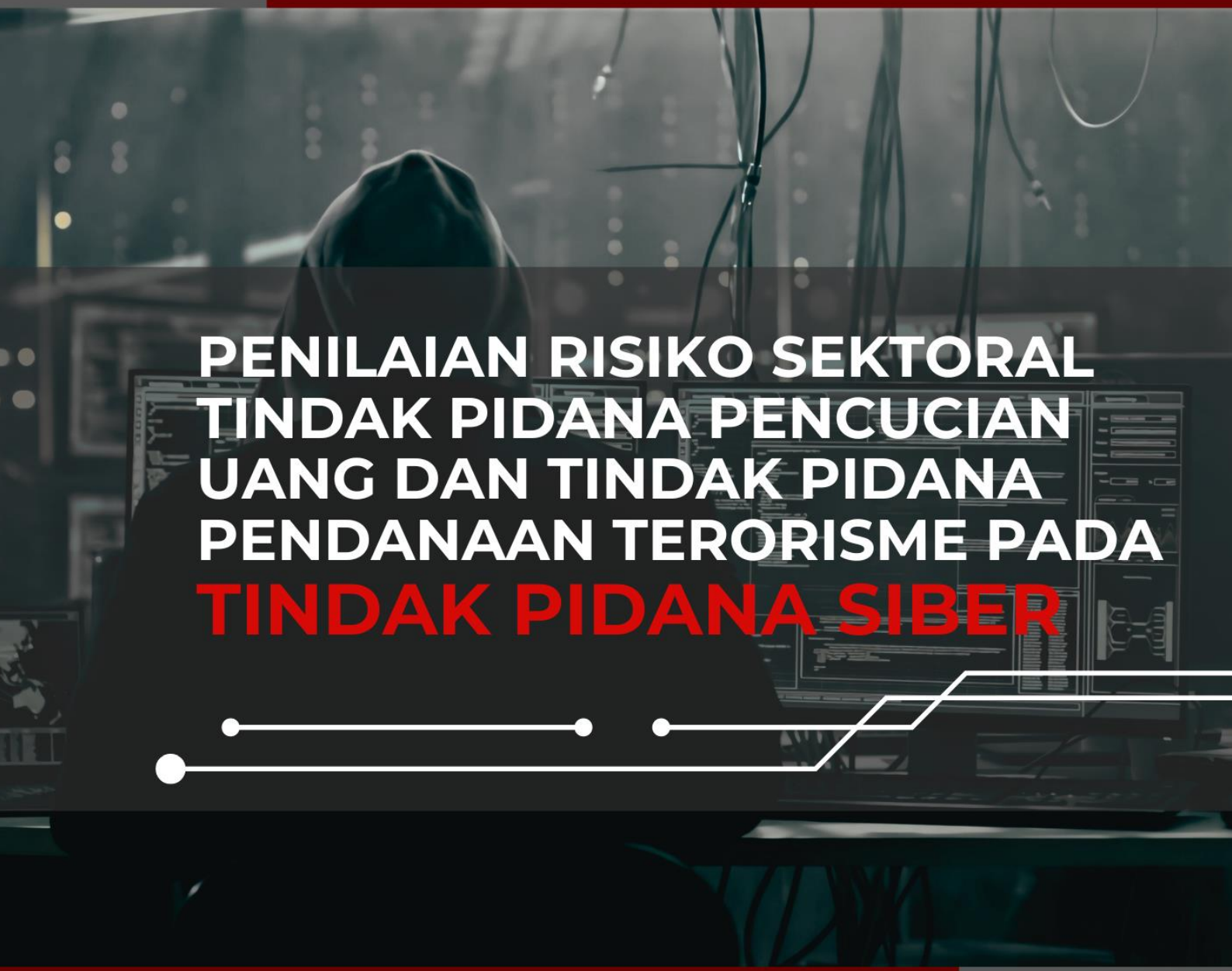
PUSAT PELAPORAN DAN ANALISIS TRANSAKSI KEUANGAN
PPATK

FATF INDONESIA
OFFICIAL 40TH MEMBER
SINCE OCTOBER 2023



PENILAIAN RISIKO SEKTORAL TINDAK PIDANA PENCUCIAN UANG DAN TINDAK PIDANA PENDANAAN TERORISME PADA TINDAK PIDANA SIBER

TAHUN 2024

KEMENTERIAN KOMUNIKASI DAN DIGITAL

KEMENTERIAN PERDAGANGAN REPUBLIK INDONESIA

PENILAIAN RISIKO SEKTORAL
TINDAK PIDANA PENCUCIAN UANG
DAN TINDAK PIDANA PENDANAAN TERORISME
PADA TINDAK PIDANA SIBER TAHUN 2024

ISBN	:	
Koordinator Penulis	:	Vidyata A. A.
Ukuran Buku	:	295 x 210 mm
Naskah	:	Penilaian Risiko Sektoral Tindak Pidana Pencucian Uang dan Tindak Pidana Pendanaan Terorisme Pada Tindak Pidana Siber Tahun 2024
Diterbitkan	:	Pusat Pelaporan dan Analisis Transaksi Keuangan

INFORMASI LEBIH LANJUT

Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK)

Indonesian Financial Transaction Reports and Analysis Center (INTRAC)

Jl. Ir. H Juanda No. 35 Jakarta 10120 Indonesia

Phone: (+6221) 3850455, 3853922

Fax: (+6221) 3856809 – 3856826

website: http://www.ppatk.go.id

TIM PENYUSUN

A. Pengarah

1. Ketua Kamar Pidana, Mahkamah Agung RI
2. Ketua Grup APUPPT, Otoritas Jasa Keuangan
3. Jaksa Agung Muda Pidana Khusus, Kejaksaan Agung RI
4. Direktur Tindak Pidana Terorisme dan Lintas Negara, Kejaksaan Agung RI
5. Direktur Tindak Pidana Ekonomi Khusus, Bareskrim POLRI
6. Direktur Tindak Pidana Siber, Bareskrim POLRI
7. Direktur Penyidikan, Densus 88 Anti Teror POLRI
8. Direktur Inteligen, Densus 88 Anti Teror POLRI
9. Direktur Keamanan Siber dan Sandi Pemerintah Pusat, Badan Siber dan Sandi Negara
10. Direktur Pengendalian Aplikasi Informatika, Kementerian Komunikasi dan Digital (d/h Direktur Pengendalian Aplikasi, Kementerian Komunikasi dan Informatika)
11. Direktur Strategi dan Kerja Sama Dalam Negeri, PPATK
12. Direktur Strategi dan Kerja Sama Internasional, PPATK
13. Direktur Pelaporan, PPATK
14. Direktur Pengawas Kepatuhan Penyedia Jasa Keuangan, PPATK
15. Direktur Analisis dan Pemeriksaan I, PPATK
16. Direktur Analisis dan Pemeriksaan II, PPATK
17. Direktur Analisis dan Pemeriksaan III, PPATK
18. Direktur Hukum dan Regulasi, PPATK
19. Kepala Pusat Pemberdayaan Kemitraan APU-PPT, PPATK
20. Kepala Departemen Kebijakan Sistem Pembayaran Bank Indonesia
21. Kepala Biro Pengawasan Perdagangan Berjangka Komoditi, Sistem Resi Gudang, dan Pasar Lelang Komoditas, Badan Pengawas Perdagangan Berjangka Komoditi
22. Kepala Biro Peraturan Perundang-Undangan dan Penindakan, Badan Pengawas Perdagangan Berjangka Komoditi

B. Tim Pelaksana

1. Perwakilan Mahkamah Agung
   1) R. Heru Wibowo Sukaten
   2) Dwi Sugiarto
2. Perwakilan Jaksa Agung Muda Pidana Khusus, Kejaksaan Agung RI
   1) Suyanto Reksasumarta
   2) Bagus Gede Mas Widipradnyana Arjaya
3. Perwakilan Direktorat Tindak Pidana Terorisme dan Lintas Negara, Kejaksaan Agung RI
   1) Erwin Indraputra
   2) Herry Wijayanto
4. Perwakilan Direktorat Tindak Pidana Siber, Bareskrim Polri
   1) I Made Redi Hartana
   2) Eko Yudha Prasetya
5. Perwakilan Direktorat Tindak Pidana Ekonomi Khusus, Bareskrim Polri
   1) Efrata Hamonangan Sinaga

2) Dwi Martono

6. Perwakilan Detasemen Khusus Anti Teror, Kepolisian Negara Republik Indonesia
   1) Daniel
   2) Jay Kesuma
   3) Sadewa Fradana Santoso
7. Perwakilan Direktorat Keamanan Siber dan Sandi Pemerintah Pusat, Badan Siber dan Sandi Negara
   1) Dony Harso
   2) Fredy Ramadani
8. Perwakilan Direktorat Pengendalian Aplikasi Informatika, Kementerian Komunikasi dan Digital (d/h Direktorat Pengendalian Aplikasi, Kementerian Komunikasi dan Informatika)
   1) Jelitha Suina Putri
   2) Ryan Abdisa Sukmadja
9. Perwakilan Otoritas Jasa Keuangan
   1) Rifki Arif Budianto
   2) Marshella Eka Ramdhania
10. Perwakilan Bank Indonesia
   1) Danarto Tri Sasongko
   2) Nabila Femiliana
11. Perwakilan Badan Pengawas Perdagangan Berjangka Komoditi, Kementerian Perdagangan
   1) Hary Lesmana
   2) Yovian Andri Prihandono
   3) Rio Ramadhani
12. Internal PPATK
   1) Diana Soraya Noor
   2) Patrick Irawan
   3) Tri Puji Raharjo
   4) Mardiansyah
   5) Vidyata A. A.
   6) Sheilla Yudiana
   7) Kristina Widhi P.
   8) Riana Rizka
   9) Dini Rahayu
   10) Aditya Akbar Apriyadi
   11) Jessie Octavillisia
   12) Ade Novita Rosseani
   13) Ibrahim Arifin
   14) Muhammad Afdal Yanuar
   15) Nelmy Pulungan
   16) Rusli Safrudin
   17) Dominicus Suseno
   18) Puri Widyaksari
   19) Damai Tri Putri
   20) Andi Emil Arya Hidayat
   21) Nur Sofia Arianti
   22) Didin Najmudin

RINGKASAN EKSEKUTIF

Tindak Pidana Siber (TP Siber) adalah salah satu jenis Tindak Pidana Asal (TPA) dari Tindak Pidana Pencucian Uang (TPPU). Insiden TP Siber cenderung meningkat dari tahun ke tahun baik di Indonesia maupun di dunia. Perkembangan ekonomi digital Indonesia yang tercatat sebagai yang tertinggi di Asia Tenggara juga menjadikan penanganan tindak pidana siber semakin penting.

Dalam rangka mitigasi risiko TPPU dan TPPT dari TP Siber di Indonesia, disusunlah penilaian risiko sectoral, untuk mengidentifikasi faktor-faktor risiko TP Siber sehingga dapat dilakukan mitigasi risiko secara efektif dan efisien. Dengan perkembangan teknologi, tindak pidana yang terjadi bisa saja memanfaatkan ruang siber, namun untuk ruang lingkup dalam kajian ini akan dibatasi TP Siber yang berdasarkan Undang-Undang Informasi dan Transaksi Elektronik (Undang-Undang Nomor 11 Tahun 2016 dan perubahan-perubahannya).

SRA TPPU dan TPPT dari TP Siber dimaksudkan untuk mengidentifikasi, menganalisis, mengevaluasi dan memitigasi risiko TPPU dan TPPT dari tindak pidana siber dengan mengidentifikasi jenis-jenis TP Siber yang berpotensi TPPU dan TPPT di Indonesia; dan mengidentifikasi dan menganalisis risiko TPPU dan TPPT dari TP Siber di Indonesia berdasarkan jenis tindak pidana siber, profil pelaku, sektor pihak pelapor, wilayah, tipologi, dan pola transaksi. Pedoman yang digunakan dalam penyusunan SRA TP Siber Tahun 2024 ini merujuk pada praktik terbaik internasional dari National Money Laundering and Terrorist Financing Assessment (FATF Guidance), Risk Assessment Support for Money Laundering/Terrorist Financing (World Bank) Review of the funds Strategy on Anti Money Laundering and Terrorist Financing (IMF), dan Terrorist Financing Risk Assessment Guidance.

Dengan menggunakan data selama periode Januari 2019 s.d. Maret 2024, yang bersumber dari bersumber dari statistik mengenai laporan transaksi keuangan mencurigakan, pelaksanaan pengawasan, pertukaran informasi FIU, hasil laporan intelijen keuangan, penyidikan, penuntutan dan putusan pengadilan, penilaian mandiri oleh ahli atau *expert* dari perwakilan pihak pelapor, pihak lembaga pengawas dan pengatur, lembaga intelijen keuangan (PPATK), dan lembaga penegak hukum, dilakukan penilaian risiko TPPU dan TPPT dari TP Siber. Pengumpulan data kualitatif dilakukan dengan penyampaian kuesioner kepada lembaga pengawas dan pengatur, lembaga penegak hukum, kementerian/lembaga terkait dan pihak

pelapor sebanyak 36 responden dengan rata-rata capaian tingkat respon (*response rate*) sebesar 94%. Selain kuesioner, dilakukan juga pengumpulan data melalui wawancara kepada 3 perwakilan lembaga pengawas dan pengatur, 4 perwakilan lembaga penegak hukum dan 2 kementerian/lembaga terkait perwakilan pihak pelapor untuk memperoleh pendalaman terhadap risiko TPPU dan TPPT dari TP Siber.

Temuan-temuan utama dari SRA TPPU dan TPPT dari TP Siber Tahun 2024 adalah sebagai berikut:

1. Berdasarkan hasil analisis dan evaluasi risiko sektoral dari TP Siber, perkembangan kejahatan siber saat ini terhadap risiko nasional perlu dipertimbangkan. Hal ini disebabkan pelaku kejahatan semakin memanfaatkan sarana siber atau teknologi canggih untuk melakukan pencucian uang yang berasal dari berbagai jenis tindak pidana. Putusan TPPU dari TP Siber masih rendah dibandingkan Tindak Pidana Asalnya sehingga penanganan TPPU dari TP Siber perlu ditingkatkan, terutama dari judi online.
2. Berdasarkan jenis TP Siber, penipuan dalam jaringan (online fraud) dan perjudian online (online gambling) dinilai berisiko tinggi TPPU.
3. Berdasarkan profil, pengusaha/wiraswasta dan pegawai swasta dinilai menjadi profil berisiko tinggi TPPU hasil TP Siber. Warga Negara Indonesia/WNI dinilai berisiko tinggi TPPU hasil TP Siber. Hasil TP Siber cenderung dilakukan pencucian uang oleh pelaku TP Siber sendiri.
4. Berdasarkan wilayah, DK Jakarta dinilai berisiko tinggi terjadi TPPU hasil TP Siber.
5. Berdasarkan sektor industri pihak pelapor, bank dinilai berisiko tinggi.
6. Berdasarkan tipologi TPPU, yang dinilai berisiko tinggi adalah penggunaan mata uang virtual dan perjudian *online*.
7. Berdasarkan pola transaksi, yang dinilai berisiko tinggi adalah transfer dan tarik/setor tunai.
8. Singapura, Amerika Serikat, Hong Kong, Republik Rakyat Tiongkok, India, dan Malaysia dinilai para responden sebagai negara-negara yang berpotensi menjadi sumber, tujuan, dan transit dana TPPU dari TP Siber.
9. Tingkat risiko TPPT belum dapat diukur dalam kajian ini karena keterbatasan data kasus. Namun dengan adanya kasus penipuan siber sebagai sumber dana TPPT di luar negeri, potensi tersebut perlu diwaspadai.

10. Penyalahgunaan teknologi keuangan (misalnya aset kripto) dan ruang siber dalam rangka komunikasi, propaganda, dan perekrutan telah nyata terjadi dan perlu diwaspadai aparat penegak hukum.

Selanjutnya, terdapat beberapa perkembangan lainnya yang dinilai oleh pihak pemangku kepentingan terkait dapat berpotensi akan digunakan secara masif di masa mendatang berdasarkan hasil pengamatan transaksi keuangan mencurigakan dan perkembangan penanganan perkara TPPU dan TPPT, antara lain:

1. Penyalahgunaan AI
2. Penyalahgunaan *e-wallet*
3. Penggunaan layanan percampuran koin/*coin mixer*
4. Pengiriman tautan/berkas yang berisi virus atau untuk percobaan mengambil alih data pengguna
5. Penggunaan *private wallet address*
6. Eksploitasi Web3 dan Aset Kripto

SAMBUTAN KEPALA PPATK

Assalamu'alaikum Warahmatullahi Wabarakatuh.

Puji syukur kita panjatkan kepada Allah SWT karena berkat rahmat dan hidayah-NYA, maka PPATK bersama *stakeholders* dalam rezim Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme (APU dan PPT) dapat menyelesaikan penyusunan laporan "Penilaian Risiko Sektoral Tindak Pidana Pencucian Uang dan Pendanaan Terorisme dari Tindak Pidana Siber Tahun 2024".

