterapkan dalam kurun waktu satu tahun sebelum dan sesudah aturan AS. Kontrol September 2024

menandakan perluasan “perang chip” AS secara langsung ke ranah komputasi kuantum, dengan pembatasan yang diberlakukan pada “komputer kuantum, peralatan terkait, komponen, material, perangkat lunak, dan teknologi yang dapat digunakan dalam pengembangan dan pemeliharaan komputer kuantum.”

Kontrol tersebut berisi pengecualian lisensi untuk ekspor ke negara-negara yang telah menerapkan pembatasan ekspor serupa, termasuk Inggris Raya, Norwegia, Belanda, Australia, dan Jepang. Menariknya, kontrol tersebut memungkinkan organisasi untuk berbagi teknologi kepada warga negara asing di AS. Hal ini biasanya dianggap sebagai "ekspor tersirat" dan karenanya tunduk pada rezim perizinan. Aturan Akhir Sementara mencatat bahwa "kesulitan ini akan sangat merugikan kemajuan berkelanjutan dari perkembangan di masa depan di bidang kuantum, yang bergantung pada karyawan warga negara asing dari tujuan tersebut." Dengan demikian, seperti yang dilaporkan, "aturan tersebut mengizinkan berbagi dengan warga negara asing yang bekerja di AS, bahkan jika mereka berasal dari negara-negara yang diidentifikasi oleh pemerintah sebagai negara yang menimbulkan kekhawatiran keamanan nasional atau dikenai embargo senjata".

Sebaliknya, aturan tersebut memberlakukan persyaratan pencatatan pada organisasi yang berbagi teknologi kuantum yang dikontrol kepada warga negara tertentu; dilaporkan bahwa ini kemungkinan merupakan latihan pengumpulan informasi yang dipimpin pemerintah untuk berpotensi meningkatkan kontrol di masa mendatang. Item yang ditambahkan ke daftar kontrol tidak berlaku untuk semua komputer kuantum dan infrastruktur pendukungnya. Sebaliknya, item-item tersebut ditujukan untuk pengembangan komputer kuantum dengan ambang batas kinerja tertentu. Secara langsung, Nomor Klasifikasi Kontrol Ekspor (ECCN) 4A906, Komputer kuantum dan “rakitan elektronik” dan “komponen” terkait, membatasi komputer kuantum dengan lebih dari 34 qubit dengan tingkat koherensi tertentu. Alasan yang mungkin untuk batasan 34-qubit

Item 4A906 juga mencakup komponen yang secara khusus terkait dengan komputer kuantum yang dikontrol. Secara paralel, ECCN 4D906 dan 4E906 telah ditambahkan untuk mencakup perangkat lunak dan teknologi yang dirancang atau dimodifikasi secara khusus untuk pengembangan atau produksi sistem tersebut. Bersama-sama, ketentuan-ketentuan ini bertujuan untuk mengatur secara komprehensif tidak hanya komputer kuantum itu sendiri tetapi juga perangkat keras, perangkat lunak, dan pengetahuan teknis pendukung yang penting yang diperlukan untuk membangun sistem yang memenuhi atau melampaui ambang batas kinerja yang ditentukan.

Bersamaan dengan pembatasan pada komputer kuantum sebagai kategori yang cukup luas, Peraturan Akhir Sementara juga menargetkan bahan baku dan barang-barang tertentu yang dianggap berada di garis depan pengembangan perangkat keras komputasi kuantum. Ini termasuk sistem pendingin kriogenik tertentu dan peralatan pengujian kriogenik (ECCN 3A904 & 3B904) serta bahan-bahan yang terkait dengan silikon dan germanium (ECCN 3C907, 3C908, 3C909) yang memiliki sifat-sifat berharga untuk jenis komputer kuantum tertentu. Tabel 6.1 merangkum ECCN utama yang relevan dengan komputasi kuantum.

Tabel 6.1 ECCN AS yang relevan dengan komputasi kuantum berdasarkan Peraturan Akhir Sementara

ECCN	Deskripsi	Penjelasan
3A901	Cryo-CMOS dan penguat sinyal	Teknologi masa depan yang dirancang untuk beroperasi pada suhu ≤4,5 K; relevan untuk komputasi kuantum yang dapat diskalakan.
3A904	Sistem dan komponen pendingin kriogenik tertentu	Mendukung sistem kuantum skala besar dengan banyak qubit fisik.
3B904	Peralatan pengujian wafer kriogenik	Memungkinkan pengujian cepat chip kuantum pada suhu kriogenik.
3C907	Material epitaksial dengan komposisi tertentu	Material yang digunakan dalam fabrikasi perangkat kuantum.
3C908	Fluorida, hidrida, klorida Si/Ge dengan material tertentu	Material untuk pengembangan qubit berbasis spin.
3C909	Si, SiO_2, Ge, GeO_2 dengan dopan tertentu	Material yang mendukung platform qubit semikonduktor.
4A906	Komputer kuantum >34 qubit atau setara, dan komponen terkait	Mencakup sistem lengkap, susunan qubit, dan perangkat kontrol/pengukuran. Tidak jelas mengapa 34 bit menjadi ambang batasnya.
4D906	Perangkat lunak untuk pengembangan/produksi barang 4A906.b atau .c	Menargetkan perangkat lunak untuk sistem kuantum tingkat lanjut.
4E906	Teknologi untuk pengembangan/produksi/penggunaan barang yang dikendalikan	Berlaku untuk data teknis atau pengetahuan terkait dengan 4A906 dan ECCN terkait.

Uni Eropa

Peran Uni Eropa dalam peraturan pengendalian ekspor secara historis kompleks, karena kompetensi Uni Eropa (pada prinsipnya) yang terbatas di bidang keamanan nasional. Untuk menyederhanakan rezim saat ini (yang diuraikan secara komprehensif oleh Bennink dkk.), barang-barang penggunaan ganda saat ini diatur oleh Uni Eropa melalui Peraturan (UE) 2021/821 ("Peraturan Penggunaan Ganda"). Peraturan Penggunaan Ganda mensyaratkan otorisasi untuk ekspor barang-barang penggunaan ganda yang tercantum dalam Lampiran I-nya, yang mereproduksi teks-teks Perjanjian Wassenaar dan rezim multilateral lainnya yang ditandatangani oleh Uni Eropa dan/atau Negara Anggotanya. Tidak seperti aturan "ekspor yang dianggap" AS, Peraturan Penggunaan Ganda tidak berlaku untuk warga negara asing yang mengakses barang-barang yang dikendalikan di dalam Uni Eropa.

Seperti yang dicatat dalam Kertas Putih Komisi Uni Eropa, Uni Eropa "tidak memiliki ketentuan hukum yang diperlukan untuk mengadopsi aturan seragam di tingkat Uni Eropa" kontrol ekspor secara independen dari apa yang diadopsi dalam rezim multilateral, kecuali di area yang sangat terbatas." Dengan demikian, Uni Eropa tidak dapat, dalam konteks komputasi kuantum, memberlakukan pembatasan ekspor di luar apa yang sudah terkandung dalam rezim

multilateral seperti Perjanjian Wassenaar. Oleh karena itu, saat ini tidak ada pembatasan ekspor khusus komputasi kuantum yang diberlakukan oleh Uni Eropa.

Sebaliknya, Negara-negara Anggota Uni Eropa telah menerapkan kontrol mereka sendiri di tingkat nasional. Peraturan Penggunaan Ganda memberikan kemungkinan ini dalam Bagian II-nya. Pasal 4 mengizinkan kontrol ekspor atas barang-barang yang tidak tercantum dalam Lampiran I yang "dimaksudkan atau mungkin dimaksudkan" untuk digunakan dalam senjata pemusnah massal. Pasal 5 memberikan ketentuan serupa untuk alat pengawasan siber. Pasal 9 memberi ruang bagi Negara Anggota untuk memberlakukan pembatasan pada berbagai macam barang, "untuk alasan keamanan publik, termasuk pencegahan tindakan terorisme, atau untuk pertimbangan hak asasi manusia." Negara Anggota harus memberitahukan Komisi Uni Eropa tentang langkah-langkah yang diadopsi berdasarkan Pasal 9, dengan Komisi ditugaskan untuk secara berulang menerbitkan kompilasi langkah-langkah ini. Seperti yang dicatat oleh Bennink, persyaratan terakhir ini tidak berlaku untuk barang-barang yang dibatasi berdasarkan Pasal 4 atau 5, yang membuat sulit untuk melacak aturan Negara Anggota yang melampaui Lampiran I Peraturan Penggunaan Ganda.

Dalam Buku Putihnya tentang Penggunaan Ganda, Komisi Uni Eropa mencatat bahwa kebuntuan multilateral baru-baru ini dan kecepatan kontrol baru yang diterapkan di luar rezim multilateral secara efektif mengesampingkan Uni Eropa, dan membuat koordinasi antar Negara Anggota menjadi bermasalah. Dalam Kertas Putihnya, Uni Eropa menguraikan beberapa cara untuk memperbaiki keadaan saat ini, dan Rekomendasi terbaru menyarankan Negara-negara Anggota untuk berkoordinasi dan berbagi informasi mengenai daftar kontrol nasional. Tindakan ini sejalan dengan upaya yang lebih luas yang dipimpin Uni Eropa dalam memfasilitasi inovasi komputasi kuantum dalam Undang-Undang Chipnya, yang menyerukan pengembangan rantai nilai chip kuantum yang terkoordinasi. Namun, saat ini, Uni Eropa masih belum memiliki peran formal dalam membatasi ekspor barang-barang yang berkaitan dengan komputer kuantum.

Negara Anggota Uni Eropa

Beberapa Negara Anggota Uni Eropa telah menerapkan kontrol ekspor komputasi kuantum dalam daftar kontrol nasional. Di antaranya adalah Belanda, Spanyol, Prancis, Italia, Jerman, dan Finlandia, bersama dengan negara Wilayah Ekonomi Eropa (EEA) Norwegia, beberapa di antaranya dibahas di bawah ini. Pada saat finalisasi bagian ini pada Agustus 2025, Kompilasi daftar kontrol nasional yang dikelola oleh Komisi Uni Eropa berdasarkan Pasal 9(4) Peraturan Penggunaan Ganda hanya merujuk pada kontrol tertentu yang diterapkan oleh Prancis dan Spanyol. Sebagian besar, kontrol tersebut dibuat dalam ketentuan yang hampir identik dengan Aturan Akhir Sementara AS yang dibahas di atas. Namun, mungkin karena perbedaan waktu penerapan aturan ini, dan tingkat perhatian Negara Anggota terhadap industri komputasi kuantum, tidak semua pembatasan ekspor AS diterapkan oleh semua Negara Anggota yang telah mengadopsi pembatasan pada teknologi komputasi kuantum. Sekali lagi, karena kerahasiaan di balik langkah-langkah ini, alasan di balik kesamaan dan perbedaan sulit untuk dipastikan. Tabel 6.2 mengilustrasikan langkah-langkah yang diterapkan oleh Spanyol, Prancis, Belanda, Italia, dan Jerman pada saat penulisan. Langkah-langkah ini

dibandingkan dengan ECCN yang setara dalam Daftar Kontrol AS. Seperti yang ditunjukkan dalam tabel, Belanda dan Italia pada dasarnya telah sepenuhnya mengadopsi kontrol yang sama dengan AS. Namun, Spanyol hanya mengadopsi ECCN 4A906 yang setara pada perangkat keras komputasi kuantum di atas 34 qubit dan komponen terkait.

Kesamaan kontrol antara Negara Anggota ini dan AS (di antara yang lain) menunjukkan tingkat kerja sama antara mitra internasional, kemungkinan “di sela-sela” diskusi Kesepakatan Wassenaar. Namun, tidak semua Negara Anggota Uni Eropa telah menerapkan pembatasan pada komputasi kuantum, dan mereka yang telah menerapkannya agak berbeda dalam pendekatannya. Selain itu, fakta bahwa hanya kontrol Spanyol dan Prancis yang spesifik untuk komputasi kuantum yang muncul dalam Kompilasi Daftar Kontrol yang dikelola oleh Komisi Uni Eropa menunjukkan masalah dengan koordinasi daftar kontrol nasional yang diatur dalam Peraturan Penggunaan Ganda untuk Komisi Uni Eropa. Masalah-masalah ini akan dihindari, atau setidaknya dikurangi, dalam pengaturan multilateral yang berfungsi suatu fakta yang dicatat oleh banyak pihak yang menyerukan "*Wassenaar Minus One*" atau setidaknya koordinasi yang lebih baik di antara Negara-negara Anggota Uni Eropa seperti yang dicatat oleh Komisi Uni Eropa.

Tabel 6.2 Barang-barang yang dibatasi ekspornya yang relevan dengan komputasi kuantum oleh beberapa Negara Anggota Uni Eropa

Nomor ECCN AS	Deskripsi	Spanyol	Prancis	Belanda	Italia	Jerman
3A901	Cryo-CMOS dan penguat sinyal		3A1901.a.15	3A901.a.15	3A901.a.15	3A1901a15
3A904	Sistem dan komponen pendingin kriogenik tertentu			3A904	3A904	3A1904
3B904	Peralatan pengujian wafer kriogenik			3B904	3B904	3B1904
3C907	Material epitaksial dengan komposisi tertentu			3C907	3C907	
3C908	Fluorida, hidrida, klorida Si/Ge dengan material tertentu			3C908	3C908	
3C909	Si, SiO_2, Ge, GeO_2 dengan dopan tertentu			3C909	3C909	
4A906	Komputer kuantum >34 qubit atau setara, dan komponen terkait	4A1901	4A1906	4A906	4A906	4A1906
4D906	Perangkat lunak untuk pengembangan/produksi barang 4A906.b atau .c		4D1901.b.3	4D901.b.3.	4D901.b.3	4D1901b3

4E906	Teknologi untuk pengembangan/produksi/ penggunaan barang yang dikendalikan		4E1901	4E901.b.3.	4E901.b.3	4E1901b3

Pemeriksaan Kontrol Khusus Komputasi Kuantum

Hingga saat ini, AS, beberapa Negara Anggota Uni Eropa, dan penandatangan Perjanjian Wassenaar lainnya seperti Australia dan Inggris telah menerapkan kontrol ekspor yang menargetkan dua dari sembilan kategori penggunaan ganda Komputer dan Elektronik. Kontrol ini mencakup kelima bagian teknis (A hingga E), meskipun diberlakukan di luar saluran Wassenaar formal. Penyertaan item dari setiap bagian menunjukkan niat regulasi yang luas untuk mencakup seluruh rantai pasokan komputasi kuantum. Di antara yurisdiksi yang diperiksa, satu-satunya tindakan umum adalah pembatasan perangkat keras komputasi kuantum tertentu, yang menunjukkan bahwa komputer kuantum itu sendiri dipandang sebagai perhatian paling kritis bagi regulator. Oleh karena itu, item ini (US ECCN 4A906) dipertimbangkan pertama kali di bagian ini, sebelum melanjutkan ke pemeriksaan item lain yang relevan dengan komputasi kuantum. Untuk menyederhanakan diskusi, pemeriksaan di bawah ini mengacu pada US ECCN kecuali dinyatakan lain.

Komputer Kuantum

Mengingat terdapat banyak paradigma komputasi kuantum yang berbeda dengan tingkat kinerja yang berbeda berdasarkan kualitas qubit, butir 4A906 mendefinisikan delapan kategori kinerja. Secara sederhana, komputer kuantum dengan kurang dari 34 qubit tidak dikontrol, dan semua komputer dengan lebih dari 2000 qubit dikontrol. Komputer antara 34 dan 1999 qubit dapat dicakup oleh aturan, tergantung pada jumlah qubit dan tingkat kesalahan gerbang *Controlled NOT* (C-Not) rata-rata komputer. Pendekatan ini mengikuti kebijaksanaan bahwa komputer kuantum dengan qubit fisik yang lebih besar tetapi tingkat kesalahan yang tinggi akan memiliki kinerja yang sebanding dengan mesin qubit yang lebih sedikit dengan tingkat kesalahan yang lebih rendah. Kategori yang berbeda tercermin dalam Tabel 6.3:

Tabel 6.3 Ambang batas rentang qubit dan tingkat kesalahan untuk penerapan kontrol ekspor pada komputer kuantum

Kategori	Rentang Qubit	Tingkat Kesalahan C-NOT
a.1	34–99	≤10−4
a.2	100–199	≤10−3
a.3	200–349	≤2 × 10−3
a.4	350–499	≤3 × 10−3
a.5	500–699	≤4 × 10−3
a.6	700–1099	≤5 × 10−3
a.7	1100–1999	≤6 × 10−3
a.8	2000+	Tidak Berlaku

Tidak jelas mengapa ambang batas kinerja spesifik ini telah ditetapkan oleh regulator. Namun, telah disarankan bahwa ambang batas 34-qubit mendekati tingkat di mana komputer kuantum tidak lagi dapat disimulasikan oleh komputer klasik. Dengan menetapkan ambang batas pada tingkat ini, regulator tampaknya menargetkan sistem yang melampaui batas kemampuan komputasi yang signifikan, sementara tetap memungkinkan pembelajaran akademis dan industri pada sistem yang kurang mampu untuk terus berlanjut tanpa batasan. Sebuah catatan oleh Biro Industri dan Keamanan AS (BIS) dalam Aturan Akhir Sementara menyatakan bahwa:

> BIS telah menentukan bahwa generasi komputer kuantum jangka pendek akan mendukung 34 atau lebih "qubit fisik" yang "sepenuhnya terkontrol", "terhubung", dan "berfungsi" pada tingkat kesalahan yang ditentukan, dan bahwa jumlah qubit dan tingkat kesalahan ini mewakili tingkat kecanggihan teknologi yang tinggi yang menjamin keamanan nasional, stabilitas regional, dan kontrol anti-terorisme.

Tabel 6.4 Jumlah qubit untuk beberapa komputer kuantum yang saat ini tersedia

Perusahaan	**Sistem**	**Qubit**
IBM	Osprey	433
IBM	Eagle	127
IBM	Heron	156
IBM	Condor	1121
Intel	Tunnel Falls	12
IonQ	Forte	36
Google	Sycamore	~53
Google	Willow	105
Microsoft	Majorana 1	8
Quantinuum	H2	56
QuEra	Aquila	256
Rigetti	Aspen-M3	80

Menemukan angka konkret dan akurat tentang tingkat kesalahan rata-rata komputer kuantum yang tersedia saat ini sulit, terutama mengingat kecenderungan perusahaan untuk memposisikan kemajuan mereka dalam komputasi kuantum dengan cara yang paling menguntungkan. Hal ini membuat penentuan apakah contoh-contoh komputer kuantum tertentu saat ini tunduk pada kontrol menjadi sulit. Memang, efek samping dari kontrol ekspor ini mungkin adalah untuk mencegah angka kinerja yang dilebih-lebihkan agar tidak terjerat oleh aturan baru. Tabel 6.4 mengilustrasikan jumlah Qubit dari sejumlah komputer kuantum yang diumumkan oleh beberapa perusahaan. Seperti yang ditunjukkan tabel, banyak dari item ini akan dibatasi oleh kontrol ekspor kecuali tingkat kesalahan C-NOT rata-rata berada di atas ambang batas yang relevan.

Dalam mengidentifikasi jumlah dan jenis qubit yang akan dihitung sesuai dengan aturan, item 4A906 hanya berlaku untuk qubit fisik yang sepenuhnya terkontrol, terhubung,

dan berfungsi. Keempat istilah ini diuraikan dalam Catatan Teknis yang menyertai item 4A906. Catatan Teknis menegaskan bahwa qubit fisik diperlakukan berbeda dari qubit logis, "karena qubit logis adalah qubit yang dikoreksi kesalahan yang terdiri dari banyak 'qubit fisik'."

Terakhir, dua Catatan lebih lanjut relevan dengan Butir 4A906.a. Catatan 1 menegaskan bahwa kontrol hanya berlaku untuk komputer kuantum berbasis gerbang dan berbasis pengukuran, bukan komputer kuantum adiabatik (atau annealing) yang terutama dirancang untuk memecahkan masalah optimasi daripada untuk komputasi kuantum universal. Catatan 2 menetapkan bahwa "qubit fisik" tidak boleh hadir secara permanen, dan aturan tersebut mencakup komputer dengan qubit yang dihasilkan selama operasi (misalnya, skema fotonik). Catatan-catatan ini juga muncul dalam padanan negara lain untuk ECCN 4A906 AS. Mereka mengungkapkan apresiasi terhadap nuansa yang harus diterapkan untuk menangkap teknologi yang ingin dibatasi oleh regulator namun juga mengisyaratkan potensi "kepatuhan kreatif" oleh perusahaan perangkat keras komputasi kuantum untuk menghindari pembatasan melalui paradigma komputasi kuantum yang mungkin lolos dari celah aturan.

Komponen, Perangkat Lunak, dan Teknologi Komputasi Kuantum

Bersamaan dengan pembatasan pada komputer kuantum tertentu di atas ambang batas 34-qubit, terdapat komponen individual dan perangkat lunak pendukung yang "dirancang khusus" untuk komputer kuantum yang dibatasi. Butir 4A906.b mencakup perangkat dan sirkuit qubit, yang masing-masing merupakan komponen fisik yang mengimplementasikan qubit (misalnya, sirkuit superkonduktor, ion terperangkap, sistem fotonik) dan sistem terintegrasi atau chip yang menampung banyak qubit dan memungkinkan interaksi antar qubit tersebut.

Butir 4A906.c membatasi komponen kontrol, yang mencakup elektronik dan sistem yang mengelola operasi qubit (misalnya, generator gelombang mikro dan modulator pulsa) dan perangkat pengukuran (misalnya, detektor foton tunggal). Hal ini, pada intinya, memastikan bahwa komponen fisik yang berbeda dari komputer kuantum yang mencapai ambang batas dalam butir 4A906.a tercakup, dan bukan hanya seluruh komputer kuantum. Pasal 4D906 juga membatasi perangkat lunak yang "dirancang khusus" atau dimodifikasi untuk pengembangan atau produksi perangkat qubit, sirkuit qubit, komponen kontrol kuantum, atau perangkat pengukuran kuantum yang dijelaskan dalam 4A906.b dan 4A906.c. Ini berarti bahwa pembatasan perangkat lunak tidak berlaku untuk perangkat lunak komputasi kuantum sebagai kategori luas (yaitu algoritma yang dirancang untuk komputer kuantum dengan ambang kinerja tertentu). Sebaliknya, kontrol tersebut difokuskan secara sempit pada perangkat lunak yang memungkinkan realisasi fisik perangkat keras kuantum. Secara praktis, ini termasuk perangkat lunak yang digunakan untuk merancang, membuat, mengkalibrasi, atau menguji infrastruktur fisik komputer kuantum seperti alat tata letak chip, generator sinyal kontrol, atau otomatisasi pengukuran. Perangkat lunak yang digunakan untuk mengembangkan algoritma kuantum, mensimulasikan sistem kuantum, atau menjalankan aplikasi pada prosesor kuantum tidak dibatasi berdasarkan 4D906, kecuali jika juga dirancang khusus untuk pengembangan atau produksi perangkat keras yang disebutkan di atas. Perbedaan ini memastikan bahwa

pengembangan perangkat lunak kuantum tujuan umum sebagian besar tetap tidak dibatasi di bawah kontrol tersebut.

Terakhir, pasal 4E906 bertujuan untuk mengendalikan "teknologi" yang berkaitan dengan pengembangan dan produksi komponen dan perangkat lunak komputasi kuantum yang disebutkan di atas, dan juga teknologi untuk penggunaan perangkat lunak yang dikendalikan dalam 4D906. Teknologi, sebagaimana didefinisikan dalam Perjanjian Wassenaar, mengacu pada "Informasi spesifik yang diperlukan untuk pengembangan, produksi, atau penggunaan suatu produk", yang berbentuk "Data teknis" dan "bantuan teknis". Ini termasuk pengetahuan teknis, metodologi desain, proses manufaktur, dokumentasi, dan bentuk pengetahuan tak berwujud lainnya yang memungkinkan pembuatan atau penerapan perangkat keras dan perangkat lunak kuantum yang terkendali. Dengan demikian, 4E906 berupaya untuk memastikan bahwa tidak hanya barang fisik dan perangkat lunak yang dikendalikan, tetapi juga keahlian mendasar yang dapat ditransfer untuk mereplikasi atau meningkatkan kemampuan tersebut di negara-negara yang dibatasi.

Peralatan Kriogenik

Banyak komputer kuantum harus beroperasi pada suhu yang sangat rendah (seringkali sedikit di atas nol absolut) untuk mempertahankan keadaan kuantum yang sensitif dari qubitnya. Hal ini berlaku untuk sistem yang berbasis pada qubit superkonduktor atau qubit spin, yang membutuhkan lingkungan kriogenik untuk meminimalkan kebisingan termal dan dekoherensi. Dalam konteks ini, 3A904 memberlakukan kontrol ekspor pada sistem dan komponen pendingin kriogenik yang mampu memberikan daya pendinginan sebesar 600 µW atau lebih pada suhu 0,1 Kelvin (−273,05 °C) atau di bawahnya selama lebih dari 48 jam. Peraturan Akhir Sementara AS menunjukkan bahwa sistem kriogenik dengan daya pendinginan terbesar umumnya diperlukan untuk komputer kuantum yang lebih canggih, dengan alasan ambang batas yang dipilih adalah "pada item yang relevan untuk pembelajaran pada sistem kuantum dengan jumlah qubit fisik yang lebih besar".

Sebagai pelengkap item ini, ECCN 3B904 memberlakukan kontrol ekspor pada peralatan pengujian wafer kriogenik tertentu yang digunakan untuk menguji dan mengkarakterisasi perangkat kuantum, seperti qubit solid-state, pada suhu kriogenik. Menurut Peraturan Akhir Sementara AS, alat-alat ini sangat penting untuk meningkatkan komputasi kuantum, karena memungkinkan pengujian perangkat qubit yang lebih cepat dan komprehensif dengan mengumpulkan data dalam jumlah besar dalam kondisi operasional. Dengan demikian, kontrol ini menargetkan kemajuan yang diantisipasi dalam pembelajaran dan alur kerja desain dari paradigma komputasi kuantum tertentu.

ECCN 3A901 memperkenalkan kontrol ekspor pada elektronik kriogenik yang, menurut Peraturan Akhir Sementara AS, sangat penting untuk pengembangan sistem kuantum canggih. Secara khusus, Peraturan tersebut mencatat bahwa "desain CMOS saat ini sedang dikembangkan yang cocok untuk beroperasi pada suhu sekitar 4K atau di bawahnya untuk keperluan komputasi kuantum", dengan batas suhu CMOS saat ini dilaporkan sekitar −40 C (233 K). Oleh karena itu, 3A901.a membatasi desain cryo-CMOS untuk beroperasi pada suhu sangat rendah ini. Dalam konteks yang sama, 3A901.b mencakup penguat sinyal yang

digunakan untuk membaca sinyal qubit lemah dengan noise sangat rendah pada suhu sangat rendah. Penambahan item-item ini mencerminkan pentingnya strategis yang diantisipasi dari elektronika kriogenik dalam memungkinkan komputasi kuantum yang terukur dan berkinerja tinggi.

Material Komputasi Kuantum

Kontrol ekspor yang diperkenalkan berdasarkan ECCN 3C907, 3C908, dan 3C909 serta padanannya di yurisdiksi lain dirancang untuk mengatur akses ke material yang diperkaya tertentu. Material ini, seperti yang dijelaskan dalam Aturan Akhir Sementara, dianggap penting untuk pengembangan komputer kuantum berbasis spin. Sistem kuantum berbasis spin menggunakan spin elektron atau inti, seringkali dalam atom silikon atau germanium, untuk merepresentasikan qubit. Karena isotop silikon dan germanium tertentu tidak memiliki spin nuklir, mereka menciptakan lingkungan kuantum yang jauh lebih tenang, mengurangi interferensi dan memungkinkan qubit untuk mempertahankan keadaannya untuk jangka waktu yang lebih lama. Hal ini menjadikan komputasi kuantum berbasis spin sebagai platform yang menjanjikan untuk membangun prosesor kuantum yang terukur dan berakurasi tinggi.

Pasal 3C907 mengontrol material berlapis yang terbuat dari silikon atau germanium yang mencakup persentase tinggi isotop tertentu. Item 3C908 berlaku untuk senyawa kimia tertentu dari silikon atau germanium yang juga mengandung isotop ini. Item 3C909 mencakup bentuk massal silikon, silikon dioksida, germanium, dan germanium dioksida dengan pengayaan isotop yang serupa. Bersama-sama, kontrol ini beroperasi lebih jauh ke hulu dalam tumpukan komputasi kuantum dengan membatasi akses ke material khusus yang membentuk dasar perangkat keras kuantum tertentu, sehingga berupaya membatasi kemampuan untuk mengembangkan sistem kuantum canggih bahkan sebelum sistem tersebut dapat dibangun.

Dampak Strategis dari Kontrol Komputasi Kuantum Plurilateral Saat Ini

Ringkasan Kontrol Saat Ini dan Pandangan yang Berlaku

Sejauh ini, bagian ini telah meneliti langkah-langkah yang muncul dari "kesepakatan ekspor kuantum misterius" antara AS dan beberapa sekutunya. Kemungkinan besar, ini hanya mewakili gelombang pertama kontrol yang ditargetkan pada teknologi komputasi kuantum, mengingat "perang chip" yang sedang berlangsung antara, antara lain, AS dan Tiongkok. Dari pemeriksaan ini, tiga poin utama dapat disimpulkan. Pertama, terdapat kekurangan harmonisasi yang jelas dibandingkan jika kontrol ini dilakukan melalui pendekatan multilateral tradisional di bawah Kesepakatan Wassenaar. Bukan berarti pendekatan tersebut akan memberikan solusi mujarab untuk kepatuhan yang seragam terhadap aturan. Seperti yang dikemukakan oleh Brunel dalam konteks regulasi semikonduktor, “pendekatan sukarela dari Kesepakatan Wassenaar jelas telah gagal”. Namun, kumpulan aturan yang ada saat ini menyebabkan ketidakpastian yang signifikan.

6.5 TANTANGAN DAN PELUANG PENGENDALIAN EKSPOR

Seperti yang telah diilustrasikan dalam bagian ini, pengendalian ekspor teknologi kuantum semakin menjadi pusat upaya nasional dan internasional untuk mengelola risiko keamanan dan ekonomi yang muncul. Terdiri dari subset yang sangat sensitif dan berkembang

pesat dari lanskap teknologi kuantum yang lebih luas, komputasi kuantum menimbulkan tantangan regulasi yang unik karena potensi penggunaan ganda yang luas dan kecepatan serta potensi terobosan teknologi yang tidak pasti. Kemampuan komputer kuantum untuk mengganggu sistem kriptografi yang ada, mempercepat penemuan material, atau mensimulasikan sistem biologis yang kompleks menimbulkan nilai strategis yang cukup besar dan dilema tata kelola yang mendalam. Namun, peluang dan tantangan penerapan pengendalian ekspor pada komputasi kuantum bukanlah sekadar subset dari perdebatan yang lebih luas tentang pengendalian ekspor teknologi yang muncul. Sebaliknya, seperti yang diilustrasikan bagian ini, masalah juga berasal dari karakteristik khas komputasi kuantum itu sendiri, seperti fondasi ilmiahnya, ketergantungan perangkat keras, dan ekosistem pembelajaran global.