Tindak Pidana Siber menimbulkan kerugian finansial yang signifikan dan berdampak negatif terhadap pemerintahan, infrastruktur, dan industri, tidak hanya di Indonesia namun juga seluruh dunia. Efek tindak pidana siber juga dapat dirasakan individual, seperti pencurian identitas, peretasan akun, dan skema pembajakan surel (*e-mail compromise*). Pencegahan dan pemberantasan tindak pidana siber tidak hanya menjadi tugas aparat penegak hukum tetapi juga berbagai pemangku kepentingan. Salah satu langkah yang ditempuh PPATK adalah penyusunan penilaian risiko sektoral dalam rangka memahami risiko Tindak Pidana Pencucian Uang dan Tindak Pidana Pendanaan Terorisme dari Tindak Pidana Siber di Indonesia.

Untuk itu saya menyambut baik atas penyusunan Laporan Penilaian Risiko Sektoral Tindak Pidana Pencucian Uang dan Tindak Pidana Pendanaan Terorisme dari Tindak Pidana Siber tahun 2024 ini dan agar dapat segera ditindaklanjuti dengan langkah strategi dan mitigasi terhadap perkembangan risiko yang telah teridentifikasi oleh seluruh pihak pemangku kepentingan terkait.

Akhir kata, saya mengucapkan terima kasih dan penghargaan kepada semua pihak yang telah memberikan kontribusi terhadap penyusunan Laporan Penilaian Risiko Sektoral Tindak Pidana Pencucian Uang dan Tindak Pidana Pendanaan Terorisme dari Tindak Pidana Siber tahun 2024.

Semoga amal usaha kita diridai Allah SWT. Amin Ya Rabbal 'Alamin.

Wassalamu'alaikum Warahmatullahi Wabarakatuh.

Jakarta, Desember 2024

Kepala Pusat Pelaporan dan Analisis Transaksi Keuangan

Dr. Ivan Yustiavandana, S.H., LL.M.

DAFTAR SINGKATAN DAN ISTILAH

No	Singkatan/Istilah	Definisi
1	APU-PPT	Anti Pencucian Uang dan Pencegahan Pendanaan Terorisme
2	ASEAN	Association of Southeast Asian Nations/Organisasi Negara-Negara Asia Tenggara
3	BSSN	Badan Siber dan Sandi Negara
4	Dark Web	Konten World Wide Web yang ada di *darknet*, jaringan *overlay* yang menggunakan Internet tetapi memerlukan perangkat lunak tertentu, konfigurasi atau otorisasi untuk mengaksesnya.
5	FATF	Financial Action Task Force on Money Laundering
6	*Foreign Predicate Crime*	TPPU yang terjadi di luar negeri dan dilakukan pencucian uang di Indonesia
7	IMF	International Monetary Fund
8	Interpol	International Criminal Police Organization/Organisasi Polisi Kriminal Internasional
9	NRA	*National Risk Assessment*/Penilaian Risiko Nasional
10	POLRI	Kepolisian Republik Indonesia
11	*Ransomware*	Ransomware adalah sejenis program jahat, atau malware, yang mengancam korban dengan menghancurkan atau memblokir akses ke data atau sistem penting hingga tebusan dibayar
12	Robinopsnal Bareskrim POLRI	Biro Pembinaan dan Operasional, Badan Reserse Kriminal, Kepolisian Negara Republik Indonesia
13	SRA	*Sectoral Risk Assessment*/Penilaian Risiko Sektoral
14	TP	Tindak Pidana
15	TPA	Tindak Pidana Asal
16	TPPT	Tindak Pidana Pendanaan Terorisme
17	TPPU	Tindak Pidana Pencucian Uang
18	UU ITE	Undang-Undang Informasi dan Transaksi Elektronik
19	WNA	Warga Negara Asing
20	WNI	Warga Negara Indonesia

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

BAB I
PENDAHULUAN

1.1. LATAR BELAKANG

Siber menurut Kamus Besar Bahasa Indonesia (KBBI) berarti sistem komputer dan informasi, dunia maya, atau berhubungan dengan internet. Kejahatan siber adalah kejahatan yang melibatkan internet, sistem komputer, atau teknologi komputer. Dalam penjelasan atas Undang-Undang Republik Indonesia Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE) disebutkan bahwa[1]:

"... karakteristik virtualitas ruang siber memungkinkan konten ilegal seperti Informasi dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan, perjudian, penghinaan atau pencemaran nama baik, pemerasan dan/atau pengancaman, penyebaran berita bohong dan menyesatkan sehingga mengakibatkan kerugian konsumen dalam Transaksi Elektronik, serta perbuatan menyebarkan kebencian atau permusuhan berdasarkan suku, agama, ras, dan golongan, dan pengiriman ancaman kekerasan atau menakut-nakuti yang ditujukan secara pribadi dapat diakses, didistribusikan, ditransmisikan, disalin, disimpan untuk didiseminasi kembali dari mana saja dan kapan saja."

Pernyataan ini semakin relevan di tengah perkembangan teknologi yang saat ini semakin cepat. Perkembangan teknologi yang sangat cepat membantu masyarakat dalam memenuhi berbagai kebutuhannya, namun juga memiliki potensi risiko kejahatan seperti pencurian, penipuan, penyalahgunaan, dan kejahatan-kejahatan lainnya.

Di Indonesia sendiri, berdasarkan data Pusiknas POLRI pada tahun 2022, kejahatan siber naik signifikan (14 kali lipat) bila dibandingkan dengan periode yang sama di 2021. Pada tahun 2023, FATF merilis laporan *Illicit Financial Flows from Cyber-Enabled Fraud*. Dalam laporan tersebut, disebutkan bahwa penipuan siber (*cyber-enabled fraud*) merupakan kejahatan terorganisasi transnasional yang sedang berkembang. Menurut *2023 Interpol Global Crime Trend Summary Report*, terdapat peningkatan yang signifikan dalam kecanggihan dan volume

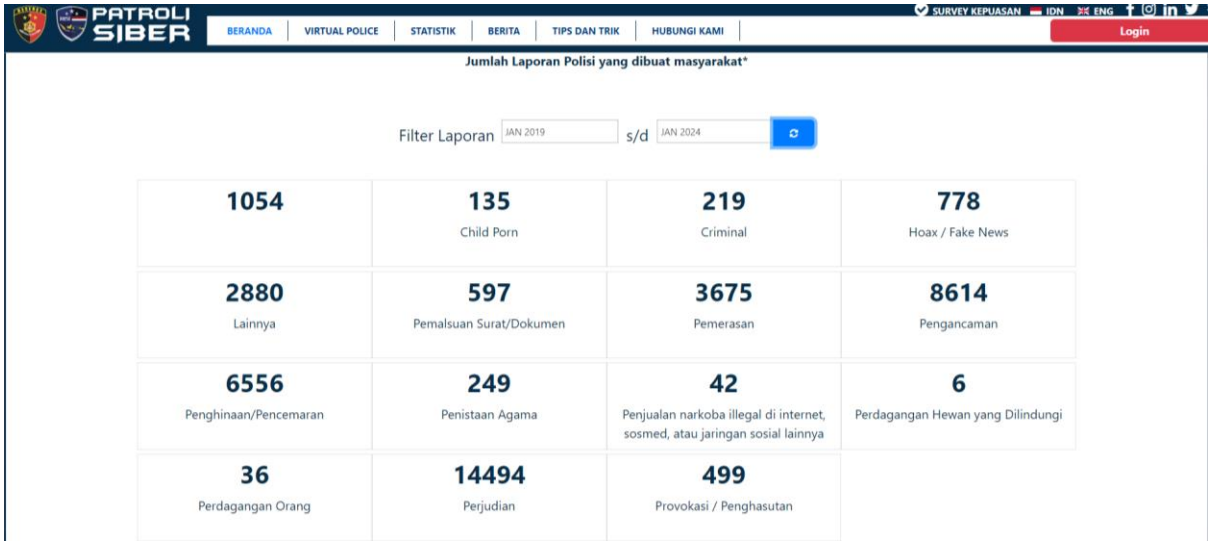
[1] Ketentuan terbaru atas UU ITE terkandung dalam Undang-Undang No. 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

serangan siber dan kejahatan yang dimungkinkan oleh siber (*cyber-enabled crime*), termasuk pelecehan seksual terhadap anak-anak dan penipuan keuangan. Penggunaan kejahatan sebagai layanan (*crime-as-a-service*)[2] mempunyai dampak khusus dalam perluasan kejahatan tersebut.

Gambar 1 Kejahatan Siber Meningkat Belasan Kali Lipat

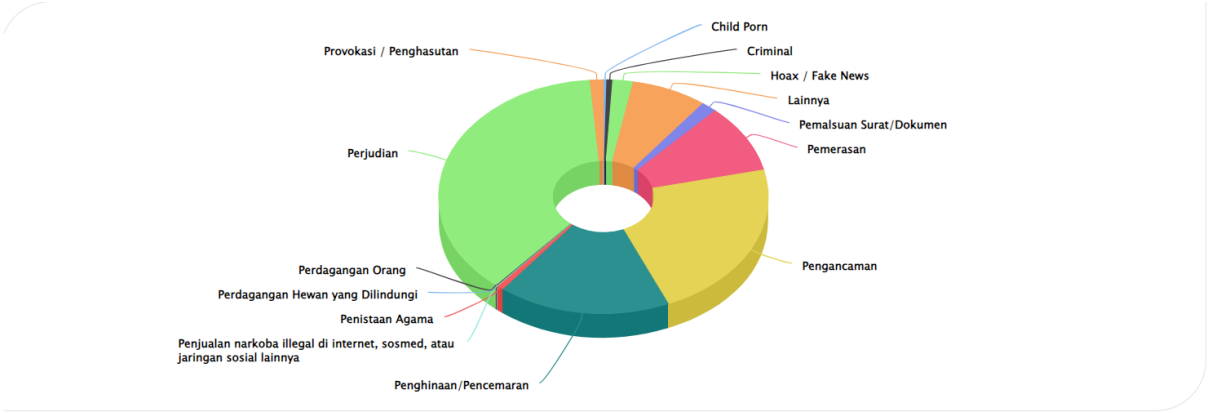
Sumber: https://pusiknas.polri.go.id/detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat

[2] *Crime-as-a-service* adalah layanan-layanan yang memungkinkan terjadinya kejahatan. Contoh *crime-as-a-service* antara lain jasa peretasan, penjualan data pribadi untuk membobol data keuangan, dan jasa pencucian uang.



Gambar 2 Statistik Jumlah Laporan Polisi yang Dibuat Masyarakat Terkait Tindak Pidana Siber

Sumber: Patrolisiber.id



Gambar 3 Diagram Pai Laporan Polisi yang Dibuat Masyarakat Terkait Tindak Pidana Siber

Sumber: Patrolisiber.id

Perkembangan ekonomi digital juga menjadikan penanganan tindak pidana siber semakin penting. Pada tahun 2022, nilai ekonomi digital Indonesia tercatat sebagai yang tertinggi di Asia Tenggara, yakni sebesar 77 miliar dolar AS, setara dengan 40% pangsa pasar ekonomi internet ASEAN. Keamanan siber juga menjadi salah satu pilar utama upaya pengembangan ekonomi digital Indonesia yang diharapkan dapat memperkuat kepercayaan masyarakat untuk berpartisipasi dalam ekonomi digital. Berdasarkan data Interpol Cyber

Assessment (Report 2021) selama periode Januari-September 2020 terdapat 2,7 juta serangan *ransomware* yang terdeteksi di negara-negara ASEAN. Indonesia sendiri berada di peringkat teratas dengan 1,3 juta kasus. Selain itu, kebocoran data akibat kejahatan siber juga berpotensi menimbulkan kerugian ekonomi dunia hingga USD 5 triliun pada tahun 2024. Dalam hal peningkatan keamanan siber ini, tidak hanya menjadi *concern* dari aparat penegak hukum tetapi juga regulator seperti Kementerian Komunikasi dan Informatika serta Badan Siber dan Sandi Negara.

Tindak pidana siber merupakan salah satu tindak pidana asal tindak pidana pencucian uang (TPPU) di Indonesia, di mana kejahatan siber termasuk dalam tindak pidana lain yang diancam dengan pidana penjara 4 (empat) tahun atau lebih. Dalam Penilaian Risiko Nasional (*National Risk Assessment*) pada tahun 2021, ditemukan bahwa penipuan, korupsi, transfer dana, narkotika dan informasi transaksi elekronik (ITE) atau siber merupakan jenis tindak pidana asal TPPU yang berkategori ancaman tinggi TPPU pada *foreign predicate crime* (TPPU yang terjadi di luar negeri dan dilakukan pencucian uang di Indonesia). Pada tahun 2022, PPATK telah menyusun *Penilaian Risiko Sektoral Tindak Pidana Pencucian Uang pada Tindak Pidana Penipuan Siber Tahun 2022*. Perkembangan kejahatan siber di Indonesia begitu pesat hingga Kepolisian RI (Polri) akan membentuk direktorat khusus untuk penanganan kejahatan siber di sembilan wilayah di Indonesia.

Dalam rangka mitigasi risiko TPPU dan TPPT dari kejahatan siber di Indonesia, salah satu upaya yang dapat dilakukan adalah penyusunan penilaian risiko sektoral, untuk mengidentifikasi faktor-faktor risiko kejahatan siber sehingga dapat dilakukan mitigasi risiko secara efektif dan efisien. Oleh karena itu, perlu diadakan kajian penilaian risiko sektoral (*Sectoral Risk Assessment*/SRA) TPPU dan TPPT dari kejahatan siber.

1.2. TUJUAN

Kajian SRA atas TPPU dan TPPT dari Tindak Pidana Siber dimaksudkan untuk mengidentifikasi, menganalisis, mengevaluasi dan memitigasi risiko TPPU dan TPPT dari Tindak Pidana Siber yang secara khusus bertujuan untuk:

1. Mengidentifikasi jenis-jenis tindak pidana siber yang berpotensi TPPU dan TPPT di Indonesia;

2. Mengidentifikasi dan menganalisis risiko TPPU dan TPPT dari tindak pidana siber di Indonesia;
3. Mengidentifikasi dan menganalisis risiko TPPU dan TPPT dari tindak pidana siber di Indonesia berdasarkan tipologi TPPU dan TPPT;
4. Mengidentifikasi dan menganalisis risiko TPPU dan TPPT dari tindak pidana siber di Indonesia berdasarkan sektor pihak pelapor yang dimanfaatkan dalam TPPU dan TPPT;
5. Mengidentifikasi dan menganalisis risiko TPPU dan TPPT dari tindak pidana siber di Indonesia berdasarkan pola transaksi yang dilakukan pelaku;
6. Mengidentifikasi dan menganalisis risiko TPPU dan TPPT dari tindak pidana siber di Indonesia berdasarkan wilayah atau provinsi; dan
7. Mengidentifikasi dan menganalisis risiko TPPU dan TPPT dari tindak pidana siber di Indonesia berdasarkan profil pekerjaan dan profil kewarganegaraan pelaku TPPU dan TPPT.

1.3. *OUTPUT*

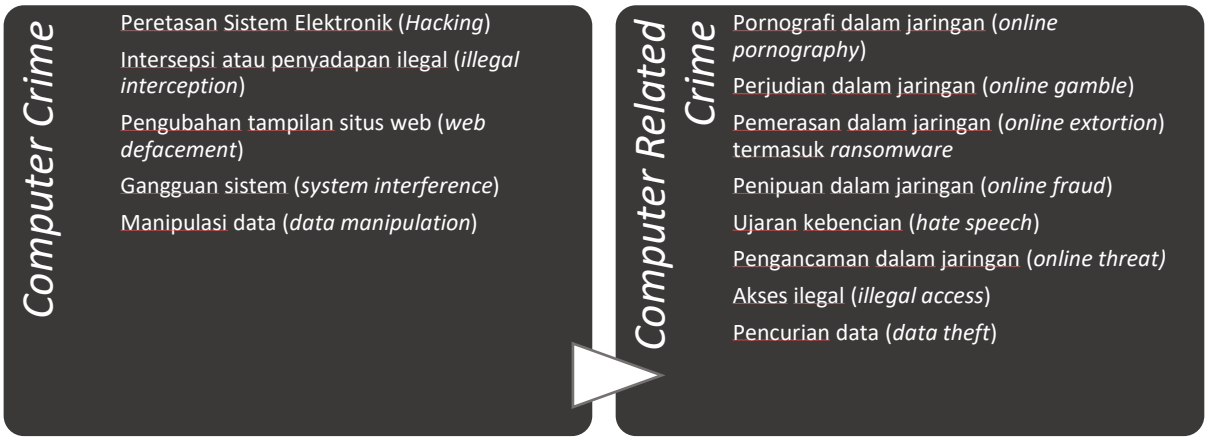
Output yang diharapkan dari kajian ini antara lain:

1. Diharapkan agar memperkuat dan memperbaharui pemahaman tentang risiko TPPU dan TPPT dari tindak pidana siber;
2. Diharapkan agar membantu kementerian/lembaga serta sektor privat untuk menyelaraskan kontrol dan strategi mitigasi secara nasional maupun institusional melalui peningkatan pemahaman tentang risiko TPPU dan TPPT dari tindak pidana siber; dan
3. Diharapkan agar pihak pelapor dapat memberikan perhatian dan meningkatkan deteksi laporan transaksi keuangan mencurigakan yang berkaitan dengan tindak pidana siber.