Peluang

Meskipun kontrol ekspor terhadap teknologi komputasi kuantum menghadirkan tantangan regulasi yang signifikan, kontrol tersebut juga menawarkan peluang penting untuk membentuk perkembangan global bidang transformatif ini. Kontrol yang dirancang dengan cermat dapat mendorong inovasi yang bertanggung jawab dengan mendorong transparansi, praktik pembelajaran yang sadar akan keamanan, dan kolaborasi internasional pada norma-norma bersama. Kontrol tersebut juga dapat berfungsi sebagai katalis untuk dialog multilateral, membantu menyelaraskan strategi nasional dan menghindari fragmentasi regulasi. Selain itu, kontrol ekspor menyediakan mekanisme untuk mengantisipasi dan mengelola risiko di masa depan, memungkinkan para pembuat kebijakan untuk beradaptasi dengan kemajuan teknologi sambil mempromosikan kepercayaan dan stabilitas dalam ekosistem pembelajaran dan komersial kuantum global. Diskusi berikut berfokus pada faktor-faktor terpilih yang dianggap penting untuk mewujudkan peluang yang dapat ditawarkan oleh kontrol ekspor yang terkalibrasi dengan baik.

Waktu

Komputasi kuantum berada pada tahap pengembangan yang lebih awal daripada teknologi yang lebih matang seperti semikonduktor yang membentuk inti dari "perang chip" yang sedang berlangsung. Karena infrastruktur, rantai pasokan, dan kumpulan talenta untuk komputasi kuantum masih dalam tahap pembentukan, kontrol ekspor dapat membentuk ekosistem sejak dini. Berbeda dengan teknologi yang sudah matang, di mana kontrol seringkali kesulitan untuk mengimbangi penyebaran yang luas, kontrol tahap awal dalam komputasi kuantum berpotensi untuk menghalangi pesaing ekonomi sebelum teknologi dan keahlian menjadi umum. Hal ini tercermin dalam kontrol yang telah diterapkan, di mana teknologi komputasi kuantum canggih tertentu, atau teknologi dengan potensi tinggi yang dirasakan, dikenakan pembatasan. Secara khusus, item yang terkait dengan pengujian wafer kriogenik mencerminkan niat tidak hanya untuk membatasi produk jadi, tetapi juga item yang dapat digunakan untuk mengembangkan teknologi kuantum lebih lanjut.

Di sisi lain, tahap awal pengembangan berarti bahwa negara-negara yang dibatasi mungkin memiliki waktu, dan insentif, untuk berinvestasi besar-besaran dalam kemampuan kuantum domestik, yang berpotensi mempercepat program mereka sendiri. Kontrol ekspor,

meskipun membatasi akses ke sistem mutakhir, tidak diragukan lagi akan semakin mendorong indigenisasi teknologi kuantum di negara-negara yang memiliki kapasitas untuk melakukannya (seperti Tiongkok), yang dapat meningkatkan fokus pada pembangunan ekosistem komputasi kuantum mandiri yang mencakup perangkat keras, perangkat lunak, dan pengembangan talenta. Seperti yang dicatat oleh Nguyen, Tiongkok telah mengumumkan terobosan mereka sendiri dalam komputasi kuantum sejak diberlakukannya kontrol ekspor oleh AS.

Jejak Fisik Infrastruktur QC

Seperti yang dilaporkan di New York Times, "salah satu masalah dalam upaya mengendalikan aliran global semikonduktor adalah bahwa semikonduktor sangat kecil, ringan, dan berharga." Sebaliknya, banyak komputer kuantum adalah sistem besar dan berat yang membutuhkan infrastruktur khusus, termasuk lemari pendingin pengenceran, sistem kriogenik, isolasi getaran, dan perisai elektromagnetik. Mesin-mesin ini tidak hanya substansial secara fisik tetapi juga sangat sensitif terhadap kondisi lingkungan, sehingga sulit untuk diangkut, direplikasi, atau disembunyikan. Sifat fisik ini menawarkan keuntungan terhadap upaya pengendalian ekspor: sebagian besar perangkat keras yang dibutuhkan untuk membangun komputer kuantum canggih pada dasarnya kurang portabel dan lebih mudah dilacak daripada, misalnya, mikrochip. Kompleksitas dan visibilitas infrastruktur pendukung dengan demikian menciptakan titik hambatan alami untuk pemantauan dan regulasi.

Ukuran dan sifat khusus infrastruktur komputasi kuantum juga memungkinkan pendekatan regulasi yang sangat terarah. Karena sistem ini hanya dapat beroperasi di lingkungan dengan suhu ultra-stabil, perisai, dan rekayasa presisi, penggunaannya terbatas pada laboratorium khusus dan aktor institusional biasanya laboratorium nasional, universitas riset, dan pusat R&D industri utama. Sentralisasi kemampuan ini memudahkan pihak berwenang untuk menerapkan skema perizinan, inspeksi, dan kepatuhan yang berfokus pada sejumlah aktor yang dapat dikelola, sekaligus mengurangi risiko proliferasi ke pengguna atau yurisdiksi yang tidak diizinkan.

Yang penting, fase pengembangan kuantum yang sarat infrastruktur ini mendukung kontrol ekspor tingkat komponen yang dapat bersifat tepat sasaran dan strategis. Alih-alih membatasi sistem secara keseluruhan, regulator dapat fokus pada teknologi pendukung penting seperti unit pendingin kriogenik, peralatan pengujian skala wafer, atau elektronik cryo-CMOS yang penting untuk kinerja tetapi tidak banyak digunakan di luar kuantum. Karena barang-barang ini tidak dikomersialkan secara luas, pembatasannya menimbulkan gesekan tambahan minimal sambil memberikan dampak strategis maksimal. Dengan cara ini, infrastruktur fisik memungkinkan rezim kontrol ekspor yang lebih terperinci dan efektif yang disesuaikan dengan domain komputasi kuantum.

Selain itu, skala dan visibilitas instalasi kuantum memperkuat penegakan hukum melalui kemampuan pengamatan dan pencegahan. Tidak seperti teknologi skala kecil atau berbasis perangkat lunak yang mungkin beroperasi secara diam-diam, komputer kuantum sulit dibangun atau dioperasikan secara diam-diam. Jejak fisik dan ketergantungan lingkungannya membuat komputer kuantum lebih transparan bagi regulator dan dinas intelijen, memfasilitasi penilaian nasional terhadap kematangan teknologi dan kepatuhan. Visibilitas ini, pada

gilirannya, dapat bertindak sebagai alat sinyal strategis mencegah pengembangan yang merugikan dan memperkuat pengawasan kolektif di antara negara-negara sekutu.

Terakhir, lintasan yang dapat diprediksi menuju sistem kuantum yang berukuran kecil dan dapat diterapkan yang dimungkinkan oleh chip fotonik, elektronik kontrol terintegrasi, dan platform atom netral memberikan regulator kesempatan penting untuk tindakan antisipatif. Dengan mengidentifikasi dan mengunci teknologi pendukung utama di awal kurva pengembangan, kerangka kerja kontrol ekspor dapat berkembang mendahului kemajuan ini. Oleh karena itu, sifat komputasi kuantum yang intensif infrastruktur saat ini bukan hanya kendala tetapi juga aset strategis. Hal ini menawarkan baik lokus langsung untuk penegakan hukum maupun peluang prediktif untuk membentuk masa depan teknologi sebelum sistem menjadi modular, portabel, dan lebih sulit dikendalikan.

Akses Cloud dan API

Faktor lain yang meningkatkan kelayakan pembatasan ekspor dalam komputasi kuantum adalah meningkatnya ketergantungan pada model akses berbasis cloud. Tidak seperti perangkat keras komputasi tradisional, yang sering dijual dan dikirim ke pengguna akhir, banyak sistem kuantum tercanggih di dunia sekarang diakses dari jarak jauh, menyediakan titik kontrol yang dapat dimanfaatkan regulator untuk penegakan hukum. Komputasi kuantum berbasis cloud, dan akses jarak jauh melalui Antarmuka Pemrograman Aplikasi (API), menawarkan regulator keuntungan langka dalam lanskap kontrol ekspor: infrastruktur akses terpusat.

Tidak seperti ekspor tradisional, yang melibatkan pengiriman satu kali dan penegakan hukum setelah kejadian, layanan cloud kuantum menyediakan titik kontrol yang berkelanjutan di mana aktivitas pengguna dapat diatur, dipantau, dan jika perlu dicabut secara aktif. Akses dapat dibatasi secara geografis atau dibatasi berdasarkan lokasi pengguna, afiliasi, atau faktor lainnya. Untuk menghindari penghindaran kontrol ini melalui langkah-langkah teknis seperti *Virtual Private Network* (VPN), penyedia dapat menerapkan verifikasi identitas yang kuat, perjanjian kontraktual, pemantauan penggunaan, dan kontrol akses untuk memastikan bahwa pengguna di yurisdiksi yang dikenai sanksi atau entitas yang menjadi perhatian tidak diberikan akses. Model kontrol dinamis ini memungkinkan pembatasan akses secara real-time ke kemampuan, pembaruan, atau tingkatan kinerja tertentu, memberikan tingkat granularitas dan responsivitas yang sulit direplikasi dalam regulasi perdagangan fisik.

Selain itu, model cloud memfasilitasi bentuk baru kemitraan penegakan hukum publik-swasta. Penyedia cloud kuantum biasanya perusahaan teknologi besar yang diatur dengan baik berada pada posisi untuk menjadi aktor garis depan dalam memastikan kepatuhan terhadap persyaratan keamanan nasional. Pemerintah dapat terlibat dengan perusahaan-perusahaan ini melalui kerangka kerja perizinan, klausul kontrol ekspor, dan protokol audit kooperatif untuk memastikan penerapan pembatasan yang konsisten di berbagai yurisdiksi. Integrasi pengawasan regulasi ke dalam arsitektur platform ini memungkinkan model yang terukur dan adaptif untuk mengontrol akses ke kemampuan kuantum yang sensitif.

Terakhir, kemampuan untuk mengelompokkan atau membagi akses di cloud membuka peluang untuk diplomasi presisi dan penetapan norma. Regulator dan penyedia layanan dapat

membedakan antara pengguna akademis, pengembang komersial, dan entitas yang berafiliasi dengan negara, menyesuaikan kontrol akses sesuai dengan kebutuhan. Misalnya, akses dengan fungsi terbatas dapat diberikan kepada lembaga pembelajaran tepercaya, sementara fitur yang lebih canggih ditahan dari pesaing strategis. Fleksibilitas ini mendukung postur kontrol ekspor yang lebih terkalibrasi yang mendorong inovasi yang bertanggung jawab dan kolaborasi ilmiah di antara sekutu, sambil menolak kemampuan canggih kepada calon musuh. Seiring dengan kematangan komputasi kuantum, akses cloud tidak hanya akan berfungsi sebagai mekanisme penegakan teknis tetapi juga sebagai alat kebijakan strategis, menyelaraskan hak akses dengan tujuan diplomatik, ilmiah, dan keamanan yang lebih luas.

Tantangan

Meskipun terdapat peluang strategis yang ditawarkan oleh kontrol ekspor pada komputasi kuantum, implementasinya penuh dengan tantangan yang sudah lama ada dan yang baru muncul. Rezim kontrol ekspor secara historis kesulitan untuk mengikuti perkembangan teknologi yang pesat, dan komputasi kuantum memperparah banyak kesulitan ini. Perkembangan pesat bidang ini, ketidakjelasan ilmiah, dan potensi penggunaan ganda membuatnya sulit untuk mendefinisikan apa yang merupakan kemampuan yang dapat dikendalikan. Hal ini semakin diperumit oleh sifat terbuka dan kolaboratif dari pembelajaran kuantum, yang mempersulit upaya untuk memantau aliran pengetahuan tanpa menghambat inovasi. Selain itu, kontrol unilateral atau yang kurang terkoordinasi berisiko menciptakan fragmentasi regulasi, mendorong jalan pintas, atau merugikan industri domestik. Mencapai keseimbangan yang tepat antara keamanan dan keterbukaan ilmiah semakin diperumit oleh ketidakpastian tentang kecepatan dan arah terobosan kuantum, sehingga regulasi yang tepat waktu dan proporsional menjadi sangat sulit dicapai. Diskusi berikut ini membahas beberapa isu kunci yang menggambarkan hambatan khas yang dihadapi rezim kontrol ekspor di bidang komputasi kuantum. Selain itu, juga dibahas potensi keuntungan dari tantangan-tantangan ini, dan cara-cara untuk mengurangi kerugiannya.

Ekosistem Internasional

Salah satu tantangan paling signifikan terhadap kontrol ekspor yang efektif dalam komputasi kuantum adalah sifat internasional yang mendalam dari ekosistem pengetahuan dan rantai pasokan. Tidak seperti industri semikonduktor, di mana AS, Taiwan, Korea Selatan, dan Belanda mendominasi segmen-segmen kunci dari rantai nilai, inovasi kuantum tersebar luas di berbagai lembaga akademik, perusahaan rintisan, dan laboratorium nasional di puluhan negara, termasuk AS, Tiongkok, Kanada, Jerman, Inggris, Denmark, Prancis, dan Australia. Tidak ada satu negara atau perusahaan dominan pun yang mengendalikan seluruh tumpukan kuantum, mulai dari material dan fabrikasi hingga perangkat lunak dan algoritma. Ini berarti bahwa tidak ada satu negara pun yang dapat secara sepihak memberlakukan kontrol yang efektif tanpa mengisolasi diri dari komunitas kuantum global, sehingga menghambat inovasi lokal.

Isolasi ini dapat terwujud dalam berbagai cara. Misalnya, kontrol ekspor bahan baku bertujuan untuk membatasi saingan geopolitik agar tidak dapat mengakses input perangkat keras kunci tertentu untuk sistem kuantum canggih. Namun, China memiliki kapasitas yang

signifikan untuk beradaptasi dan menanggapi pembatasan-pembatasan ini. Seperti yang dicatat dalam siaran pers dari Parlemen Uni Eropa setelah resolusi tentang topik tersebut, "China memiliki monopoli semu atas ekspor bahan baku penting, unsur tanah jarang, dan magnet permanen." Mengingat kontrol ekspornya sendiri baru-baru ini sebagai balasan terhadap AS, China juga dapat menarik bahan baku dari AS dan sekutunya.

Selain itu, banyak perusahaan kuantum dan program pembelajaran Barat bergantung pada jalur bakat internasional, dengan para peneliti yang dilatih atau berkolaborasi lintas batas, terutama dari China. Kontrol ekspor komputasi kuantum baru-baru ini berlaku untuk "teknologi" (yaitu US ECCN 4E906), yang secara luas mencakup "[informasi spesifik yang diperlukan untuk pengembangan, produksi, atau penggunaan suatu produk]". Namun, mengingat pengecualian AS pada "ekspor yang dianggap" kepada warga negara asing, kontrol tersebut saat ini tidak berlaku untuk transfer pengetahuan yang difasilitasi oleh individu. Hal ini secara teoritis dapat diubah, dan ada mekanisme lain untuk membantu mengurangi transfer pengetahuan seperti pembatasan visa. Namun, pendekatan seperti itu berisiko mengecualikan keahlian internasional secara tidak proporsional, dan menghambat kolaborasi lintas batas yang sah yang mungkin terhambat oleh birokrasi yang berbelit-belit.

Fragmentasi dan Upaya Duplikat

Meskipun kontrol ekspor bertujuan untuk mencegah akses musuh terhadap teknologi kuantum yang sensitif, kontrol tersebut juga dapat menghambat kolaborasi antar sekutu, yang menyebabkan fragmentasi upaya pembelajaran dan investasi duplikat. Erosi multilateralisme baru-baru ini dan pergeseran ke rezim nasional atau plurilateral telah menyebabkan rezim kontrol yang berbeda. Hal ini dapat mendorong bahkan mitra dekat untuk mengejar jalur pengembangan kuantum paralel karena kehati-hatian atau kebutuhan strategis, yang merugikan kemajuan kolektif sekutu.

Fragmentasi ini dapat mengakibatkan infrastruktur yang berlebihan (misalnya, beberapa negara membangun platform perangkat keras kuantum yang serupa), alokasi bakat dan pendanaan yang tidak efisien, dan hambatan untuk kolaborasi lintas batas, bahkan di antara mitra tepercaya. Hasil seperti itu tidak hanya memperlambat kemajuan kolektif tetapi juga merusak tujuan keamanan yang seharusnya dilayani oleh kontrol ekspor. Ekosistem kuantum global dapat menjadi terisolasi, dengan interoperabilitas yang berkurang, lebih sedikit standar bersama, dan pertukaran ilmiah yang berkurang.

Masalah ini dapat dikurangi melalui kontrol multilateral yang lebih terkoordinasi, seperti strategi "*Wassenaar Minus One*" yang disebutkan di atas. Di tingkat regional, kontrol Uni Eropa yang terkoordinasi seperti yang disarankan oleh Komisi Uni Eropa yang melampaui perjanjian internasional seperti Perjanjian Wassenaar dapat mencegah pemilihan forum intra-Eropa. Namun, fragmentasi juga dapat dilihat sebagai fitur strategis daripada kelemahan, terutama mengingat tahap awal, tidak pasti, dan sensitif secara geopolitik dari pengembangan teknologi kuantum. Pendekatan nasional yang beragam dapat berfungsi sebagai eksperimen dalam desain regulasi, memungkinkan negara-negara untuk menguji kerangka kerja kontrol yang disesuaikan dengan basis industri, postur keamanan, dan kekuatan teknologi mereka. Selain itu, duplikasi kemampuan strategis di seluruh negara sekutu dapat memberikan

ketahanan rantai pasokan, mengurangi titik ketergantungan tunggal, dan meningkatkan pencegahan kolektif. Dalam lingkungan di mana konsensus lambat dan keselarasan geopolitik parsial, fragmentasi dapat memungkinkan fleksibilitas, pilihan, dan daya tanggap berpotensi menjadikannya batu loncatan pragmatis menuju koordinasi jangka panjang daripada hambatan langsung.

Pemilihan Forum, Arbitrase Regulasi, dan Kepatuhan Strategis

Komplikasi lebih lanjut dalam penegakan kontrol ekspor kuantum adalah risiko pemilihan forum. Rantai nilai kuantum yang tersebar secara internasional, perusahaan atau peneliti mencari yurisdiksi dengan pengawasan regulasi terlemah untuk mengakses teknologi yang dibatasi atau berkolaborasi lebih bebas, sehingga melemahkan tujuan kontrol. Sehubungan dengan itu, untuk semikonduktor, “beban kepatuhan sebagian besar akan jatuh pada perusahaan swasta”, yang secara ekonomi termotivasi untuk mematuhi peraturan seminimal mungkin. Kontrol ekspor berupaya menghilangkan pasar yang berpotensi menguntungkan dari pelaku korporasi. Keputusan yang rasional secara ekonomi mungkin adalah untuk pindah lokasi, mengabaikan pembatasan ekspor, atau menghindarinya (misalnya, dengan menjual kepada perantara dengan pembatasan yang kurang ketat, yang dapat menjual kembali ke negara-negara yang dibatasi).

Meskipun demikian, pendekatan nasional yang berbeda juga dapat memperkenalkan persaingan regulasi yang produktif yang memungkinkan eksperimen dan penyempurnaan kebijakan. Yurisdiksi dengan kontrol yang bijaksana dan terkalibrasi dengan baik dapat muncul sebagai simpul tepercaya dalam kerangka kerja internasional, menarik talenta dan investasi sambil mempertahankan keselarasan dengan tujuan keamanan yang lebih luas. Dalam pengertian ini, apa yang mungkin tampak sebagai "forum shopping" juga dapat mencerminkan bentuk pencarian keselarasan strategis, di mana perusahaan dan lembaga bermigrasi menuju lingkungan yang menyeimbangkan kekhawatiran keamanan nasional dengan keterbukaan ilmiah dan kejelasan hukum. Alih-alih mengikis kontrol, dinamika semacam itu jika diatur secara transparan dapat mendukung ekosistem kepatuhan adaptif dan merangsang inovasi dalam bagaimana rezim ekspor diimplementasikan dan ditingkatkan.

Paradigma Komputasi Kuantum Baru dan Laju Perkembangannya

Tantangan lebih lanjut bagi rezim kontrol ekspor adalah munculnya paradigma komputasi kuantum baru yang tidak sesuai dengan kerangka peraturan yang telah ditetapkan saat ini. Inti dari kontrol yang disebutkan di atas sebagian besar berfokus pada komputer kuantum berbasis gerbang, yang diukur berdasarkan jumlah qubit dan tingkat kesalahan, tetapi terdapat beragam arsitektur alternatif yang berkembang pesat. Sistem-sistem ini mungkin tidak menggunakan qubit tradisional atau gerbang CNOT, sehingga sulit untuk menerapkan ambang batas kinerja standar. Misalnya, komputer kuantum fotonik dapat mencapai daya komputasi tinggi tanpa pernah melampaui ambang batas jumlah qubit, sementara sistem atom netral dapat dikonfigurasi ulang secara dinamis, mengaburkan batas antara perangkat keras dan perangkat lunak dan membuat benchmarking menjadi sulit. Dapat dibayangkan bahwa platform komputasi kuantum di masa depan dapat lebih menantang definisi peraturan.

Keragaman ini menciptakan potensi titik buta regulasi, di mana sistem yang kuat mungkin berada di luar cakupan kontrol saat ini hanya karena mereka menggunakan metrik atau arsitektur baru. Selain itu, karena keunggulan kuantum dapat muncul dari terobosan algoritmik atau arsitektur, dan bukan hanya kinerja perangkat keras mentah, kontrol yang hanya didasarkan pada spesifikasi fisik dapat dengan cepat menjadi usang. Seperti yang dijelaskan di tempat lain dalam volume ini, regulator menghadapi dilema Collingridge, di mana intervensi awal dalam teknologi yang muncul sulit dilakukan karena pemahaman yang terbatas tentang dampak masa depannya, namun menunda regulasi hingga konsekuensinya jelas seringkali berarti teknologi tersebut telah terlalu mapan untuk dikendalikan secara efektif.

Ungkapan umum bahwa kecepatan pembuatan peraturan dilampaui oleh kecepatan inovasi benar adanya di ruang kuantum, yang sering ditandai dengan terobosan transformatif yang tiba-tiba. Perbandingan ini bahkan lebih jelas ketika mempertimbangkan kontrol multilateral, yang mungkin lebih diinginkan untuk meningkatkan harmonisasi dan koordinasi, namun biasanya lebih lambat daripada proses regulasi nasional karena kebutuhan untuk membangun konsensus di antara blok besar negara-negara dengan berbagai kepentingan strategis dan kemampuan teknologi. Dengan cara ini, kompleksitas teknologi dan dinamika geopolitik dapat, secara bersamaan, menghambat tata kelola yang tepat waktu dan efektif.

Kesulitan Mengendalikan Barang Tak Berwujud

Kontrol yang baru diperkenalkan pada komputasi kuantum berlaku untuk barang berwujud seperti bahan baku dan perangkat keras komputasi, serta barang tak berwujud seperti perangkat lunak dan "teknologi". Mengendalikan aliran elemen-elemen ini menghadirkan tantangan tersendiri. Tidak seperti barang fisik, perangkat lunak dan barang digital dapat ditransmisikan secara instan melintasi perbatasan melalui cara digital, seringkali tanpa meninggalkan jejak yang jelas. Kode sumber, file desain, dan dokumentasi teknis dapat dibagikan melalui saluran terenkripsi, platform cloud, atau bahkan komunikasi informal dalam lingkungan akademis atau profesional. Hal ini membuat penegakan hukum jauh lebih sulit, terutama ketika batas antara pembelajaran terbuka dan teknologi yang terkontrol menjadi kabur. “Perang Kripto” tahun 1990-an memberikan ilustrasi yang jelas tentang dinamika ini, di mana kontrol ekspor terhadap algoritma enkripsi yang kuat pada akhirnya gagal, karena pengetahuan dan perangkat lunak yang mendasarinya dapat menyebar melalui publikasi akademis, komunitas sumber terbuka, dan lembaga akademis dan komersial dari negara-negara dengan kontrol yang kurang ketat. Hal ini menghambat perkembangan akademis dan komersial di negara-negara yang mempertahankan kontrol yang lebih ketat (yaitu AS), yang menyebabkan pelonggaran kontrol tersebut pada akhirnya.

Komputasi kuantum menghadapi dilema serupa. Sifat global dan kolaboratif dari pembelajaran komputasi kuantum berarti bahwa sebagian besar pengetahuan yang relevan dikembangkan di lingkungan akademis terbuka, di mana norma transparansi dan berbagi informasi berlaku. Upaya untuk membatasi penyebaran barang-barang tidak berwujud berisiko bertentangan dengan norma-norma ini, berpotensi menghambat kolaborasi internasional atau memengaruhi kepatuhan oleh pihak yang diatur.

6.6 RISIKO DAN MANFAAT PENGENDALIAN EKSPOR KOMPUTASI KUANTUM

Tata kelola teknologi kuantum melalui kontrol ekspor menghadirkan tantangan kebijakan yang rumit dan semakin mendesak. Seperti yang dieksplorasi dalam buku ini, teknologi kuantum khususnya komputasi kuantum memiliki potensi transformatif yang sangat besar, tetapi juga menimbulkan kekhawatiran serius terkait keamanan nasional, kedaulatan digital, ekonomi, dan etika. Di tengah meningkatnya ketegangan dan persaingan geopolitik, kontrol ekspor telah muncul sebagai alat utama dalam mengelola risiko-risiko ini, yang bertujuan untuk mencegah proliferasi kemampuan sensitif. Namun, implementasinya juga mengungkap ketegangan dalam rezim regulasi yang ada, khususnya untuk yurisdiksi seperti AS, Uni Eropa, dan negara-negara anggotanya yang memiliki komitmen kuat terhadap inovasi, daya saing ekonomi, dan kolaborasi ilmiah internasional.

Pada saat yang sama, kontrol ekspor menawarkan peluang untuk membentuk pengembangan teknologi kuantum secara bertanggung jawab. Kontrol ekspor dapat berfungsi sebagai mekanisme untuk mempromosikan transparansi, mendorong adopsi awal praktik pembelajaran yang sadar keamanan, dan mendorong dialog internasional seputar norma dan nilai-nilai fundamental yang muncul. Jika dirancang dengan mempertimbangkan kemampuan adaptasi dan koordinasi global, kontrol ekspor dapat mencapai keseimbangan antara keamanan dan keterbukaan mengurangi risiko tanpa membatasi kemajuan secara berlebihan.

Salah satu wawasan utama dari bagian ini adalah bahwa komputasi kuantum menghadirkan serangkaian fitur struktural unik yang sangat cocok untuk kontrol ekspor yang ditargetkan. Skala, kompleksitas, dan ketergantungan infrastruktur dari perangkat keras kuantum saat ini menciptakan hambatan alami untuk penegakan hukum tidak seperti teknologi penggunaan ganda lainnya seperti semikonduktor atau model AI. Demikian pula, munculnya model akses berbasis cloud menawarkan platform yang persisten dan terpusat untuk kontrol waktu nyata, pembatasan geografis, dan akses yang berbeda. Fitur-fitur ini memberikan keuntungan langka dalam hal keterlacakan dan respons kebijakan, memungkinkan pendekatan yang lebih adaptif dan berlapis untuk mengatur akses ke teknologi yang baru muncul.

Dalam mempertimbangkan pergeseran dari rezim multilateral tradisional, bagian ini juga telah menguraikan logika strategis potensial di balik kerangka kerja plurilateral yang muncul. Meskipun fragmentasi dan pemilihan forum sering dipandang sebagai risiko, pendekatan nasional yang berbeda dapat mendukung eksperimen regulasi, membangun ketahanan rantai pasokan, dan menawarkan pilihan strategis dalam lanskap geopolitik yang dinamis. Alih-alih menandakan kekacauan, arsitektur yang muncul ini mungkin mencerminkan model yang lebih gesit dan sesuai tujuan terutama tanpa adanya konsensus di forum pengendalian ekspor tradisional.

Terakhir, langkah menuju pengendalian tidak hanya barang fisik tetapi juga teknologi pendukung, pengetahuan tak berwujud, dan kemampuan pra-komersial menunjukkan evolusi yang lebih luas dalam filosofi pengendalian ekspor. Negara-negara tidak lagi hanya bereaksi terhadap risiko proliferasi mereka mulai membentuk lingkungan pembelajaran global secara proaktif. Sikap antisipatif ini, jika diimbangi dengan transparansi dan proses yang semestinya,

dapat memainkan peran sentral dalam mengarahkan inovasi kuantum ke arah yang aman, kolaboratif, dan berkelanjutan secara strategis.

BAB 7
QIT DAN HUKUM INTERNASIONAL: DIMENSI STRATEGIS-GEOPOLITIK

Penggunaan teknologi komputasi oleh Negara untuk tujuan ofensif dan defensif telah menjadi ciri utama hubungan internasional kontemporer. Teknologi informasi kuantum (QIT) diharapkan dapat memengaruhi dinamika ini dengan mentransformasikan kemampuan Negara dalam keamanan siber, enkripsi, dan pemeriksaan informasi. Bagian ini mengkaji bagaimana penggunaan strategis QIT oleh Negara beririsan dengan prinsip dan aturan hukum internasional publik. Pemeriksaan ini menempatkan QIT dalam yurisprudensi kedaulatan, yurisdiksi, dan penggunaan kekuatan, dengan mengacu pada Manual Tallinn dan sumber-sumber hukum internasional terkait. Bagian ini juga mengeksplorasi bagaimana teori permainan dapat menjelaskan pola kerja sama dan persaingan kuantum antar Negara baik dalam masa damai maupun konflik.

7.1 QIT DAN HUKUM INTERNASIONAL: KERANGKA PENERAPAN DOKTRIN

Pembelajaran dan pengembangan dalam teknologi informasi kuantum (QIT) termasuk komputasi kuantum, komunikasi kuantum, dan penginderaan kuantum semakin didorong oleh potensi nilai strategisnya bagi Negara. Teknologi ini bukan hanya inovasi ilmiah tetapi juga alat pengaruh dan persaingan prospektif dalam urusan internasional. Seiring dengan perkembangan dan kematangan kemampuan kuantum, dampak potensialnya terhadap hukum internasional publik, khususnya yang berkaitan dengan tata kelola operasi siber, kedaulatan, dan penggunaan kekuatan, perlu diperiksa.