BAB II
TINJAUAN PUSTAKA

2.1. Sejarah Tindak Pidana Siber

Tindak pidana siber adalah "aktivitas kejahatan dengan komputer atau jaringan komputer menjadi alat, sasaran atau tempat terjadinya kejahatan" (Aziz, 2019). Tindak pidana siber dapat dibagi menjadi dua kelompok besar, yaitu kejahatan terhadap komputer (*computer crime*) yaitu upaya untuk menyusupi atau mendapatkan akses elektronik tanpa izin ke sistem, layanan, sumber daya atau informasi elektronik; dan kejahatan yang menggunakan komputer (*computer-enabled crime*) yaitu aktivitas ilegal (misalnya penipuan, pencucian uang, pencurian identitas) yang dilakukan atau difasilitasi oleh sistem dan perangkat elektronik, seperti jaringan dan komputer.



Gambar 4 *Computer Crime* dan *Computer-Enabled Crime*

Sumber: Patrolisiber.id

Tindak pidana "siber" pertama tercatat di Prancis pada tahun 1834 (Wolf, 2024). Ketika itu, pelaku menyusup dalam sistem telegraf Prancis dan mencuri data mengenai pasar keuangan. Tindak pidana siber modern pertama dianggap dilakukan oleh Allen Scherr pada tahun 1962, di mana ia mencuri kata sandi (*password*) dari database kartu absen dan kemudian melakukan serangan kepada jaringan komputer Massachusetts Institute of Technology (MIT). Pada 1971, virus komputer pertama di dunia diciptakan oleh Bob Thomas, meskipun virus tersebut tidak disebarkan ke dalam sistem komputer. Pada tahun 1981, Ian Murphy menjadi orang pertama yang ditangkap atas tindak pidana siber setelah tindakannya meretas sistem perusahaan AT&T dan membuat kekacauan dengan mengubah jam di sistem komputer.

Kemudian pada 1988 Robert Morris melepaskan Morris Worm yang dianggap sebagai serangan siber utama di internet. *Ransomware* pertama muncul pada tahun 1989.

Kemudian pada dekade 1990-an, Vladimir Levin diketahui adalah peretas pertama yang mencoba merampok bank. Pada tahun 1995, ia meretas sistem Citibank dan mentransfer lebih dari 10 juta dolar AS ke beberapa rekening bank di seluruh dunia. Meski virus komputer pertama diciptakan tahun 1971, virus komputer relatif tidak diketahui publik hingga munculnya virus Melissa pada Maret 1999. Sebuah dokumen yang diunggah daring dan menjanjikan akses ke video dewasa, virus tersebut akan mengambil alih aplikasi Microsoft Word milik seseorang, lalu berpindah ke Microsoft Outlook, dan menyebar sendiri dengan mengirimkan dirinya ke berbagai akun email. Virus ini menyebabkan kerugian sekitar 80 juta dolar AS dan merupakan salah satu virus besar pertama yang menyebar ke luar AOL (America Online, sebuah perusahaan media massa multinasional).

Tindak pidana siber yang pertama kali diadili di Indonesia terjadi pada tahun 1988 (Dimila, 2019). Pada saat itu, rekening BNI 1946 cabang New York dibobol oleh Rudy Demsy, mantan staf BNI New York. Setelah itu, cukup banyak kasus tindak pidana siber yang terjadi di Indonesia, di mana yang diserang selain situs web Pemerintah juga toko *online* atau *e-commerce* dan situs-situs lainnya yang memiliki kelemahan dalam keamanan sibernya. Salah satu kasus yang terjadi di dunia termasuk Indonesia adalah *ransomware* WannaCry di mana *ransomware* tersebut menginfeksi lebih dari 200 ribu komputer pada tahun 2017 (Anjelina & Afifah, 2024). Kemudian setelah disebutkan di latar belakang, tindak pidana siber di Indonesia meningkat 14 kali lipat antara tahun 2021 dan 2022. Untuk memitigasi ancaman tindak pidana siber yang semakin meningkat ini, Direktorat Reserse Siber di 8 Kepolisian Daerah (Sumatera Utara, Metro Jaya, Jawa Barat, Jawa Tengah, Jawa Timur, Bali, Sulawesi Tengah dan Papua) resmi dibentuk pada 20 September 2024 (R, 2024).

2.2. Konvensi Tindak Pidana Siber

Konvensi Tindak Pidana Siber (*Convention on Cybercrime*) atau Konvensi Budapest adalah traktat internasional pertama yang berupaya mengatasi kejahatan internet dan komputer (kejahatan siber) dengan menyelaraskan undang-undang nasional, meningkatkan teknik investigasi, dan meningkatkan kerja sama antarnegara. Konvensi ini diadopsi pada 8 November 2001, dan hingga April 2023, 68 negara di dunia telah meratifikasi konvensi

tersebut, dan 2 negara (Irlandia dan Afrika Selatan) telah menandatangani namun tidak meratifikasinya. Indonesia tidak meratifikasi Konvensi Budapest, namun pengaturan tindak pidana siber di Indonesia sebagian mengambil sumber dari Konvensi tersebut. Tindak pidana yang diatur dalam Konvensi Budapest antara lain:

A. *Offences against the confidentiality, integrity and availability of computer data and systems Illegal access* (Tindak Pidana terhadap Kerahasiaan, Keutuhan dan Ketersediaan Data dan Sistem Komputer Akses secara Ilegal)
   a. *Illegal interception* (penyadapan ilegal)
   b. *Data interference* (gangguan data)
   c. *System interference* (gangguan sistem)
   d. *Misuse of devices* (penyalahgunaan perangkat)

B. *Computer-related offences* (Tindak pidana terkait komputer)
   a. *Computer-related forgery* (pemalsuan terkait komputer)
   b. *Computer-related fraud* (penipuan terkait komputer)

C. *Content-related offences* (Tindak pidana terkait konten)
   a. *Offences related to child pornography* (Tindak pidana terkait pornografi anak)

D. *Offences related to infringements of copyright and related rights* (Tindak pidana terkait pelanggaran hak cipta dan hak terkait)

E. *Ancillary liability and sanctions* (Tanggung jawab dan sanksi tambahan)
   a. *Attempt and aiding or abetting* (percobaan dan pembantuan atau pemufakatan jahat)
   b. *Corporate liability* (tanggung jawab korporasi)

2.3. Pengaturan Tindak Pidana Siber di Indonesia

Tindak pidana siber di Indonesia diatur dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik, dan Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Berikut pokok-pokok pidana siber di Indonesia:

Tabel 1 Pengaturan Tindak Pidana Siber di Indonesia

No	Perbuatan	Ancaman Pidana	Paralelisme dengan Budapest Convention
1.	Pasal 27 ayat (1) Undang-Undang No. 1 Tahun 2024 Setiap Orang dengan sengaja dan tanpa hak menyiarkan, mempertunjukkan, mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan untuk diketahui umum.	Pasal 45 ayat (1) Undang-Undang No. 1 Tahun 2024 (1) Setiap Orang yang dengan sengaja dan tanpa hak menyiarkan, mempertunjukkan, mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan yang melanggar kesusilaan untuk diketahui umum sebagaimana dimaksud dalam Pasal 27 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). Pasal 52 Undang-Undang Nomor 11 Tahun 2008 (1) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 ayat (1) menyangkut kesusilaan atau eksploitasi seksual terhadap anak dikenakan pemberatan sepertiga dari pidana pokok. Pasal 52 ayat (4) Undang-Undang Nomor 11 Tahun 2008 (4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.	Tindak Pidana Terkait Konten
2.	Pasal 27 ayat (2) Undang-Undang No. 1 Tahun 2024 Setiap Orang dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan, dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian.	Pasal 45 ayat (3) Undang-Undang No. 1 Tahun 2024 (3) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan, mentransmisikan, dan/ atau membuat dapat diaksesnya Informasi Elektronik dan/ atau Dokumen Elektronik yang memiliki muatan perjudian sebagaimana dimaksud dalam Pasal 27 ayat (2) dipidana dengan pidana penjara paling lama 10	Tindak Pidana Terkait Konten

No	Perbuatan	Ancaman Pidana	Paralelisme dengan Budapest Convention
		(sepuluh)tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah). Pasal 52 ayat (4) Undang-Undang Nomor 11 Tahun 2008 (4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.	
3.	Pasal 27A Undang-Undang No. 1 Tahun 2024 Setiap Orang dengan sengaja menyerang kehormatan atau nama baik orang lain dengan cara menuduhkan suatu hal, dengan maksud supaya hal tersebut diketahui umum dalam bentuk Informasi Elektronik dan/ atau Dokumen Elektronik yang dilakukan melalui Sistem Elektronik.	Pasal 45 ayat (4) Undang-Undang No. 1 Tahun 2024 (4) Setiap Orang yang dengan sengaja menyerang kehormatan atau nama baik orang lain dengan cara menuduhkan suatu hal, dengan maksud supaya hal tersebut diketahui umum dalam bentuk Informasi Elektronik dan/ atau Dokumen Elektronik yang dilakukan melalui Sistem Elektronik sebagaimana dimaksud dalam Pasal 27A dipidana dengan pidana penjara paling lama 2 (dua) tahun dan/ atau denda paling banyak Rp400.000.000,00 (empat ratus juta rupiah). (6) Dalam hal perbuatan sebagaimana dimaksud pada ayat (4) tidak dapat dibuktikan kebenarannya dan bertentangan dengan apa yang diketahui padahal telah diberi kesempatan untuk membuktikannya, dipidana karena fitnah dengan pidana penjara paling lama 4 (empat) tahun dan/atau denda paling banyak Rp750.000.00O,00 (tujuh ratus lima puluh juta rupiah). Pasal 52 ayat (4) Undang-Undang Nomor 11 Tahun 2008 (4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.	Tindak Pidana Terkait Konten
4.	Pasal 27B Undang-Undang No. 1 Tahun 2024	Pasal 45 ayat (8) Undang-Undang No. 1 Tahun 2024	Tindak Pidana Terkait Konten

No	Perbuatan	Ancaman Pidana	Paralelisme dengan Budapest Convention
	(1) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik, dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, memaksa orang dengan ancaman kekerasan untuk: a. memberikan suatu barang, yang sebagian atau seluruhnya milik orang tersebut atau milik orang lain; atau memberi utang, membuat pengakuan utang, atau menghapuskan piutang.	(8) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik, dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, memaksa orang dengan ancaman kekerasan untuk: a. memberikan suatu barang, yang sebagian atau seluruhnya milik orang tersebut atau milik orang lain; atau b. memberi utang, membuat pengakuan utang, atau menghapuskan piutang, sebagaimana dimaksud dalam Pasal 27B ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). Pasal 52 ayat (4) Undang-Undang Nomor 11 Tahun 2008 (4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.	
4.	Pasal 27B Undang-Undang No. 1 Tahun 2024 (2) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik, dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan ancarnan pencemaran atau dengan ancaman akan membuka rahasia, memaksa orang supaya: a. memberikan suatu barang yang sebagian atau seluruhnya milik orang tersebut atau milik orang lain; atau	Pasal 45 ayat (10) Undang-Undang No. 1 Tahun 2024 (10) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik, dengan maksud untuk menguntungkan diri sendiri atau orang lain secara melawan hukum, dengan ancaman pencemaran atau dengan ancaman akan membuka rahasia, memaksa orang supaya: a. memberikan suatu barang yang sebagian atau seluruhnya milik orang tersebut atau milik orang lain; atau	Tindak Pidana Terkait Konten

No	Perbuatan	Ancaman Pidana	Paralelisme dengan Budapest Convention
	b. memberi utang, membuat pengakuan utang, atau menghapuskan piutang.	b. memberi utang, membuat pengakuan utang, atau menghapuskan piutang, sebagaimana dimaksud dalam Pasal 27B ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). Pasal 52 ayat (4) Undang-Undang Nomor 11 Tahun 2008 (4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.	
5.	Pasal 28 Undang-Undang No. 1 Tahun 2024 (1) Setiap Orang dengan sengaja dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan yang mengakibatkan kerugian materiel bagi konsumen dalam Transaksi Elektronik.	Pasal 45A Undang-Undang No. 1 Tahun 2024 (1) Setiap Orang yang dengan sengaja mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik yang berisi pemberitahuan bohong atau informasi menyesatkan yang mengakibatkan kerugian materiel bagi konsumen dalam Transaksi Elektronik sebagaimana dimaksud dalam Pasal 28 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). Pasal 52 ayat (4) Undang-Undang Nomor 11 Tahun 2008 (4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.	Penipuan Terkait Komputer
6.	Pasal 28 Undang-Undang No. 1 Tahun 2024 (2) Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik yang sifatnya menghasut, mengajak,	Pasal 45A ayat (2) Undang-Undang No. 1 Tahun 2024 (2) Setiap Orang yang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan Informasi Elektronik dan/atau Dokumen Elektronik yang sifatnya menghasut,	Tindak Pidana Terkait Konten

No	Perbuatan	Ancaman Pidana	Paralelisme dengan Budapest Convention
	atau memengaruhi orang lain sehingga menimbulkan rasa kebencian atau permusuhan terhadap individu dan/atau kelompok masyarakat tertentu berdasarkan ras, kebangsaan, etnis, warna kulit, agama, kepercayaan, jenis kelamin, disabilitas mental, atau disabilitas fisik.	mengajak, atau orang lain sehingga menimbulkan rasa kebencian atau permusuhan terhadap individu dan/atau kelompok masyarakat tertentu berdasarkan ras, kebangsaan, etnis, warna kulit, agama, kepercayaan, jenis kelamin, disabilitas mental, atau disabilitas frsik sebagaimana dimaksud dalam Pasal 28 ayat (2) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). Pasal 52 ayat (4) Undang-Undang Nomor 11 Tahun 2008 (4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.	
7.	Pasal 28 Undang-Undang No. 1 Tahun 2024 (3) Setiap Orang dengan sengaja menyebarkan Informasi Elektronik dan/atau Dokumen Elektronik yang diketahuinya memuat pemberitahuan bohong yang menimbulkan kerusuhan di masyarakat.	Pasal 45A Ayat (3) Undang-Undang No. 1 Tahun 2024 (3) Setiap Orang yang dengan sengaja menyebarkan Informasi Elektronik dan/atau Dokumen Elektronik yang diketahuinya memuat pemberitahuan bohong yang menimbulkan kerusuhan di masyarakat sebagaimana dimaksud dalam Pasal 28 ayat (3) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/ atau denda paling banyak Rp1.000.000.000,00 (satu miliar rupiah). Pasal 52 ayat (4) Undang-Undang Nomor 11 Tahun 2008 (4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.	Tindak Pidana Terkait Konten
8.	Pasal 29 Undang-Undang No. 1 Tahun 2024 Setiap Orang dengan sengaja dan tanpa hak Informasi Elektronik dan/atau Dokumen Elektronik secara langsung kepada korban	Pasal 45B Undang-Undang No. 1 Tahun 2024 Setiap Orang yang dengan sengaja dan tanpa hak mengirimkan Informasi Elektronik dan/atau Dokumen Elektronik secara langsung	Tindak Pidana Terkait Konten

No	Perbuatan	Ancaman Pidana	Paralelisme dengan Budapest Convention
	yang berisi ancaman kekerasan dan/atau menakutnakuti.	kepada korban yang berisi ancaman kekerasan dan/ atau menakutnakuti sebagaimana dimaksud dalam Pasal 29 dipidana dengan pidana penjara paling lama 4 (empat) tahun dan/ atau denda paling banyak Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah). Pasal 52 ayat (4) Undang-Undang Nomor 11 Tahun 2008 (4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.	
9.	Pasal 30 Undang-Undang No. 11 Tahun 2008 (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik milik Orang lain dengan cara apa pun. (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan tujuan untuk memperoleh Informasi Elektronik dan/atau Dokumen Elektronik. (3) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum mengakses Komputer dan/atau Sistem Elektronik dengan cara apa pun dengan melanggar, menerobos, melampaui, atau menjebol sistem pengamanan.	Pasal 46 Undang-Undang No. 11 Tahun 2008 (1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (1) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah). (2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah). (3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 30 ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah). Pasal 52 ayat (2), (3) dan (4) Undang-Undang Nomor 11 Tahun 2008 (2) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik	Akses Ilegal