Selama beberapa dekade terakhir, kajian hukum internasional dan praktik negara telah berkembang untuk membahas regulasi aktivitas dunia maya. Pertanyaan-pertanyaan sentral meliputi bagaimana norma hukum yang ada mengatur perilaku negara dalam operasi siber, apa yang merupakan intervensi atau penggunaan kekuatan yang melanggar hukum, dan bagaimana tanggung jawab harus dikaitkan dalam lingkungan teknologi yang kompleks. Munculnya QIT menghadirkan dimensi baru bagi diskusi ini. Oleh karena itu, isu yang dibahas dalam bagian ini bukanlah apakah QIT harus diatur berdasarkan hukum internasional, tetapi bagaimana doktrin yang ada berlaku ketika teknologi yang mendasarinya bersifat kuantum.

Pertanyaan ini tepat waktu. Kedaulatan negara semakin bergantung pada infrastruktur informasi dan digital yang mendukung pemerintahan, pertahanan, dan aktivitas ekonomi. Infrastruktur yang sama juga mewakili potensi kerentanan, karena negara-negara yang bermusuhan dapat menargetkan atau mengeksploitasinya untuk keuntungan strategis. Perkembangan dalam kecerdasan buatan dan sistem siber telah menantang kategori hukum yang ada. Munculnya QIT menambah kompleksitas lebih lanjut: karakteristik non-klasiknya, seperti superposisi dan keterikatan, dapat memungkinkan mode tindakan baru yang secara operasional atau konseptual berbeda dari yang dimungkinkan oleh komputasi klasik. Fitur-fitur ini dapat mengubah cara Negara memperoleh, melindungi, dan memperdebatkan informasi,

dan dengan demikian menimbulkan pertanyaan tentang yurisdiksi, atribusi, dan kontrol di bawah hukum internasional.

Bagian ini mengkaji sejauh mana perkembangan teknologi ini memerlukan instrumen hukum baru atau dapat diakomodasi dalam kerangka kerja yang ada. Bagian ini berangkat dari premis bahwa hukum internasional sudah berlaku untuk aktivitas Negara yang melibatkan QIT, sama seperti halnya untuk bentuk operasi siber lainnya. Namun, penerjemahan prinsip-prinsip yang sudah dikenal seperti uji tuntas, kedaulatan, dan larangan penggunaan kekerasan ke dalam domain kuantum membutuhkan kehati-hatian interpretatif. Mengintegrasikan penalaran kuantum dan hukum membutuhkan perhatian pada bagaimana fenomena spesifik kuantum diterjemahkan menjadi kapasitas yang berbeda untuk tindakan Negara, seperti dekripsi, simulasi, atau kemampuan penginderaan tingkat lanjut yang dapat memberikan asimetri informasi di antara Negara-negara.

7.2 DAMPAK GEOPOLITIK TEKNOLOGI KUANTUM

Gambaran Umum

Kemampuan QIT yang semakin berkembang, terutama kemajuan menuju perangkat komputasi kuantum yang toleran terhadap kesalahan dan berpotensi memfasilitasi dekripsi informasi yang dienkripsi secara klasik, telah memotivasi peningkatan pertimbangan dampak QIT terhadap keamanan nasional, infrastruktur nasional, keunggulan kompetitif ekonomi, dan ekosistem informasi di dalam dan antar Negara. Pada bagian ini, kami meninjau dampak utama QIT yang berkaitan dengan karakteristik utama hukum internasional publik dan hukum konflik. Seperti yang akan kita bahas, keamanan nasional merupakan ciri khas integral dari prinsip yurisprudensi kedaulatan Negara yang menjadi inti hukum internasional publik. Untuk mempelajari dampak geopolitik QIT, kami memetakan perilaku Negara ke klasifikasinya dalam hal komputasi kuantum, komunikasi kuantum, dan penginderaan kuantum. Kemudian dalam artikel ini, kami mempertimbangkan tiga skenario strategis yang melibatkan Negara dan pengaruhnya terhadap perilaku strategis.

Dampak Strategis Komputasi Kuantum

Komputasi kuantum memiliki potensi aplikasi yang luas dalam konteks strategis. Dampak kemampuan komputasi kuantum berasal dari aspek unik komputasi kuantum itu sendiri, seperti simulasi sistem fisik, termasuk sistem kimia dan biologi, sintesis material, dan material komposit yang lebih efisien, dengan cara yang secara teknis tidak mungkin dilakukan pada komputer klasik untuk kelas masalah tertentu. Namun, mungkin aplikasi utama komputer kuantum dalam konteks permusuhan negara terletak pada kemampuannya untuk memecahkan masalah simulasi, optimasi, dan dekripsi yang kompleks. Potensi penggunaan algoritma kuantum untuk memecahkan masalah optimasi, pencarian, dan dekripsi dengan cepat dengan cara yang tidak mungkin dilakukan pada komputer klasik merupakan inti dari dampak strategisnya. Yang perlu diperhatikan secara khusus adalah kemampuan untuk, pada prinsipnya, memecahkan kelas masalah yang sulit dipecahkan (membutuhkan sumber daya komputasi eksponensial untuk dipecahkan) di luar jangkauan komputasi klasik. Kami akan membahas beberapa di antaranya di bawah ini.

Kriptografi

Teknik algoritma kuantum (seperti yang berbasis pada transformasi Fourier kuantum dan algoritma Shor) untuk mendekripsi sistem kriptografi kunci publik yang ada, seperti RSA, Diffie-Hellman, dan Kriptografi Kurva Elips, mewakili apa yang umumnya dianggap sebagai aplikasi utama komputasi kuantum dalam skenario strategis yang saling bertentangan antar Negara, baik di masa damai maupun selama konflik. Kemampuan kriptografi kuantum (jika terwujud) juga diantisipasi akan sangat penting bagi badan intelijen Negara, memungkinkan dekripsi komunikasi yang dicegat dari pihak lawan dan kemampuan untuk menguji ketahanan rezim enkripsi kriptografi Negara (atau sekutunya) terhadap serangan pihak lawan. Karena enkripsi sangat penting bagi fungsi Negara modern, manfaat strategis dari kapasitas dekripsi yang moderat sekalipun dianggap signifikan secara strategis. Dari segi pertahanan, protokol kriptografi pasca-kuantum yang bertujuan untuk mengamankan sistem informasi dan komunikasi dari serangan musuh kuantum telah menjadi fokus utama upaya pembelajaran di antara negara-negara.

Simulasi

Sistem kuantum pada prinsipnya dapat digunakan untuk mensimulasikan sistem klasik tertentu secara lebih efisien dan lebih cepat daripada komputer klasik (dan untuk menggabungkan informasi yang lebih rinci), yang relevan dengan, misalnya, pemodelan skenario, yang merupakan inti dari perencanaan militer. Komputer kuantum pada prinsipnya juga mampu mensimulasikan sistem kuantum lain secara lebih efisien, suatu proses yang penting untuk memahami material dan kimia yang kompleks. Simulasi semacam itu di masa depan dapat memungkinkan simulasi dan perancangan baju besi, bahan peledak, dan sistem energi yang lebih baik atau memodelkan penggunaan, misalnya, agen biologis oleh aktor Negara (atau non-Negara), sehingga memungkinkan kesiapan yang lebih baik terhadap bioterorisme atau perang kimia. Misalnya, simulasi interaksi molekuler dapat membantu merancang penawar atau bahan pelindung terhadap senjata kimia.

Optimasi dan Pembelajaran Mesin

Algoritma kuantum menawarkan potensi untuk memecahkan masalah optimasi kompleks tertentu, seperti logistik dan alokasi sumber daya, manajemen rantai pasokan, dan perencanaan misi (skenario pra-konflik, dan selama konflik, untuk sistem komando dan kendali), yang sangat penting dalam operasi militer. Aplikasi umum lainnya mencakup pengambilan keputusan yang lebih baik atau lebih cepat, analitik prediktif, atau prosedur verifikasi, meskipun sejauh mana sistem kuantum memberikan keuntungan praktis masih belum diketahui secara umum. Perluasan metode tersebut adalah penggunaan algoritma kuantum (seringkali bersamaan dengan algoritma klasik) untuk pembelajaran mesin kuantum. Contoh aplikasi prospektif yang sedang diteliti meliputi algoritma yang ditingkatkan kuantum (hibrida) untuk klasifikasi data yang cepat, seperti misalnya citra satelit, atau pemrosesan kumpulan data skala besar dengan lebih cepat.

Seperti yang kami catat di bawah ini, sistem komputasi kuantum secara inheren tertanam dalam arsitektur komputasi klasik. Secara praktis, ini berarti bahwa infrastruktur komputasi kuantum Negara kemungkinan besar berbasis cloud dan didistribusikan di seluruh

jaringan komunikasi kuantum di mana bangunan komputer kuantum tetap dihubungkan melalui saluran komunikasi klasik. Lebih lanjut, seperti yang dicatat dalam diskusi kami tentang hukum internasional yang mengatur penerapan QIT, operasi siber strategis dan aktivitas terkait QIT antar Negara, seperti halnya dengan rekan-rekan klasiknya, akan terjadi baik dalam skenario damai maupun konflik.

Komunikasi Kuantum, Jaringan Kuantum, dan Dampak Strategis Kriptografi Kuantum

Komunikasi kuantum, jaringan kuantum, dan kriptografi kuantum (yang secara khusus kita bahas dalam konteks komunikasi di sini) memiliki dampak strategis yang signifikan bagi negara. Dari perspektif strategis, komunikasi kuantum memberikan peluang dan tantangan bagi aktor negara. Negara-negara dengan kemampuan komunikasi kuantum yang canggih dapat mengamankan infrastruktur penting, komunikasi militer, dan sistem keuangan terhadap ancaman siber kuantum dan klasik. Pada saat yang sama, komunikasi kuantum mengintensifkan persaingan geopolitik karena negara-negara bersaing untuk mengembangkan teknologi kuantum yang unggul, termasuk kripto pemeriksaan kuantum untuk mendekripsi komunikasi musuh. Komunikasi kuantum menggabungkan QKD, protokol berbasis keterikatan, jaringan kuantum, dan QRNG untuk menawarkan keamanan dan fungsionalitas. Ini adalah landasan dari internet kuantum yang sedang berkembang dan memiliki dampak transformatif untuk komunikasi yang aman, komputasi terdistribusi, dan dinamika strategis internasional. Meskipun demikian, implementasinya menimbulkan tantangan teknologi dan geopolitik yang signifikan.

Kriptografi Pasca-Kuantum

Kriptografi pasca-kuantum telah menjadi fokus utama upaya pembelajaran oleh negara-negara yang berupaya mengamankan jaringan mereka terhadap potensi gangguan, intersepsi, dan spionase dari pihak lawan. Hal ini terwujud dalam program PQC jangka panjang NIST di Amerika Serikat yang mengarah pada rezim standardisasi PQC. PQC merupakan prioritas utama bagi negara-negara yang mampu menggunakan teknologi kuantum karena potensi keamanan informasi yang ditawarkannya terhadap pihak lawan yang menggunakan QIT, seperti untuk spionase atau selama konflik.

Jaringan Kuantum

Salah satu potensi menarik dari teknologi jaringan kuantum adalah mengatasi keterbatasan (termasuk atenuasi) dan risiko intervensi pada serat optik terestrial melalui penggunaan metode komunikasi kuantum berbasis satelit. Contohnya termasuk satelit sains eksperimental kuantum Tiongkok, Micius, yang memungkinkan distribusi QKD dan keterikatan berbasis satelit.

Distribusi Kunci Kuantum (QKD)

QKD adalah protokol komunikasi yang aman secara prospektif yang memungkinkan dua pihak untuk menghasilkan dan berbagi kunci kriptografi rahasia dengan jaminan bahwa setiap upaya penyadapan akan terdeteksi. QKD menawarkan prospek komunikasi ultra-aman dengan memanfaatkan mekanika kuantum untuk mendeteksi penyadapan. Negara-negara mungkin dapat menggunakan QKD untuk infrastruktur komunikasi kritis, seperti saluran diplomatik, militer, dan intelijen negara, memastikan kerahasiaan dan integritas dalam operasi sensitif.

Internet Kuantum dan Infrastruktur Strategis

Jaringan komunikasi kuantum, termasuk sistem berbasis satelit komunikasi kuantum, mewakili bentuk penting prospektif penggunaan QIT di masa damai dan konflik. Jaringan tersebut memiliki kemampuan penggunaan ganda tertentu, terutama dalam menghubungkan sistem pertahanan nasional dan industri kritis secara aman dan prospektif dalam skenario konflik.

Penginderaan Kuantum

Sejumlah kasus penggunaan prospektif penginderaan kuantum memiliki potensi dampak strategis.

Deteksi Kapal Selam

Deteksi kapal selam dapat memiliki konsekuensi signifikan bagi hubungan strategis antar negara nuklir karena dampaknya terhadap kemampuan serangan balasan suatu negara jika terjadi konflik bersenjata nuklir. Metode deteksi kapal selam yang ada saat ini bergantung pada deteksi anomali magnetik, yang mengukur gangguan pada medan magnet Bumi yang disebabkan oleh zat logam di dalam lambung kapal selam. Penerapan prospektif sensor kuantum terletak pada potensinya untuk meningkatkan sensitivitas terhadap gangguan ini, sehingga memungkinkan deteksi pada jarak yang lebih jauh. Namun, dengan kondisi teknologi terkini, terdapat tantangan teknis signifikan yang menghambat penggunaan sensor kuantum untuk deteksi kapal selam. Tantangan tersebut meliputi kebisingan laut (di mana gangguan magnetik dari sumber seperti arus laut dan endapan mineral, mengganggu tanda magnetik kapal selam), persyaratan kedekatan (semua sensor, termasuk sensor kuantum, bekerja lebih baik di dekat kapal selam), jangkauan terbatas (magnetometer kuantum seperti yang menggunakan magnetometer pusat nitrogen-vakum memiliki jangkauan operasional terbatas), variabilitas target (di mana kapal selam dapat memvariasikan tanda magnetiknya melalui metode seperti degaussing) dan pergerakan kapal selam itu sendiri. Pemeriksaan empiris teknologi penginderaan kuantum saat ini (dan teknologi baru seperti gravimetri kuantum dan radar apertur sintetis) menunjukkan bahwa pelacakan kapal selam dalam waktu dekat tidak mungkin terjadi.

Pelacakan Rudal

Sensor kuantum juga memiliki potensi aplikasi pelacakan rudal melalui peningkatan akurasi sistem navigasi inersia yang digunakan dalam rudal balistik. Navigasi inersia bergantung pada akselerometer dan giroskop untuk melacak gerakan suatu objek tanpa referensi eksternal. Sensor kuantum dapat meningkatkan presisi instrumen tersebut dan dengan demikian memungkinkan penargetan yang lebih halus. Teknologi ini juga dapat memberikan keuntungan secara prinsip dengan mengurangi kesalahan penyelarasan awal, mengurangi penyimpangan giroskopik karena sumber kebisingan lain (seperti panas atau energi kinetik), meskipun hal ini memerlukan penanggulangan tantangan teknis tertentu untuk memastikan ketahanannya.

Jaringan Sensor Kuantum

Jaringan sensor kuantum juga dapat dihubungkan untuk menciptakan arsitektur komunikasi kuantum yang sangat sensitif. Jaringan sensor dan komunikasi kuantum

memanfaatkan karakteristik fisik teknologi sensor kuantum dan protokol komunikasi kuantum untuk menciptakan jaringan sensor kuantum terdistribusi di seluruh jarak geospasial yang lebih luas sambil mempertahankan manfaat fitur keamanan komunikasi kuantum. Sistem kuantum yang digunakan sebagai sensor kuantum terikat dengan sistem kuantum lain dalam jaringan jarak jauh. Contoh protokol kandidat yang dieksplorasi secara teoritis adalah mengintegrasikan penginderaan dan komunikasi kuantum melalui entanglement.

Sejumlah protokol yang mengeksplorasi jaringan sensor kuantum telah muncul baru-baru ini, termasuk protokol QISAC yang memanfaatkan keadaan Bell untuk penginderaan dan komunikasi kuantum simultan. Dalam hal ini, Alice menyiapkan dan mengirimkan pasangan foton terikat ke Bob melalui saluran kuantum. Kedua pihak melakukan pengukuran acak pada subset partikel untuk mengkonfirmasi keamanan saluran dengan partikel yang tersisa dikodekan dengan informasi dan digunakan dalam operasi penginderaan oleh Alice (seperti untuk estimasi parameter). Bob mengukur keadaan yang diterima, mendekode pesan, dan mengambil statistik pengukuran yang dimaksud. Proposal lain mencakup keterikatan multipartit berbasis rongga, sistem penginderaan kuantum terdistribusi menggunakan keadaan atomik yang diperas spin yang memanfaatkan keterikatan non-lokal untuk efek penskalaan yang lebih baik.

Tantangannya meliputi masalah desain dan rekayasa teknis, terutama pada tahap NISQ, tetapi juga secara lebih luas fakta bahwa keterikatan kuantum berkurang setelah setiap penggunaan (atau pengukuran) jaringan kuantum itu sendiri. Dalam istilah ilmu informasi kuantum, keterikatan kuantum adalah sumber daya (artinya itu adalah sumber daya yang diperlukan untuk jenis komputasi atau informasi tertentu yang tidak mungkin diperoleh dengan cara lain dan bahwa itu berkurang setelah digunakan).

7.3 FAKTOR TEKNIS YANG MEMPENGARUHI QIT STRATEGIS

Taksonomi Strategis Klasik dan Kuantum

Pada bagian ini, kita akan secara singkat membahas sejumlah faktor teknis terkait penggunaan QIT strategis. Seperti halnya perbandingan antara pemrosesan informasi kuantum dan klasik itu sendiri (seperti yang umum dalam ilmu informasi ketika menggambarkan saluran klasik dan kuantum), perilaku strategis Negara yang terkait dengan QIT dapat diklasifikasikan secara taksonomi dalam hal hubungan kuantum dan klasik:

Klasik-ke-Klasik

Meliputi penggunaan pemrosesan informasi klasik sehubungan dengan teknologi informasi klasik (misalnya, serangan siber konvensional).

Klasik-ke-Kuantum

Meliputi penggunaan pemrosesan informasi klasik untuk bertindak dalam kaitannya dengan QIT.

Kuantum-ke-Klasik

Meliputi penggunaan sumber daya kuantum dan QIT untuk bertindak atas informasi klasik (atau sistem pemrosesan informasi), seperti yang dicontohkan misalnya oleh algoritma kuantum untuk mendekripsi informasi yang dienkripsi secara klasik.

Kuantum-ke-Kuantum

Melibatkan penggunaan langsung proses spesifik kuantum pada sumber daya kuantum. Taksonomi ini merupakan cara yang berguna untuk menempatkan hubungan antara teknologi kuantum dan klasik dalam konteks perilaku strategis. Terdapat juga kompleksitas tambahan dari sistem hibrida yang memanfaatkan baik teknologi klasik maupun kuantum (QIT akan selalu terintegrasi dalam infrastruktur sistem informasi klasik). Kami mencatat hal ini dan merangkum taksonomi ini dalam Tabel 7.1 di bawah ini. Kami menggunakan taksonomi ini dalam pemodelan skenario perilaku strategis Negara dan pemeriksaan kami tentang dampaknya di bawah hukum internasional publik di bawah ini.

Tabel 7.1 Perbandingan tindakan pemrosesan informasi klasik, hibrida, dan kuantum musuh negara yang diterapkan pada infrastruktur klasik, hibrida, dan kuantum. Serangan klasik-ke-klasik mewakili tindakan musuh klasik terhadap infrastruktur klasik.

Pemrosesan Informasi	Infrastruktur		
	Infrastruktur Klasik	Infrastruktur Hibrida	Infrastruktur Kuantum
Pemrosesan Klasik	Serangan siber yang disponsori negara yang menargetkan sistem klasik (misalnya, meretas basis data pemerintah, mengganggu jaringan listrik).	Penggunaan metode klasik untuk menyusup ke sistem hibrida (misalnya, mengeksploitasi kelemahan dalam skema kriptografi hibrida).	Spionase terhadap fasilitas pembelajaran kuantum menggunakan teknik pengawasan dan pemeriksaan klasik.
Pemrosesan Hibrida	Serangan berbasis kuantum pada sistem klasik (misalnya, menggunakan optimasi yang terinspirasi kuantum untuk mengidentifikasi kerentanan dalam infrastruktur).	Operasi berbasis negara yang menggabungkan metode klasik dan kuantum untuk membobol jaringan hibrida (misalnya, mencegat komunikasi klasik-kuantum).	Manipulasi komponen kuantum dalam sistem hibrida untuk mengganggu atau menonaktifkan fungsinya.
Pemrosesan Kuantum	Serangan kriptografi kuantum pada saluran komunikasi klasik (misalnya, memecahkan enkripsi klasik menggunakan komputasi kuantum).	Interferensi berbasis kuantum dalam sistem hibrida (misalnya, menggunakan simulasi kuantum untuk mengganggu jaringan hibrida).	Musuh negara yang secara langsung menyerang jaringan atau sistem kuantum (misalnya, mengganggu keterikatan kuantum atau mencegat komunikasi kuantum).

Sistem Kuantum Tertanam Secara Klasik

Fakta penting dari QIT dari perspektif tata kelola dan strategis adalah bahwa semua QIT harus tertanam dalam arsitektur pemrosesan informasi klasik. Karakteristik kuantum ontologis dari sistem informasi kuantum (misalnya, keadaan kuantum dalam superposisi atau keadaan kuantum terikat) tidak dapat diamati secara langsung. Sebaliknya, representasi mereka direkonstruksi melalui hasil statistik pengukuran klasik yang muncul dari pengukuran berulang pada salinan sistem kuantum yang identik. Statistik pengukuran ini pada gilirannya digunakan untuk merekonstruksi, misalnya, keadaan kuantum melalui tomografi keadaan atau proses. Sifat non-klasik yang melekat pada sistem kuantum direpresentasikan secara klasik melalui paradigma non-deterministik seperti probabilitas. Dalam bahasa informasi kuantum, pengukuran adalah saluran kuantum-ke-klasik. Cara sistem kuantum dikendalikan juga berbasis klasik: kontrol kuantum, seperti kontrol yang diperlukan agar komputer kuantum melakukan komputasi kuantum, pada akhirnya bergantung pada penerjemahan instruksi dan informasi dari sistem klasik (sistem pengendali atau saluran masukan manusia) ke sistem kuantum.

Ini adalah poin penting yang perlu diingat. Dalam serangan siber, seperti penetrasi infrastruktur siber negara musuh, proses komputasi aktual yang mendasari penetrasi tersebut dalam jaringan klasik musuh akan bersifat klasik. Bukan berarti, misalnya, algoritma kuantum dapat diterapkan pada jaringan klasik musuh (untuk mendapatkan keuntungan kuantum yang ditawarkan oleh algoritma tersebut misalnya). Bagi musuh negara dengan komputer kuantum, pada prinsipnya dimungkinkan untuk, misalnya, meretas infrastruktur klasik di sekitar perangkat kuantum untuk menyematkan salinan algoritma tertentu dengan cara, misalnya, mengganggu deskripsi klasik dari protokol kompilasi kuantum, tetapi potensi ini pada gilirannya bergantung pada mediasi informasi antara sistem klasik dan kuantum.

Serangan Kuantum-ke-Kuantum Langsung Sulit tetapi Mungkin

Pada prinsipnya, tentu saja dimungkinkan bagi dua sistem kuantum untuk berinteraksi dengan cara yang 'langsung kuantum' karena kedekatan sistem tersebut menyebabkan mereka terhubung dengan cara spesifik kuantum, seperti melalui keterikatan. Namun, operasi siber 'kuantum-ke-kuantum' murni yang direkayasa akan sangat menantang, jika bukan tidak mungkin, untuk dilakukan pada tingkat teknologi saat ini. Hal ini karena interaksi langsung antara sistem kuantum dua Negara tanpa mediasi klasik membutuhkan jaringan komputer kuantum tersebut yang secara fisik berarti menghubungkan seluruh atau sebagian sistem tersebut satu sama lain. Meskipun komputer kuantum seperti halnya komputer klasik selalu terhubung dengan lingkungannya sampai batas tertentu, tantangan teknis untuk menghubungkan tersebut dalam konteks permusuhan sangat besar. Dengan demikian, prospek perangkat QIT seluler yang digunakan oleh musuh Negara untuk kegiatan spionase di dalam Negara saingan sangat kecil jika bukan tidak mungkin karena kondisi mendasar yang diperlukan agar sistem kuantum tetap kuat, terkendali, dan stabil.

Pengecualian untuk skenario ini, yang akan kita bahas lebih lanjut di bawah, adalah ketika sistem kuantum dua Negara saling terikat. Mungkin tampak tidak masuk akal bahwa dua aktor Negara akan dengan sukarela mengentangle sumber daya QIT mereka meskipun mereka

adalah musuh, tetapi banyak contoh musuh yang berbagi sumber daya selama skenario kompetitif dan bahkan konflik yang ada sepanjang sejarah. Dalam kasus kuantum, contoh utamanya adalah berbagi QIT melalui jaringan kuantum. Seperti yang dibahas di atas, jaringan komputasi kuantum dapat secara signifikan memengaruhi daya dan kemampuan komputasi. Keseluruhan internet kuantum secara harfiah lebih besar daripada jumlah bagian-bagiannya. Hal ini dapat dilihat secara sederhana dari fakta bahwa jumlah keadaan komputasi (dan dimensi ruang Hilbert) dari sistem n qubit adalah 2^n. Dengan demikian, seiring bertambahnya jumlah qubit n, dimensi ruang Hilbert meningkat secara eksponensial. Di masa damai, Negara-negara akan termotivasi untuk menghubungkan perangkat kuantum mereka untuk memanfaatkan keuntungan komputasi dari koordinasi kooperatif sumber daya bersama tersebut. Negara-negara mungkin kemudian menjadi musuh tetapi juga dapat memutuskan untuk berbagi sumber daya selama konflik.

Prospek berbagi sumber daya QIT, seperti sistem kuantum yang terikat, bukanlah hal yang sepenuhnya tidak mungkin. Dalam skenario ini, pada prinsipnya kita memiliki sesuatu yang menyerupai cara kuantum 'langsung' di mana setiap Negara memengaruhi Negara lain melalui tindakan kuantum yang memengaruhi sistem kuantum yang saling terikat. Perlu dicatat bahwa mengendalikan serangan semacam itu (misalnya, di mana satu Negara memutuskan untuk berinteraksi dengan jaringan kuantum untuk mengganggunya) dalam kebanyakan kasus akan membutuhkan masukan klasik (yaitu, masukan klasik ke dalam rezim kontrol). Interferensi kuantum-ke-kuantum semacam itu pada prinsipnya dapat berupa interferensi dengan data kuantum dan proses QIT itu sendiri, seperti bagaimana komputasi berlangsung atau bagaimana komunikasi kuantum melalui jaringan terjadi.

Serangan Siber Klasik-ke-Kuantum dapat Mengganggu QIT dan Infrastruktur Kuantum

Meskipun prospek aktor Negara mengganggu musuh Negara lain melalui interaksi kuantum-ke-kuantum langsung mungkin tampak jauh, perilaku permusuhan klasik-ke-kuantum oleh Negara dimungkinkan. Perilaku tersebut dibentuk oleh penggunaan pemrosesan informasi klasik, seperti strategi serangan siber klasik konvensional, yang diarahkan ke infrastruktur kuantum musuh Negara. Karena setiap infrastruktur QIT pasti tertanam dalam sistem informasi klasik yaitu sistem yang mengirimkan informasi dari sistem kuantum (misalnya melalui perekaman dan penyimpanan hasil pengukuran) dan ke dalam sistem (melalui sinyal kontrol klasik, atau protokol yang dijelaskan secara klasik untuk distilasi atau persiapan keadaan) saluran klasik tersebut dapat dimanfaatkan untuk aktivitas permusuhan.

Sebagian Besar Aktivitas Kuantum yang Bersifat Adversarial Akan Terbatas Secara Lokal

Konsekuensi dari hal tersebut di atas adalah bahwa, setidaknya berdasarkan perkiraan saat ini dan jangka pendek, setiap penggunaan QIT untuk tindakan adversarial Negara kemungkinan besar akan terbatas pada perangkat QIT yang sebagian besar tidak bergerak, atau perangkat QIT yang mobilitasnya terbatas (seperti yang terintegrasi ke dalam platform seluler lainnya). Kasus penggunaan ofensif yang paling masuk akal berkaitan dengan kriptografi kuantum dan penginderaan kuantum di mana misalnya jaringan komputer kuantum

yang tidak bergerak digunakan untuk mendekripsi komunikasi klasik yang dicegat, atau jaringan sensor kuantum stasioner digunakan untuk mendeteksi aktivitas musuh Negara.

Pengecualiannya, sekali lagi, adalah di mana tindakan adversarial melibatkan sistem kuantum terikat yang secara geografis jauh, tetapi yang dapat ditindaklanjuti secara non-lokal oleh interaksi suatu Negara dengan sistem kuantum terikatnya sendiri. Skenario seperti itu tentu akan melibatkan prinsip non-lokalitas, tetapi tindakan aktual suatu Negara (misalnya, yang mungkin berupaya mengganggu jaringan kuantum bersama dengan cara tersebut) tetap mengharuskan mereka untuk bertindak secara lokal pada sistem kuantum lokal mereka sendiri.

Hal ini karena substrat fisik, seperti qubit dari sistem yang terikat, pada dasarnya bersifat lokal. Meskipun mereka menunjukkan tingkat non-lokalitas, konsentrasi probabilitas (ukuran) dalam hampir semua kasus realistis akan berada dalam batas spasial yang sangat sempit (sebagian karena sistem tersebut perlu dilokalisasi untuk diwujudkan dan dikendalikan sejak awal). Unsur kontrol tetap, dalam pengertian ini, bersifat lokal. Tabel 7.2 menyajikan beberapa contoh spekulatif tentang bagaimana pemrosesan informasi klasik dan aktivitas siber oleh suatu Negara dapat secara antagonis menargetkan dan bertindak melawan infrastruktur kuantum Negara lain.

Tabel 7.2 Taksonomi tindakan permusuhan klasik-ke-kuantum oleh Negara termasuk contoh bagaimana pemrosesan informasi klasik dapat digunakan untuk mengganggu atau mencampuri infrastruktur kuantum Negara lain

Jenis Aktivitas Adversarial	**Contoh**
Gangguan Sistem Kontrol Klasik	Mengganggu perangkat keras atau perangkat lunak klasik yang bertanggung jawab untuk mengendalikan sistem kuantum, seperti memodifikasi urutan pulsa atau mengganggu generator sinyal yang digunakan dalam implementasi gerbang kuantum.
Peretasan Infrastruktur Klasik yang Mendukung Sistem Kuantum	Menargetkan sistem klasik yang mendukung komputer kuantum, seperti pusat data, server kontrol, atau jaringan yang mengirimkan instruksi klasik ke sistem kuantum.
Manipulasi Instruksi Klasik	Mengubah instruksi klasik yang digunakan untuk menginisialisasi atau mengoperasikan sistem kuantum, seperti merusak parameter inisialisasi qubit atau urutan gerbang dalam program kuantum.
Interferensi Klasik dengan Algoritma Kuantum	Menyisipkan deskripsi klasik yang berbahaya dari algoritma kuantum atau Hamiltonian ke dalam sistem kuantum sebelum kompilasi kuantum, menyebabkan sistem kuantum berperilaku tidak benar.
Serangan Siber pada Node Jaringan Kuantum	Melancarkan serangan siber klasik pada node jaringan kuantum untuk mengganggu pembangkitan keterikatan atau transmisi keadaan kuantum.

Pencegatan Komunikasi Klasik dalam Protokol Kuantum	Mencegat atau mengganggu saluran komunikasi klasik yang digunakan dalam distribusi kunci kuantum atau protokol koreksi kesalahan.
Gangguan Fisik Sistem Kuantum	Menggunakan alat klasik untuk mengganggu lingkungan sistem kuantum secara fisik, seperti menimbulkan interferensi elektromagnetik atau memodifikasi kontrol suhu.
Malware Klasik dalam Sistem Kuantum	Menyisipkan malware klasik ke dalam antarmuka klasik-kuantum, seperti merusak pembaruan firmware untuk perangkat kuantum atau menyuntikkan kode berbahaya ke dalam simulator klasik sistem kuantum.
Gangguan Proses Kompilasi Kuantum	Menargetkan kompiler klasik yang menerjemahkan algoritma kuantum tingkat tinggi menjadi instruksi yang dapat dieksekusi untuk perangkat keras kuantum tertentu, menyebabkan kesalahan pada sirkuit kuantum yang dihasilkan.
Serangan Klasik pada Jaringan Sensor Kuantum	Menggunakan metode komputasi klasik atau pengacauan sinyal untuk mengganggu pengoperasian sensor kuantum, seperti radar kuantum atau magnetometer, dengan mengganggu lapisan pemrosesan data klasiknya.

QIT Dapat Meningkatkan Strategi Serangan Siber

Seperti yang disebutkan di atas, salah satu motivasi utama penggunaan komputasi kuantum adalah keberadaan algoritma tertentu yang pada prinsipnya memungkinkan dekripsi komunikasi dan data yang dienkripsi secara klasik. Algoritma yang paling terkenal adalah algoritma Shor, algoritma kuantum berdasarkan kelas transformasi Fourier kuantum yang pada prinsipnya menyediakan cara untuk mendekripsi informasi yang dikodekan menggunakan protokol enkripsi klasik seperti RSA secara klasik (paling lama dalam waktu polinomial). Meskipun praktik dekripsi menggunakan komputer kuantum yang menjalankan algoritma tersebut kompleks dan tunduk pada batasan, dampak potensial inilah yang menjadi fokus utama, bahkan sangat penting, bagi Negara-negara, yang memotivasi sebagian besar pendanaan yang mendorong pembelajaran ke dalam komputasi kuantum dan QIT. Kerahasiaan informasi dan enkripsi memiliki sejarah yang kaya di seluruh konflik dan interaksi antar Negara. Contoh terkenal keterlibatan Turing dalam dekripsi perangkat enkripsi Enigma Reich Ketiga adalah contoh praktis yang relevan.

Semua aparat keamanan nasional modern bergantung pada protokol enkripsi modern untuk komunikasi dan integritas data mereka. Keamanan informasi juga sangat penting untuk imperatif strategis mendasar seperti sikap nuklir dan doktrin yang membentuk dan mendefinisikan geopolitik negara modern. Sebagai analogi dengan teknologi nuklir dan teknologi penggunaan ganda lainnya, fakta penggunaan ganda teknologi tersebut membentuk pendekatan tata kelola terhadapnya. Dalam praktiknya, penggunaan QIT, seperti perangkat komputasi kuantum untuk mengeksekusi varian algoritma Shor untuk memecahkan kode klasik, mewakili pendekatan hibrida yang akan memanfaatkan teknik penyadapan dan spionase klasik-ke-klasik untuk mengumpulkan data (kami mengesampingkan penggunaan

penginderaan kuantum untuk tujuan ini) dan kemudian teknik pemrosesan informasi kuantum untuk mendekripsi dan mengembalikan informasi yang telah didekripsi ke register klasik.

Dekripsi Kuantum Tidak Memberikan Kemahatahuan

Kita akan membahas lebih detail aspek teknis dari kemungkinan penggunaan sistem informasi kuantum untuk dekripsi di bagian-bagian berikut. Namun, penting untuk memperhatikan kendala praktis pada QIT yang digunakan dalam serangan siber, misalnya dalam kripto pemeriksaan, pengumpulan data (penyadapan) serangan penipuan. QIT bukanlah semacam oracle mahatahu. Dengan demikian, bahkan penerapan algoritma Shor pada data yang dikumpulkan dan disimpan akan membutuhkan waktu yang cukup lama di setiap kemungkinan. Kontrol dan batasan klasik akan terus berlaku. Meskipun demikian, penggunaan dan kombinasi QIT dalam aktivitas ofensif siber yang terkait dengan dekripsi merupakan konsekuensi signifikan dari teknologi yang membentuk respons pemerintah dan institusional terhadap teknologi kuantum.

Dekripsi Kuantum dan Infrastruktur Klasik

Penggunaan ofensif QIT juga dapat diklasifikasikan dengan cara yang meminjam dari riset keamanan siber klasik. Serangan siber ofensif berbasis kuantum terhadap sistem informasi klasik mengeksploitasi kelemahan sistem tersebut untuk memungkinkan dan memperkuat dampaknya. Mereka juga harus terlibat dengan sistem dan infrastruktur klasik. Contohnya meliputi:

Pengumpulan Data

Di mana data klasik disimpan terlebih dahulu hingga kripto pemeriksaan kuantum dimungkinkan.

Pemrosesan Data

Di mana informasi yang dikumpulkan dalam serangan saluran samping dapat dicari lebih efisien (misalnya, menggunakan algoritma gaya Grover yang disebutkan di atas), atau di mana pencarian lintasan melalui jaringan kompleks dapat dioptimalkan pada komputer kuantum.

Simulasi Kuantum

Di mana data dikumpulkan dengan cara yang memungkinkan, misalnya, pemodelan skenario oleh Negara untuk merencanakan strategi serangan siber yang efektif.

Keterikatan

Di mana keterikatan dapat memungkinkan koordinasi yang tidak dapat dilacak di antara musuh yang bekerja sama. Serangan berbasis kripto pemeriksaan yang mengandalkan pemeriksaan data yang dikumpulkan atau disimpan dalam register mencakup komponen klasik. Metode berbasis kuantum, seperti penerapan algoritma Shor dan protokol kuantum dekripsi terkait juga melibatkan aktivitas klasik. Dengan demikian, serangan simpan-sekarang, dekripsi-nanti (SNDL) dapat melibatkan intersepsi klasik dari komunikasi yang dikodekan secara klasik untuk dekripsi selanjutnya. Kripto pemeriksaan juga dapat mengganggu distribusi kunci klasik, seperti protokol pertukaran Diffie-Hellman, memungkinkan intersepsi atau peniruan identitas.

Penginderaan Kuantum

Penginderaan kuantum juga memiliki aplikasi dalam aktivitas siber yang bersifat antagonis dan defensif. Kami menguraikan beberapa contoh di bawah ini:

Serangan Saluran Samping yang Ditingkatkan

Sensitivitas sensor kuantum terhadap spektrum elektromagnetik dan gangguan emisi akustik dapat memungkinkan pengumpulan data yang lebih rinci atau beresolusi lebih tinggi sebagai bagian dari strategi serangan siber yang lebih luas.

Deteksi Serangan

Perangkat penginderaan kuantum mungkin dapat mendeteksi penggunaan perangkat intersepsi itu sendiri (misalnya, di mana sinyal daya rendah atau gangguan yang menunjukkan teknologi intersepsi atau yang setara dengan penyadapan telepon digunakan oleh musuh). Proposal lain yang lebih bersifat spekulatif mencakup peningkatan penginderaan kuantum yang digunakan dalam sistem radar.

7.4 PENGARUH QIT TERHADAP PERILAKU STRATEGIS

Dilema dan Keseimbangan

Fitur unik teknologi informasi kuantum memiliki dampak terhadap bagaimana Negara-negara yang menggunakan teknologi tersebut berperilaku strategis dalam menanggapi satu sama lain dengan cara yang pada prinsipnya berbeda dari perilaku strategis klasik. Kita dapat menilai hal ini melalui studi skenario yang melibatkan sumber daya kuantum (seperti sumber daya komunikasi kuantum) sambil mempertimbangkan bagaimana Negara-negara dapat bertindak secara kooperatif atau non-kooperatif selama masa damai atau konflik.

Dampak strategis teknologi kuantum dimodelkan secara teoritis oleh teori permainan kuantum yang mewakili subset pembelajaran tentang strategi kuantum yang mempertimbangkan efek diferensial dari pengambilan keputusan yang melibatkan pemrosesan informasi kuantum. Karena permainan dan perilaku multi-agen, termasuk Negara, dapat dilihat dalam hal sistem terdistribusi (dan bahkan dimodelkan sebagian menggunakan algoritma terdistribusi), teori permainan kuantum memiliki hubungan khusus dengan arsitektur sirkuit dan kerangka kerja sistem kuantum terdistribusi. Dampak dan hasil dari teori permainan kuantum meliputi hal-hal berikut.

Keseimbangan yang Berbeda

Variasi kuantum dari permainan klasik memungkinkan pemain untuk berbagi keadaan kuantum yang terikat, sehingga menghasilkan strategi keseimbangan di mana kedua pemain dapat mencapai imbalan yang lebih tinggi daripada dalam konteks keseimbangan Nash klasik, seperti dalam versi kuantum dari dilema Tahanan yang memungkinkan hasil kerja sama. Hasil strategis ini tidak mungkin terjadi secara klasik.

Dilema Ketat

Yang disebut 'dilema ketat' di mana insentif dan agensi rasional pemain dapat menyebabkan hasil suboptimal dan non-Pareto, dalam kasus tertentu dapat digantikan jika sumber daya kuantum tersedia (sekali lagi, dilema Tahanan adalah kasus kanonik). Secara intuitif, ketersediaan sumber daya kuantum mengubah strategi kerja sama dan pembelotan

klasik. Secara klasik, kerja sama biasanya bergantung pada (i) mekanisme penegakan eksternal seperti perjanjian, pengawasan pihak ketiga, atau pertimbangan reputasi untuk memotivasi perilaku Negara atau (ii) interaksi berulang antar Negara untuk membangun kepercayaan atau (iii) sumber daya atau kepentingan bersama yang berisiko jika kerja sama tidak dilakukan. Ketersediaan sumber daya kuantum menyediakan mekanisme penegakan diri yang efektif. Hal ini karena dua alasan. Pertama, keterikatan bersama memotivasi perilaku jujur untuk mengurangi kemungkinan suatu Negara secara diam-diam mengubah strateginya atau menipu dalam komunikasi karena teorema tanpa kloning dan kendala pengukuran.

Dengan demikian, komunikasi Negara dapat dikodekan menggunakan metode keterikatan atau dienkripsi dengan cara yang dapat mendeteksi perubahan strategi dan pengambilan keputusan (misalnya, keputusan untuk membelot atau tidak), memotivasi Negara untuk bertindak jujur karena keputusan mereka dapat dideteksi atau diverifikasi (gagasan utamanya adalah bahwa mewajibkan komunikasi Negara melalui saluran kuantum karena hanya komunikasi melalui saluran tersebut yang valid misalnya dalam konteks dilema tahanan akan menimbulkan dinamika yang berbeda dari kasus klasik). Kedua, protokol kuantum dapat memverifikasi keacakan dan oleh karena itu perilaku strategis yang bergantung pada keacakan, seperti di mana distribusi hasil bergantung pada prosedur yang disepakati yang melibatkan pengambilan sampel acak, menyediakan sarana untuk menegakkan hasil yang disepakati melalui protokol kriptografi.

Asumsi di Balik Keterikatan

Protokol berbasis keterikatan memerlukan tingkat kerja sama tertentu dan bergantung pada sejumlah asumsi, termasuk:

Kerja Sama dalam Penggunaan Sumber Daya Kuantum

Negara-negara harus pada suatu tahap telah sepakat untuk berbagi sumber daya kuantum (keterikatan yang tidak disengaja tidak mungkin terjadi), misalnya melalui jaringan komunikasi kuantum (walaupun negara-negara tersebut mungkin kemudian menjadi bermusuhan) agar keadaan kuantum yang terikat dapat diakses oleh keduanya.

Kemampuan Teknis

Negara-negara harus memiliki sumber daya dan keahlian teknis untuk memanfaatkan sumber daya kuantum (kita akan membahas ini di bawah dalam konteks payung komputasi strategis di mana negara-negara tertentu memiliki akses ke sumber daya komputasi AI atau kuantum dan negara-negara lain tidak, yang memengaruhi pilihan strategis mereka).

Rasionalitas

Negara-negara diasumsikan rasional atau sebagian besar rasional untuk menyadari manfaat kerja sama dibandingkan pembelotan.

Perilaku Ekonomi

Sumber konten lain yang lebih spekulatif untuk perilaku strategis ekonomi Negara adalah perilaku ekonomi kuantum antar Negara. Ini termasuk analog kuantum dari perilaku ekonomi klasik, seperti kontrak, teori prinsipal-agen, pertukaran komoditas dan desain pasar, bersama dengan prinsip-prinsip asimetri informasi. Negara-negara yang terlibat dalam perilaku kooperatif dan kompetitif di masa damai sering melakukannya melalui saluran

ekonomi dan ketersediaan sumber daya kuantum yang digunakan untuk melakukan aktivitas ekonomi sehingga memunculkan bentuk-bentuk perilaku strategis yang baru. Kami mempertimbangkan aktivitas perilaku strategis Negara sehubungan dengan QIT secara lebih rinci di bawah ini.

7.5 SKENARIO GEOPOLITIK

Gambaran Umum

Pemeriksaan teknis QIT menimbulkan pertanyaan tentang skenario praktis dan terapan di mana QIT akan memunculkan perilaku strategis Negara. Apakah penggunaan QIT memunculkan efek geopolitik unik yang berbeda dari teknologi komputasi dan informasi lainnya? Dan konsekuensi apa yang mungkin ditimbulkan oleh efek ini terhadap hukum internasional? Untuk mempertimbangkan bagaimana prospek teknis penggunaan QIT memiliki konsekuensi dalam kerangka hukum internasional yang dibahas di bagian sebelumnya, kita mempertimbangkan perilaku strategis di sepanjang dimensi yang berbeda.

Pertama, apakah Negara berada dalam masa damai (didefinisikan sebagai tidak adanya konflik bersenjata antar Negara) atau dalam konflik (didefinisikan sebagai adanya konflik antar Negara, yang mungkin bersifat biner antara Negara atau antara aliansi). Untuk setiap skenario tersebut, kita mempertimbangkan apakah Negara bertindak secara kooperatif (seperti mitra dagang di masa damai atau sekutu dalam konflik) atau secara antagonis (seperti pesaing ekonomi di masa damai atau musuh dalam perang). Dengan menggunakan taksonomi ini, pemodelan skenario kemudian dapat mempertimbangkan bagaimana berbagai kelas penggunaan QIT dapat diterapkan.

Untuk memberikan ilustrasi untuk jenis kegiatan, kami menyajikan beberapa contoh prospektif dalam Tabel 7.3. Ini termasuk: (i) masalah optimasi, seperti kegiatan logistik atau perencanaan strategis; (ii) simulasi kuantum, untuk penemuan material atau simulasi strategis; (iii) kripto pemeriksaan, termasuk kerja sama kriptografi pasca-kuantum atau dekripsi antagonis; (iv) pembelajaran mesin dan AI yang ditingkatkan menggunakan QIT; (v) pencarian dan penambangan data menggunakan QIT (misalnya algoritma berbasis Grover); (vi) komputasi awan kuantum untuk memungkinkan antarmuka yang lebih luas antar Negara ke QIT terdistribusi; (vii) kriptografi pasca-kuantum untuk memperkuat keamanan informasi Negara. Kami menggunakan taksonomi ini di bagian selanjutnya untuk mengembangkan skenario yang digunakan dalam pemeriksaan kami tentang dampak hukum internasional publik dari penggunaan QIT strategis lebih lanjut.

Tabel 7.3 Penggunaan strategis QIT, menyoroti penggunaan teknologi kuantum di masa damai dan konflik, dibagi menjadi konteks kerja sama dan permusuhan

Kategori	**Teknologi Kuantum dalam Hubungan Internasional**			
	Masa Damai		**Konflik**	
	Kerja Sama	**Bersifat antagonis**	**Kooperatif**	**Bermusuhan**

Masalah Optimasi	Kolaborasi dalam optimalisasi logistik untuk bantuan bencana atau pengembangan infrastruktur bersama.	Memantau kemajuan antagonis dalam optimasi logistik atau strategi perdagangan kompetitif.	Optimalisasi bersama logistik dan perencanaan untuk operasi militer sekutu.	Mengganggu perencanaan militer musuh atau mencampuri rantai pasokan atau memprediksi perilaku strategis musuh.
Simulasi Kuantum	Pembelajaran bersama tentang produk kimia kuantum, farmasi.	Mensimulasikan pasar kompetitif atau negosiasi.	Pengembangan material canggih dan strategi pertahanan.	Memanfaatkan simulasi untuk mendapatkan keuntungan di medan perang.
Kripto pemeriksaan	Pengembangan kolaboratif kriptografi pasca-kuantum.	Mencegat komunikasi terenkripsi pihak lawan untuk intelijen pasar.	Pengujian sistem komunikasi aman di antara sekutu.	Mendekripsi jaringan komunikasi musuh selama konflik.
Pembelajaran Mesin dan AI	Infrastruktur AI sipil bersama yang ditingkatkan secara kuantum untuk kepentingan publik (misalnya, kota pintar).	Memantau aktivitas AI pihak lawan untuk potensi aplikasi militer.	Penggunaan komputasi kuantum dengan AI untuk intelijen medan perang dan pengambilan keputusan.	Menggunakan QIT dengan AI untuk sistem militer otonom dan peperangan siber.
Pencarian	Penambangan data kuantum untuk tujuan kemanusiaan global.	Penambangan data komunikasi pesaing pasar.	Penginderaan kuantum untuk melacak dan mencari pergerakan pasukan musuh.	Pencarian sistem yang digunakan untuk membantu serangan siber terhadap musuh.
Komputasi Awan Kuantum	Komputasi awan kuantum bersama untuk pembelajaran global kolaboratif.	Jaringan sensor kuantum untuk deteksi.	Jaringan kuantum yang aman untuk koordinasi militer antar sekutu.	Memungkinkan penggunaan QIT secara terdistribusi selama konflik.

Kriptografi Pasca-Kuantum	Kolaborasi global untuk membangun standar kriptografi yang tangguh.	Mengembangkan tindakan penanggulangan terhadap kemajuan kriptografi yang merugikan.	Mengimplementasikan komunikasi tahan kuantum di antara sekutu.	Mengeksploitasi kerentanan dalam sistem kriptografi musuh.

Pemodelan Skenario Strategis

Untuk mempelajari dampak penggunaan QIT (dan dampaknya berdasarkan hukum internasional) dalam strategi negara, kami mempertimbangkan skenario sederhana perilaku strategis negara yang terkait dengan QIT. Skenario yang kami gunakan dirancang untuk secara sengaja menyoroti penerapan prinsip-prinsip hukum internasional publik terhadap aktivitas siber yang terutama diuraikan dalam manual Tallinn 2.0 tentang Hukum Internasional yang berlaku untuk Operasi Siber (Manual). Setiap skenario dibangun untuk berfokus pada aspek unik atau *sui generis* dari QIT yang berkaitan dengan perilaku negara, berkonsentrasi pada kemampuan unik yang dimungkinkan oleh QIT yang tidak dapat dilakukan oleh metode klasik. Fokus pekerjaan kami ini terutama pada perilaku yang saling bertentangan selama masa damai dan konflik, tetapi kami mencatat sejumlah kerangka kerja peraturan internasional yang juga berlaku untuk perilaku kooperatif di masa damai dan selama konflik. Untuk setiap skenario, kami mempertimbangkan perilaku negara yang saling bertentangan: di masa damai, kami menganggap perilaku yang saling bertentangan sebagai kompetitif; sedangkan dalam situasi konflik, kami menganggap perilaku tersebut sebagai ofensif. Hal ini dapat diuraikan sebagai berikut:

Masa Damai/Kooperatif

Di mana setiap Negara berupaya mengkoordinasikan penggunaan sumber daya kuantum mereka untuk bertindak secara kooperatif guna mencapai suatu tujuan, yang mungkin berupa pembangunan, atau perluasan, infrastruktur kuantum terdistribusi, inisiatif pembelajaran global, dan sebagainya.

Masa Damai/Permusuhan

Di mana satu atau lebih Negara berupaya menggunakan sumber daya kuantum untuk bertindak secara permusuhan guna memperoleh keuntungan atas Negara lain, misalnya melalui keunggulan kompetitif ekonomi, atau spionase siber.

Konflik/Kooperatif

Meliputi situasi di mana Negara-negara dapat membentuk aliansi atau koalisi selama konflik yang memengaruhi bagaimana mereka dapat menggunakan sumber daya kuantum mereka.

Konflik/Permusuhan

Di mana Negara menggunakan sumber daya kuantum mereka untuk berusaha memperoleh keunggulan militer. Kami juga membahas secara singkat konsekuensi dari kepemilikan kemampuan QIT yang asimetris, karena asimetri dalam teknologi dapat memotivasi perilaku Negara, seperti menyerang atau bertindak (misalnya dalam pertahanan

diri antisipatif) untuk memperoleh keuntungan sebelum kesenjangan teknologi menjadi terlalu besar. Dalam pengertian dasar di mana kepemilikan QIT memberikan keunggulan komparatif sehubungan dengan keputusan strategis, seperti dalam konflik atau negosiasi, setiap skenario di atas mewakili permainan sederhana yang strukturnya, seperti potensi keseimbangan Nash, dapat dipelajari untuk menginformasikan model mainan perilaku strategis.

Pendekatan teori permainan untuk memodelkan dampak, misalnya, kekuatan kecenderungan untuk mengambil tindakan tertentu sebagai cerminan dari bobot atau pentingnya yang diberikan Negara pada tindakan tersebut (seperti respons terhadap serangan siber, atau penggunaan QIT secara permusuhan) merupakan minat pembelajaran independen dan mampu memanfaatkan kumpulan karya yang berkembang tentang permainan kuantum yang disebutkan di atas. Namun, fokus kita justru pada penggunaan skenario-skenario ini untuk menguraikan dampak hukum internasionalnya. Untuk tujuan ini, dua skenario utama dan variasinya akan dibahas.

Skenario 1: Infrastruktur Kuantum Asimetris

Dalam Skenario 1 (Tabel 7.4 di bawah), Negara A memiliki akses ke QIT sementara Negara B tidak. Kemudian kita mempertimbangkan dua contoh di mana Negara A menggunakan QIT-nya secara antagonis: di masa damai untuk melakukan spionase industri dan dalam situasi konflik untuk mendekripsi komunikasi militer. Kita akan mempertimbangkan bagaimana asimetri QIT ini memengaruhi perilaku strategis mereka dan mempelajari konsekuensinya berdasarkan hukum internasional di bagian selanjutnya.

Tabel 7.4 Skenario 1—Infrastruktur Kuantum Asimetris

Item	**Deskripsi**
Negara Bagian	Negara A (dengan QIT) dan Negara B (tanpa QIT).
Teknologi	Negara A memiliki akses ke komputer kuantum ideal dan jaringan sensor kuantum (terdiri dari sensor kuantum yang terletak di dalam dan di luar wilayahnya) yang terhubung melalui internet kuantum (di dalam wilayahnya).
Masa Damai	Negara A melakukan spionase melalui serangan dekripsi SNDL terhadap Negara B, mencegat atau melakukan spionase untuk memperoleh data tentang produksi industri Negara B, menyimpannya, dan mendekripsinya menggunakan komputer kuantumnya. Pencegatan terjadi baik di dalam maupun di luar wilayahnya. Informasi yang telah didekripsi digunakan untuk memperoleh keunggulan kompetitif ekonomi.
Konflik	Negara A mendekripsi komunikasi militer yang sangat sensitif secara strategis dan menggunakan jaringan sensor kuantumnya untuk menguping Negara B dan mendekripsi komunikasinya. Negara A memanfaatkan kemampuannya untuk mendekripsi komunikasi klasik guna menentukan kunci privat dan protokol klasik yang digunakan oleh Negara B untuk mengenkripsi jaringannya. Negara A menggunakan informasi tersebut untuk meluncurkan operasi siber yang melumpuhkan

	jaringan pengawasan militer Negara B dan untuk memperoleh keuntungan militer strategis.

Skenario 2: Jaringan Kuantum yang Terjerat

Dalam Skenario 2 (Tabel 7.5 di bawah), kita menambahkan lebih banyak kompleksitas dan variasi. Negara A dan Negara B sama-sama memiliki akses ke satu sumber daya kuantum, misalnya internet kuantum, jaringan kuantum terdistribusi di mana kedua sumber daya kuantum mereka (misalnya sumber daya qubit) terjerat.

Tabel 7.5 Skenario 2—Jaringan Kuantum yang Terjalin

Item	**Deskripsi**
Negara Bagian	Negara Bagian A (dengan QIT) dan Negara Bagian B (dengan QIT).
Teknologi	Negara A dan Negara B berbagi sumber daya kuantum yang saling terkait dalam bentuk komputer kuantum berbasis qubit yang saling terkait dan internet kuantum berbasis keterkaitan. Negara A dan B awalnya mengaitkan sumber daya kuantum mereka dan berpartisipasi dalam pembentukan internet kuantum di seluruh wilayah yurisdiksi mereka. Internet kuantum tersebut digunakan di dalam setiap Negara dan oleh setiap Negara secara internasional.
Masa Damai	Negara A memanfaatkan sumber daya keterikatan bersama untuk memecahkan masalah kompleks seperti memfaktorkan bilangan bulat besar untuk kripto pemeriksaan atau mensimulasikan struktur molekul yang rumit—tugas yang ditingkatkan oleh korelasi kuantum. Meskipun kedua Negara menggunakan internet kuantum untuk pertukaran ilmiah yang aman, Negara A secara diam-diam mengukur qubit terikat tertentu, secara halus mengekstrak pola sensitif dari data kuantum Negara B tanpa memicu alarm yang jelas.
Konflik	Negara A mencegat atau memanipulasi qubit terikat yang membawa arahan rahasia Negara B, sehingga merusak distribusi kunci kuantum yang aman dan koordinasi strategis waktu nyata. Dengan memanfaatkan QIT-nya, Negara A mengganggu komunikasi dan proses pengambilan keputusan penting Negara B. Jaringan kuantum—yang dulunya merupakan platform komputasi kooperatif—kini memperkuat kemampuan ofensif Negara A, memberikannya intelijen dan kendali atas operasi militer Negara B yang paling sensitif.

7.6 HUKUM INTERNASIONAL DAN TEKNOLOGI INFORMASI KUANTUM

Gambaran Umum

Setelah meninjau lanskap teknologi QIT, kita sekarang memeriksa sumber-sumber hukum internasional yang mengatur penggunaan strategis teknologi informasi kuantum oleh Negara. Sebagai seperangkat teknologi informasi, kita mempertimbangkan bagaimana penggunaan teknologi informasi kuantum ditempatkan dalam hukum internasional yang lebih luas yang mengatur sistem informasi klasik, yang sering disebut dengan istilah 'teknologi siber'.

Kita memeriksa konvensi utama, kebiasaan, dan sumber-sumber yurisprudensi internasional lainnya tentang penggunaan sistem informasi oleh Negara secara umum.

Tidak ada perjanjian dalam hukum internasional yang secara khusus dirancang untuk mengatur penggunaan teknologi informasi atau aktivitas siber oleh Negara. Kami mengandalkan prinsip-prinsip utama hukum internasional dan aktivitas siber Negara sebagaimana diuraikan dalam Manual Tallinn. Kemudian, kami memberikan pemeriksaan skenario interaksi permusuhan antar Negara menggunakan QIT yang dijelaskan di atas untuk mengidentifikasi konsekuensi atau dilema unik yang muncul berdasarkan yurisprudensi internasional dari penggunaan QIT tersebut.

Kerangka konseptual yang kami adopsi adalah pemeriksaan hukum internasional yang khas. Secara khusus (dan sebagaimana akan kami bahas di bawah), ini mengurutkan imperatif normatif dan hukum menurut prinsip kanonik kedaulatan Negara sebagaimana diuraikan dalam perjanjian, hukum adat, dan yurisprudensi. Kedaulatan Negara menetapkan pembenaran atas hak, kewajiban, dan kepentingan Negara berdasarkan hukum internasional, termasuk definisi kedaulatan teritorial dan lainnya, tindakan yang melanggar kedaulatan, dan tindakan Negara yang dibenarkan dalam hal pelestarian kedaulatan Negara. Secara praktis, ini menempatkan QIT dalam konteks instrumental, baik sebagai infrastruktur, alat pemeliharaan Negara, atau sebagai teknologi ofensif atau defensif.

Manual ini umumnya dianggap sebagai sumber hukum internasional terkemuka, jika bukan yang terkemuka, yang membahas penerapan hukum internasional pada teknologi siber dan teknologi komputasi untuk konflik berbasis negara. Manual ini memeriksa bagaimana hukum internasional berlaku untuk operasi siber dan perang siber. Manual ini dikembangkan bekerja sama dengan Pusat Keunggulan Pertahanan Siber Kooperatif NATO oleh sekelompok ahli internasional dan memeriksa bagaimana hukum internasional yang ada (misalnya, Piagam PBB, hukum konflik bersenjata, dan kedaulatan negara) berlaku untuk operasi siber. Manual ini mengkaji doktrin hukum internasional yang berlaku untuk aktivitas siber yang terjadi baik selama masa damai maupun skenario konflik. Mengingat statusnya yang berpengaruh dalam kajian yurisprudensi tentang aktivitas siber internasional, kami fokus pada isi Manual sebagai sarana untuk memeriksa konsekuensi penggunaan QIT oleh negara.