No	Perbuatan	Ancaman Pidana	Paralelisme dengan Budapest Convention
		dipidana dengan pidana pokok ditambah sepertiga. (3) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah dua pertiga. (4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.	
10.	Pasal 31 Undang-Undang Nomor 19 Tahun 2016 (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atau penyadapan atas Informasi Elektronik dan/atau Dokumen Elektronik dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain. (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan intersepsi atas transmisi Informasi Elektronik dan/atau Dokumen Elektronik yang tidak bersifat publik dari, ke, dan di dalam suatu Komputer dan/atau Sistem Elektronik tertentu milik Orang lain, baik yang tidak menyebabkan perubahan apa pun maupun yang menyebabkan adanya perubahan, penghilangan, dan/atau penghentian Informasi Elektronik dan/atau Dokumen Elektronik yang sedang ditransmisikan.	Pasal 47 Undang-Undang Nomor 11 Tahun 2008 Pasal 47 Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 31 ayat (1) atau ayat (2) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp800.000.000,00 (delapan ratus juta rupiah). Pasal 52 ayat (2), (3) dan (4) Undang-Undang Nomor 11 Tahun 2008 (2) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga. (3) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik	Penyadapan Ilegal

No	Perbuatan	Ancaman Pidana	Paralelisme dengan Budapest Convention
		dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah dua pertiga. (4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.	
11.	Pasal 32 Undang-Undang Nomor 11 Tahun 2008 (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun mengubah, menambah, mengurangi, melakukan transmisi, merusak, menghilangkan, memindahkan, menyembunyikan suatu Informasi Elektronik dan/atau Dokumen Elektronik milik Orang lain atau milik publik. (2) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum dengan cara apa pun memindahkan atau mentransfer Informasi Elektronik dan/atau Dokumen Elektronik kepada Sistem Elektronik Orang lain yang tidak berhak. (3) Terhadap perbuatan sebagaimana dimaksud pada ayat (1) yang mengakibatkan terbukanya suatu Informasi Elektronik dan/atau Dokumen Elektronik yang bersifat rahasia menjadi dapat diakses oleh publik dengan keutuhan data yang tidak sebagaimana mestinya.	Pasal 48 Undang-Undang Nomor 11 Tahun 2008 (1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (1) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda paling banyak Rp2.000.000.000,00 (dua miliar rupiah). (2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (2) dipidana dengan pidana penjara paling lama 9 (sembilan) tahun dan/atau denda paling banyak Rp3.000.000.000,00 (tiga miliar rupiah). (3) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 32 ayat (3) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp5.000.000.000,00 (lima miliar rupiah). Pasal 52 ayat (2), (3) dan (4) Undang-Undang Nomor 11 Tahun 2008 (2) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik	Gangguan Data

No	Perbuatan	Ancaman Pidana	Paralelisme dengan Budapest Convention
		dipidana dengan pidana pokok ditambah sepertiga. (3) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah dua pertiga. (4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.	
12.	Pasal 33 Undang-Undang Nomor 11 Tahun 2008 Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan tindakan apa pun yang berakibat terganggunya Sistem Elektronik dan/atau mengakibatkan Sistem Elektronik menjadi tidak bekerja sebagaimana mestinya.	Pasal 49 Undang-Undang Nomor 11 Tahun 2008 Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 33, dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah). Pasal 52 ayat (2), (3) dan (4) Undang-Undang Nomor 11 Tahun 2008 (2) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga. (3) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik	Gangguan Sistem

No	Perbuatan	Ancaman Pidana	Paralelisme dengan Budapest Convention
		Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah dua pertiga. (4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.	
13.	Pasal 34 Undang-Undang Nomor 11 Tahun 2008 (1) Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum memproduksi, menjual, mengadakan untuk digunakan, mengimpor, mendistribusikan, menyediakan, atau memiliki: a. perangkat keras atau perangkat lunak Komputer yang dirancang atau secara khusus dikembangkan untuk memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33; b. sandi lewat Komputer, Kode Akses, atau hal yang sejenis dengan itu yang ditujukan agar Sistem Elektronik menjadi dapat diakses dengan tujuan memfasilitasi perbuatan sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 33.	Pasal 50 Undang-Undang Nomor 11 Tahun 2008 Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 34 ayat (1) dipidana dengan pidana penjara paling lama 10 (sepuluh) tahun dan/atau denda paling banyak Rp10.000.000.000,00 (sepuluh miliar rupiah). Pasal 52 ayat (2), (3) dan (4) Undang-Undang Nomor 11 Tahun 2008 (2) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga. (3) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah dua pertiga.	Penyalahgunaan Perangkat

No	Perbuatan	Ancaman Pidana	Paralelisme dengan Budapest Convention
		(4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga. Pasal 52 ayat (2), (3) dan (4) Undang-Undang Nomor 11 Tahun 2008 (2) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga. (3) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah dua pertiga. (4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.	
14.	Pasal 35 Undang-Undang Nomor 11 Tahun 2008 Setiap Orang dengan sengaja dan tanpa hak atau melawan hukum melakukan manipulasi, penciptaan, prubahan, penghilangan, pengrusakan Informasi Elektronik dan/atau Dokumen Elektronik dengan tujuan agar Informasi Elektronik dan/atau Dokumen Elektronik tersebut dianggap seolah-olah data yang otentik.	Pasal 51 Undang-Undang Nomor 11 Tahun 2008 (1) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 35 dipidana dengan pidana penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah). (2) Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 36 dipidana dengan pidana	Pemalsuan dan penipuan terkait komputer

No	Perbuatan	Ancaman Pidana	Paralelisme dengan Budapest Convention
		penjara paling lama 12 (dua belas) tahun dan/atau denda paling banyak Rp12.000.000.000,00 (dua belas miliar rupiah).	
15.	Pasal 36 Undang-Undang Nomor 11 Tahun 2008 Setiap Orang dengan sengaja dan tanpa hak melakukan perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 34 yang mengakibatkan kerugian materiel bagi Orang lain.	Pasal 52 ayat (2), (3) dan (4) Undang-Undang Nomor 11 Tahun 2008 (2) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga. (3) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah dua pertiga. (4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.	
16.	Pasal 37 Undang-Undang Nomor 11 Tahun 2008 Setiap Orang dengan sengaja melakukan perbuatan yang dilarang sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 36 di luar wilayah Indonesia terhadap Sistem Elektronik yang berada di wilayah yurisdiksi Indonesia.	Pasal 52 ayat (2), (3) dan (4) Undang-Undang Nomor 11 Tahun 2008 (2) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau yang digunakan untuk layanan publik dipidana dengan pidana pokok ditambah sepertiga.	

No	Perbuatan	Ancaman Pidana	Paralelisme dengan Budapest Convention
		(3) Dalam hal perbuatan sebagaimana dimaksud dalam Pasal 30 sampai dengan Pasal 37 ditujukan terhadap Komputer dan/atau Sistem Elektronik serta Informasi Elektronik dan/atau Dokumen Elektronik milik Pemerintah dan/atau badan strategis termasuk dan tidak terbatas pada lembaga pertahanan, bank sentral, perbankan, keuangan, lembaga internasional, otoritas penerbangan diancam dengan pidana maksimal ancaman pidana pokok masing-masing Pasal ditambah dua pertiga. (4) Dalam hal tindak pidana sebagaimana dimaksud dalam Pasal 27 sampai dengan Pasal 37 dilakukan oleh korporasi dipidana dengan pidana pokok ditambah dua pertiga.	

BAB III
METODOLOGI PENELITIAN

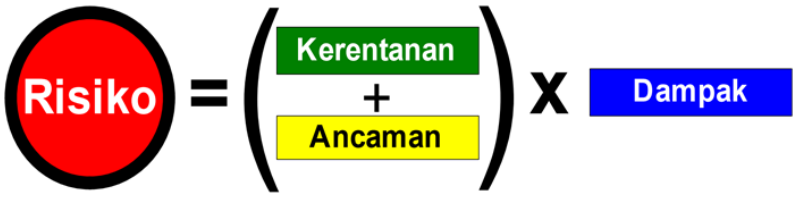
3.1. METODE PENELITIAN

Metodologi penelitian yang digunakan dalam SRA Siber tahun 2024 adalah *mixed method explanatory sequential design*. Metodologi ini merupakan kombinasi yang menggabungkan metodologi penelitian kualitatif dan kuantitatif secara berurutan. Pendekatan kuantitatif menggunakan data statistik dari transaksi keuangan mencurigakan, pengawasan, pertukaran informasi FIU, hasil laporan intelijen keuangan, penyidikan, penuntutan dan putusan pengadilan. Sedangkan pendekatan kualitatif menggunakan penilaian mandiri oleh ahli atau *expert* dari pihak pelapor, lembaga pengawas dan pengatur, lembaga intelijen keuangan (PPATK), dan lembaga penegak hukum mengenai kualitas aspek pencegahan dan pemberantasan tindak pidana pendanaan pencucian uang dan pendanaan terorisme pada tindak pidana siber.

Pedoman yang digunakan dalam penyusunan SRA Siber tahun 2024 merujuk pada praktik terbaik internasional dari *National Money Laundering and Terrorist Financing Assessment* (FATF Guidance), *Risk Assessment Support for Money Laundering/Terrorist Financing* (World Bank) *Review of the funds Strategy on Anti Money Laundering and Terrorist Financing* (IMF), dan *Terrorist Financing Risk Assessment Guidance*.

3.2. RUANG LINGKUP DAN LANGKAH-LANGKAH PENILAIAN RISIKO

Ruang lingkup SRA Siber tahun 2024 mencakup identifikasi jenis-jenis tindak pidana siber yang berpotensi TPPU dan TPPT di Indonesia, dan identifikasi dan analisis risiko TPPU dan TPPT dari tindak pidana siber di Indonesia yang terdiri dari tipologi TPPU dan TPPT, sektor pihak pelapor yang dimanfaatkan dalam TPPU dan TPPT, wilayah atau provinsi dan profil pelaku. Dalam panduan dari FATF Guidance dijelaskan bahwa risiko merupakan formulasi fungsi sebagai berikut:



Gambar 5 Formulasi Penilaian Risiko

a. Ancaman (*Threat*), merupakan seseorang atau sekelompok orang, benda atau kegiatan yang berpotensi menimbulkan kerugian, misalnya negara, masyarakat, perekonomian, dan lain-lain. Dalam konteks TPPU/TPPT, hal ini mencakup penjahat, kelompok teroris dan fasilitatornya, dananya, serta serta aktivitas TPPU atau TPPT di masa lalu, sekarang dan masa depan

b. Kerentanan (*Vulnerability*), merupakan hal-hal yang dapat dimanfaatkan oleh ancaman atau yang dapat mendukung atau memfasilitasi aktivitasnya. Dalam konteks penilaian risiko TPPU/TPPT, melihat kerentanan sebagai hal yang berbeda dari ancaman berarti memusatkan perhatian pada, misalnya, faktor-faktor yang mewakili kelemahan dalam sistem atau pengendalian APU/PPT atau ciri-ciri tertentu di suatu negara. Hal ini juga dapat mencakup fitur sektor tertentu, produk keuangan, atau jenis layanan yang menjadikannya menarik untuk tujuan TPPU atau TPPT.

c. Kecenderungan (*Likelihood*), merupakan peluang kemungkinan mengenai seberapa besar kemungkinan kejadian aktivitas pencucian uang dan pendanaan terorisme.

d. Dampak (*Consequence*), merupakan akibat atau kerugian yang mungkin ditimbulkan oleh TPPU atau TPPT dan mencakup dampak dari aktivitas kriminal dan teroris yang mendasarinya terhadap sistem dan lembaga keuangan, serta perekonomian dan masyarakat secara umum. Konsekuensi dari TPPU atau TPPT dapat bersifat jangka pendek atau jangka panjang dan juga berhubungan dengan populasi, komunitas tertentu, lingkungan bisnis, atau kepentingan nasional atau internasional, serta reputasi dan daya tarik sektor keuangan suatu negara.

e. Tren yang baru muncul dan/atau berkembang (*Emerging Trend*), merupakan suatu saluran atau *channel* yang baru muncul dan/atau berkembang sebagai sarana

pencucian uang dan pendanaan terorisme sebelum terlihat dampaknya secara meluas.

3.3. TAHAPAN PENILAIAN RISIKO

Dalam melakukan penyusunan SRA Siber tahun 2024 terdapat beberapa tahapan kegiatan yang dilakukan selama periode 2024, sebagai berikut:

A. Tahapan Persiapan

1. Penyusunan proposal SRA Siber tahun 2024 pada Januari 2024.
2. Ekspose internal proposal SRA Siber tahun 2024 pada Februari 2024
3. Penyusunan tim internal dan eksternal penyusunan SRA Siber tahun 2024 pada Maret 2024.
4. Pertemuan bersama regulator, penegak hukum, dan Kementerian/Lembaga mengenai urgensi penyusunan SRA Siber pada April 2024.
5. Pengiriman kuesioner kepada responden regulator, penegak hukum, Kementerian/Lembaga dan pihak pelapor pada Mei 2024.
6. Pelaksanaan wawancara kepada responden regulator, penegak hukum dan Kementerian/Lembaga pada Juni 2024.

B. Tahapan Pelaksanaan

a. Identifikasi Risiko

Tahapan ini dilakukan proses identifikasi faktor risiko yang akan dianalisis, serta mengidentifikasi kebutuhan jenis data dan informasi. Tahapan ini dilaksanakan pada Agustus-Oktober 2024.

b. Analisis Risiko

Tahapan analisis risiko merupakan kelanjutan dari tahapan identifikasi risiko menggunakan variabel kerentanan, ancaman, dan konsekuensi. Tujuan dari langkah ini adalah untuk menganalisis faktor risiko yang teridentifikasi guna memahami sifat, sumber, kemungkinan dan konsekuensi dalam rangka untuk menetapkan tingkatan nilai relatif untuk masing-masing faktor risiko.

c. Evaluasi Risiko

Tahapan evaluasi ini berisikan proses pengambilan hasil yang ditemukan selama proses analisis untuk menentukan prioritas dalam mengatasi risiko, dengan mempertimbangkan tujuan penilaian risiko pada

awal proses penilaian. Tahapan ini sekaligus berkontribusi dalam pengembangan strategi untuk mitigasi risiko yang mengarah ke pengembangan strategi untuk mengatasi risiko.

C. Tahapan Peluncuran atau Diseminasi

Tahapan peluncuran atau diseminasi ini dilakukan untuk memberikan pemahaman dan meningkatkan kesadaran (*awareness)* bersama mengenai risiko sektoral TPPU dan TPPT pada Tindak Pidana Siber Tahun 2024. Adapun pelaksanaan peluncuran atau diseminasi sebagai berikut:

1. Finalisasi Laporan pada Desember 2024.
2. Peluncuran dan komunikasi kepada regulator, penegak hukum, dan K/L terkait Hasil Laporan SRA Siber Tahun 2024 yang dijadwalkan akan dilaksanakan pada tahun 2025.

3.4. SUMBER DATA

Penyusunan SRA Siber tahun 2024 ini dilakukan dengan menggunakan data selama periode Januari 2019 s.d. Maret 2024. Pendekatan kuantitatif menggunakan data statistik yang bersumber dari data statistik mengenai laporan transaksi keuangan mencurigakan, pelaksanaan pengawasan, pertukaran informasi FIU, hasil laporan intelijen keuangan, penyidikan, penuntutan dan putusan pengadilan. Sedangkan pendekatan kualitatif menggunakan penilaian mandiri oleh ahli atau *expert* dari perwakilan pihak pelapor, pihak lembaga pengawas dan pengatur, lembaga intelijen keuangan (PPATK), dan lembaga penegak hukum. Seluruh data dan informasi tersebut digunakan untuk melakukan identifikasi, analisis dan evaluasi terhadap risiko tindak pidana pencucian uang dan pendanaan terorisme pada tindak pidana siber.

Pengumpulan data kualitatif dilakukan dengan penyampaian kuesioner kepada lembaga pengawas dan pengatur, lembaga penegak hukum, kementerian/lembaga terkait dan pihak pelapor sebanyak 36 responden dengan rata-rata capaian tingkat respon (*response rate)* sebesar 94%, rincian sebagai berikut:

a. 3 responden dari 3 perwakilan lembaga pengawas dan pengatur dengan rata-rata tingkat respons *(response rate)* sebesar 100%;
b. 5 responden dari 5 perwakilan lembaga penegak hukum dengan rata-rata tingkat respons *(response rate)* sebesar 100%;

c. 1 responden dari 1 perwakilan kementerian/lembaga terkait dengan rata-rata tingkat respons (*response rate*) sebesar 100%; dan

d. 24 responden dari 26 perwakilan pihak pelapor dengan rata-rata tingkat respons (*response rate*) sebesar 92%.

Selain kuesioner, dilakukan juga pengumpulan data melalui wawancara kepada 3 perwakilan lembaga pengawas dan pengatur, 4 perwakilan lembaga penegak hukum dan 2 kementerian/lembaga terkait untuk memperoleh pendalaman terhadap risiko TPPU dan TPPT pada Tindak Pidana Siber. Topik-topik yang dibahas dalam kuesioner dan wawancara SRA antara lain:

Tabel 2 Topik-Topik Kuesioner dan Wawancara SRA

Kuesioner	Wawancara
1. Persepsi ancaman, kerentanan dan dampak TPPU dan TPPT dari masing-masing jenis Tindak Pidana Siber per PoC 2. Jumlah dan nominal kasus (penyidikan, penuntutan, putusan) TPPU dan TPPT Tekfin per jenis TP Siber (khusus penegak hukum) 3. Studi Kasus 4. Mitigasi risiko TPPU dan TPPT dari Tindak Pidana Siber	1. Persepsi Kecenderungan TPPU dan TPPT dari tindak pidana siber (konvensional atau digital) 2. Kebijakan lembaga dalam pencegahan dan pemberantasan TP Siber dan/atau TPPU dan TPPT 3. Ancaman baru/emerging threat TPPU dan TPPT dari Tindak Pidana Siber 4. Indikator transaksi mencurigakan TPPU dan TPPT dari Tindak Pidana Siber 5. Kemampuan pihak pelapor mendeteksi transaksi keuangan mencurigakan dan pemenuhan data kasus, pengawasan pihak pelapor, dan penanganan perkara TP Siber dan/atau TPPU dan TPPT 6. Bentuk kerja sama domestik dan internasional 7. Tantangan 8. Rekomendasi a. Bidang pencegahan b. Bidang pemberantasan c. Bidang kerja sama

BAB IV
HASIL PENILAIAN RISIKO

4.1. HASIL PENILAIAN RISIKO

A. Tingkat Risiko TPPU

Berdasarkan data putusan pengadilan yang berhasil dihimpun, hanya sedikit kasus TPPU yang tindak pidana asalnya adalah tindak pidana siber (8 kasus) jika dibandingkan jumlah seluruh putusan TPPU selama periode kajian (Januari 2019 s.d. Maret 2024). Sesuai Buletin Statistik Anti Pencucian Uang & Pencegahan Pendanaan Terorisme (APUPPT) total putusan pengadilan TPPU sejak Januari 2020 s.d. Juni 2024 berjumlah 673 perkara. Hasil Penilaian Risiko Nasional terhadap Tindak Pidana Pencucian Uang Tahun 2021 menyebutkan bahwa Risiko Tindak Pidana ITE menjadi Tindak Pidana Asal TPPU adalah Rendah secara domestik dan memiliki ancaman tinggi dalam konteks *foreign predicate crime*. Namun, perlu adanya pertimbangan terhadap risiko nasional ke depannya karena pelaku kejahatan semakin memanfaatkan sarana siber atau teknologi canggih untuk melakukan pencucian uang yang berasal dari berbagai jenis tindak pidana. Seperti akan dibahas pada bagian selanjutnya, pelaku kejahatan memanfaatkan berbagai teknologi seperti AI, web3, aset kripto, dan lain sebagainya.

Pemerintah telah memberikan perhatian yang meningkat terhadap perjudian *online* hingga membentuk Satuan Tugas Pemberantasan Judi *Online* (Satgas Judi *Online*) berdasarkan Keputusan Presiden Nomor 21 Tahun 2024. Hingga Juni 2024, Bareskrim POLRI dalam Satgas Pemberantasan Judi *Online* telah mengungkap 318 kasus TP perjudian daring dan berhasil menangkap 464 tersangka (Humas Polri, 2024). Transaksi judi *online* menembus Rp283 triliun hingga November 2024 (Aswara, 2024). Menurut statistik penghentian transaksi PPATK, judi *online* juga memiliki nilai yang sangat tinggi, mencapai Rp1 triliun antara 2022-Agustus 2024.

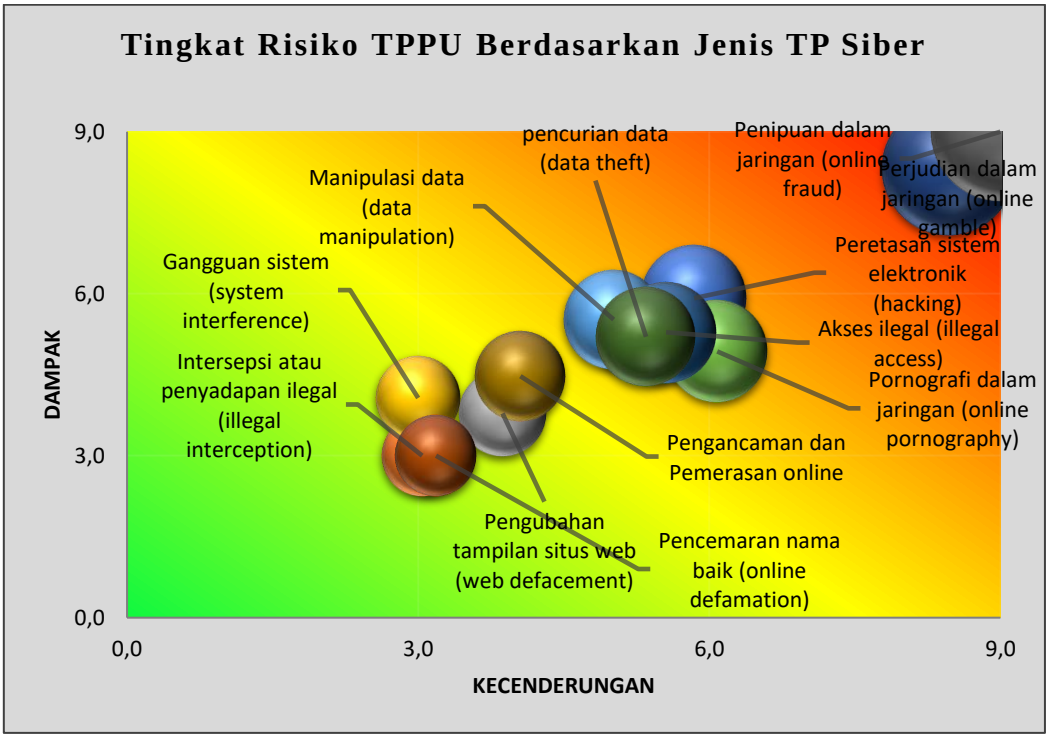
Dalam rancangan Rencana Pembangunan Jangka Menengah Nasional (RPJMN) 2025-2029, pemberantasan judi dan TPPU menjadi Prioritas Nasional 7 (Memperkuat Reformasi Politik, Hukum, dan Birokrasi, serta Memperkuat Pencegahan dan Pemberantasan Korupsi, Narkoba, Judi dan Penyelundupan). Putusan TPPU dari TP Siber masih rendah dibanding

Tindak Pidana Asalnya, sehingga perlu adanya peningkatan penanganan TPPU-nya, terutama dari judi *online*.

Berdasarkan hasil kuesioner, responden menilai kecenderungan pelaku TP Siber sama dengan TPPU adalah menengah/cukup mungkin. Dalam kasus yang ditemukan di Indonesia, ditemukan bahwa beberapa pelaku TP Siber juga adalah pelaku TPPU. Selain menanyakan kecenderungan pelaku TP Siber juga merupakan pelaku TPPU, kami menanyakan kecenderungan pelaku TP Siber dalam melakukan pencucian uang dalam wawancara, apakah secara *instrumental digital laundering* (salah satu tahapan pencucian uang saja yang dilaksanakan secara digital) atau *integral digital laundering* (seluruh tahapan pencucian uang dilaksanakan secara digital) dan hasilnya menunjukkan sebagian besar responden (67%) berpendapat bahwa pelaku TP siber cenderung melakukan pencucian uang secara *integral digital laundering*. Dalam kasus yang ditemukan, pelaku tidak hanya melakukan pencucian uang secara digital namun masih ada yang menggunakan rekening tabungan (cara lama).

Adapun penilaian risiko TPPU dari Tindak Pidana Siber berdasarkan POC yang telah ditentukan sebelumnya dapat dirangkum sebagai berikut:

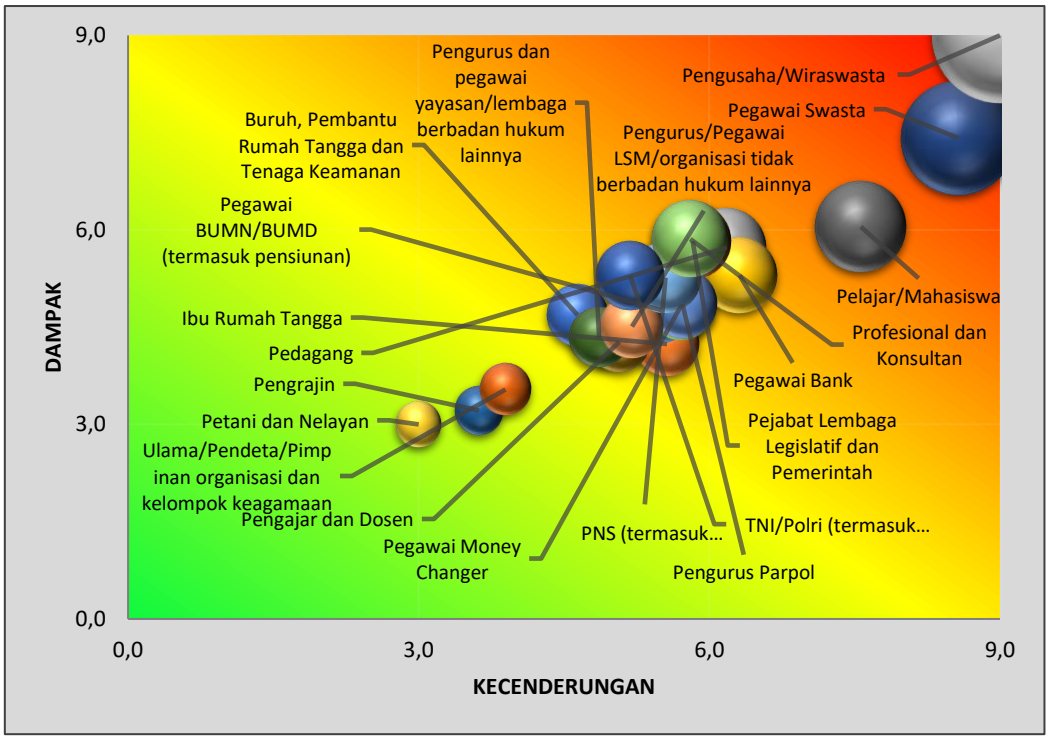
1. **Tingkat Risiko TPPU Hasil Tindak Pidana Siber Berdasarkan Jenis Tindak Pidana Siber**



Gambar 6 Tingkat Risiko TPPU Hasil TP Siber Berdasarkan Jenis TP Siber

Penipuan dalam jaringan (*online fraud*) dan **perjudian *online*** (*online gambling*) dinilai sebagai jenis tindak pidana siber yang berisiko tinggi TPPU. Berdasarkan data e-MP Robinopsnal Bareskrim POLRI pada 23 Desember 2022, penipuan melalui media elektronik menempati peringkat kedua kasus kejahatan siber yang ditangani POLRI (2.131 kasus) setelah manipulasi data autentik (3.723 kasus) untuk periode 1 Januari s.d. Desember 2022 (Pusiknas Bareskrim Polri, n.d.). Kemudian pada tahun 2023 kasus penipuan menempati peringkat pertama dengan jumlah 1.414 kasus (Tribratanews.polri.go.id, 2023). Sementara itu, peretasan sistem elektronik (*hacking*) dinilai berisiko menengah TPPU. Dari laporan intelijen PPATK, ditemukan bahwa terdapat indikasi *hacking* terhadap bank di Indonesia. Jenis tindak pidana siber lainnya dinilai berisiko rendah terhadap TPPU.

2. Tingkat Risiko TPPU Hasil Tindak Pidana Siber Berdasarkan Profil Pelaku

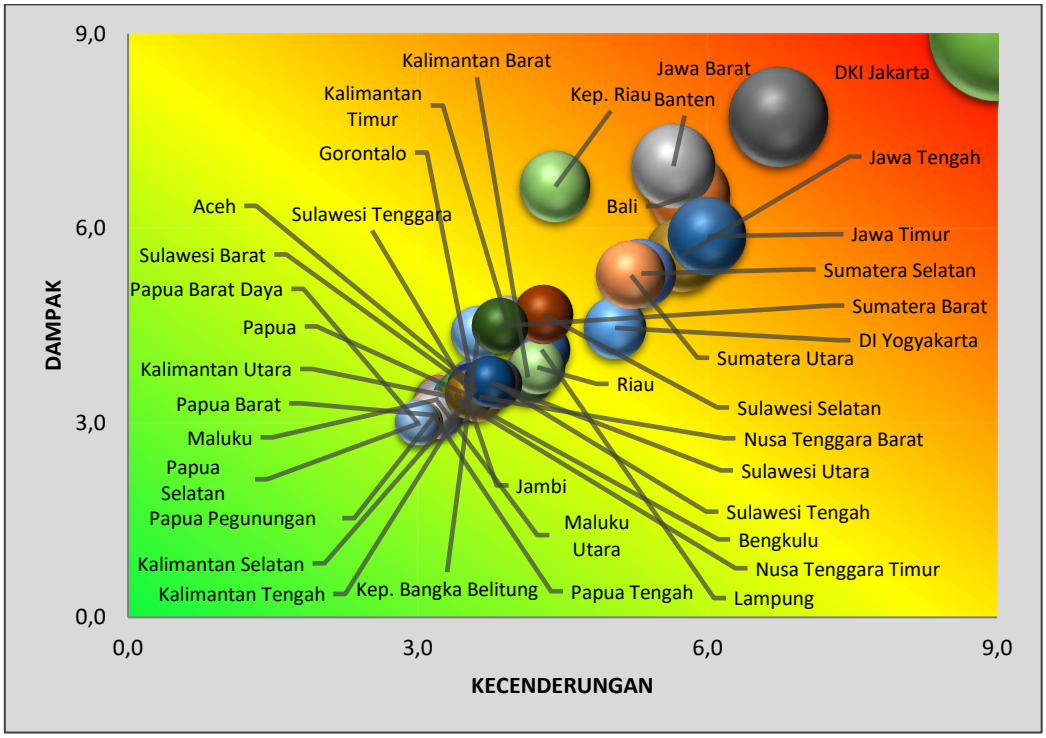


Gambar 7 Tingkat Risiko TPPU Hasil TP Siber Berdasarkan Profil Pelaku

Pengusaha/wiraswasta dan **pegawai swasta** dinilai menjadi profil yang berisiko tinggi TPPU hasil TP Siber. Pelajar/Mahasiswa, Pedagang, Profesional dan Konsultan, Pejabat Lembaga Legislatif dan Pemerintah, dan Pegawai Bank dinilai berisiko menengah TPPU hasil TP Siber. Pejabat Lembaga Legislatif dan Pemerintah dianggap berisiko

menengah karena ditemukan beberapa kasus judi *online* yang melibatkan pejabat pemerintah. Profil-profil lainnya dianggap berisiko rendah.

3. Tingkat Risiko TPPU Hasil Tindak Pidana Siber Berdasarkan Wilayah



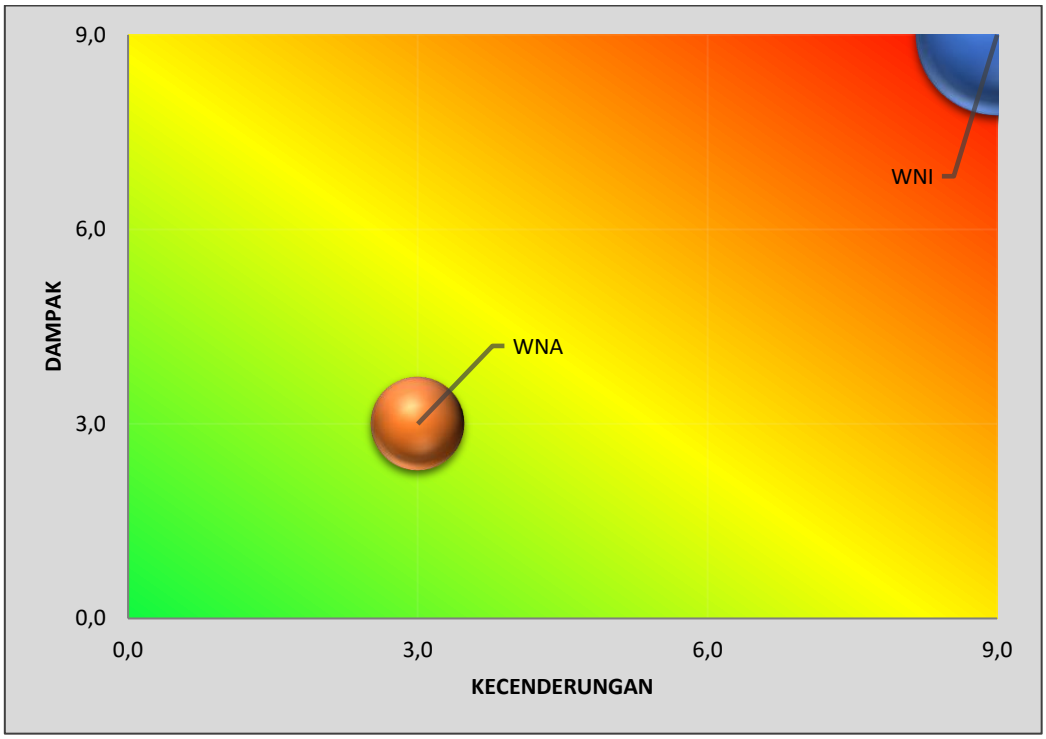
Gambar 8 Tingkat Risiko TPPU Hasil TP Siber Berdasarkan Wilayah

Tindak pidana siber pada dasarnya terjadi di ruang siber yang tidak terbatas kepada wilayah tertentu. Namun untuk keperluan kajian ini, diperoleh data mengenai lokasi kejadian atau pengadilan dari TP Siber. **DK Jakarta** dinilai berisiko tinggi berdasarkan wilayah, sedangkan Jawa Barat, Banten, Bali dan Jawa Timur dinilai berisiko menengah.