Pada bagian selanjutnya, kami mempertimbangkan sejauh mana yurisprudensi siber internasional dapat memperoleh manfaat dari konsep tambahan untuk menangani konsekuensi unik dari QIT bersama dengan pertimbangan jenis instrumen hukum internasional yang dapat dipertimbangkan sebagai sarana untuk mengatur (secara aktif dan preventif) penggunaan strategis QIT oleh negara. Komputasi kuantum yang digunakan hanya untuk dekripsi (bukan misalnya intersepsi menggunakan perangkat kuantum) dalam kebanyakan kasus akan bergantung pada pengumpulan atau intersepsi informasi secara klasik, memasukkan informasi tersebut ke dalam komputer kuantum yang menjalankan algoritma kuantum untuk mendekripsi informasi tersebut, yang keluarannya akan direpresentasikan secara klasik. Setiap tindakan yang diakibatkan oleh hal ini akan bersifat klasik. Salah satu cara untuk memahami hal ini adalah dengan membandingkannya dengan teknologi kecerdasan buatan klasik.

Dampak AI dapat dipahami sebagai (i) epistemik, yang memungkinkan prediksi yang lebih akurat atau asimetri informasi yang lebih besar yang tindakannya hanyalah komunikasi dan pengiriman pesan (misalnya, respons terhadap pertanyaan, keluaran dari proses komputasi) dan (ii) agensi, di mana sistem AI, seperti agen berbasis AI (baik agen tradisional maupun agen model bahasa) dapat berinteraksi dengan lingkungan dan dunia melalui tindakan, secara kausal memengaruhi beberapa perubahan. Sistem informasi kuantum dapat memanfaatkan algoritma kuantum atau bentuk keunggulan kuantum untuk memperoleh keunggulan secara epistemik, tetapi tindakan kuantum spesifik yang dapat dilakukan terbatas (misalnya, di mana misalnya beberapa efek kuantum unik, seperti keterikatan, menyebabkan beberapa perubahan dalam keadaan lingkungan). Sederhananya, komputasi klasik (misalnya, AI klasik) berpikir dan bertindak secara klasik, sementara komputasi kuantum berpikir secara kuantum tetapi (dalam skenario yang kita perhatikan) bertindak secara klasik. Untuk menyempurnakan pemeriksaan kita lebih lanjut, kita melanjutkan dengan taksonomi strategis klasik-kuantum yang telah dijelaskan di atas.

Sebelum menyajikan pemeriksaan yang lebih lengkap tentang konsep-konsep kunci dari Manual yang berkaitan dengan QIT, kami menyertakan di bawah ini diskusi tentang beberapa tema konseptual yang berulang yang muncul ketika mempertimbangkan efek dan aplikasi QIT. Seperti yang kami catat di atas, QIT berakar pada fenomena dan hukum mekanika kuantum. Fitur unik dari sistem pemrosesan informasi kuantum yang berbeda dari sistem klasik memunculkan perbedaan ontologis dan epistemik spesifik yang memiliki konsekuensi bagi sejumlah konsep biasa, tetapi relatif mendasar, yang mendasari yurisprudensi hukum internasional publik. Kami mencantumkan beberapa di bawah ini sebelum mempertimbangkan bagian-bagian tertentu dari Manual secara detail. Fenomena utama yang kami fokuskan adalah superposisi kuantum dan keterikatan kuantum.

Ketidakpastian Sistem Kuantum

Meskipun perhatian besar diberikan pada cara teoritis dan terapan untuk mengatur evolusi kuantum melalui spesifikasi Hamiltonian, hasil pengukuran keadaan kuantum yang berevolusi bersifat stokastik. Yurisprudensi tentang aktivitas siber dalam hubungan internasional sebagaimana diuraikan dalam Manual membedakan antara lapisan fisik, logis, dan sosial dari dunia maya. Hal ini didasarkan pada konsepsi klasik tentang substrat fisik yang mendasari sistem informasi yang berperilaku klasik, yang sifat-sifatnya pada prinsipnya diketahui atau terukur dan konsisten dan di mana ketidakpastian pada dasarnya bersifat epistemik. Seperti yang telah disebutkan dalam bagian-bagian sebelumnya, secara umum hasil pengukuran sistem kuantum pada dasarnya tidak pasti, seperti misalnya ketidakpastian mengenai posisi dan momentum.

Ketika suatu keadaan kuantum $|\psi\rangle$ diukur, postulat pengukuran menyatakan bahwa keadaan tersebut runtuh menjadi eigenstate yang relevan. Superposisi suatu keadaan kuantum dengan demikian tidak dapat diamati secara langsung seperti halnya kita dapat mengamati representasinya secara langsung. Keadaan tersebut direpresentasikan sebagai artefak statistik pengukuran. Dalam praktiknya, ini berarti bahwa banyak salinan identik dari sistem kuantum disiapkan melalui prosedur persiapan keadaan dan diukur. Hal ini agak

bertentangan dengan tata kelola dan hukum yang terbiasa dengan prinsip-prinsip fundamental klasik tentang persistensi, kontinuitas, identifikasi, dan kesatuan sehingga objek yang menjadi subjek tata kelola dapat dipastikan dan pasti. Dapat dimengerti bahwa asumsi-asumsi klasik ini meresap dalam hukum internasional, termasuk perlakuan terhadap objek dan aktivitas siber dalam Manual di bawah ini. Ketika mempertimbangkan dampak teknologi kuantum, penting untuk mengenali perbedaan antara ontologi kuantum dan klasik (seperti fakta bahwa tidak ada satu sistem kuantum kontinu tunggal yang tetap dalam superposisi saat diukur berulang kali, melainkan seseorang harus menginisialisasi ulang keadaan kuantum atau memiliki beberapa contoh yang disiapkan secara identik). Namun, ketidakpastian ontologis yang melekat pada sistem kuantum tidak berarti bahwa sistem kuantum itu ajaib, tidak dapat diketahui, tidak dapat dikendalikan, dan sebagainya. Sebaliknya, seperti yang akan kita bahas di bawah ini, hukum pada umumnya dilengkapi untuk beradaptasi dengan cara yang memperhitungkan fenomena kuantum tersebut.

Yurisdiksi

Ketidakpastian ontologis yang melekat pada keadaan kuantum pada prinsipnya menimbulkan ketidakpastian dalam deskripsi posisinya. Posisi keadaan kuantum, seperti keadaan misalnya elektron, dijelaskan dengan mengacu pada probabilitas (ukuran) pada rentang posisi. Misalnya, posisi elektron dijelaskan oleh massa probabilitas atau fungsi kepadatan sedemikian rupa sehingga pengukuran berulang memungkinkan distribusi tersebut untuk diperkirakan (tergantung pada noise dan sebagainya). Hal ini dicontohkan oleh paradigma 'partikel dalam kotak' yang sederhana namun mencerahkan yang menunjukkan bagaimana distribusi posisi elektron bukanlah klasik, tetapi sebenarnya meluas secara luas hanya dengan probabilitas asimtotik nol untuk ditemukan di luar kotak. Dalam praktiknya, meskipun ketidakpastian dalam sifat kuantum merupakan fitur utama, jenis ketidakpastian ini tidak terlalu memengaruhi masalah yurisdiksi seperti lokasi teritorial dari sistem qubit tunggal atau multi-qubit.

Meskipun demikian, pandangan kami adalah bahwa karena hampir semua ukuran probabilitasnya terkonsentrasi dalam interval yang sangat sempit sehingga dalam praktiknya ekor distribusi pada dasarnya dapat diabaikan dari perspektif yurisdiksi. Dalam kasus keterikatan (*entanglement*), pertanyaannya lebih rumit karena kombinasi status ontologis superposisi dan keterikatan menimbulkan, setidaknya menurut banyak argumen dalam mekanika kuantum dan fondasi kuantum, fakta bahwa posisi fisik dari yang saling terkait dianggap non-lokal. Namun, seperti yang kami catat di bawah ini, konsep proksi seperti lokus kendali memberikan cara untuk menyesuaikan diri dengan gagasan dalam yurisprudensi yurisdiksi Negara.

Kendali

Yurisprudensi klasik untuk tata kelola teknologi dan keamanan siber didasarkan pada gagasan klasik tentang kendali. Secara implisit, misalnya, dalam diskusi tentang tanggung jawab Negara untuk mengendalikan penggunaan teknologi sibernya sendiri, atau penggunaan oleh aktor-aktor dalam yurisdiksinya, terdapat gagasan tentang kemampuan kendali atas sistem siber itu sendiri: bahwa sistem tersebut dapat diarahkan untuk berevolusi, berfungsi,

dan berkinerja dengan cara tertentu. Kewajiban untuk melakukan uji tuntas atau kewajiban untuk mengambil tindakan pencegahan ketika menggunakan operasi siber dalam konflik bersenjata, misalnya, menekankan kontrol pada tingkat yang lebih besar atau lebih kecil. Hukum memang mentolerir ketidakpastian dan kurangnya kontrol atas sistem siber ketika serangan siber yang seharusnya sah menjadi tidak sah karena kegagalan untuk mengendalikannya telah menyebabkan kerusakan tambahan yang tidak dapat dibenarkan. Ada juga pengakuan bahwa sistem siber sangat kompleks, sehingga seringkali sulit untuk melakukan kontrol penuh atasnya. Namun QIT sampai batas tertentu secara teknis tidak sesuai dengan asumsi ini. Hasil pengukuran keadaan kuantum tidak terkontrol. Paling-paling tingkat kontrol atas statistik pengukuran dikelola melalui rekayasa yang andal sehingga statistik pengukuran dapat diprediksi dengan keyakinan yang cukup.

Kontrol dalam Skenario Keterikatan Itu Rumit

Ketika dua Negara berbagi sumber daya yang terikat, siapa yang dapat dikatakan mengendalikan sistem yang terikat tersebut? Dan apa artinya mengendalikan sistem seperti itu? Dalam praktiknya, Negara-negara yang berbagi sumber daya tersebut akan berbagi sejumlah besar keadaan kuantum yang disiapkan dan terikat secara identik. Dengan berbagi ini berarti bahwa setiap qubit fisik (yang secara agregat akan membentuk satu set qubit logis) secara fisik terletak di dalam yurisdiksi suatu Negara (atau dikendalikan olehnya) sehingga Negara tersebut dapat mengendalikan bagaimana ia berinteraksi dengan qubitnya. Dengan mengukur (atau interaksi setara lainnya), Negara tersebut menyebabkan qubitnya sendiri dan qubit Negara lain runtuh ke dalam keadaan pengukuran dengan probabilitas tertentu. Setiap Negara tidak dapat mengendalikan sendiri hasil pengukuran kuantum (dan dengan demikian operasi siber, misalnya komputasi selanjutnya yang bergantung padanya).

Penerapan kekuatan dalam pengertian konvensional terjadi melalui interaksi suatu Negara dengan qubitnya sendiri yang terikat, dan pada dasarnya hal ini menyebabkan, karena keterentangan, statistik pengukuran Negara lain menjadi berkorelasi. Terlepas dari stokastisitas, sejauh pengukuran suatu Negara dapat dikatakan menyebabkan statistik pengukuran Negara lain menjadi berkorelasi, maka pada intinya Negara yang mengukur telah mengerahkan apa yang menurut hukum dianggap sebagai tingkat kontrol tertentu atas qubit Negara lain.

Pengetahuan dan Koreksi Kesalahan

Banyak kewajiban Negara yang berkaitan dengan aktivitas siber bergantung pada tingkat pengetahuan Negara tentang aktivitas siber tersebut. Ini termasuk hukum kebiasaan mengenai uji tuntas Negara, penilaian pencegahan oleh Negara tentang dampak operasi siber, dan standar mengenai kemampuan untuk memperkirakan konsekuensi secara wajar. Hukum internasional memang mentolerir ketidakpastian dalam pengetahuan atau keadaan epistemik suatu Negara. Informasi kuantum diperoleh melalui statistik pengukuran yang digunakan untuk merekonstruksi keadaan atau proses kuantum secara tomografis (Hamiltonian). Hal ini biasanya (mengingat teknologi saat ini) tidak mungkin dilakukan untuk apa pun selain sistem multi-qubit kecil. Jadi, apa yang diketahui dan bahkan dapat diketahui tentang sistem kuantum tunduk pada tingkat ketidakpastian praktis yang lebih tinggi dibandingkan dengan sistem

klasik, bersama dengan perbedaan mendasar bahwa sistem kuantum tidak berada dalam keadaan yang pasti.

Secara umum, hukum internasional sudah memiliki mekanisme untuk menangani ketidakpastian teknologi atau konsekuensial, tetapi perlu diperhatikan perbedaan sejauh spesifikasi teknis mungkin menjadi persyaratan di bawah berbagai aturan atau kebiasaan. Selain itu, semua pemrosesan informasi kuantum memerlukan koreksi kesalahan karena sensitivitas substrat kuantum tempat QIT direkayasa. Persyaratan untuk koreksi kesalahan berarti jenis rezim kontrol yang berlaku untuknya berbeda dan menjadi lebih kompleks. Koreksi kesalahan memiliki dampak penting untuk kontrol sistem kuantum karena rezim kontrol harus memperhitungkan pelapisan dan pengkodean, misalnya, kode koreksi kesalahan. Mereka juga harus diarahkan sedemikian rupa sehingga tidak merusak atau mengganggu persyaratan untuk koreksi kesalahan yang toleran terhadap kesalahan. Koreksi kesalahan lebih lanjut membatasi sejauh mana sistem kuantum dapat didiagnosis atau diawasi.

Kekuatan

Seperti yang akan kami uraikan secara panjang lebar di bawah ini, konsep kekuatan merupakan inti dari hukum konflik bersenjata dan juga aktivitas siber oleh Negara selama masa damai. Manual ini mengakui bahwa kekuatan untuk tujuan operasi siber mencakup lebih dari sekadar kekuatan kinetik, atau bahkan katalis fisik lainnya, dengan mencatat peran sentral yang dimainkan oleh konsep kausalitas dalam hukum siber internasional publik. Dengan demikian, penerapan kekuatan biasanya dibingkai dalam istilah kausal, di mana suatu peristiwa siber memiliki konsekuensi tertentu. Penerapan kekuatan dalam pengaturan kuantum dijelaskan oleh formalisme dan paradigma matematika yang kompleks. Paradigma kekuatan kuantum berbeda dalam cara yang dijelaskan oleh kausalitas kuantum. Sebagian besar hal ini tidak akan relevan secara langsung untuk aktivitas Negara yang menggunakan QIT. Namun, dalam kasus keterikatan (*entanglement*), perlu dicatat bagaimana penerapan 'gaya' terjadi: satu Negara berinteraksi mengukur qubitnya sendiri dan, karena keterikatan ontologis qubit tersebut dengan qubit Negara lain, hal ini dianggap menyebabkan keruntuhan fungsi gelombang pada qubit Negara lain tersebut.

Namun, gaya tidak merambat melalui ruang perantara dengan cara biasa, misalnya seperti gelombang yang merambat melalui medan elektromagnetik. Meskipun demikian, pembingkaian gaya dalam hal kausalitas memang memberikan cara agar yurisprudensi biasa dapat diterapkan, dengan memperhatikan bahwa sifat stokastik dari hasil kuantum berarti bahwa suatu Negara mungkin tidak selalu dapat mengontrol hasil pengukuran, sehingga deskripsi klasik tentang kausalitas tetap berbeda. Dalam pengertian ini, kausalitas kuantum dikondisikan melalui probabilitas tertentu dari suatu efek daripada kepastian hasil.

Salah satu tantangan lain dalam kasus teknologi informasi kuantum dan yurisprudensi adalah fakta bahwa pengujian kausalitas dalam hukum cenderung bersifat kontrafaktual. Ini berarti bahwa hukum berupaya untuk memeriksa apa yang mungkin terjadi jika bukan karena intervensi yang dimaksud sebagai cara untuk memastikan dampak kausalnya. Namun dalam kasus sistem mekanika kuantum, seseorang paling-paling hanya dapat menyatakan hasil yang berbeda dengan probabilitas tertentu atau yang diperkirakan. Meskipun ketidakpastian

mengenai pemeriksaan kontrafaktual cukup umum dalam hukum dalam kasus kuantum, ketidakpastian ini tidak dapat direduksi. Bahkan dengan semua informasi di dunia, jenis pemeriksaan kontrafaktual yang dilakukan hukum tersebut bermasalah karena pengukuran kuantum pada dasarnya bersifat acak, yang berarti hasil pengukurannya pada dasarnya tidak pasti.

Penerapan Definisi Sistem Informasi Manual Tallinn pada QIT

Manual ini dibagi menjadi empat Bagian, masing-masing berisi pemeriksaan yurisprudensi dan klaim normatif mengenai penerapan hukum internasional pada dunia maya, komputasi, dan teknologi informasi dalam konteks ofensif dan defensif serta protokol komunikasi. Setiap Bagian selanjutnya diuraikan menjadi Bagian-bagian yang terdiri dari aturan (konvensional dan kebiasaan) hukum internasional publik yang relevan dengan aktivitas dan operasi dunia maya. Cakupan Manual ini luas dan telah menjadi subjek pembelajaran yang cukup besar sejak publikasinya.

Fokusnya adalah pada dua prinsip fundamental hukum konflik internasional. Yang pertama adalah *jus ad bellum*, prinsip yang mengatur kapan dan apakah suatu Negara diizinkan untuk menggunakan kekuatan. Yang kedua adalah prinsip *jus in bello* yang mengatur penggunaan kekuatan dan pelaksanaan operasi militer oleh suatu Negara selama konflik, termasuk batasan yang dirancang untuk melindungi orang, objek, dan aktivitas tertentu.

Manual ini juga menyajikan pemeriksaan ekstensif tentang hukum internasional publik yang mengatur operasi siber selama masa damai. Di bawah ini kita akan meneliti bagaimana prinsip-prinsip hukum internasional yang diuraikan dalam Manual yang berlaku untuk dunia maya juga berlaku untuk dunia maya kuantum yang kita definisikan secara luas sebagai teknologi informasi kuantum yang dibahas di atas (dengan tabel perbandingan yang tercantum dalam Tabel 7.6). Dalam banyak kasus, prinsip-prinsip hukum dunia maya yang biasa berlaku dan diwariskan dalam skenario dunia maya kuantum karena secara umum dapat diklasifikasikan sebagai aktivitas siber, aset siber, dan sebagainya. Tetapi dalam kasus lain, terutama di mana sifat-sifat mekanika kuantum yang tidak biasa sangat penting untuk fungsi, penggunaan, atau distribusi QIT, menurut kami, terdapat perbedaan spesifik (terutama berkaitan dengan keterikatan).

Ruang Siber dan QIT

Sebelum memeriksa sejumlah ketentuan utama Manual dan dampak QIT terhadap pemeriksaan yurisprudensi di dalamnya, kita mempertimbangkan isu-isu ambang batas sejauh mana QIT sesuai dengan definisi pemrosesan informasi yang telah ditetapkan dan pokok bahasan Manual ini. Kita mempertimbangkan definisi yang relevan dalam Glosarium yang berkaitan dengan QIT. Istilah siber didefinisikan untuk menunjukkan hubungan dengan teknologi informasi yang jelas mencakup QIT yang dirinci di bagian sebelumnya.

Infrastruktur siber (juga sinonim dengan 'perangkat keras') didefinisikan sebagai perangkat komunikasi, penyimpanan, dan komputasi tempat sistem informasi dibangun dan beroperasi. Dengan demikian, infrastruktur siber secara alami akan mencakup infrastruktur QIT, baik infrastruktur khusus kuantum maupun infrastruktur klasik di mana QIT secara inheren tertanam.

Ruang siber didefinisikan untuk mencakup lingkungan yang dibentuk oleh komponen fisik dan non-fisik untuk menyimpan, memodifikasi, dan bertukar data menggunakan jaringan komputer. Aktivitas siber didefinisikan sebagai aktivitas apa pun yang melibatkan penggunaan infrastruktur siber atau menggunakan cara siber untuk memengaruhi pengoperasian infrastruktur tersebut. Aktivitas tersebut mencakup, tetapi tidak terbatas pada, operasi siber. Istilah terakhir ini, operasi siber, didefinisikan mencakup penggunaan kemampuan siber untuk mencapai tujuan di atau melalui ruang siber. Istilah ini digunakan dalam konteks operasional yang dominan. Istilah relevan lainnya termasuk pengintaian siber, termasuk penggunaan kemampuan siber untuk memperoleh informasi tentang aktivitas, sumber daya informasi, atau kemampuan sistem. Jelas, masing-masing istilah ini mencakup kesetaraan teknologi informasi kuantum dalam maknanya.

Sistem siber didefinisikan dalam hal sistem komputer. Definisi 'komputer' itu sendiri tidak termasuk tetapi akan mengasumsikan makna umumnya. Sistem komputer didefinisikan mencakup satu atau lebih komputer yang saling terhubung dengan perangkat lunak dan perangkat periferal terkait, termasuk sensor dan/atau pengontrol (logika yang dapat diprogram), yang terhubung melalui jaringan komputer. Sistem komputer dapat bersifat umum (misalnya, laptop) atau khusus (misalnya, 'sistem pelacakan pasukan biru'). Dengan demikian, sistem komputer mencakup perangkat QIT tunggal, termasuk penginderaan kuantum dan setiap node kuantum. Meskipun definisi di atas mencakup komputasi terhubung (dan dengan demikian terdistribusi) dalam pengertian jaringan terdistribusi klasik, Manual ini juga memuat definisi jaringan komputer, yaitu suatu bentuk infrastruktur perangkat atau node yang saling terhubung yang memungkinkan pertukaran data. Media pertukaran data dapat berupa kabel (misalnya, Ethernet melalui twisted pair, fiber optik, dll.), nirkabel (misalnya, Wi-Fi, Bluetooth), atau kombinasi keduanya. Dengan demikian, jaringan komputer akan mencakup komputer kuantum yang terhubung jaringan dan, dapat dikatakan, perangkat jaringan komunikasi kuantum, misalnya, yang mengandalkan keterikatan sebagai teknologi nirkabel. Demikian pula, definisi internet, yaitu sistem global jaringan komputer yang saling terhubung yang menggunakan rangkaian Protokol Internet dan kebijakan perutean yang jelas, akan mencakup proposal utama untuk internet kuantum dan jaringan kuantum terdistribusi secara umum (walaupun dengan beberapa perbedaan halus, tetapi tidak material, mengenai apa yang dianggap sebagai, misalnya, perutean pada jaringan kuantum).

Istilah Data Kuantum

Definisi kunci lainnya kemungkinan juga akan mencakup QIT dan analog kuantum dari konsep pemrosesan informasi klasik. Misalnya, data didefinisikan sebagai elemen dasar yang dapat diproses atau dihasilkan oleh komputer untuk menyampaikan informasi dengan pengukuran data digital fundamental yang diidentifikasi sebagai byte. Meskipun qubit biasanya dibedakan dari bit, qubit (dan secara luas byte kuantum) dapat dilihat sebagai bentuk informasi klasik yang tunduk pada ontologi kuantum: qubit, misalnya, tetap dapat direpresentasikan (dan biasanya direpresentasikan) dalam bentuk bit yang mengambil nilai 0 atau 1 (misalnya $|\psi\rangle = a\,|\,0\rangle + b\,|\,1\rangle$) meskipun secara probabilistik.

Infrastruktur data kuantum (seperti memori kuantum dan bahkan hanya data yang dikodekan dalam sistem kuantum) juga akan termasuk dalam konsep pusat data, yang didefinisikan sebagai fasilitas fisik yang digunakan untuk penyimpanan dan pemrosesan volume data yang besar. Basis data didefinisikan sebagai kumpulan data yang saling terkait yang disimpan bersama dalam satu atau lebih file terkomputerisasi, yang mencakup penyimpanan data kuantum. Sedikit perbedaan dari perspektif kuantum berkaitan dengan keadaan superposisi dan keterikatan. Di mana data berada dalam keadaan superposisi, konsep disimpan bersama atau disimpan secara teknis agak berbeda dari perspektif informasi kuantum.

Ingat, tidak seperti komputer klasik, sebagian besar komputasi kuantum didasarkan pada kemampuan untuk menginisialisasi keadaan identik, mengukur sejumlah besar keadaan tersebut untuk memungkinkan statistik pengukuran diperoleh (seluruh proses disebut eksperimen dalam beberapa konteks). Dengan demikian, keadaan yang diinisialisasi dalam superposisi berisi data probabilistik dan setiap eksperimen, setelah diukur, akan meruntuhkan superposisi yang relevan (kita menggunakan contoh non-multistate yang sederhana di sini). Kita tidak dapat mengakses data yang disimpan, yaitu, dikodekan, dalam sistem kuantum (seperti qubit) secara langsung seperti yang dimungkinkan dengan data klasik, di mana pengukuran sistem tidak mengganggunya. Data dalam pengertian kuantum lebih mengacu pada abstraksi yang secara efektif direkonstruksi melalui eksperimen dan interaksi berulang, daripada identik dengan konsepsi klasik tentang penyimpanan.

Demikian pula, di mana data dikodekan dalam sistem kuantum terikat (yang menurut konstruksi harus berada dalam keadaan superposisi) yang didistribusikan di seluruh batas yurisdiksi fisik Negara, data dalam sistem kuantum yang dikendalikan oleh suatu Negara dapat dipengaruhi oleh tindakan pengukuran Negara lain pada sistem terikat tersebut. Dengan demikian, sekali lagi konsepsi klasik tentang data memiliki fitur yang sedikit berbeda dengan data kuantum karena segera setelah suatu Negara mengukur sistem, data yang dikodekan di dalamnya berubah karena keruntuhan ontologis superposisi (dan interaksi dekoherensi apa pun). Namun, dalam praktiknya, persyaratan persiapan dan pengukuran yang identik dapat dan kemungkinan besar hanya akan dilihat sebagai elemen prosedural sehingga sistem kuantum keadaan superposisi dan keadaan terikat akan memenuhi definisi data dan istilah terkait lainnya, sehingga termasuk dalam definisi klasik untuk tujuan Manual ini.

Definisi data mencakup penggunaan pusat data dalam jaringan terdistribusi, yang menetapkan bahwa pusat data dapat digunakan hanya oleh pengguna yang tergabung dalam satu perusahaan atau dibagi di antara beberapa perusahaan, seperti pada pusat data 'komputasi awan' (lihat di atas). Pusat data dapat bersifat stasioner atau bergerak (misalnya, ditempatkan dalam kontainer kargo yang diangkut melalui kapal, truk, atau pesawat terbang). Sekali lagi, setiap definisi ini secara kategoris mencakup padanan QIT.

Definisi Ruang Siber

Terdapat sejumlah istilah teknis lain yang didefinisikan dalam Manual yang analog kuantumnya kemungkinan besar akan termasuk di dalamnya tanpa banyak kontroversi. Salah satu definisi yang sangat relevan mengingat motivasi ofensif dan defensif untuk penggunaan

QIT adalah peperangan elektronik sebagai penggunaan energi elektromagnetik (EM) atau energi terarah untuk mengeksploitasi spektrum elektromagnetik. Peperangan elektronik mencakup intersepsi atau identifikasi emisi EM (relevan dengan strategi ofensif kuantum simpan-sekarang-dekripsi-nanti) dan secara luas mencakup penggunaan energi EM, pencegahan penggunaan spektrum EM secara bermusuhan oleh musuh, dan tindakan untuk memastikan penggunaan spektrum tersebut secara efisien oleh Negara pengguna. Seperti yang dibahas di atas, penggunaan QIT tidak setara dalam tindakannya dengan sistem informasi klasik. Meskipun semua sistem QIT bergantung pada spektrum elektromagnetik dalam beberapa bentuk, 'tindakan' dari sistem kuantum bukanlah, misalnya, gelombang elektromagnetik kausal yang merambat secara lokal melalui medan elektromagnetik dengan cara yang sama seperti pulsa elektromagnetik atau bahkan komunikasi atau pensinyalan sederhana dalam konteks klasik.

Makna yang dimaksudkan dari peperangan elektronik di bawah definisi ini berbeda secara material. Penggunaan QIT untuk tindakan ofensif masih tercakup dalam definisi lain, seperti aktivitas siber, tetapi sistem kuantum tidak bertindak dengan cara yang sama seperti sistem klasik. Misalnya, bahkan dalam kasus negara-negara yang saling bermusuhan yang berbagi sumber daya yang terikat, gagasan klasik tentang satu negara yang bertindak terhadap negara lain dengan cara mengukur serangkaian qubit yang terikat bukanlah tindakan lokal (klasik). Sebaliknya, hal itu terkadang digambarkan sebagai tindakan 'menakutkan' dari jarak jauh.

Istilah *serangan siber* dan *spionase siber* didefinisikan dengan merujuk pada Aturan 92 dan 32 masing-masing. Aturan 92 mendefinisikan serangan siber sebagai operasi siber, baik ofensif maupun defensif, yang secara wajar diharapkan menyebabkan cedera atau kematian pada orang atau kerusakan atau penghancuran pada objek. Sebagaimana dicatat dalam Manual, operasi non-kekerasan, seperti operasi siber psikologis dan spionase siber, tidak memenuhi syarat sebagai serangan berdasarkan definisi tersebut (yang mengacu pada Pasal 49(1) Protokol Tambahan I dalam persyaratan konsekuensialisnya untuk penerapan kekuatan atau kekerasan atau bentuk interaksi kausal lainnya dengan efek serupa). Seperti halnya konsepsi yurisprudensial lainnya tentang kausalitas, kedekatan dan kausalitas efektif menjadi masalah ketika menyangkut tindakan tidak langsung yang dapat dikatakan menyebabkan efek seperti kerugian.

Tumpukan Ruang Siber Ontologis

Manual ini mengadopsi kerangka hierarkis bertumpuk atau berlapis untuk ruang siber, mendefinisikannya dalam tiga lapisan (Aturan 1.4, hal. 12): (i) lapisan fisik, yang terdiri dari komponen jaringan fisik (perangkat keras), (ii) lapisan logis, yang sesuai dengan koneksi yang ada antara komponen jaringan, yang terdiri dari abstraksi tingkat tinggi seperti aplikasi, data, dan protokol untuk pertukaran data di seluruh lapisan fisik, dan (iii) lapisan sosial, yang terdiri dari para pemangku kepentingan (individu dan kelompok) yang terlibat dalam aktivitas siber. Hierarki ini penting karena hak, kewajiban, dan tanggung jawab tertentu yang timbul berdasarkan pemeriksaan yurisprudensi Manual ini diuraikan dalam lapisan yang berbeda, mirip dengan tumpukan tata kelola.

Dengan demikian (seperti yang akan kita bahas lebih detail di bawah), prinsip-prinsip dasar kedaulatan Negara ditafsirkan sesuai dengan ketiga lapisan ruang siber tersebut. Dan lebih lanjut, seperti yang akan kita pemeriksaan di bawah ini, hal ini memiliki dampak terhadap penerapan prinsip-prinsip tersebut. Dengan demikian, meskipun semua QIT tertanam secara fisik dan relatif lokal, ruang logis menunjukkan sifat yang berbeda. Misalnya, penerapan prinsip yurisdiksi, kedaulatan, dan kontrol pada qubit yang terikat setidaknya harus memperhitungkan non-lokalitasnya dalam ruang posisi karena, misalnya, ukuran probabilitas atas ruang fisik tersebut yang menentukan lokasi, katakanlah, elektron yang digunakan sebagai qubit hampir seluruhnya terkonsentrasi pada apa yang oleh hukum dianggap sebagai lokasi fisik qubit. Namun, ketika qubit fisik tersebut terikat dan/atau menjadi bagian dari qubit logis melalui keterentangan lintas yurisdiksi, lapisan logis dari qubit logis (dan sistem terikat secara keseluruhan) lebih sulit ditentukan dalam hal koordinat geometris sederhana.