4. Tingkat Risiko TPPU Hasil Tindak Pidana Siber Berdasarkan Warga Negara Pelaku Tindak Pidana Siber

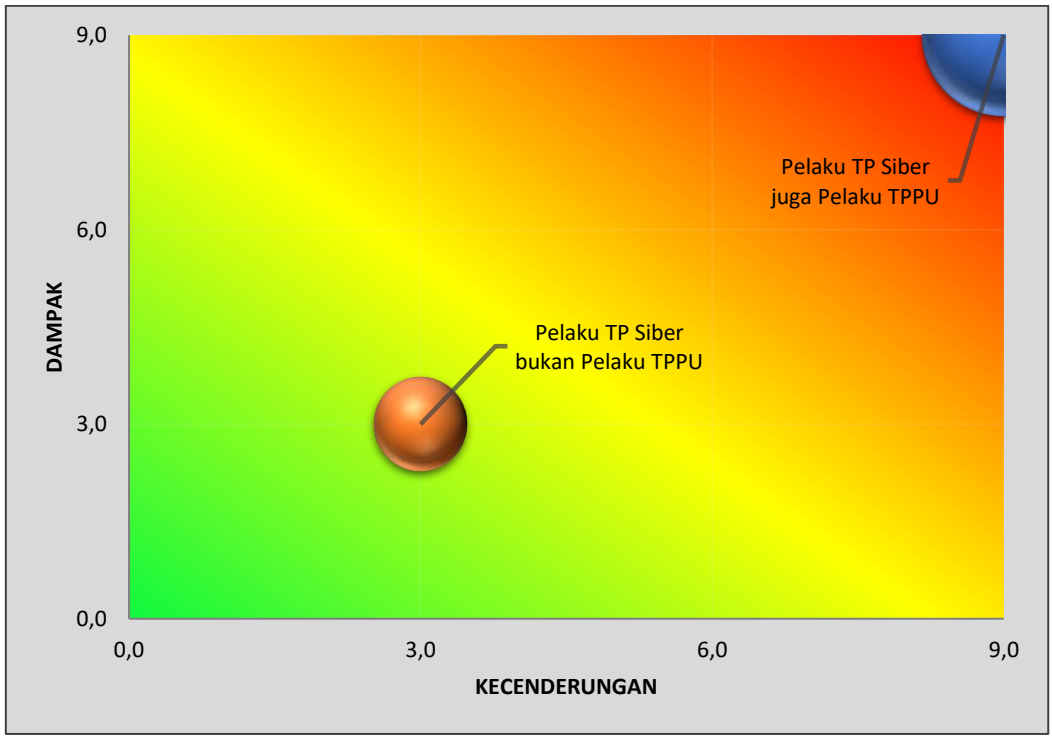
Warga Negara Indonesia dinilai berisiko tinggi TPPU dari hasil Tindak Pidana Siber, sedangkan WNA berisiko rendah. Dalam beberapa kasus Tindak Pidana Siber memang terdapat beberapa pelaku WNA, contohnya pada kasus 103 WNA yang menyalahgunakan izin tinggal dan diduga melakukan kejahatan siber (Kantor Imigrasi Khusus Kelas 1 TPI Batam, 2024). Meski terdapat prinsip teritorialitas berdasarkan KUHP, tidak selalu memungkinkan dijatuhkan pidana kepada WNA di Indonesia. Selain itu

dalam konteks Tindak Pidana Siber, bisa saja pelaku WNA berada di luar negeri sehingga sulit diadili di Indonesia.



Gambar 9 Tingkat Risiko TPPU Berdasarkan Warga Negara Pelaku TP Siber

5. Tingkat Risiko TPPU Hasil Tindak Pidana Siber Berdasarkan Peran Pelaku Tindak Pidana Siber

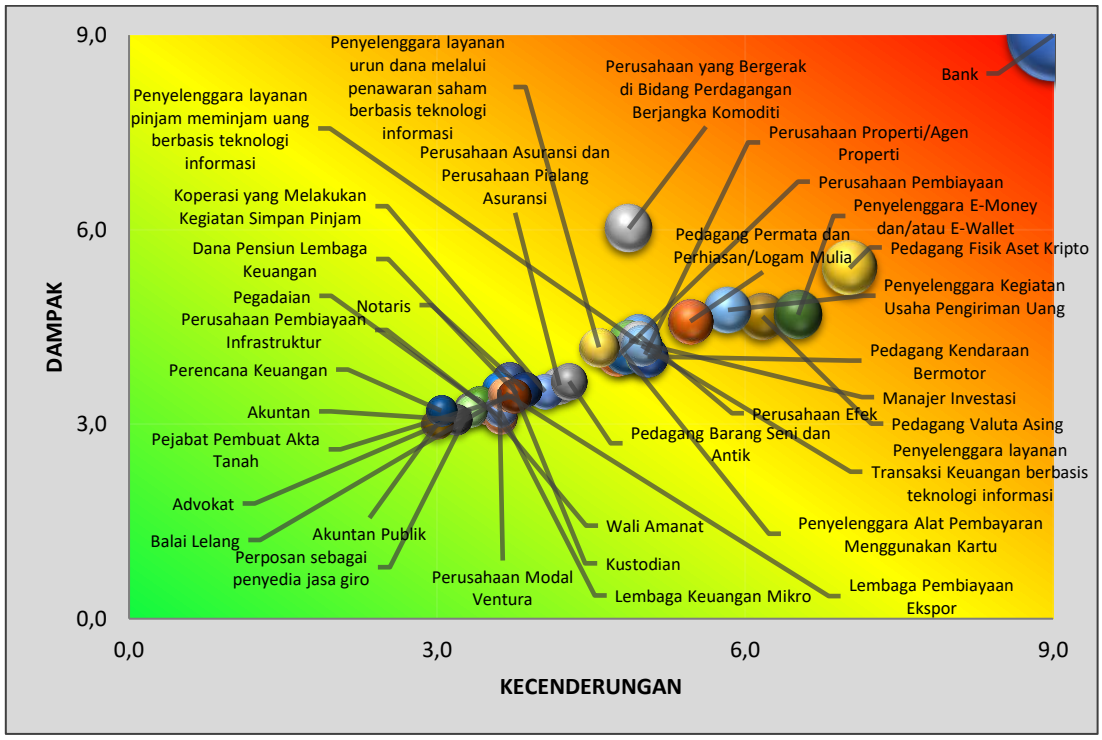


Gambar 10 Tingkat Risiko TPPU Hasil Tindak Pidana Siber Berdasarkan Peran Pelaku Tindak Pidana Siber

Berdasarkan hasil penilaian, ditemukan bahwa dari kasus TPPU hasil TP Siber yang ditemukan di Indonesia, **pelaku TP Siber cenderung juga menjadi pelaku TPPU**.

6. Tingkat Risiko TPPU Hasil Tindak Pidana Siber Berdasarkan Sektor Industri Pihak Pelapor

Sektor industri pihak pelapor yang dianggap berisiko tinggi TPPU hasil Tindak Pidana Siber adalah **Bank**. Sementara itu, Pedagang Fisik Aset Kripto dinilai berisiko menengah dan pihak pelapor lainnya dianggap berisiko rendah. Pelaku TPPU hasil TP Siber masih cukup banyak menyalahgunakan sektor perbankan untuk pencucian uang, dan beberapa mulai bergeser kepada aset kripto.

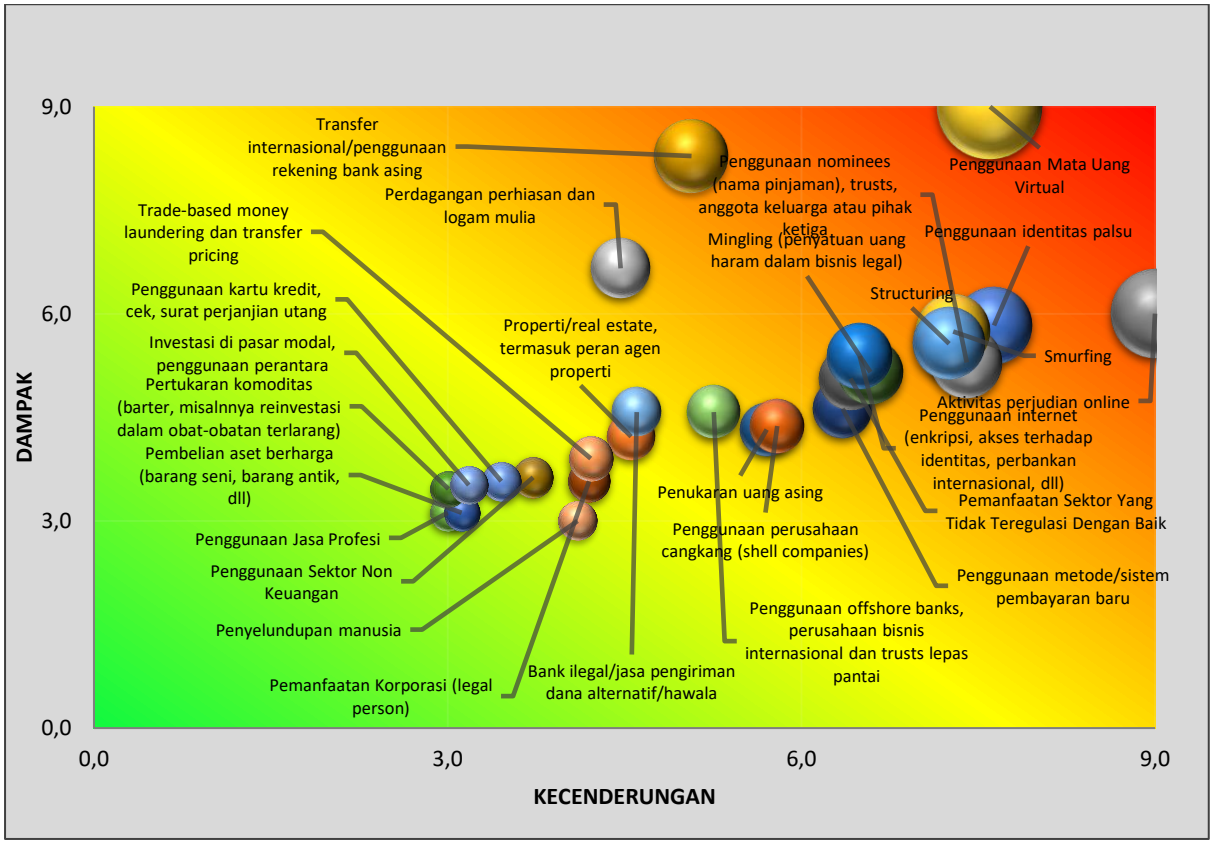


Gambar 11 Tingkat Risiko TPPU Hasil Tindak Pidana Siber Berdasarkan Sektor Industri Pihak Pelapor

7. Tingkat Risiko TPPU Hasil Tindak Pidana Siber Berdasarkan Tipologi TPPU

Tipologi TPPU hasil TP Siber yang berisiko tinggi di Indonesia adalah **penggunaan mata uang virtual** dan **perjudian *online***. Penggunaan mata uang virtual/aset kripto di sini belum tentu difasilitasi Pedagang Fisik Aset Kripto di dalam negeri karena aset kripto

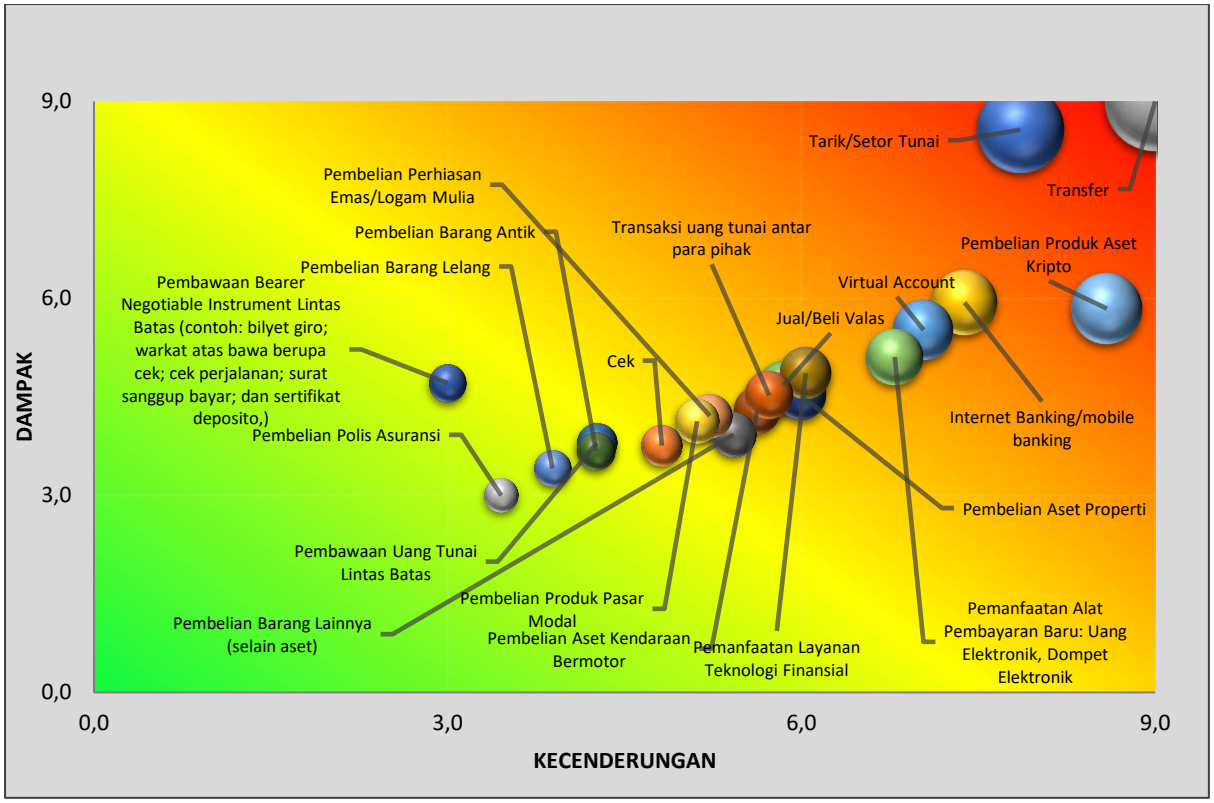
tidak hanya dapat diperoleh dari Pedagang Fisik Aset Kripto di dalam negeri, tetapi bisa dengan menambang/*mining*, transaksi dari orang ke orang (*peer-to-peer*), dan Pedagang Fisik Aset Kripto di luar negeri. Jika transaksi aset kripto melalui Pedagang Fisik Aset Kripto di Indonesia, akan lebih mudah dilacak aparat penegak hukum, karena Pedagang Fisik Aset Kripto merupakan salah satu pihak pelapor. Namun jika pelaku menggunakan jasa Pedagang Fisik Aset Kripto di luar negeri, penegak hukum di Indonesia akan mengalami kesulitan dalam melacaknya.



Gambar 12 Tingkat Risiko TPPU Hasil TP Siber Berdasarkan Tipologi TPPU

8. Tingkat Risiko TPPU Hasil Tindak Pidana Siber Berdasarkan Pola Transaksi

Berdasarkan pola transaksi, pola transaksi yang dinilai berisiko tinggi TPPU hasil TP Siber adalah **transfer** dan **tarik/setor tunai**. *Internet banking/mobile banking,* pembelian produk aset kripto, *virtual account,* dan pemanfaatan alat pembayaran baru (uang elektronik dan dompet elektronik) dinilai berisiko menengah.



Gambar 13 Tingkat Risiko TPPU Hasil TP Siber Berdasarkan Pola Transaksi

9. Potensi Risiko Negara Tujuan, Asal, dan Transit TPPU Hasil TP Siber

Seperti telah dibahas pada bagian sebelumnya, TP Siber tidak mengenal batas wilayah atau teritorial. Untuk itu, kami menanyakan kepada responden negara-negara mana saja yang berpotensi menjadi negara tujuan, negara asal, dan transit TPPU hasil TP Siber. Hasilnya adalah sebagai berikut:

Tabel 3 Potensi Risiko Negara Tujuan, Asal dan Transit TPPU Hasil TP Siber

No	Negara Tujuan Pengiriman Dana TPPU dari Indonesia	Negara Asal Pengiriman Dana TPPU ke Indonesia	Negara Transit Dana TPPU ke Indonesia	Negara Transit Dana TPPU dari Indonesia
1	Singapura	Amerika Serikat	Singapura	Singapura
2	Amerika Serikat	Republik Rakyat Tiongkok	Hong Kong	Malaysia
3	Hong Kong	India	Republik Rakyat Tiongkok	Amerika Serikat

Alasan responden menyebutkan negara-negara di atas berpotensi menjadi negara asal, tujuan, dan transit dana TPPU hasil TP Siber adalah sebagai berikut:

Gambar 14 Alasan Responden Menjawab Negara-Negara yang Berpotensi Menjadi Negara Asal, Tujuan, dan Transit Dana TPPU Hasil TP Siber

B. Tingkat Risiko TPPT

Berdasarkan data yang telah dikumpulkan dan temuan di lapangan, hanya dapat dilakukan penilaian risiko TPPU dari Tindak Pidana Siber. Adapun penilaian risiko TPPT belum dapat dilakukan untuk saat ini karena selama periode kajian (2020 s.d. 2024) belum ditemukan kasus TPPT yang pendanaannya berasal dari Tindak Pidana Siber. Kasus TPPT yang pendanaannya berasal dari tindak pidana siber pernah ditemukan pada tahun 2012 (Kasus CAHYA FITRIANTA sesuai putusan nomor 113/PID/2013/PT.DKI), di mana terdakwa melakukan pendanaan terorisme dengan cara meretas situs investasi. Sesuai hasil Penilaian Risiko Nasional (*National Risk Assessment*) Tindak Pidana Pendanaan Terorisme dan Pendanaan Proliferasi Senjata Pemusnah Massal Tahun 2021, modus pendanaan terorisme di Indonesia selama periode 2016-2020 dilakukan dengan cara yang legal atau tampak legal (PPATK, 2021).

Contohnya adalah sponsor pribadi (*terrorist financier/fundraiser*), penyimpangan pengumpulan donasi melalui organisasi kemasyarakatan (ormas), dan usaha bisnis yang sah.

Meski kasus TPPT dari Tindak Pidana Siber belum ditemukan lagi di Indonesia, bukan berarti teroris atau organisasi teroris tidak memanfaatkan ruang siber untuk melakukan pendanaan atau kegiatan lainnya. Sebagai contoh, senjata yang digunakan untuk serangan di Paris tahun 2015 dan Munchen tahun 2016 diduga diperoleh dari *dark web* (United Nations Office of Counter-Terrorism & United Nations Interregional Crime and Justice Research Institue, 2024). Selain itu, ruang siber juga dimanfaatkan untuk komunikasi, propaganda, dan perekrutan (Malik, 2018; Australian Strategic Policy Institute, 2021). Menurut Levi West, Direktur *Terrorism Studies*, Charles Sturt University Graduate School for Policing and Security, teroris belum banyak beralih ke pendanaan berbasis aktivitas siber, namun untuk perekrutan sudah menggunakan ruang siber (Australian Strategic Policy Institute, 2022).

Pada tahun 2023, Global Terrorism Index menyebutkan Burkina Faso (Afrika Barat) sebagai negara dengan Indeks Terorisme tertinggi, disusul oleh Israel (Asia Barat) dan Mali (Afrika Barat). Dengan jatuhnya ISIS/ISIL, memang terdapat pergeseran peta terorisme global ke wilayah sekitar Afrika Barat. Dalam konteks wilayah Sahel (pertemuan antara daerah sub-Sahara Afrika dan Timur Tengah), ruang siber yang kurang terawasi dan kurangnya mekanisme untuk mengatur arus kas lintas batas dianggap dapat mempercepat proses bertambahnya sel-sel jihad di negara-negara Afrika Barat di masa yang akan datang, atau kelompok-kelompok yang sudah ada akan terus mengonsolidasikan kekuatan dengan memperluas jaringan dan basis rekrutmen mereka. Disebutkan pula bahwa penipuan siber dapat menjadi sumber pendanaan penting bagi kelompok jihad di sana (Australian Strategic Policy Institute, 2022). FATF (2020) juga menyebutkan pandemi Covid-19 dapat meningkatkan kasus Tindak Pidana Siber seperti penipuan dan dapat berdampak pada pendanaan daring oleh teroris yang berkedok donasi Covid-19.

Perkembangan Teknologi selain ruang siber juga dimanfaatkan pelaku terorisme atau pendanaan terorisme untuk melakukan pendanaan terorisme, misalnya Aset Kripto (*Crypto Asset/Virtual Asset*[3]). Sebelum marak Aset Kripto, sarana pengiriman uang melalui internet juga

[3] FATF menggunakan istilah Aset Virtual/*Virtual Asset* namun Indonesia menggunakan istilah Aset Kripto sesuai Peraturan Menteri Perdagangan Nomor 99 Tahun 2018 tentang Kebijakan Umum Penyelenggaraan Berjangka Aset Kripto (*Crypto Asset*). Aset Kripto berbeda dengan Aset Virtual FATF karena Aset Kripto di Indonesia tidak diizinkan

telah digunakan oleh teroris atau pendana teroris untuk memindahkan dana (Sa'diyah, 2017). Secara internasional, Al-Qaeda diketahui melakukan penggalangan dana melalui Aset Kripto (U.S. Immigration and Customs Enforcement, 2020).

Kasus dugaan pendanaan terorisme melalui penipuan siber ditemukan di Amerika Serikat, di mana fasilitator ISIS melakukan penjualan masker N95 yang berstandar FDA (Food and Drug Administration) Amerika Serikat, di mana sebenarnya masker tersebut tidak berstandar FDA (U.S. Immigration and Customs Enforcement, 2020). Meski TPPT melalui Tindak Pidana Siber belum terjadi kembali di Indonesia, kasus penipuan siber sebagai sumber dana TPPT yang terjadi di Amerika Serikat ini perlu diwaspadai, begitu pula dengan pemanfaatan ruang siber dan teknologi keuangan dalam pendanaan terorisme.

4.2. ANCAMAN BARU (*EMERGING THREAT*)

Ancaman baru atau *emerging threat* TPPU dan TPPT dari hasil TP Siber menurut responden antara lain:

1. Penyalahgunaan AI

   Teknologi *Artificial Intelligence*/AI (kecerdasan buatan) semakin banyak digunakan sekarang ini. Teknologi AI yang mungkin dimanfaatkan pelaku kejahatan adalah AI generatif, misalnya membuat gambar/video yang menyerupai wajah orang asli, serta suara orang asli untuk mengelabui sistem keamanan penyedia jasa keuangan.

2. Penyalahgunaan *e-wallet*

   Dompet elektronik atau *e-wallet* pada dasarnya adalah teknologi yang diciptakan untuk mempermudah pembayaran, namun oleh pelaku kejahatan disalahgunakan sebagai sarana penampungan dana dan pemindahan dana.

digunakan sebagai alat pembayaran. Namun untuk tujuan kajian ini, dapat dianggap Aset Kripto adalah Aset Virtual sesuai definisi FATF.

3. Penggunaan layanan percampuran koin/*coin mixer*

Layanan percampuran koin dapat mengaburkan jejak aset kripto karena dapat mencampurkan aset-aset kripto dan mentransfernya kembali sehingga tampak legal.

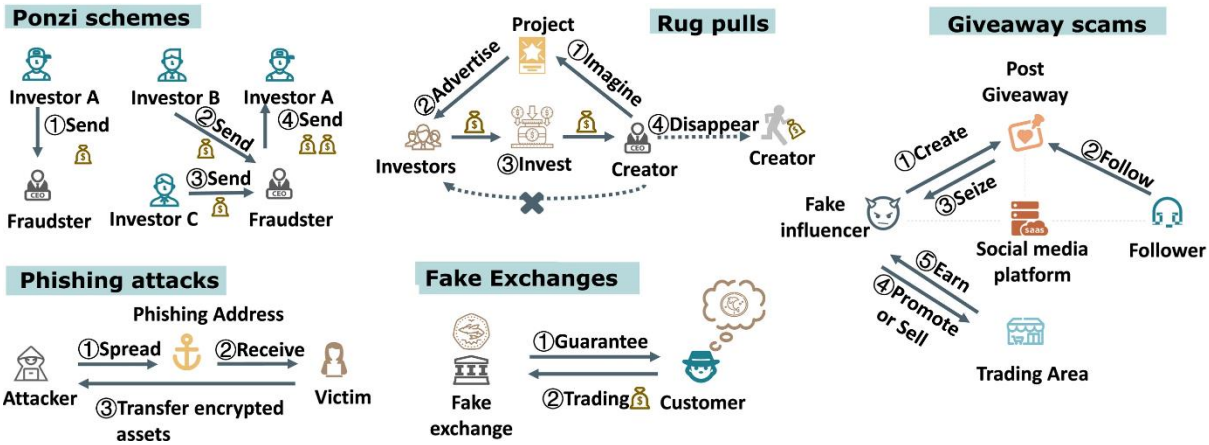
4. Pengiriman tautan/berkas yang berisi virus atau untuk percobaan mengambil alih data pengguna

Modus ini merupakan modus tindak pidana siber yang cukup marak beberapa tahun terakhir, yaitu pengiriman pesan melalui aplikasi perpesanan yang berisi tautan atau berkas yang ternyata berisi virus atau dapat memasang aplikasi yang dapat mencuri data pengguna.

5. Penggunaan *private wallet address*

Aset kripto memungkinkan transaksi tidak hanya melalui pedagang fisik aset kripto namun juga transaksi pribadi dari orang ke orang. Penggunaan alamat dompet pribadi atau *private wallet address* dapat menyulitkan penyidik dalam melacak dana.

6. Eksploitasi Web3 dan Aset Kripto



Gambar 15 Skema Penipuan dengan Aset Kripto

Sumber: Wu et al. (2023)

Web3 adalah generasi internet terbaru yang menggunakan teknologi *blockchain* untuk mendekatkan pengguna dengan aset digital dan identitas mereka. Aset kripto menjadi pusat ekonomi berbasis Web3 ini. Belum seragamnya regulasi *blockchain* di seluruh dunia

memungkinkan Web3 dieksploitasi pelaku kejahatan. Di pasar aset kripto, penipu menggunakan karakteristik aset kripto yang bersifat pseudonim untuk melakukan penipuan aset kripto yang tidak dapat dilacak dan mencoba menipu investor untuk mendapatkan keuntungan yang diperoleh secara tidak sah.

4.3. TIPOLOGI DAN STUDI KASUS

Di bagian ini akan dibahas studi kasus berdasarkan putusan pengadilan di Indonesia terkait TP Siber dan TPPU (7 kasus) dan 1 kasus yang berasal dari Australia. Dari kasus-kasus di bawah, dapat disimpulkan hal-hal sebagai berikut:

1. Pelaku masih menggunakan rekening bank untuk menampung dan memindahkan dana.
2. Pelaku masih membeli barang fisik untuk menyamarkan asal-usul hasil tindak pidana.
3. Pelaku memanfaatkan pedagang fisik aset kripto di dalam dan luar negeri untuk menyembunyikan dan menyamarkan asal-usul hasil tindak pidana.

Kasus 1

TPA Akses Ilegal

Berdasarkan Putusan no. 355/Pid.Sus/2021/PN Dps

I GEDE ADNYA SUSILA bekerja sebagai Marketing Kredit di BPR Lestari Cabang Benoa, Denpasar. I MADE DARMAWAN merupakan salah satu nasabah PT BPR Lestari Cab. Benoa. Bahwa bermula sekitar tanggal 18 Juni 2020, istri dari I MADE DARMAWAN dihubungi oleh I GEDE ADNYA SUSILA yang memberitahukan akan datang ke warung untuk bertemu. Kemudian I GEDE ADNYA SUSILA memberitahukan ada produk layanan perbankan yang harus diaktifkan, yaitu aplikasi LESTARI MOBILE dan menawarkan untuk menginstall aplikasi tersebut pada handphone I MADE DARMAWAN. Selanjutnya I MADE DARMAWAN menyerahkan handphone nya dan I GEDE ADNYA SUSILA mendownload aplikasi Mobile Lestari serta meminta alamat email I MADE DARMAWAN dan diberikan. Setelah menginstall aplikasi tersebut, I GEDE ADNYA SUSILA mengembalikan handphone kepada I MADE DARMAWAN dengan memberitahukan bahwa aplikasi sudah aktif, namun I MADE DARMAWAN tidak mengetahui apakah mobile banking tersebut telah aktif atau belum karena saat itu tidak dicoba untuk melakukan transaksi.

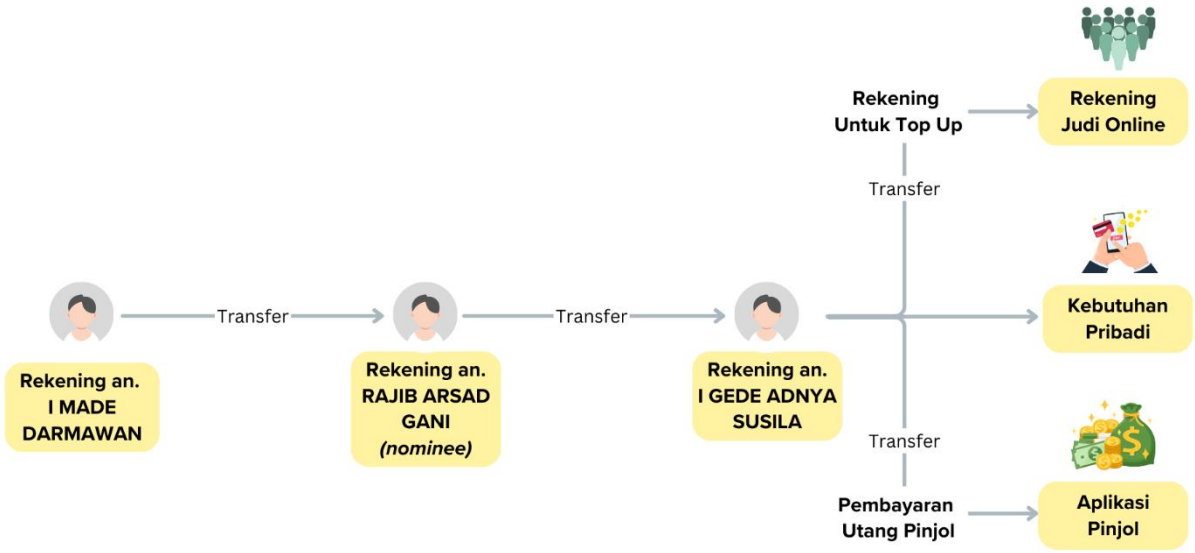
Pada saat yang bersamaan, I GEDE ADNYA SUSILA juga mendownload aplikasi LESTARI MOBILE di handphonenya sendiri. Setelah selesai mendownload aplikasi tersebut selanjutnya

I GEDE ADNYA SUSILA melakukan proses aktivasi di handphone I MADE DARMAWAN dan di handphone nya sendiri secara bersamaan dengan mengisi data nasabah berupa nomor rekening, nomor hp, dan alamat email nasabah. Selanjutnya I MADE DARMAWAN selaku nasabah menerima kode OTP melalui email dan sms dan I GEDE ADNYA SUSILA memasukkan kode OTP tersebut ke handphone miliknya, sedangkan di handphone I MADE DARMAWAN tidak memasukkan kode OTP tersebut. Tidak lama kemudian, I MADE DARMAWAN menerima telpon konfirmasi aktivasi LESTARI MOBILE dari layanan aktivasi dan saat itu I GEDE ADNYA SUSILA mempersilahkan untuk menjawab konfirmasi dari layanan aktivasi tersebut. Selanjutnya I GEDE ADNYA SUSILA membuat PIN *mobile banking* untuk digunakan melakukan transaksi, kemudian I GEDE ADNYA SUSILA mengembalikan handphone I MADE DARMAWAN sambil menyampaikan bahwa LESTARI MOBILE telah aktif, padahal pada kenyataannya tidak aktif, melainkan yang aktif adalah mobile banking yang ada pada handphone milik I GEDE ADNYA SUSILA saja. Bahwa selanjutnya I GEDE ADNYA SUSILA menggunakan Lestari Mobile milik I MADE DARMAWAN yang ada pada handphone I GEDE ADNYA SUSILA untuk melakukan transaksi transfer dana dari rekening milik I MADE DARMAWAN ke beberapa rekening termasuk rekening I GEDE ADNYA SUSILA sendiri, dengan rincian sebagai berikut:

1. Bulan Juni 2020 terdapat 3 kali transaksi dengan total nominal Rp150.000.000, yang ditransfer melalui Mobile Banking ke Rekening BCA 0380658160 an. RAJIB ARSAD GANI.
2. Bulan Juli 2020 terdapat 8 kali transaksi dengan total nominal Rp277.100.000, yang ditransfer melalui Mobile Banking ke Rekening BCA 0380658160 an. RAJIB ARSAD GANI.
3. Bulan Agustus 2020 terdapat 14 kali transaksi dengan total nominal Rp453.050.000, yang ditransfer melalui Mobile Banking ke Rekening BCA 0380658160 an. RAJIB ARSAD GANI.
4. Bulan September 2020 terdapat 3 kali transaksi dengan total nominal Rp96.500.000, yang ditransfer melalui Mobile Banking ke Rekening BCA 0380658160 an. RAJIB ARSAD GANI.
5. Bulan Oktober 2020 terdapat 11 kali transaksi dengan total nominal Rp425.000.000, dengan rincian 7 kali transaksi yang ditransfer melalui Mobile Banking ke Rekening BCA 0380658160 an. RAJIB ARSAD GANI dengan total nominal sebesar Rp280.000.000 serta 4 kali transaksi yang ditransfer melalui QR Mobile Banking ke Rekening BPR Lestari 0100050466 an. ADNYA SUSILA dengan total nominal sebesar Rp145.000.000.