7.7 HUKUM INTERNASIONAL UMUM DAN RUANG SIBER

Bagian I Hukum Internasional Umum dan Ruang Siber dari Manual ini menetapkan prinsip-prinsip dasar hukum internasional yang berlaku di ruang siber, dengan mencatat bahwa hukum internasional publik sudah berlaku untuk Negara-negara sehubungan dengan aktivitas ruang siber. Prinsip bahwa hukum sebagaimana adanya, lex lata, sudah berlaku untuk dunia maya, berlaku pula untuk QIT dalam banyak hal. Kami meneliti kekhususan prinsip-prinsip hukum internasional yang ada terkait dunia maya, menelusuri struktur Manual dan mengkaji bagaimana dan apakah penerapan prinsip-prinsip tersebut pada klasifikasi dunia maya berbasis QIT berbeda secara signifikan.

Kedaulatan

Yurisdiksi Kedaulatan

Bagian 1 (Kedaulatan) mencakup penerapan prinsip-prinsip kedaulatan Negara secara kanonik (Aturan 1), yang menetapkan bagaimana prinsip ini memberikan wewenang eksklusif kepada Negara atas infrastruktur siber mereka. Terlepas dari abstraksi ruang siber sebagai virtual, keberadaan dan yurisdiksi ruang siber, bahwa ruang siber dibentuk oleh objek dan melibatkan aktivitas yang dilakukan oleh orang dan entitas yang atasnya kedaulatan dan yurisdiksi Negara berlaku (tanpa Negara yang berdaulat atas ruang siber global karena sebagian lokasinya berada di dalam Negara lain). Aktivitas ruang siber di dalam wilayah suatu Negara (Aturan 2) dianggap tunduk pada kedaulatan Negara, penerapan kedaulatan yang langsung. Prinsip ini berlaku untuk aset siber publik (Negara) dan swasta, misalnya, fakta penentunya adalah apakah suatu Negara dapat menjalankan kedaulatan atas aset tersebut, bukan konfigurasi kepemilikan domestik.

Kedaulatan internal semacam itu terkait dengan *domaine reservé* suatu Negara (Aturan 66), yaitu bidang-bidang aktivitas yang dianggap secara eksklusif berada dalam yurisdiksi domestik suatu Negara berdaulat, artinya bidang-bidang tersebut tidak tunduk pada campur tangan atau regulasi oleh hukum internasional atau entitas eksternal (di mana intervensi yang melanggar hukum dianggap sebagai pelanggaran kedaulatan). Lapisan fisik dunia maya dianggap secara jelas tunduk pada kedaulatan Negara. Manual ini menyarankan bahwa

kedaulatan meluas ke prinsip kontrol atas aspek-aspek lapisan logis dunia maya di dalam wilayah suatu Negara, dengan memberikan contoh legislasi Negara yang mewajibkan protokol interoperabilitas. Pertanyaan tentang hubungan antara kontrol dan kedaulatan ini akan kita bahas di bawah ini dalam konteks jaringan komunikasi kuantum berbasis keterikatan yang digunakan bersama oleh Negara-negara di mana tindakan setiap Negara yang mengukur qubit terikat-nya sendiri memiliki efek fisik dan logis pada jaringan kuantum dan konsekuensi bagi penggunaannya.

Aturan 3 membahas prinsip kedaulatan eksternal, yang memungkinkan pelaksanaan aktivitas siber dalam hubungan internasional yang tunduk pada batasan yang diberlakukan oleh hukum internasional. Prinsip ini dianggap berasal dari kesetaraan kedaulatan Negara (seperti yang tercatat dalam, misalnya, pasal 2(1) Piagam PBB). Artinya, tidak ada kedaulatan tunggal tertinggi dari satu Negara atas Negara lain. Dengan demikian, Negara-negara bebas untuk membuat pengaturan, misalnya perjanjian siber atau mengeluarkan opinio juris tentang hukum dan praktik kebiasaan yang berkaitan dengan operasi siber.

Dalam Skenario 1, kedaulatan setiap Negara meluas ke infrastruktur klasik dan siber di dalam yurisdiksinya, dengan infrastruktur siber klasik dan kuantum dari setiap Negara merupakan perluasan instrumental dari kedaulatannya. Dalam Skenario 2, kedaulatan setiap Negara atas sistem kuantum yang terikat lebih kompleks daripada dalam Skenario 1. Sistem kuantum yang terikat menunjukkan karakteristik non-lokal yang tidak secara langsung sesuai dengan yurisdiksi teritorial atau ekstrateritorial. Kedaulatan setiap Negara meluas ke kendali atas qubit yang secara fisik terletak di dalam yurisdiksinya. Namun, fakta ini membuat kendali eksklusif setiap Negara atas qubitnya menjadi bermasalah (seperti yang disebutkan di atas). Sifat keterkaitan yang sangat erat dari sumber daya yang saling terkait tersebut berpotensi menjadi objek *de jure* dan *de facto* yang (sejauh keterkaitannya) tunduk pada kedaulatan bersama masing-masing Negara.

Kedaulatan Bersama

Meskipun tidak dibahas dalam Manual ini, prinsip hukum internasional tentang kondominium (atau *coimperium*) dapat memberikan sumber yang digunakan untuk memeriksa kedaulatan bersama, seperti atas sumber daya yang saling terkait. Dalam hukum internasional, kondominium terjadi ketika dua atau lebih Negara berbagi dan menjalankan wewenang pemerintahan atas wilayah tertentu tanpa ada satu Negara pun yang menikmati kedaulatan eksklusif. Konsep ini berakar pada tradisi hukum Romawi dan perdata, di mana kepemilikan bersama dan kedaulatan bersama diakui sebagai konstruksi hukum.

Secara historis, pengaturan semacam itu melibatkan pelaksanaan bersama kekuasaan kedaulatan, seperti yang terlihat di wilayah perbatasan Eropa atau wilayah kolonial, sementara contoh yang lebih baru sering kali mencerminkan bentuk administrasi atau pengawasan regulasi yang terbatas daripada kedaulatan penuh. Dalam sebuah kondominium, negara-negara yang terlibat harus mengelola dan mengendalikan otoritas bersama mereka melalui perjanjian atau kesepakatan yang dinegosiasikan dengan cermat, yang menetapkan prinsip-prinsip yang menjaga kedaulatan negara lain, seperti prinsip non-diskriminasi, kebebasan pergerakan orang dan barang, batasan pengerahan militer, dan mekanisme pengambilan

keputusan dan penyelesaian sengketa. Pengaturan ini dipandu oleh prinsip-prinsip hukum internasional tetapi sebagian besar telah digantikan oleh rezim kelembagaan modern seperti perjanjian dan organisasi bilateral dan multilateral internasional.

Pelanggaran Kedaulatan

Aturan 4 menetapkan prinsip setara siber bahwa negara-negara tidak diizinkan untuk melakukan operasi siber yang melanggar kedaulatan negara lain, dengan pengecualian yang diakui dalam hukum internasional (seperti yang diizinkan oleh Dewan Keamanan PBB) (lihat Aturan 76) atau berdasarkan hak negara untuk membela diri. Kewajiban ini hanya berlaku antar negara, bukan oleh negara terhadap aktor non-negara. Dengan demikian, meskipun Negara memiliki jalan untuk menanggapi serangan siber aktor non-Negara misalnya, hak untuk menanggapi tidak dianggap ada di bawah naungan tanggapan terhadap pelanggaran kedaulatan (walaupun suatu Negara dapat melanggar kewajiban uji tuntas mereka dengan secara sembrono mengizinkan aktivitas tersebut).

Perluasan prinsip kedaulatan ke infrastruktur siber swasta juga akan berlaku untuk QIT sebagai bagiannya. Pelanggaran yang dilakukan terhadap Negara lawan di dalam yurisdiksi lawan itu sendiri akan merupakan pelanggaran kedaulatan terlepas dari itu. Manual tersebut mencatat bahwa operasi siber yang melanggar hukum terhadap infrastruktur siber Negara dapat merupakan pelanggaran kedaulatan Negara (Aturan 4) sambil menetapkan prinsip-prinsip kekebalan kedaulatan dan kekebalan (Aturan 5).

Aturan 4 menetapkan sejumlah kriteria. Pencegatan sinyal Negara target dari luar wilayah Negara tersebut tidak melanggar kedaulatan Negara karena operasi siber tersebut tidak terwujud dalam infrastruktur siber Negara target (dengan beberapa kualifikasi mengenai privasi). Tiga tingkatan pelanggaran meliputi (i) kerusakan fisik, (ii) hilangnya fungsi, dan (iii) pelanggaran terhadap integritas teritorial. Dengan demikian, dalam Skenario 1, penyadapan sinyal klasik oleh Negara A di luar wilayah Negara B, dan dekripsi sinyal tersebut, tidak akan merupakan pelanggaran kedaulatan Negara B itu sendiri.

Spionase siber tidak memiliki signifikansi hukum sehubungan dengan pelanggaran kedaulatan itu sendiri. Dalam kasus konflik Skenario 1, campur tangan Negara A melalui penonaktifan jaringan pengawasan militer Negara B akan merupakan hilangnya fungsi yang setara dengan pelanggaran kedaulatan (tetapi lihat di bawah untuk mengetahui apakah itu melanggar hukum atau tidak). Ini juga dapat merupakan campur tangan terhadap fungsi pemerintahan Negara B.

Dalam Skenario 2, faktor yang mempersulit adalah sifat keterikatan dari sumber daya kuantum bersama. Sekadar memanfaatkan sumber daya keterikatan bukanlah bentuk kerusakan itu sendiri, dan dilarang karena bahkan aktivitas kerja sama pun dapat melakukannya. Namun secara teknis, hal itu dapat dianggap sebagai hilangnya fungsi karena, seperti yang telah disebutkan sebelumnya, keterikatan kuantum adalah sebuah sumber daya.

Apakah biaya peluang akan setara dengan hilangnya fungsi (seperti di mana Negara-negara sebelumnya telah menyetujui sebaliknya) adalah masalah yang tidak jelas, tetapi hal itu menunjukkan dampak hukum yang agak tidak biasa yang muncul dari sumber daya bersama yang saling terkait. Meskipun demikian, penggunaan sumber daya yang saling terkait

tersebut dengan cara yang merupakan spionase dan merusak fungsi dapat dianggap sebagai pelanggaran jika sesuatu seperti tujuan atau niat diperhitungkan dalam operasi siber.

Uji Tuntas

Bagian 2 (Uji Tuntas) mencakup prinsip umum uji tuntas, kewajiban Negara untuk melakukan uji tuntas guna mengendalikan aktivitas (terutama aktor swasta) di wilayahnya terkait objek yang berada di bawah kedaulatannya agar tidak merugikan Negara lain (Aturan 6) (Aturan *Corfu*). Kewajiban ini tidak dianggap sebagai lex lata dan bahkan sebagai kebiasaan pun tidak dianggap sebagai kewajiban positif untuk mencegah penggunaan infrastruktur siber (jadi bukan dalam bentuk jaminan untuk memastikan hal ini tidak terjadi, atau bahkan untuk mengambil tindakan sedemikian rupa sehingga hal itu tidak mungkin terjadi), tetapi lebih ditujukan untuk tidak secara sadar mengizinkan aktivitas tersebut, sesuatu yang mirip dengan kewajiban upaya terbaik.

Pertanyaan tentang pengetahuan suatu Negara dibahas lebih lanjut di bawah ini. Yurisprudensi mempertimbangkan apakah Negara transit (perantara) yang dilalui aktivitas siber yang bersifat antagonis bertanggung jawab. Aturan 7 menetapkan pertimbangan mengenai beban dan kewajiban Negara untuk mematuhi prinsip uji tuntas. Sebagaimana disebutkan di atas, pada umumnya tidak ada kewajiban tanggung jawab mutlak bagi Negara untuk mencegah aktivitas siber di dalam yurisdiksinya yang akan melanggar hukum internasional. Namun, sejauh kewajiban umum berlaku, hal itu dianggap secara alami meluas ke operasi dan aktivitas siber di dalam perbatasan suatu Negara, yang akan mencakup QIT sebagai bagian darinya. Tanggung jawab suatu Negara untuk bertindak atau mengurangi aktivitas tersebut dibatasi oleh tingkat pengetahuan aktual atau konstruktif mereka. Skenario 1 dan 2 di atas hanya melibatkan aktor Negara, sehingga kami menghindari pertimbangan tersebut dalam konteks ini. Namun, kami mempertimbangkan beberapa isu yurisprudensi yang muncul dalam konteks penggunaan QIT.

Pengetahuan

Kewajiban uji tuntas bergantung pada standar yurisprudensi pengetahuan Negara. Seperti yang disebutkan di atas dan seperti yang sering terjadi pada operasi siber klasik, sulit untuk mengidentifikasi aktivitas atau operasi siber tertentu, atau sulit untuk menetapkan kausalitas. Operasi tersebut sering diidentifikasi melalui dampaknya daripada, misalnya, pengawasan pemrosesan informasi itu sendiri. Tantangan serupa berlaku dalam kasus QIT di mana, misalnya, pemantauan komputer kuantum yang mungkin digunakan untuk mendekripsi informasi terenkripsi klasik negara lain tidak dapat dilakukan secara langsung dengan mengamati proses kuantum yang terjadi (walaupun mungkin ada cara alternatif untuk mengidentifikasi niat untuk, misalnya, menerapkan algoritma Shor).

Konsekuensi Merugikan

Apa yang dianggap sebagai “konsekuensi merugikan yang serius” untuk tujuan Aturan 2 adalah masalah tingkatan. Tentu saja, pada prinsipnya strategi dekripsi membahayakan keamanan informasi negara lain atau spionase yang signifikan (seperti, misalnya, spionase siber yang memungkinkan pembuatan senjata pemusnah massal) dapat dikatakan memenuhi ambang batas ini. Sejauh mana secara kualitatif dekripsi tersebut hanya mungkin dilakukan

melalui penggunaan QIT (sebagai bagian dari serangan SNDL) maka, pada prinsipnya, akan menjadi jenis penggunaan QIT yang akan membentuk faktor penyebab konsekuensi merugikan yang serius. Namun, logika yurisprudensi sebagaimana yang tercantum dalam Manual pada poin uji tuntas pertama ini berada pada tingkat abstraksi sehingga fakta bahwa QIT digunakan untuk tujuan tersebut, dapat dikatakan, tidak akan secara material mengubah pemeriksaan hukum.

Kontrol dan Yurisdiksi

Kasus yang agak lebih menarik, meskipun terpencil, adalah pertimbangan kedua dalam prinsip kewajiban Negara mengenai uji tuntas, yaitu bahwa Negara harus melakukan uji tuntas atas infrastruktur siber instrumental (pemerintah) yang dikendalikannya. Kembali ke skenario kita yang sedang berlangsung di mana dua Negara berbagi sumber daya yang saling terkait, dapat dibayangkan bahwa prinsip tersebut harus diperluas ke keputusan kontrol oleh satu Negara ketika berinteraksi dengan qubit yang saling terkait miliknya sendiri, misalnya, dengan dampak langsung pada Negara lain (seperti bertindak pada sistem yang saling terkait dengan cara yang berdampak buruk pada kemampuan Negara lain untuk menggunakan sistem kuantum dengan cara tertentu). Sekali lagi, model mainan ini tampak terpencil, tetapi seperti yang telah kita catat di atas, sangat mungkin bahwa Negara dapat berbagi sumber daya dalam skenario kompetitif dan bahkan konflik. Perbedaan yurisprudensi yang ditarik antara yurisdiksi dan kontrol sangat relevan. Meskipun diskusi mengenai uji tuntas membedakan antara kontrol yang dilakukan oleh Negara versus aktor non-Negara, perbedaan ini berguna dalam kasus sumber daya kuantum non-lokal seperti QIT yang terikat. Dapat dikatakan, menggemakan poin kita di atas bahwa kontrol sumber daya kuantum pada akhirnya adalah operasi lokal (bahkan jika memungkinkan tindakan non-lokal terjadi), bahwa ketika menyangkut non-lokalitas, kontrol adalah 9/10 dari yurisdiksi.

Bagian 3 (Yurisdiksi) menetapkan prinsip-prinsip yurisprudensi umum mengenai Negara yang menjalankan yurisdiksi (yang berasal dari status kedaulatannya). Yurisdiksi mengacu, secara yurisprudensi, pada kompetensi suatu Negara untuk mengatur orang, objek, dan perilaku berdasarkan hukum domestik Negara tersebut, dalam batas-batas hukum internasional, secara teritorial (di dalam wilayahnya) atau ekstrateritorial. Kompetensi yurisdiksi dibagi menjadi tiga bentuk (Aturan 8) (i) preskriptif (legislatif); (ii) penegakan hukum, yang mencakup wewenang Negara untuk menegakkan hukum melalui tindakan eksekutif dan administratif; dan (iii) yudisial (adjudikatif), yang berkaitan dengan kompetensi badan peradilan suatu Negara (pengadilan) untuk mengatur sengketa yang menjadi yurisdiksinya. Aturan 8 menetapkan bahwa dengan tunduk pada batasan-batasan tertentu, Negara dapat menjalankan yurisdiksi teritorial dan ekstrateritorial atas aktivitas siber.

Dalam kasus terakhir ini, penggunaan infrastruktur informasi klasik dan kuantum untuk aktivitas siber ekstrateritorial seperti serangan siber atau spionase siber seringkali seperti yang terjadi saat ini akan ditargetkan secara ekstrateritorial. Perlu dicatat bahwa yurisdiksi penegakan ekstrateritorial lebih terbatas daripada yurisdiksi preskriptif, yaitu Negara dapat membuat undang-undang dalam batas yurisdiksi preskriptif mereka (misalnya, terkait dengan aktivitas di luar wilayah mereka), namun penegakannya terutama terbatas di dalam wilayah

Negara tersebut. Aturan 9 menetapkan bahwa yurisdiksi teritorial berlaku untuk infrastruktur siber, aktivitas siber, dan sebagainya yang memiliki keterkaitan teritorial tersebut. Secara khusus, Aturan 9 (c) mencakup aktivitas siber yang memiliki dampak substansial di wilayah suatu Negara, sedangkan penegakan yurisdiksi ekstrateritorial dicakup oleh Aturan 10–12. Seperti halnya aktivitas siber, aktivitas terkait QIT (seperti yang terintegrasi ke dalam infrastruktur siber klasik) pada prinsipnya dapat berasal dari beberapa Negara, melintasi beberapa Negara yang menyebabkan yurisdiksi yang diperebutkan atas aktivitas siber tertentu.

Dalam Skenario 2, beberapa Negara yang berbagi infrastruktur jaringan kuantum terdistribusi menghadapi tantangan yurisdiksi baru dan menarik yang telah kita bahas di atas. Pada prinsipnya, suatu Negara dapat membuat undang-undang tentang bagaimana sumber daya kuantum akan digunakan berdasarkan hak prerogatif yurisdiksionalnya. Jika Negara B menggunakan sumber daya yang saling terkait tersebut dengan cara yang sesuai dengan wewenang yurisdiksional Negara B, maka dilema jelas akan muncul. Poin kuncinya sekali lagi adalah yurisdiksi bersama atas sumber daya non-lokal yang berkorelasi, yang berbeda dari kasus klasik.

Hukum Tanggung Jawab Internasional

Bagian 4 (Hukum tanggung jawab internasional) terutama merinci hukum internasional kebiasaan yang tercantum dalam Pasal-Pasal Komisi Hukum Internasional tentang Tanggung Jawab Negara mengenai tanggung jawab negara. Hukum tanggung jawab negara menetapkan kriteria hukum untuk mengaitkan operasi siber kepada suatu Negara (Negara yang bertanggung jawab) dan keadaan di mana tindakan tersebut merupakan penggunaan kekuatan oleh Negara yang bertanggung jawab terhadap Negara lain (Negara yang dirugikan). Ini mencakup aturan pembuktian dan bagaimana tanggung jawab dikaitkan. Seperti halnya serangan siber klasik, Negara penerima aktivitas siber mungkin memiliki sedikit waktu untuk merespons dalam ketidakpastian (*ex ante*).

Dalam kasus seperti itu, Negara berkewajiban untuk bertindak dan merespons secara wajar. Faktor-faktor yang mengarah pada kewajaran meliputi sifat, cakupan, dan luasnya respons, keandalan informasi, dan tingkat keparahan tindakan. Respons yang lebih parah umumnya menimbulkan beban pembuktian yang lebih besar. Ini dapat menjadi masalah dalam kasus QIT: apakah dekripsi rahasia militer, yang dapat mengubah keseimbangan dalam suatu konflik, merupakan penggunaan QIT yang sangat parah yang akan menyebabkan reaksi yang lebih cepat? Lalu bagaimana suatu Negara dapat mengetahuinya? Terlebih lagi, apa yang dianggap sebagai bukti yang menjadi subjek kewajiban pengungkapan bermasalah dalam kasus QIT, misalnya, apakah itu statistik pengukuran, atau spesifikasi algoritma, dll.? Aturan 14 menetapkan bahwa Negara bertanggung jawab atas aktivitas siber yang dapat diatribusikan kepada mereka yang merupakan pelanggaran kewajiban hukum internasional. Prinsip tanggung jawab telah mapan sehingga tanggung jawab suatu Negara adalah untuk tindakan yang melanggar hukum internasional (termasuk pelanggaran kewajiban hukum internasionalnya). Kewajiban tersebut berbeda di masa damai dan selama konflik dan tidak terbatas pada aturan yang bersifat saling bertentangan, tetapi dapat mencakup sejumlah

instrumen pengaturan lainnya. Definisi tersebut tidak bersumber dari hukum internasional itu sendiri dan melibatkan niat untuk menyebabkan kerugian. Karakter pelanggaran hukum internasional dari serangan siber tidak bergantung pada sumber geografisnya itu sendiri. Skenario kita di atas mengasumsikan tanggung jawab Negara atas penggunaan QIT, tetapi mungkin saja atribusi tanggung jawab tidak jelas ketika sumber daya QIT bersama atau ganda digunakan.

Operasi Siber yang Tidak Diatur Secara Per Se

Bagian 5 (Operasi siber yang tidak diatur secara per se oleh hukum internasional) mencakup aktivitas siber oleh Negara yang, meskipun bukan subjek peraturan khusus *atau lex specia-lis*, dapat tunduk pada hukum internasional secara tidak langsung. Contoh yang diberikan dalam Aturan 32 (Spionase siber di masa damai) adalah serangan siber dan spionase yang dilakukan di luar konflik bersenjata Negara. Spionase siber didefinisikan oleh Manual sebagai "setiap tindakan yang dilakukan secara diam-diam atau dengan dalih palsu yang menggunakan kemampuan siber untuk mengumpulkan, atau mencoba mengumpulkan, informasi" (Aturan 32) dan dapat mencakup aktivitas siber berupa pengawasan, pemantauan, penangkapan, eksfiltrasi data atau informasi lainnya. Spionase siber dapat diarahkan ke ketiga lapisan tumpukan ruang siber (fisik, logis, dan sosial). Secara fisik, ini dapat mencakup penyematan kode selama proses manufaktur yang kemudian dapat diaktifkan atau digunakan. Secara logis, ini dapat mencakup perangkat lunak berbahaya algoritma kuantum misalnya.

Pandangan yang dianut dalam Manual tersebut adalah bahwa hukum internasional kebiasaan tidak secara otomatis melarang spionase karena kurangnya praktik negara dan opinio juris, tetapi spionase dapat dilakukan dengan cara atau memiliki efek yang melanggar hukum menurut hukum internasional, seperti jika spionase tersebut merupakan kelas aktivitas terlarang lainnya seperti serangan siber yang melanggar hukum. Dalam Skenario 1, penggunaan jaringan sensor kuantum untuk spionase dan penyadapan dapat menimbulkan pertanyaan tentang legalitas aktivitas tersebut. Dengan demikian, meskipun spionase siber itu sendiri tidak dilarang oleh hukum, pemeriksaan tujuan atau kausal yang lebih disukai dalam riset akan menyatakan bahwa jika efek dari aktivitas tersebut merugikan hak negara lain, misalnya menempatkan mereka pada risiko militer, maka aktivitas tersebut dapat melanggar ketentuan lain.

7.8 QIT DALAM MASA DAMAI: INTERVENSI DAN PENGGUNAAN KEKERASAN

Sesuai dengan pembagian aktivitas Negara antara situasi damai dan konflik yang dibingkai oleh perilaku kooperatif atau antagonis, kami mempertimbangkan konsekuensi spesifik QIT selama masa damai. Bagian III (Kedamaian dan keamanan internasional dan aktivitas siber) dari Manual ini membahas penggunaan teknologi siber yang antagonis selama masa damai, dengan fokus pada gradasi aktivitas siber yang, meskipun antagonis, tidak mencapai ambang batas untuk skenario konflik. Aturan 65 hingga 80 mencakup berbagai prinsip yurisprudensi yang berlaku untuk skenario kami di atas. Kami fokus pada beberapa di antaranya yang terutama berkaitan dengan spionase siber dan, khususnya, skenario kedua

kami dan sumber daya yang saling terkait. Seperti bagian lain dari Manual ini, pembahasan yurisprudensi berfokus pada hukum dan prinsip yang berlaku secara umum.

Larangan Intervensi

Sub-Bagian 13 (Penyelesaian damai) membahas aktivitas siber selama masa damai. Aturan 65 mencakup prinsip bahwa Negara-negara harus melakukan upaya realistis untuk menyelesaikan perselisihan mereka yang melibatkan aktivitas siber secara damai agar tidak membahayakan perdamaian dan keamanan internasional. Aturan 66 dari Manual tersebut mencakup prinsip non-intervensi (yang berasal dari prinsip dasar kedaulatan) bahwa suatu Negara tidak boleh campur tangan, termasuk menggunakan aktivitas siber, dalam urusan internal atau eksternal Negara lain. Aturan ini dianggap sebagai hukum kebiasaan hukum internasional, yang sering kali diuraikan dalam pernyataan dan *opinio juris* Negara. Urusan internal berkaitan dengan *domaine reservé* suatu Negara, ini termasuk konfigurasi politik, ekonomi, dan sosial suatu Negara.

Pemaksaan melalui aktivitas siber saja tidak cukup untuk merupakan pelanggaran terhadap larangan intervensi: aturan ini bersifat bertujuan, yaitu, pemaksaan harus diarahkan untuk menargetkan hak, kewajiban, atau tanggung jawab Negara (termasuk posisi atau tindakannya), meskipun ada perdebatan mengenai apakah merampas kendali atau sumber daya suatu Negara dapat dianggap sebagai bentuk intervensi. Spionase siber tidak dianggap menggunakan kekerasan karena tidak adanya unsur paksaan (Aturan 32). Skenario 1 dan 2 di atas berkaitan dengan pertanyaan intervensi, dalam kasus pertama, peretasan ke infrastruktur siber kritis musuh; dalam kasus kedua, tindakan intervensi muncul karena sifat keterkaitan sumber daya kuantum bersama di antara Negara-negara dalam skenario tersebut.

Dalam Skenario 2, karena pengukuran oleh satu Negara (atau interaksi serupa lainnya) terhadap qubitnya sendiri memiliki efek fisik (dan logis) pada qubit Negara lain, maka tindakan Negara pertama tersebut secara wajar dapat dianggap secara kausal memengaruhi Negara yang bersangkutan. Dengan menggunakan paradigma komputasi yang memiliki keadaan, keadaan qubit diubah secara kausal dan dengan demikian pertanyaannya adalah apakah perubahan keadaan tersebut merupakan pelanggaran terhadap larangan tersebut. Pengaruh kausal ini secara langsung dapat memenuhi pelanggaran terhadap larangan tersebut.

Jelas ada kebutuhan untuk membedakan antara perilaku kooperatif dan kompetitif (bermusuhan) dalam skenario masa damai. Perilaku kooperatif, secara lebih luas, adalah perilaku yang disetujui oleh masing-masing Negara yang bersangkutan berdasarkan hak kedaulatannya, yang akan dan dapat mencakup penggunaan sumber daya yang saling terkait oleh Negara lain dengan cara yang memengaruhi Negara pertama. Dalam skenario kompetitif, situasinya agak lebih kompleks. Ada pertanyaan yurisprudensi tentang sejauh mana suatu Negara dapat dikatakan telah menyetujui perubahan keadaan sumber daya yang saling terkait di mana perubahan keadaan tersebut menyebabkan kerugian kompetitif.

Penggunaan Kekerasan dan QIT

Bagian 14 (Penggunaan kekerasan) dari Manual ini mencakup hukum dan yurisprudensi internasional mengenai penggunaan kekerasan, dengan fokus pada larangan umum penggunaan kekerasan dan pengecualian seperti kekerasan yang diizinkan oleh Dewan

Keamanan (lihat Aturan 76 di bawah) dan hukum kebiasaan pertahanan diri negara (Pasal 51 Piagam PBB, lihat Aturan 71 di bawah).

Keadaan di mana penggunaan kekerasan dilakukan melalui aktivitas siber dan, jika demikian, dibenarkan (*jus ad bellum*) tetap menjadi bidang yurisprudensi internasional yang terus berkembang. Aturan 68 merangkum larangan tersebut dalam konteks dunia maya, dengan menyatakan bahwa operasi siber yang merupakan ancaman atau penggunaan kekerasan terhadap integritas teritorial atau kemerdekaan politik negara mana pun (atau yang tidak sesuai dengan tujuan Perserikatan Bangsa-Bangsa) adalah melanggar hukum internasional. Prinsip ini berasal dari hukum kebiasaan internasional (seperti Pasal 2(4) Piagam PBB).

Ambang batas yang harus dipenuhi oleh QIT adalah (i) secara kausal terhubung dengan penggunaan kekuatan, (ii) merupakan ancaman atau penggunaan kekuatan, dan (iii) sebagai ancaman penggunaan kekuatan, hal itu merusak integritas teritorial atau kemerdekaan politik (kita kesampingkan pertanyaan tentang ketidaksesuaian dengan tujuan PBB). Penerapan prinsip ini bersifat bertujuan, bukan instrumental. Bukan penggunaan infrastruktur siber oleh satu Negara, atau bahkan infrastruktur siber Negara lain yang secara langsung terpengaruh, melainkan dampak dari aktivitas siber tersebut. Mengenai apakah suatu aktivitas siber dapat dikaitkan dengan suatu Negara, lihat pembahasan tentang atribusi sebelumnya.

Dalam kasus penggunaan QIT, ada sejumlah pertanyaan termasuk mengenai sifat penggunaan dan apakah hal itu dapat dianggap sebagai penerapan kekuatan yang telah kita bahas di atas. Penggunaan QIT sebagai tindakan informasi ditangani dengan mempertimbangkan dampak kausalnya daripada penerapan kekuatan kinetik atau fisik apa pun. Hal ini agak rumit, seperti yang kami catat di atas, dalam kasus sumber daya yang terikat karena penggunaan sumber daya yang terikat oleh suatu Negara pada dasarnya dapat merupakan penerapan gaya pada sumber daya yang terikat dari Negara lain.

Dengan demikian, dalam Skenario 2, pada prinsipnya kedua Negara dapat berinteraksi dengan qubit mereka sendiri sedemikian rupa sehingga memengaruhi qubit Negara lain, sehingga membentuk hubungan fisik (bukan sekadar hubungan sebagian akibat tidak langsung) antara tindakan dan efek Negara. Tetapi seperti yang kami catat di atas, apakah interaksi ini akan menghasilkan hasil yang berbeda justru yang membuat sistem kuantum berbeda: tindakan yang sama oleh Negara yang sama pada qubit yang terikat yang sama atau qubit itu sendiri dapat menghasilkan hasil yang berbeda, sehingga setiap rasa determinisme antara tindakan suatu Negara dan hasilnya berbeda dengan kasus klasik.

Larangan Penggunaan Kekerasan

Aturan 69 (Larangan ancaman atau penggunaan kekerasan) menetapkan definisi kapan operasi siber merupakan penggunaan kekerasan, yaitu ketika skala dan dampaknya sebanding dengan operasi non-siber yang mencapai tingkat penggunaan kekerasan. Prinsip ini diambil dari yurisprudensi, khususnya putusan Mahkamah Internasional (ICJ) dalam kasus Nikaragua. Ambang batas penggunaan kekerasan dianggap lebih rendah daripada "serangan bersenjata", yang terakhir merupakan syarat yang diperlukan untuk merespons secara sah dalam membela diri. Penggunaan kekerasan dengan konsekuensi yang lebih serius dianggap sebagai

penggunaan yang "paling berat". Terdapat perdebatan mengenai hal ini, dengan Amerika Serikat berpendapat bahwa setiap penggunaan kekerasan yang melanggar hukum merupakan serangan bersenjata. Manual ini menetapkan taksonomi untuk mempertimbangkan apakah suatu operasi siber merupakan penggunaan kekerasan.

Tingkat Keparahan

Tingkat keparahan operasi siber yang ditunjukkan oleh cakupan, durasi, dan intensitas konsekuensi merupakan faktor yang paling signifikan; semakin parah, semakin besar kemungkinan memenuhi ambang batas penggunaan kekerasan. Dengan demikian, kerusakan fisik atau kerugian akan dianggap sebagai penggunaan kekuatan (seperti peretasan infrastruktur informasi untuk menyebabkan kerusakan fisik).

Kecepatan

Kecepatan operasi siber merupakan faktor kedua yang perlu dipertimbangkan. Semakin cepat dan mendesak operasi siber, semakin kecil peluang untuk merespons secara damai. Semakin cepat, semakin besar kemungkinan operasi tersebut dianggap sebagai penggunaan kekuatan.

Keterkaitan langsung (penyebab langsung)

Kedekatan sebagian akibat yang lebih erat antara operasi siber awal dan dampaknya juga penting. Semakin dekat kedekatan temporal, semakin besar kemungkinan operasi tersebut memiliki karakter penggunaan kekuatan.

Invasivitas

Tingkat intrusi operasi siber ke dalam infrastruktur informasi negara lain, dengan penetrasi infrastruktur yang lebih kritis lebih mungkin berkontribusi untuk memenuhi ambang batas penggunaan kekuatan. Secara umum, seperti yang biasanya terjadi dalam hukum, semakin mudah dipastikan dampak dari operasi siber, semakin besar bukti yang dapat diajukan untuk membenarkan penetapan operasi siber sebagai penggunaan kekuatan. Faktor-faktor lain meliputi: (i) apakah operasi tersebut memiliki karakter militer (seperti yang disebabkan oleh lembaga militer suatu negara, atau menargetkan lembaga militer negara lain); dan (ii) keterlibatan negara, apakah negara dan instrumen pemerintahannya melaksanakan operasi siber, atau apakah aktor lain terlibat. Ancaman kekuatan (Aturan 70) didefinisikan serupa dalam hal ancaman operasi siber yang merupakan penggunaan kekuatan yang melanggar hukum.

Penggunaan QIT pada prinsipnya dapat memenuhi jenis operasi siber (walaupun bersamaan dengan infrastruktur klasik) yang memenuhi batasan tingkat keparahan, urgensi, langsung, atau invasivitas. Sebagai contoh, jika teknologi penginderaan kuantum dapat secara efektif mengungkap kapal selam bersenjata nuklir (dengan memperhatikan ketidakmungkinan terjadinya hal ini saat ini, lihat bagian V D (Penginderaan Kuantum) di atas), maka tingkat keparahan operasi siber ini akan sangat besar, berpotensi mengubah keseimbangan kekuatan geopolitik. Dampak informasi lainnya, seperti dekripsi infrastruktur komunikasi penting suatu Negara selama masa damai (atau konflik) juga dapat memenuhi ambang batas tersebut (Skenario 1). Dalam kasus Skenario 2, gangguan terhadap sumber daya kuantum yang terikat

mungkin bersifat langsung, segera, dan berpotensi invasif dan parah tergantung pada seberapa besar ketergantungan Negara target pada sumber daya tersebut di masa mendatang.

7.9 PENGGUNAAN QIT SELAMA KONFLIK

Setelah penggunaan kekuatan melalui operasi siber merupakan serangan bersenjata, dua Negara dapat dikatakan berada dalam skenario konflik. Dalam hal ini, klasifikasi operasi siber sebagai serangan bersenjata kemudian memicu tersedianya hak membela diri terhadap serangan bersenjata berdasarkan Pasal 51 Piagam PBB dan hukum kebiasaan internasional. Skenario 1 dan 2 di atas sama-sama membayangkan penggunaan QIT (*Quiique-Induced Threat*) ketika terjadi konflik.

Pembelaan Diri

Aturan 71 (Pembelaan diri terhadap serangan bersenjata) baik Pasal 51 maupun hukum internasional kebiasaan mengakui hak inheren pembelaan diri individu dan kolektif. Serangan bersenjata harus memiliki karakteristik lintas batas (mempengaruhi kepentingan teritorial atau ekstrateritorial suatu Negara). Seperti yang dicatat dalam Manual, media serangan tidak relevan dengan apakah operasi tersebut merupakan serangan bersenjata, sehingga pada prinsipnya penggunaan kausal QIT dapat dianggap sebagai serangan bersenjata berdasarkan aturan ini. Ambang batas pasti di mana operasi siber akan dianggap sebagai serangan bersenjata diakui sebagai tidak pasti. Contoh yang dibahas baik dalam riset maupun Manual adalah operasi siber Stuxnet tahun 2010 yang menyebabkan kerusakan pada infrastruktur nuklir Iran (sentrifugal). Serangan Stuxnet dianggap sebagai penggunaan kekuatan tetapi pandangan berbeda mengenai apakah itu memenuhi syarat sebagai serangan bersenjata.

Selain itu, ada juga pertanyaan tentang apakah serangkaian operasi siber yang berurutan dan/atau kumulatif secara agregat dapat dianggap sebagai serangan bersenjata, dan apakah kerusakan yang kurang dari kerusakan fisik masih dapat dianggap sebagai serangan bersenjata untuk tujuan doktrin internasional. Doktrin serupa mengenai kemungkinan terjadinya dampak yang wajar (dan kecerobohan atau kesengajaan) juga dipertimbangkan dalam Manual sebagai efek yang diperhitungkan ketika menilai klasifikasi operasi siber sebagai serangan bersenjata atau tidak (dengan catatan bahwa niat dianggap tidak penting per se).

Akibatnya, dalam Skenario 1, mungkin masuk akal bahwa kasus penggunaan konflik QIT untuk dekripsi informasi militer strategis untuk memberikan keuntungan militer dapat dibenarkan sebagai penggunaan kekuatan untuk membela diri misalnya. Dalam Skenario 2, gangguan infrastruktur komunikasi kritis sebagai respons terhadap serangan yang akan segera terjadi juga dapat dianggap sebagai penggunaan kekuatan yang sah melalui operasi siber kuantum.

Kebutuhan dan Proporsionalitas

Penggunaan kekuatan sebagai sarana pertahanan diri harus sesuai dengan kriteria kebutuhan dan proporsionalitas (Aturan 72), dua prinsip yang telah lama diakui. Kebutuhan mensyaratkan bahwa respons non-kekerasan tidak cukup untuk menanggapi serangan bersenjata, bukan berarti tidak ada pilihan lain, meskipun keberadaan alternatif (misalnya, firewall atau tindakan balasan yang dapat diimplementasikan secara wajar) akan menjadi

faktor dalam mempertimbangkan legitimasi penggunaan kekuatan dalam pertahanan diri. Proporsionalitas berkaitan dengan tingkat kekuatan yang diperlukan, bertindak sebagai batasan terhadap luas dan tingkat keparahan respons suatu Negara (tetapi perlu dicatat bahwa itu bukan persyaratan untuk membalas dengan cara yang sama). Tidak jelas sejauh mana, misalnya, dekripsi massal komunikasi Negara musuh melalui penggunaan QIT mungkin tidak proporsional, tetapi pada prinsipnya luas dan tingkat keparahan konsekuensi dari dekripsi yang meluas tersebut dapat menjadi faktor dalam pemeriksaan mengenai proporsionalitas penggunaan QIT.

Ancaman, Ketergesaan, dan Pembelaan Diri Antisipatif

Aturan 73 (Ancaman dan ketergesaan) menetapkan bahwa hak untuk menggunakan kekuatan dalam membela diri terhadap serangan bersenjata siber muncul jika serangan tersebut sudah dekat dan segera terjadi. Negara tidak perlu menunggu dengan pasif hingga serangan terjadi sebelum merespons berdasarkan doktrin tersebut. Pembelaan diri antisipatif dengan demikian terbatas pada kasus-kasus di mana serangan sudah dekat. Konsep pembelaan diri antisipatif mengacu pada penggunaan kekuatan oleh suatu Negara untuk membela diri terhadap serangan bersenjata yang sudah dekat yang belum terjadi tetapi akan segera terjadi.

Konsep ini berakar pada hukum internasional kebiasaan dan sering dikaitkan dengan Kasus Caroline (1837), yang menetapkan kriteria untuk pembelaan diri yang sah dalam situasi di mana kebutuhannya mendesak, luar biasa, dan tidak menyisakan pilihan cara, serta tidak ada waktu untuk pertimbangan. Prinsip ini kadang-kadang diungkapkan sebagai 'kesempatan terakhir yang memungkinkan' yang berarti kesempatan terakhir bagi suatu Negara untuk secara efektif membela diri, meskipun perbedaan antara tahap persiapan yang tidak memiliki kualitas mendesak dan tahap di mana musuh dapat dikatakan mampu melakukan serangan tersebut relevan dengan masalah ini. Selain itu, pertimbangan strategis, seperti kebutuhan untuk bertindak secara antisipatif tanpa memberi sinyal kepada musuh tentang tindakan tersebut.

Pemberian sinyal niat dan pengambilan tindakan persiapan oleh pihak lawan umumnya dianggap sebagai syarat yang diperlukan (tetapi tidak cukup) untuk serangan pencegahan antisipatif terhadap negara lawan, standarnya kurang lebih seperti apakah negara target potensial dapat secara wajar menyimpulkan bahwa pihak lawan telah membentuk niat dan memiliki kemampuan untuk menyerang. Ketidakmampuan untuk membentuk kesimpulan ini membatasi negara target pada respons yang tidak termasuk penggunaan kekuatan.

Manual ini juga memberikan pembahasan tentang kapan pembelaan diri kolektif sah menurut hukum internasional. Hal ini akan sangat relevan dalam kasus jaringan kuantum di mana satu atau lebih negara sekutu berupaya menggunakan jaringan tersebut terhadap pihak lawan. Hal ini menimbulkan pertanyaan strategis dan hukum yang lebih menarik, tetapi kami tidak membahas skenario ini secara langsung di sini. Salah satu pertanyaan yang menarik adalah sejauh mana Negara B mungkin memiliki hak untuk melakukan pembelaan diri antisipatif jika mengantisipasi penggunaan QIT yang akan segera terjadi yang akan memiliki efek dekripsi yang parah atau dahsyat. Contoh ekstrem dari hal ini telah disinggung di atas, di

mana, misalnya, suatu Negara menganggap dekripsi yang melemahkan kemampuan serangan balasan nuklirnya sebagai hal yang cukup serius untuk membenarkan penggunaan persenjataan nuklirnya sendiri atau respons signifikan lainnya.

7.10 QIT DAN KONFLIK BERSENJATA SIBER

Bagian IV (Hukum konflik bersenjata siber) dari Manual ini menguraikan secara rinci penerapan hukum konflik bersenjata terhadap operasi siber. Aturan 80 mencatat bahwa operasi siber termasuk dalam lingkup hukum konflik bersenjata. Istilah "konflik bersenjata" secara formal berasal dari Konvensi Jenewa 1949 I-IV45 (Pasal 2) dan secara yurisprudensi dianggap sinonim dengan "perang". Manual ini mendefinisikan konflik bersenjata sebagai situasi permusuhan (dalam kasus kita, antar Negara) termasuk yang menggunakan sarana siber, dengan kriteria ambang batas yang berbeda dalam kasus konflik internasional (Aturan 82) dan non-internasional (Aturan 83). Operasi siber dapat diatur oleh hukum konflik bersenjata meskipun operasi tersebut sendiri tidak merupakan serangan bersenjata. Luasnya keterkaitan bersifat kontekstual, tetapi secara umum berkaitan dengan operasi siber untuk mendukung permusuhan.

Faktor Geografis

Seperti yang disebutkan dalam Manual (Aturan 81), pertimbangan geografis relevan untuk karakterisasi legalitas operasi siber. Operasi siber selama konflik dapat dilakukan di dan di wilayah negara-negara yang terlibat dalam konflik (dengan perbedaan antara konflik internasional dan non-internasional). Aturan 82 menetapkan bahwa konflik bersenjata internasional ada setiap kali terdapat permusuhan di antara beberapa negara (yang dapat mencakup operasi siber) (Pasal 2 Konvensi Jenewa 1949) dengan ketentuan bahwa negara-negara bertindak melalui proksi atau aktor non-negara. Untuk tujuan kita, kita hanya berfokus pada konflik semacam itu (bukan non-internasional). Seperti halnya prinsip-prinsip lain yang mengatur perilaku permusuhan antar negara, terdapat perdebatan tentang ambang batas yang harus dipenuhi agar suatu tindakan oleh suatu negara dapat dianggap sebagai konflik bersenjata internasional, dengan beberapa pandangan bahwa konflik bersenjata apa pun sudah cukup, berbeda dengan pandangan lain yang menyatakan tingkat konflik *de minimis* yang lebih besar (seperti misalnya terkait sengketa perbatasan yang terjadi secara berkala). Hal ini sangat relevan dengan operasi siber yang seringkali bertingkat dalam cakupannya dan di mana spionase siber memainkan peran persiapan dan bertahap yang penting terhadap setiap permusuhan yang muncul. Baik dalam Skenario 1 maupun Skenario 2, pada prinsipnya setelah permusuhan dimulai, maka jenis tindakan yang direncanakan untuk Negara A harus memenuhi kriteria geografis.

Serangan Siber

Aturan 92 menetapkan definisi "serangan siber", seperti yang disebutkan di atas, yaitu operasi siber (ofensif atau defensif) yang secara wajar diharapkan menyebabkan cedera atau kematian pada orang atau kerusakan atau penghancuran pada objek. "Serangan" adalah istilah hukum yang darinya mengalir konsekuensi seperti mengenai penargetan (penargetan warga sipil dan infrastruktur sipil dilarang). Istilah tersebut mengandung makna kekerasan ofensif

atau defensif terhadap musuh. Seperti yang dicatat dalam Manual, tindakan kekerasan tidak terbatas pada definisi kinetik atau vernakular. Sebaliknya, konotasinya adalah kausalitas, oleh karena itu konsekuensi yang disebabkan oleh suatu tindakan, seperti operasi siber, menjadi dasar untuk mengklasifikasikannya sebagai serangan siber. Dalam hal ini, kekerasan mengacu pada konsekuensi dari suatu tindakan, bukan tindakan itu sendiri. Gagasan tentang kerugian konsekuensial termanifestasi dalam konsep kerugian, bahaya, cedera, dan istilah lain dalam berbagai sumber hukum internasional. Konsep kausalitas mencakup konsekuensi yang dapat diperkirakan secara wajar termasuk kerusakan, kehancuran, cedera, atau kematian. Dengan demikian, penggunaan operasi siber untuk menimbulkan kehancuran atau kerugian besar dalam beberapa cara kemungkinan akan memenuhi syarat penggunaan tersebut sebagai serangan siber.

Dari perspektif komputasi, operasi siber terhadap data dan 'entitas non-fisik' lainnya atau entitas yang didefinisikan secara lebih abstrak dapat menjadi sasaran serangan. Demikian pula, gangguan berbasis operasi siber terhadap fungsionalitas suatu objek dapat disamakan dengan kerusakan pada fungsionalitas objek tersebut. Ini dapat mencakup korupsi sistem kontrol perangkat lunak dengan cara yang menimbulkan kerugian. Pandangan lain berpendapat bahwa gangguan terhadap infrastruktur siber saja sudah dapat dianggap sebagai serangan, bukan hanya kerugian konsekuensial lebih lanjut. Poin penting yang dibahas dalam Manual ini adalah efek kumulatif pada misalnya fungsionalitas sosial (seperti gangguan email massal), namun hal ini dipandang oleh beberapa riset sebagai terlalu jauh dari hukum konflik bersenjata itu sendiri. Demikian pula, operasi siber yang hanya berupa ketidaknyamanan, atau bahkan spionase, gagal memenuhi ambang batas serangan siber.

Selain itu, pendekatan konsekuensialis terhadap klasifikasi serangan juga mencakup serangan yang dicoba tetapi tidak berhasil, atau operasi siber yang tujuannya adalah untuk menyebabkan kerugian tetapi mungkin belum dieksekusi, seperti penyisipan pintu belakang (*backdoor*) malware atau virus. Pemeriksaan serupa dalam kasus QIT akan berlaku seperti pada kasus klasik dalam hal ini. Misalnya, apakah gangguan terhadap sumber daya terikat bersama dalam Skenario 2 cukup untuk dianggap sebagai serangan, seperti halnya pada kasus klasik, akan menjadi pertanyaan kontekstual.

Prinsip-Prinsip Konflik Bersenjata Lainnya

Prinsip-prinsip konflik bersenjata lainnya yang relevan dengan pertimbangan penggunaan QIT mencakup dua prinsip utama hukum internasional kebiasaan tentang konflik bersenjata yang diakui oleh ICJ. Prinsip-prinsip tersebut adalah prinsip pembedaan (Aturan 93), bahwa satu-satunya objek yang sah adalah pasukan militer musuh, dan larangan penderitaan yang tidak perlu (Aturan 104). Kedua aturan ini pada dasarnya berfokus pada meminimalkan penargetan non-kombatan (warga sipil, dll.) dan berupaya untuk memberlakukan kewajiban kehati-hatian pada Negara untuk menghindari kerugian mereka. Konsep-konsep ini terwujud dalam pembedaan antara objek sipil dan sasaran militer. Sasaran militer (sebagai istilah hukum) didefinisikan dalam Aturan 100 untuk mencakup objek-objek yang berdasarkan sifat, lokasi, tujuan, atau penggunaannya memberikan kontribusi efektif terhadap aksi militer dan yang penghancuran, penangkapan, atau netralisasi total atau

sebagiannya, dalam keadaan yang berlaku pada saat itu, menawarkan keuntungan militer yang pasti. Meskipun pertanyaan apakah data sebagai suatu kategori merupakan sasaran militer itu sendiri masih diperdebatkan, mengingat pentingnya data bagi keamanan negara modern dan operasi konflik bersenjata, masuk akal untuk berasumsi bahwa data dapat menjadi sasaran militer (lihat pentingnya data intelijen sepanjang sejarah) dan salah satu yang akan menjadi target penggunaan kekuatan berbasis QIT seperti yang diuraikan dalam Skenario 1 dan Skenario 2.

Penggunaan objek sipil untuk tujuan militer dapat menjadikannya sasaran militer. Untuk tujuan ini, yang sangat menarik bagi teknologi informasi adalah protokol penggunaan ganda yang dibahas di atas. Aturan 101 menetapkan bahwa infrastruktur siber yang digunakan untuk tujuan sipil dan militer ganda dianggap sebagai sasaran militer asalkan penghancurannya memberikan keuntungan militer. Hal ini didasarkan pada perbedaan (Aturan 100) antara objek sipil dan objek militer, berdasarkan Pasal 52(1) Protokol Tambahan I. Dengan demikian, sasaran militer adalah sasaran yang memberikan kontribusi efektif terhadap aksi militer sedemikian rupa sehingga menyerang atau merusaknya akan memberikan keuntungan militer bagi agresor. Keuntungan ini haruslah pasti. Pertimbangan penggunaan ganda dapat menimbulkan kewajiban kehati-hatian bagi Negara untuk memastikan bahwa (sesuai dengan prinsip pembedaan dan pelarangan penderitaan yang tidak perlu) kerugian sipil atau kerusakan pada infrastruktur sipil dikurangi.

Seperti yang dicatat dalam Manual, aktivitas siber menghadirkan kesulitan karena penggunaan gandanya seringkali tidak dapat dibedakan secara geografis atau infrastruktur, seperti dalam kasus jaringan yang digunakan untuk tujuan sipil dan militer ganda. Sejauh mana serangan dapat dilokalisasi terhadap target yang tersebar, seperti internet, oleh karena itu penting dan juga relevan dengan pertimbangan seputar respons proporsional. Aturan 102 mengandung prinsip kehati-hatian untuk pertimbangan yang cermat sebelum infrastruktur penggunaan ganda tersebut menjadi sasaran. Pertimbangan penggunaan ganda ini penting karena QIT, bersama dengan teknologi komputasi lainnya, kemungkinan memiliki fungsi penggunaan ganda yang cukup besar. Hal ini sebagian disebabkan oleh infrastruktur yang cukup besar yang dibutuhkan untuk mendukung QIT: komputer kuantum tidak dibayangkan akan semobil perangkat komputasi klasik. Pada dasarnya, bangunan-bangunan tersebut tidak dapat dipindahkan dan kemungkinan besar akan digunakan untuk kombinasi keperluan negara dan sipil mengingat betapa sulitnya pembangunannya.

Metode Perang

Manual ini membahas pertimbangan mengenai sarana dan metode perang siber, dengan mencatat bahwa hukum umum mengenai legalitas senjata dan metode juga akan berlaku dalam kasus siber. Aturan 103 mendefinisikan sarana perang siber dalam hal senjata siber dan sistem siber terkaitnya. Metode perang didefinisikan mencakup taktik, teknik, dan prosedur siber yang digunakan untuk melakukan permusuhan. Keduanya merupakan istilah teknis dalam yurisprudensi internasional. Manual ini mendefinisikan senjata siber dalam hal sarana siber yang digunakan, dirancang, atau dimaksudkan untuk menyebabkan kerusakan atau kehancuran, pada dasarnya kriteria yang sama untuk menjadikan operasi siber sebagai

serangan siber (berdasarkan Aturan 92). Istilah ini mencakup senjata siber dan sistem senjata, yang pertama merupakan aspek dari sistem yang digunakan untuk menyebabkan kerusakan, kehancuran, atau cedera. Sarana siber secara luas dianggap mencakup perangkat, material, instrumen, mekanisme, atau perangkat lunak untuk serangan siber.

Manual ini membedakan antara sistem komputasi yang dapat menjadi sarana peperangan, berbeda dengan infrastruktur siber (misalnya internet) yang tidak dianggap sebagai sarana peperangan, meskipun karena dugaan kurangnya kendali. Dalam kasus internet kuantum, hal ini mungkin berbeda karena internet dalam kasus tersebut terbatas dan dipengaruhi oleh sejumlah Negara yang terbatas. Metode peperangan menyangkut strategi yang digunakan, misalnya strategi penolakan layanan daripada instrumennya. Jelas penggunaan QIT akan termasuk dalam kategori konseptual ini dengan aturan serupa yang berlaku. Dengan demikian dalam Skenario 2, Negara A harus mempertimbangkan efek dari gangguan terhadap sumber daya kuantum Negara B atau internet kuantumnya bahkan jika hanya melakukannya melalui interaksi dengan qubit terikat miliknya sendiri.

Manual ini juga memeriksa berbagai prinsip yang berlaku seperti larangan terhadap sarana atau metode peperangan siber. Ini termasuk: metode dan sarana yang menyebabkan cedera berlebihan atau penderitaan yang tidak perlu (Aturan 104); Larangan penggunaan tanpa pandang bulu (Aturan 105) termasuk efek bola salju atau gaya viral yang menyebar dan jebakan siber, yaitu perangkat siber yang dapat beroperasi secara tak terduga (dan karenanya tanpa pandang bulu) (Aturan 106). Aturan 110 menetapkan prinsip-prinsip konsekuensial yang mewajibkan Negara-negara yang menggunakan sarana perang siber untuk memastikan mereka melakukannya dalam kerangka hukum konflik bersenjata dan bahwa, selain itu, jika mereka adalah pihak pada Protokol Tambahan I, mereka melakukan uji tuntas pencegahan yang memadai terkait pengembangan, akuisisi, atau adopsi sarana baru untuk memastikan kepatuhan terhadap kewajiban internasional tersebut.

Dalam kasus QIT, hal ini dapat dikatakan melibatkan sesuatu yang serupa dengan mempertimbangkan bagaimana penerapan QIT dalam berbagai konteks memiliki dampak yang berbeda dibandingkan dengan teknologi informasi klasik. Hal ini pada gilirannya berkaitan dengan konsep yang telah dibahas sebelumnya dalam diskusi kita tentang keharusan arsitektur tata kelola teknologi yang terperinci untuk sistem QIT yang sedang berkembang. Jenis kewajiban uji tuntas (*due diligence*) yang dibebankan kepada negara-negara ini memberikan motivasi tentang bagaimana dan mengapa instrumen tata kelola spesifik teknologi dibenarkan, bahkan mungkin diperlukan, dari perspektif hukum internasional.

Pelaksanaan Serangan Siber

Sejumlah aturan dalam Manual ini mencakup pelaksanaan dan perilaku aktual dari serangan siber. Aturan 111 menegaskan kembali bahwa perilaku serangan yang tidak pandang bulu (misalnya, menyerang target yang bukan target yang sah, atau gagal membedakan antara objek sipil dan non-sipil) dilarang. Hal ini diambil dari Pasal 51(4)(a) hingga (c) Protokol Tambahan I dan merupakan bagian dari hukum internasional kebiasaan. Aturan ini berbeda dari Aturan 105 di atas karena menyangkut kasus-kasus di mana suatu sistem yang mungkin memiliki kapasitas untuk penargetan diskriminatif dalam kasus-kasus tertentu gagal

memenuhi kriteria diskriminatif tersebut, yaitu sarana diskriminatif yang digunakan secara tidak pandang bulu. Dengan demikian, kemampuan untuk membedakan dianggap sebagai prinsip utama dari pelaksanaan operasi perang siber dan pada gilirannya terhubung dengan kewajiban Negara untuk melakukan pemeriksaan pencegahan yang wajar terhadap dampak aktivitas siber ofensif mereka. Aturan 112 mencakup kasus di mana serangan siber yang menargetkan sasaran militer siber dapat menyebabkan dampak yang tidak proporsional dan melanggar hukum terhadap kelas objek yang dilindungi (misalnya, warga sipil atau infrastruktur). Dengan demikian, bahkan jika serangan siber itu sendiri terhadap sistem penggunaan ganda mungkin proporsional, serangan tersebut dapat melanggar persyaratan ini, meskipun apakah itu terjadi atau tidak jelas bergantung pada konteks dan fakta pada saat itu.

Pertimbangan proporsionalitas yang berkaitan dengan serangan siber dipertimbangkan dalam Aturan 113, di mana serangan siber dianggap tidak memenuhi standar proporsionalitas (berdasarkan Protokol Tambahan I) dalam kasus di mana kerusakan pada warga sipil, objek sipil, atau kelas yang dilindungi lainnya berlebihan dibandingkan dengan keuntungan militer konkret dan langsung yang mungkin diperoleh dengan melakukannya. Aturan ini merupakan aturan kebiasaan dalam hukum internasional konflik bersenjata. Fokusnya adalah pada kerugian insidental dan kerusakan tambahan yang tidak menjadikan serangan siber melanggar hukum per se, tetapi memerlukan perhitungan antara kerugian tambahan dan keuntungan militer yang harus dilakukan atau ditunjukkan oleh Negara agresor.

Konsep serupa seperti yang dibahas di atas dalam hal ambang batas aktivitas siber yang merupakan serangan bersenjata berlaku ketika menentukan apakah operasi siber dapat menimbulkan kerugian tambahan yang cukup untuk memenuhi larangan tersebut. Kerugian tambahan terkadang diuraikan menjadi (i) efek langsung tingkat pertama dan (ii) efek yang tertunda atau dimediasi oleh peristiwa atau tindakan lain. Manual mencatat kesulitan dalam menilai apa yang merupakan keuntungan militer yang berlebihan dan apa yang merupakan keuntungan militer yang cukup, meskipun mencatat sejumlah sumber yang membahas preferensi untuk dampak konkret dan langsung yang dapat diukur dalam menilai keuntungan militer. Prinsip ini mengandung unsur kehati-hatian yang mewajibkan Negara untuk bertindak secara wajar dalam melakukan penilaian awal atas pertimbangan tersebut, seperti yang dipersyaratkan untuk serangan konvensional (sebagai uji kewajaran objektif).

Namun, kepastian hasil itu sendiri tidak diperlukan, terutama mengingat kesulitan memperkirakan kerugian tambahan sebelumnya. Hal ini sampai batas tertentu menyentuh ketidakpastian yang melekat pada penggunaan QIT. Prinsip-prinsip kehati-hatian tersebut konsisten dengan prinsip-prinsip lain yang dianut oleh Manual Hukum Konflik Internasional, seperti kewajiban negara-negara yang berperang untuk selalu berhati-hati selama permusuhan untuk menghindari kerugian terhadap golongan objek yang dilindungi (Aturan 114), persyaratan untuk memverifikasi target sebisa mungkin untuk menghindari kerugian terhadap golongan objek yang dilindungi (Aturan 115) serta aturan-aturan lebih lanjut yang mewajibkan pemilihan sarana dan metode serangan siber yang menghormati prinsip-prinsip dan proporsionalitas yang serupa (Aturan 117).

Aturan 118 menetapkan aturan di mana, jika terdapat kelas serangan siber yang setara untuk memperoleh keuntungan militer serupa, Negara-negara harus memilih tindakan (serangan siber) yang meminimalkan kerugian dan bahaya terhadap kelas objek yang dilindungi. Aturan 121 lebih lanjut menegaskan kembali prinsip-prinsip kehati-hatian tersebut, yang mengharuskan Negara-negara untuk mengambil tindakan pencegahan yang diperlukan untuk menghindari kerugian atau bahaya terhadap kelas yang dilindungi dari serangan siber (berdasarkan Pasal 58(c) Protokol Tambahan I dan perlindungan terhadap bahaya operasi militer). Kemampuan canggih QIT tidak menciptakan pengecualian terhadap aturan ini. Pihak-pihak yang berperang, seperti Negara A dalam Skenario kita di atas, tetap harus melakukan penilaian proporsionalitas untuk menentukan apakah kerusakan tambahan dapat dibenarkan. Kecepatan, kerahasiaan, atau kompleksitas serangan yang ditingkatkan oleh QIT tidak membebaskan Negara-negara dari uji keseimbangan ini.

Pengkhianatan dan Penipuan

Sejumlah aturan mengatur larangan terhadap pengkhianatan, di mana dilarang membunuh atau melukai lawan dengan menggunakan pengkhianatan (Aturan 122), misalnya melukai kombatan yang menyerah atau akan menyerah setelah menerima penyerahan mereka. Konsep dasarnya mengacu pada gagasan pengkhianatan yang diatur dalam Pasal 37(1) Protokol Tambahan I. Aturan pengkhianatan memiliki empat unsur: (i) mengundang kepercayaan lawan, (ii) niat untuk mengkhianati kepercayaan tersebut, (iii) perlindungan khusus yang diberikan dalam hukum internasional, dan (iv) kematian atau cedera lawan.

Manual ini mempertimbangkan berbagai pandangan mengenai apakah Aturan tersebut dapat mencakup sistem siber, seperti ketika Negara-negara menyetujui sistem pemantauan komputasi dan satu Negara melakukan pelanggaran, atau mekanisme otentikasi yang menipu digunakan oleh satu Negara. Pengkhianatan dibedakan dari tipu daya siber, yang sah, dan tidak berlaku untuk penghancuran properti. Namun hal ini berkaitan (Aturan 124) dengan penggunaan indikator musuh yang tidak tepat. Meskipun kami tidak fokus pada hal ini dalam artikel ini, ada pertimbangan teori permainan yang menarik yang muncul sehubungan dengan Skenario 2 kami di mana Negara-negara berbagi sumber daya yang saling terkait dan dapat memberi sinyal keputusan mereka untuk berkomitmen pada strategi tertentu.

7.11 PERBANDINGAN DENGAN HUKUM TELEKOMUNIKASI

Uni Telekomunikasi Internasional

Salah satu bidang minat terakhir dari Manual yang kami sebutkan adalah antara komunikasi kuantum dan hukum telekomunikasi internasional. Sebagian besar Negara adalah pihak dalam instrumen hukum internasional yang mengatur regulasi telekomunikasi internasional, contoh utamanya adalah rezim perjanjian yang ditetapkan dalam Uni Telekomunikasi Internasional (badan PBB yang mengatur telekomunikasi internasional). Sebagai subbagian dari hukum internasional, hukum telekomunikasi internasional mencakup penyediaan layanan dan infrastruktur telekomunikasi dan karenanya memainkan peran sentral dalam memfasilitasi operasi siber oleh Negara-negara secara global.

Rezim ini relevan baik sebagai titik perbandingan dengan proposal komunikasi kuantum dan internet kuantum maupun sebagai model tentang bagaimana, jika internet kuantum atau yang serupa didirikan di antara Negara-negara, infrastruktur jaringan kuantum tersebut dapat diatur. Penting juga untuk memeriksa sejauh mana rezim ITU mungkin sudah mencakup sistem QIT. ITU telah memulai serangkaian inisiatif pengembangan standar yang berkaitan dengan protokol QKD, yang meliputi persyaratan fungsional, arsitektur fungsional, manajemen kunci dan kontrol, dengan pembelajaran tambahan di bidang kriptografi pasca-kuantum juga dipertimbangkan.

Sumber Hukum dan Kewajiban Negara

Sumber utama prinsip yurisprudensi diatur dalam Konstitusi ITU dan serangkaian Peraturan Telekomunikasi Internasional. Telekomunikasi didefinisikan sebagai setiap transmisi, emisi, atau penerimaan tanda, sinyal, tulisan, gambar, dan suara atau informasi apa pun melalui kawat, radio, optik, atau sistem elektromagnetik lainnya. Definisi ini dianggap netral terhadap teknologi, sehingga secara wajar dapat dianggap mencakup komunikasi kuantum dan metode komunikasi non-klasik dalam cakupannya. Komunikasi internasional sebagaimana tercantum dalam Manual menyangkut transmisi data melintasi perbatasan negara dan melalui wilayah ekstrateritorial, sedangkan layanan telekomunikasi internasional adalah penyediaan kemampuan telekomunikasi antar negara.

Konstitusi ITU menetapkan sejumlah prinsip, termasuk asumsi tentang kerahasiaan komunikasi korespondensi internasional (Pasal 37(1)). Aturan 61 dari Manual, berdasarkan Pasal 38 Konstitusi ITU, menetapkan prinsip bahwa Negara harus mengambil langkah-langkah untuk melindungi pembentukan infrastruktur telekomunikasi internasional yang diperlukan untuk telekomunikasi yang cepat dan tanpa gangguan. Ini termasuk memelihara infrastruktur siber suatu Negara yang didirikan untuk tujuan ini. Negara dianggap memiliki kewajiban perilaku yang setara dengan kewajiban 'upaya terbaik', sehingga tunduk pada kewajaran dan kelayakan. Ini termasuk kewajiban untuk menjaga pengamanan operasional dan memastikan data dapat ditransmisikan secara andal dan efisien.

Kedaulatan dan Telekomunikasi

Sifat utama kedaulatan Negara diakui dalam konstitusi ITU (Pasal 35 dan 34(2)). Negara-negara mempertahankan hak prerogatif kedaulatan untuk menangguhkan komunikasi siber internasional di wilayah mereka (dan harus memberi tahu Negara-negara lain tentang hal ini) dan juga dapat menghentikan transmisi komunikasi siber pribadi yang bertentangan dengan hukum domestik (Aturan 2). Konstitusi ITU dan Aturan 63 menetapkan prinsip-prinsip di mana Negara-negara tidak boleh mengganggu frekuensi elektromagnetik (radio) yang dilindungi. Kewajiban Negara dimodifikasi selama konflik bersenjata (suatu bentuk *lex specialis*) di mana misalnya pengacauan atau gangguan lain dapat dianggap sah dalam keadaan tertentu. Berdasarkan Aturan 64, Negara-negara mempertahankan kebebasan penuh terkait instalasi radio militer mereka. Meskipun khusus untuk spektrum elektromagnetik, aturan-aturan tersebut memberikan dasar untuk pengembangan yurisprudensi untuk komunikasi kuantum. Selain itu, kerangka kerja ITU berfungsi sebagai contoh jenis instrumen multilateral yang dapat dengan mudah diadaptasi untuk tata kelola penggunaan QIT oleh Negara-negara.

7.12 INTEGRASI QIT DALAM HUKUM INTERNASIONAL PUBLIK

Pemeriksaan kami yang disajikan dalam bagian ini menunjukkan bahwa integrasi teknologi informasi kuantum (QIT) ke dalam hukum internasional publik merupakan perluasan yang penting, tetapi tidak destabilisasi, dari yurisprudensi siber yang ada. Meskipun QIT memperkenalkan perbedaan teknis dan konseptual dari sistem informasi klasik, banyak prinsip dasar hukum internasional terutama yang tercermin dalam Manual tetap dapat diadaptasi ke konteks yang muncul ini. Oleh karena itu, diskusi ini mengarah pada evolusi bertahap interpretasi hukum daripada kebutuhan untuk rekonstruksi doktrin secara menyeluruh.

Kontribusi analitis utama dari bagian ini adalah pengembangan taksonomi strategis klasik-kuantum yang membedakan interaksi antara sistem klasik dan kuantum klasik-ke-klasik, klasik-ke-kuantum, kuantum-ke-klasik, dan kuantum-ke-kuantum. Kerangka kerja ini menyediakan cara terstruktur untuk menggambarkan aktivitas Negara di seluruh infrastruktur hibrida dan mengklarifikasi bahwa sebagian besar operasi kuantum yang dapat diprediksi, setidaknya dalam jangka pendek, akan tetap tertanam dalam sistem klasik. Dengan demikian, hal ini memungkinkan penerapan penalaran hukum yang telah mapan mengenai operasi siber ke dalam konteks kuantum, sambil tetap memungkinkan kasus-kasus di mana sifat-sifat khas sistem kuantum seperti keterikatan atau dekoherensi memerlukan interpretasi yang lebih halus.

Dalam bagian ini, kami juga telah meneliti bagaimana QIT menantang asumsi-asumsi tertentu yang tersirat dalam hukum internasional tentang kontrol, sebagian akibat, dan pengetahuan. Sistem kuantum pada dasarnya bersifat probabilistik dan non-deterministik, yang menimbulkan pertanyaan tentang bagaimana doktrin hukum yang didasarkan pada kemampuan untuk meramalkan atau niat dapat diterapkan. Namun, seperti yang kami catat di atas, masalah-masalah ini tidak membuat doktrin yang ada menjadi tidak berlaku. Sebaliknya, mereka mengundang reinterpretasi sederhana tentang kontrol dan tanggung jawab. Misalnya, dalam jaringan berbasis keterikatan, yurisdiksi mungkin lebih dipahami melalui konsep lokus kendali yaitu, kapasitas praktis suatu Negara untuk memengaruhi perilaku sistem kuantum daripada gagasan kedaulatan yang bersifat teritorial semata.

Pendekatan kami tetap konsisten dengan prinsip-prinsip umum tanggung jawab negara dan uji tuntas, meskipun diterapkan pada substrat teknis yang lebih kompleks. Penggunaan teori permainan kuantum untuk mengilustrasikan interaksi strategis menambahkan dimensi lebih lanjut pada pemeriksaan konsekuensi strategis dari QIT. Kerangka kerja pengambilan keputusan kuantum menunjukkan bahwa sumber daya kuantum bersama dapat mengubah insentif untuk kerja sama atau pembelotan, yang dalam beberapa kasus mengarah pada keseimbangan yang lebih stabil atau transparan antar negara. Model-model ini bersifat ilustratif daripada prediktif, tetapi menunjukkan bahwa konsep-konsep perilaku rasional dan pencegahan timbal balik yang telah mapan dapat diadaptasi ke konteks kuantum tanpa meninggalkan teori strategis atau prinsip hukum yang ada.

Pemeriksaan kami juga menemukan bahwa kemampuan informasi kuantum cenderung meningkatkan, daripada menggulingkan, struktur hukum internasional yang mengatur

penggunaan kekuatan, spionase, dan kedaulatan. Komputasi kuantum dapat menyediakan cara baru untuk dekripsi atau simulasi, dan komunikasi kuantum dapat memperkuat keamanan jaringan negara, tetapi aktivitas ini tetap tunduk pada perbedaan yang sudah dikenal antara spionase yang sah, intervensi yang dilarang, dan penggunaan kekuatan. Demikian pula, meskipun teknologi kuantum dapat memperkuat asimetri informasi antar Negara, teknologi ini tidak memperkenalkan bentuk kekuasaan yang berada di luar jangkauan konseptual norma-norma yang ada. Fokus hukum internasional pada dampak bukan pada teknologi spesifik membuatnya mampu mengakomodasi perkembangan tersebut.

Dari perspektif tata kelola, QIT memiliki banyak karakteristik yang sama dengan teknologi penggunaan ganda sebelumnya. Oleh karena itu, mekanisme yang ada untuk pengendalian dan transparansi teknologi seperti yang dikembangkan untuk kemampuan nuklir dan siber tingkat lanjut menawarkan templat untuk mengelola risiko kuantum. Sebagaimana terlihat melalui perbandingan dengan hukum telekomunikasi internasional, struktur kelembagaan yang ada, dengan adaptasi, dapat berfungsi untuk mengkoordinasikan jaringan dan standar komunikasi kuantum yang muncul.

Secara keseluruhan, meskipun QIT membawa kemungkinan dan tantangan teknis baru, kerangka hukum internasional yang ada menyediakan kerangka kerja yang cukup fleksibel untuk mengatasinya. Fitur khas sistem kuantum stokastisitas, superposisi, dan keterikatan memperumit penerapan prinsip-prinsip yang telah mapan seperti kedaulatan dan uji tuntas, tetapi tidak melemahkannya. Generalitas hukum internasional, ketergantungannya pada definisi fungsional, dan penekanannya pada efek daripada mekanisme semuanya mendukung keberlanjutan. Oleh karena itu, lintasan respons hukum kemungkinan besar adalah penyempurnaan interpretatif daripada perpecahan doktrinal, karena Negara dan para sarjana secara progresif mengklarifikasi bagaimana teknologi kuantum sesuai dengan struktur hukum internasional publik yang abadi.

7.13 KESIMPULAN

Teknologi kuantum muncul sebagai kemampuan strategis dan domain yang menimbulkan pertanyaan tata kelola dan interpretasi yang khas bagi hukum internasional. Karakteristik uniknya menciptakan modalitas baru pengendalian dan komunikasi informasi yang dapat memengaruhi perilaku Negara baik dalam masa damai maupun konflik. Namun, seperti yang disarankan oleh pemeriksaan sebelumnya, perkembangan ini tidak secara fundamental menggantikan arsitektur hukum yang sudah berlaku untuk teknologi informasi. Sebaliknya, QIT memperluas cakupan kerangka kerja yang ada, mengundang interpretasi yang lebih bernuansa terhadap prinsip-prinsip seperti kedaulatan, yurisdiksi, uji tuntas, dan penggunaan kekuatan.

Diskusi kita telah menunjukkan bahwa hukum internasional kemungkinan memiliki elastisitas konseptual yang cukup untuk mengakomodasi tantangan yang ditimbulkan oleh QIT. Sebagian besar aplikasi komputasi, komunikasi, dan penginderaan kuantum yang dapat diprediksi akan tetap tertanam dalam infrastruktur klasik, yang berarti bahwa sebagian besar aktivitas Negara yang melibatkan QIT masih dapat dinilai melalui doktrin hukum siber yang

telah mapan. Jika diperlukan penyempurnaan seperti dalam menentukan tanggung jawab atas tindakan dalam sistem yang saling terkait atau mendefinisikan kendali dalam lingkungan probabilistik hal ini dapat dicapai melalui interpretasi bertahap daripada melalui perombakan doktrin. Kemampuan adaptasi hukum internasional terletak pada fokusnya pada dampak perilaku Negara daripada mekanisme yang menghasilkan dampak tersebut, sehingga membuatnya tahan terhadap evolusi teknologi.

Pada saat yang sama, kemampuan teknis QIT menciptakan pola interaksi strategis yang baru. Komputasi kuantum pada prinsipnya dapat memungkinkan dekripsi informasi yang secara klasik aman; komunikasi kuantum dapat membuat jaringan tertentu efektif tahan terhadap manipulasi; dan penginderaan kuantum dapat membentuk kembali keseimbangan informasi kekuatan antar Negara. Kemampuan ini menggambarkan bagaimana asimetri informasi, bukan kapasitas kinetik, dapat semakin menentukan keunggulan strategis. Hal ini juga memperkuat kebutuhan untuk mempertimbangkan bagaimana prinsip-prinsip yang ada yang mengatur spionase, intervensi, dan proporsionalitas berlaku dalam konteks di mana sebagian akibat dan pengetahuan bersifat probabilistik daripada deterministik.

Meskipun QIT masih dalam tahap pengembangan, potensi penggunaan gandanya telah melibatkan rezim kontrol ekspor dan non-proliferasi yang ada. Mekanisme ini menyediakan antarmuka hukum langsung antara pembelajaran kuantum dan tata kelola internasional, membatasi transfer teknologi dan membentuk distribusi kemampuan global. Seiring dengan kematangan teknologi, instrumen serupa dapat menawarkan dasar untuk pengawasan internasional yang lebih terkoordinasi. Model tata kelola di masa depan dapat mencakup perjanjian multilateral yang menetapkan standar untuk kontrol ekspor QIT, membatasi operasi siber ofensif yang ditingkatkan kuantum, atau mempromosikan transparansi dalam aplikasi penginderaan kuantum. Badan pengatur regional atau global dapat mengawasi penyebaran jaringan komunikasi berbasis keterikatan, dengan mengambil pelajaran dari preseden kelembagaan hukum telekomunikasi internasional. Rezim verifikasi yang disesuaikan dengan QIT seperti yang mengaudit jaringan distribusi kunci kuantum atau fasilitas komputasi skala besar dapat lebih memperkuat kepercayaan dan akuntabilitas antar Negara.

Singkatnya, QIT memperkenalkan cara-cara teknis baru yang melaluinya perilaku strategis yang sudah dikenal dilakukan, tetapi tampaknya belum memerlukan cabang hukum internasional yang terpisah. Tugas utamanya bersifat interpretatif: untuk memastikan bahwa prinsip-prinsip yang ada berkembang seiring dengan kemampuan teknologi. Dalam hal ini, tata kelola teknologi kuantum merupakan contoh kemampuan berkelanjutan hukum internasional publik untuk beradaptasi dengan perubahan ilmiah dan teknologi tanpa kehilangan koherensi atau kekuatan normatifnya.

Tabel 8.6 Perbandingan Definisi dari Glosarium Manual Tallinn dalam Konteks Klasik dan Kuantum. Tabel ini menyoroti perbedaan dan persamaan antara konsep informasi klasik dan kuantum.

Definisi	**Klasik**	**Kuantum**

Infrastruktur siber	Termasuk perangkat keras klasik seperti server, perangkat penyimpanan, dan jaringan komunikasi.	Mencakup perangkat keras khusus kuantum seperti prosesor kuantum, perangkat komunikasi kuantum, dan infrastruktur klasik yang mendukungnya.
Ruang siber	Lingkungan yang dibentuk oleh komponen fisik dan non-fisik yang memungkinkan penyimpanan, modifikasi, dan pertukaran data menggunakan jaringan komputer klasik.	Meluas hingga mencakup jaringan kuantum dan lingkungan yang memungkinkan komunikasi berbasis keterikatan dan pemrosesan data kuantum.
Aktivitas siber	Setiap aktivitas yang menggunakan infrastruktur atau cara klasik untuk memengaruhi operasinya, seperti peretasan atau pelanggaran data.	Aktivitas yang melibatkan penggunaan sistem kuantum, seperti enkripsi yang ditingkatkan secara kuantum atau serangan berbasis kuantum pada sistem klasik.
Operasi siber	Penggunaan kemampuan siber klasik untuk mencapai tujuan di atau melalui dunia maya, seringkali melibatkan operasi ofensif atau defensif.	Memanfaatkan kemampuan kuantum untuk tujuan seperti komunikasi kuantum yang aman atau serangan berbasis algoritma kuantum pada enkripsi klasik.
Pengintaian siber	Penggunaan alat klasik untuk mengumpulkan informasi tentang sistem, jaringan, atau kemampuan, seperti pemindaian atau penambangan data.	Menggunakan teknik kuantum, seperti penginderaan yang ditingkatkan secara kuantum, untuk mendeteksi musuh atau memeriksa sistem dengan presisi yang lebih tinggi.
Sistem komputer	Perangkat klasik yang saling terhubung, termasuk sistem tujuan umum dan sistem khusus, yang terhubung melalui jaringan klasik.	Meliputi komputer kuantum, sistem penginderaan kuantum, dan simpul jaringan kuantum yang terintegrasi dengan sistem klasik.
Jaringan komputer	Infrastruktur perangkat klasik yang saling terhubung yang memungkinkan pertukaran data melalui media berkabel atau nirkabel.	Meluas ke jaringan komunikasi kuantum, memanfaatkan keterikatan dan teleportasi kuantum untuk pertukaran data yang aman.
Internet	Sistem global jaringan klasik yang saling terhubung menggunakan protokol standar untuk komunikasi dan perutean.	Menggabungkan konsep internet kuantum, memungkinkan komunikasi aman menggunakan protokol kuantum bersamaan dengan sistem perutean klasik.
Data	Elemen digital dasar yang diproses atau dihasilkan oleh komputer	Data kuantum yang direpresentasikan oleh qubit, disimpan dalam keadaan superposisi

	klasik, biasanya direpresentasikan dalam byte.	atau terikat, memerlukan pengukuran berulang untuk ekstraksi.
Pusat data	Fasilitas fisik yang menampung infrastruktur klasik untuk penyimpanan dan pemrosesan data, termasuk layanan cloud.	Termasuk pusat data kuantum untuk menyimpan dan memproses informasi kuantum bersamaan dengan infrastruktur data klasik.
Perang elektronik	Penggunaan energi elektromagnetik untuk mengeksploitasi atau mengganggu sistem komunikasi dan penginderaan klasik.	Dapat melibatkan penginderaan kuantum untuk mendeteksi emisi elektromagnetik atau serangan kuantum yang menargetkan sistem klasik.
Serangan siber	Operasi ofensif atau defensif yang menyebabkan cedera, kehancuran, atau kerusakan menggunakan cara siber klasik.	Gangguan berbasis kuantum yang menargetkan sistem klasik atau kuantum, seperti induksi dekoherensi atau intersepsi komunikasi kuantum.
Spionase siber	Metode klasik untuk memperoleh informasi secara diam-diam, seperti peretasan atau penyadapan komunikasi.	Spionase yang ditingkatkan secara kuantum menggunakan penginderaan kuantum atau mengeksploitasi kelemahan dalam protokol komunikasi kuantum.

DAFTAR PUSTAKA

Abdikhakimov, I. (2025). QUANTUM TECHNOLOGIES AND HUMAN RIGHTS UNDER INTERNATIONAL LAW. *Elita. uz-Elektron Ilmiy Jurnal*, *3*(2), 590-597.

ABDURAMANI, E., & IMERI, F. (2025). GOVERNING QUANTUM SUPREMACY: ETHICAL CHALLENGES AND POLICY FRAMEWORKS. *Journal of Natural Sciences and Mathematics of UT*, *10*(19-20), 349-357.

Aboy, M., Compagnucci, M. C., & Minssen, T. (2026). Quantum Technology Governance: Legal and Regulatory Perspectives. In *Quantum Technology Governance I: Law and Regulation* (pp. 1-10). Singapore: Springer Nature Singapore.

Atladóttir, D., Roch, N., Leese, M., & Zimmermann, V. (2025). A quantum of responsibility? A comparison of national quantum governance frameworks and expert views. *Digital Society*, *4*(2), 54.

Bagianikian, J. (2020). The Legal Frontier: Understanding Regulations for AI, Quantum Computing, and Blockchain. *International Journal of Advanced Engineering Technologies and Innovations*, *1*(1), 137-156.

Baitulmal, A., & Adem, N. (2023). Why should and how can quantum technologies be leveraged at national levels?. *IET Quantum Communication*, *4*(2), 96-101.

Balarabe, K. (2025). Quantum computing and the law: Navigating the legal implications of a quantum leap. *European Journal of Risk Regulation*, *16*(2), 794-813.

Davis, P. A. E., Aboy, M., Bygrave, L. A., Minssen, T., Gasser, U., & Compagnucci, M. C. (2026). EU cybersecurity regulation in the quantum age. In *Quantum Technology Governance I: Law and Regulation* (pp. 149-179). Singapore: Springer Nature Singapore.

DeRose, K. (2023). Establishing the legal framework to regulate quantum computing technology. *Catholic University Journal of Law and Technology*, *31*(2), 145-172.

Ghazaleh, S. A., Alabady, H. S., Al-Khaldi, I., & Abu-Moghli, M. A. M. (2025). Securing the Digital Future: A Proactive Legal Framework for Quantum Computing Challenges. *Journal of Cultural Analysis and Social Change*, 4843-4850.

Girasa, R., & Scalabrini, G. J. (2022). *Regulation of innovative technologies: Blockchain, artificial intelligence and quantum computing*. Springer Nature.

Habib Lantyer, V. (2025). Quantum Computing and Artificial Intelligence: Regulation, Potentialities, Challenges, and the Global Landscape. *Potentialities, Challenges, and the Global Landscape (April 15, 2025)*.

Herian, R. (2025). As much as faith: A speculation on quantum computing with fiduciary law in public governance. In *Public governance and emerging technologies: Values, trust, and regulatory compliance* (pp. 217-238). Cham: Springer Nature Switzerland.

Jenet, A. (2020). Standards4quantum: making quantum technology ready for industry. Putting science into standards. In *Putting science into standards (May 1, 2020). JRC conference and workshop report*.

Koellner, E. (2024). Navigating Legal Challenges in the Age of Disruptive Technologies: AI, Quantum Computing, and Intellectual Property in Space. *Quantum Computing, and Intellectual Property in Space (August 15, 2024)*.

Kop, M., Aboy, M., De Jong, E., Gasser, U., Minssen, T., Cohen, I. G., ... & Laflamme, R. (2023). Towards responsible quantum technology. *Harvard Berkman Klein Center for Internet & Society Research Publication Series*, *1*.

Lenarczyk, G., Minssen, T., & Aboy, M. (2026). IP in superposition: patents, trade secrets, and open innovation in quantum information technology. In *Quantum Technology Governance I: Law and Regulation* (pp. 99-123). Singapore: Springer Nature Singapore.

Leopold, H. (2026). Governance for Quantum Technologies: A Necessity for Responsible Technology Development. In *DefenceTech Governance* (pp. 203-231). Springer, Cham.

Lloyd-Jones, S., & Manwaring, K. (2024). Quantum Resilience in the Australian National Security Legislative Framework.

Lukoseviciene, A. (2025). Regulating quantum computers: insights into early patterns and trends in academic regulatory conversations on the 'quantum revolution'. *Law, Innovation and Technology*, *17*(1), 241-270.

Marchant, G. E., Bazzi, R., Bowman, D., Connor, J., Davis III, R. A., Kang, E., ... & Marchant, M. (2024). Learning from emerging technology governance for guiding quantum technology. *Arizona State University Sandra Day O'Connor College of Law Paper*, (4923230), 24-33.

Neuwirth, R. J. (2025). A Future European Union'Quantum Act'? Critical Lessons from the Global AI Governance Debate. *Critical Lessons from the Global AI Governance Debate (August 01, 2025)*.

Nguyen, A. (2025). Export controls as innovation marketing?: Sociotechnical imaginaries in the ringfencing of quantum technologies. *Law, Technology and Humans*, *7*(1), 68-83.

Nousiainen, K., Martinez Aponte, E., & Waber, B. N. (2026). Navigating the Quantum Frontier: Emerging Legal and Developmental Challenges. *Law and Development Review*, (0).

Paglieri, L., Bonomi Savignon, A., Scalabrini, F., & Costumato, L. (2025). Navigating the quantum frontier: examining government strategy to the next technological revolution. *Transforming Government: People, Process and Policy*, *19*(4), 700-724.

Perrier, E., & Aboy, M. (2026). Quantum Information Technology and The Law. In *Quantum Technology Governance I: Law and Regulation* (pp. 11-98). Singapore: Springer Nature Singapore.

Rehman, A. (2026). Governing the Quantum Frontier: Regulatory Challenges and Policy Frameworks for Responsible Quantum Computing. *Journal of Emerging Technology and Digital Transformation*, *5*(2), 107-113.

Saurabh, K. (2025). Towards quantum ethics, sustainability and governance agenda. *Information Discovery and Delivery*.

Smith, H. L., Aboy, M., Davis, P. A. E., & Minssen, T. (2025). Quantum Governance in the Making: Why Standards Matter. *Available at SSRN 5853722*.

Suter, V., Pöhlmann, G., Ma, C., & Meckel, M. (2026). Quantum technologies and geopolitics: comparing parliamentary rhetoric. *EPJ Quantum Technology*, *13*(1), 10.

Ten Holter, C. (2023). *Towards a methodology for prospective governance in quantum computing technologies* (Doctoral dissertation, University of Oxford).

Thiyagarajan, N., Loganathan, V., Vishnulakshmi, K., & Raj, V. (2026). Legal and regulatory frameworks for secure quantum blockchain in healthcare. In *AI-enabled Sustainable Healthcare* (pp. 225-246). Academic Press.

Umbrello, S., Seskir, Z. C., & Vermaas, P. E. (2024). Communities of quantum technologies: Stakeholder identification, legitimation and interaction. *International Journal of Quantum Information*, *22*(07), 2450012.

Vogiatzoglou, P., & van Hoboken, J. (2025). The EU's Digital Sovereignty and Quantum Technologies: To What End?. *Forthcoming in Law, Innovation and Technology*, *18*(2).

Zafar, A. (2025). Quantum computing in finance: Regulatory readiness, legal gaps, and the future of secure tech innovation. *European Journal of Risk Regulation*, 1-32.

TATA KELOLA TEKNOLOGI DI BIDANG HUKUM DAN REGULASI

Dr. Ir. Agus Wibowo, M.Kom, M.Si, MM.

BIO DATA PENULIS

Penulis memiliki berbagai disiplin ilmu yang diperoleh dari Universitas Diponegoro (UNDIP) Semarang. dan dari Universitas Kristen Satya Wacana (UKSW) Salatiga. Disiplin ilmu itu antara lain teknik elektro, komputer, manajemen, ilmu sosiologi dan ilmu hukum. Penulis memiliki pengalaman kerja pada industri elektronik dan sertifikasi keahlian dalam bidang Jaringan Internet, Telekomunikasi, Artificial Intelligence, Internet Of Things (IoT), Augmented Reality (AR), Technopreneurship, Internet Marketing dan bidang pengolahan dan analisa data (komputer statistik), Ilmu Perpajakan.

Penulis adalah pendiri dari Universitas Sains dan Teknologi Komputer (Universitas STEKOM) dan juga seorang dosen yang memiliki Jabatan Fungsional Akademik Lektor Kepala (Associate Professor) yang telah menghasilkan puluhan Buku Ajar ber ISBN, HAKI dari beberapa karya cipta dan Hak Paten pada produk IPTEK. Sejak tahun 2023 penulis tercatat sebagai Dosen luar biasa di Fakultas Ekonomi & Bisnis (FEB) Universitas Diponegoro Semarang. Penulis juga terlibat dalam berbagai organisasi profesi dan industri yang terkait dengan dunia usaha dan industri, khususnya dalam pengembangan sumber daya manusia yang unggul untuk memenuhi kebutuhan dunia kerja secara nyata.

YAYASAN PRIMA AGUS TEKNIK

PENERBIT :
YAYASAN PRIMA AGUS TEKNIK
Jl. Majapahit No. 605 Semarang
Telp. (024) 6723456. Fax. 024-6710144
Email : penerbit_ypat@stekom.ac.id