6. Bulan November 2020 terdapat 2 kali transaksi dengan total nominal Rp53.500.000 yang ditransfer melalui QR Mobile Banking ke Rekening BPR Lestari 0100050466 an. ADNYA SUSILA.

Dengan total transaksi transfer adalah sejumlah Rp1.455.150.000. Bahwa semua uang tersebut digunakan oleh I GEDE ADNYA SUSILA untuk mengikuti permainan judi online dan juga untuk biaya kepentingan pribadinya.



Gambar 16 Gambaran Kasus I Gede Adnya Susila

Perbuatan terdakwa sebagaimana diatur dan diancam pidana melanggar Pasal 32 Ayat (2) Jo Pasal 48 Ayat (2) UU RI Nomor 19 Tahun 2016 tentang Perubahan atas UU RI Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta Pasal 3 UU RI Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang dengan pidana penjara selama 5 (lima) tahun dan denda sejumlah Rp.2.000.000.000,00 (dua milyar rupiah), dengan ketentuan apabila denda tersebut tidak dibayar diganti dengan pidana kurungan selama 3 (tiga) bulan.

Kasus 2

TPA Pornografi dan Judi Online

Berdasarkan Putusan Nomor 345/PID.SUS/2020/PT BDG

Reynaldi Marcellino alias Lim Sui Liong Alias Ali merupakan pemilik dari website yang memuat konten pornografi dengan alamat situs https://zonalendir.net/. Muatan konten pornografi yang terdapat di website tersebut tidak hanya memuat konten pornografi dewasa,

melainkan pula melibatkan anak sebagai objek. Website tersebut turut memasang iklan yang tercatat sebanyak 28 konten yang terdiri dari 22 forum porno dengan total 917.559 utas dan 145.359 anggota, serta 6 (enam) forum yang terdiri dari 34.043 utas dan 2.630 anggota.

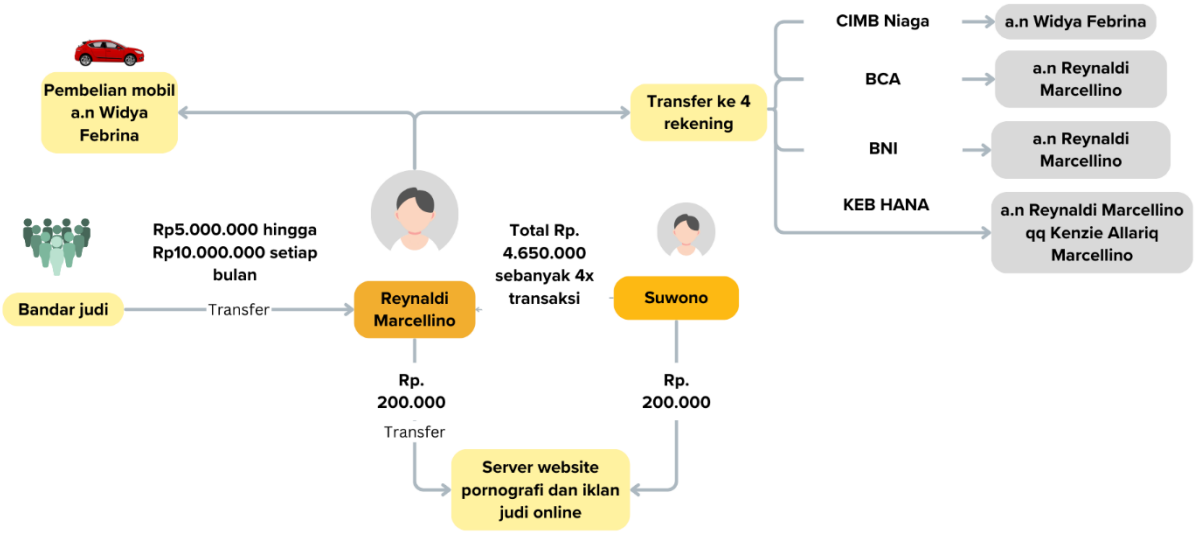
Hasil penelusuran penyidik menghasilkan bukti bahwa terdapat keterlibatan pihak lain atas nama Suwarno alias Eno. Terdakwa Reynaldi dan Eno sepakat untuk melakukan kerja sama secara finansial dalam hal penyediaan website yang memuat konten pornografi dan konten iklan judi online. Kerja sama ini mencakup penyewaan server pada laman www.ditusuk.in, serta membuat website baru dengan alamat web http://terselubung.us.

Terdakwa Reynaldi Marcellino memperoleh cerita, foto, video yang mengandung unsur pornografi atau melanggar kesusilaan dengan cara terdakwa mengambil dari forum www.semprot.com yang merupakan forum yang memuat konten pornografi serta penyedia prostitusi online terbesar di Indonesia. Konten yang mengandung unsur pornografi atau melanggar kesusilaan tersebut dapat dilihat oleh siapa saja pengunjung tanpa harus menjadi member terlebih dahulu.

Keuntungan yang didapat dari semua website forum yang dimiliki terdakwa sejak pertama kali beroperasi sampai diputus oleh Pengadilan adalah sekitar Rp100.000.000 (seratus juta rupiah). Keuntungan finansial tersebut digunakan terdakwa untuk biaya operasional website, membeli handphone, komputer, laptop dan kebutuhan hidup sehari-hari. Terdakwa turut membeli 1 (satu) unit mobil merk Wulling warna hitam metalik Tahun 2017 dengan identitas Nomor Polisi F-1015-BA. Perbuatan terdakwa dalam membeli barang-barang dengan uang keuntungan dari pemasangan iklan di website yang memuat konten asusila ini termasuk perbuatan membelanjakan harta hasil tindak pidana dan terdapat upaya untuk menyamarkan asal-usul harta hasil tindak pidana.

Terdakwa terbukti melanggar Pasal 45 ayat (1) Undang-Undang Nomor 19 tahun 2016 tentang Perubahan Atas Undang-undang Nomor 11 tahun 2008 tentang Informasi dan Transaksi Elektronik jo pasal 55 ayat (1) ke-1 KUHP, Pasal 3 Undang-Undang Nomor 8 Tahun 2010 Tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang dan Undang-undang Nomor 8 Tahun 1981 tentang Hukum Acara Pidana serta peraturan perundang-undangan lain yang bersangkutan. Pidana yang dijatuhkan kepada Reynaldi Marcellino alias Lim Sui Liong adalah hukuman penjara selama 8 (delapan) tahun dikurangi masa terdakwa berada dalam tahanan sementara dengan perintah supaya terdakwa tetap ditahan dan

membayar denda sebesar Rp1.000.000.000 (satu miliar rupiah) subsidiair 6 (enam) bulan kurungan.



Gambar 17 Gambaran Kasus Reynaldi Marcellino alias Lim Sui Liong Alias Ali

Kasus 3

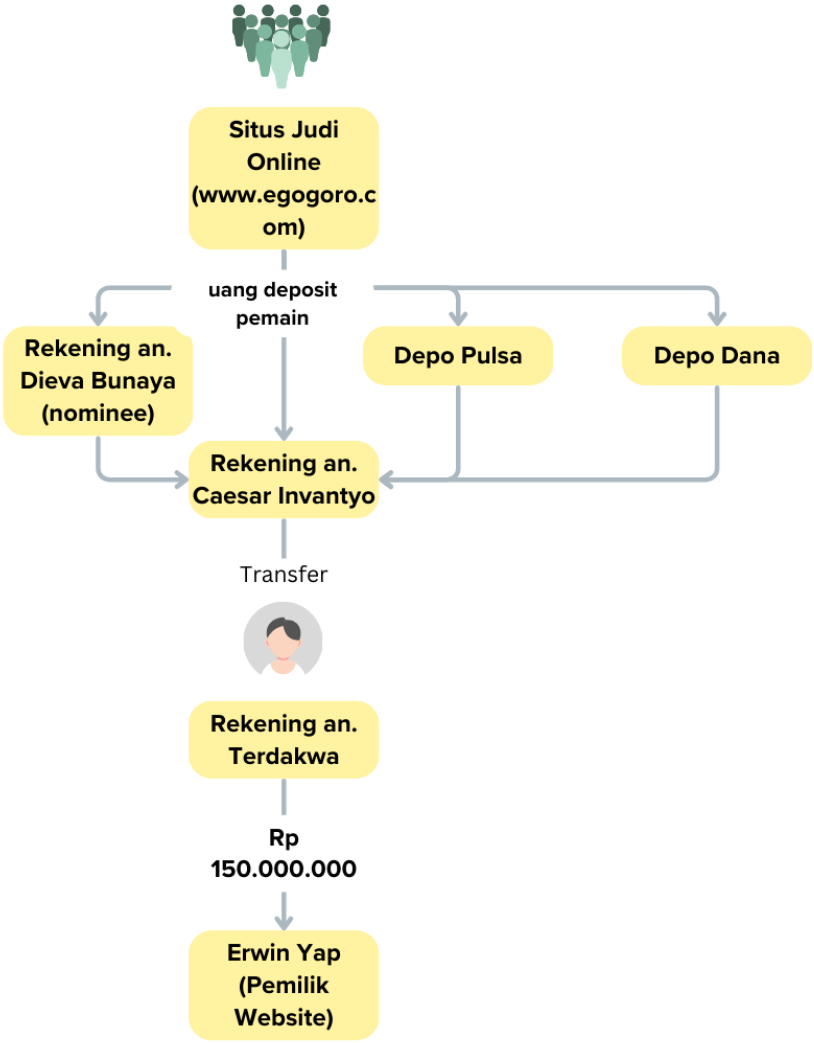
TPA Perjudian secara Online

Berdasarkan Putusan no. 94/Pid.Sus/2024/PN Jkt.Utr

Indradi Als. Indradi Halim Als. OOW anak dari Bahtiar Halim merupakan team leader marketing pada website judi online www.egogoro.com yang menyediakan permainan judi bola online, slot, dan casino. Terdakwa berperan dalam mengelola website dan mengatur karyawan agar mencari atau mengajak orang lain untuk bermain judi di website tersebut. Sebelum memulai permainan, pemain harus terlebih dahulu memasukan uang deposit ke dalam akun judi online miliknya. Para karyawan yang telah direkrut oleh terdakwa memiliki tugas dalam membantu proses deposit termasuk pencairan dana yang dilakukan pemain. Uang deposit dari pemain ditampung pada nomor rekening:

1. Rekening BCA 0403062950 an. Dieva Bunaya yang diperoleh terdakwa dengan cara membeli kepada pihak ketiga;
2. Rekening BNI 1438849085 an. Caesar Ivantyo yang merupakan karyawan sales marketing website www.egogoro.com ;
3. BRI 721001012690536 an. Caesar Ivantyo;
4. Mandiri 60011499815 an. Caesar Ivantyo;
5. Depo pulsa ke nomor Telkomsel 081283879894; dan

6. Depo Dana ke nomor Smartfren 08886392504.



Gambar 18 Gambaran Kasus Indradi Als. Indradi Halim Als. OOW

Penyelenggaraan website judi online tersebut menghasilkan omset sebesar Rp300.000.000,00 dengan keuntungan yang diperoleh sebesar Rp150.000.000,00. Keuntungan tersebut kemudian oleh Caesar Ivantyo ditransfer ke rekening terdakwa yang selanjutnya disetorkan kepada Erwin Yap (berkewarganegaraan Singapura) selaku pemilik situs website www.egogoro.com. Terdakwa terbukti sah dan menyakinkan bersalah melakukan tindak pidana Turut serta dengan sengaja dan tanpa hak mendistribusikan dan/mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki muatan perjudian dan menempatkan, mentransfer, mengalihkan, memberlanjakan, membayarkan, mengibahkan, menitipkan, membawa keluar negeri, mengubah bentuk, menukarkan dengan mata uang atau surat berharga atau perbuatan lain atas harta kekayaan yang diketahuinya atau patut diduganya merupakan hasil tindak pidana dengan tujuan

menyembunyikan atau menyamarkan asal usul harta kekayaan. Terdakwa dijatuhi pidana penjara selama 1 (Satu) Tahun dan 6 (Enam) bulan dan denda sejumlah Rp75.000.000,00 (Tujuh puluh lima juta rupiah).

Kasus 4

TPA Phishing

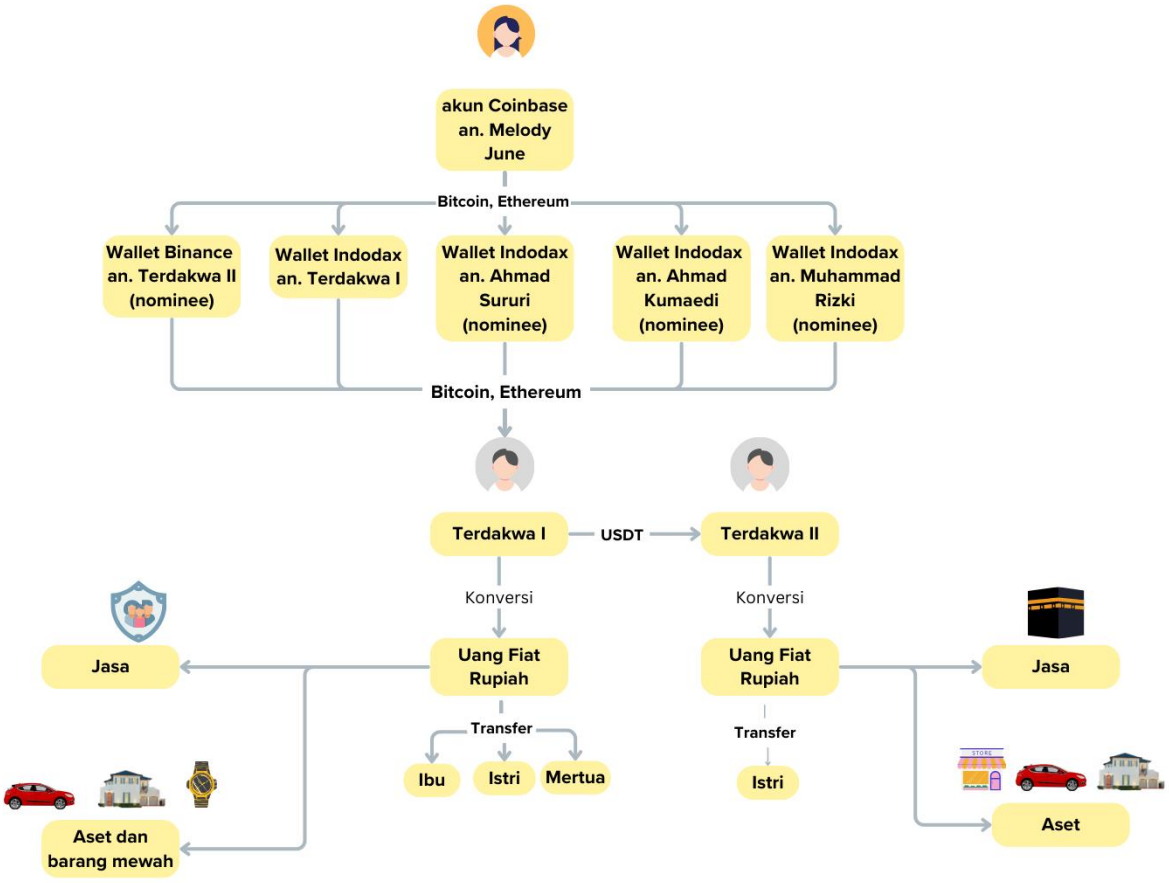
Berdasarkan Putusan No. 511/Pid.Sus/2023/PM JKT.SEL

Muhammad Fauji Alfariz (terdakwa I) melalui akun Facebook Kristen memperoleh alamat email dengan domain hotmail sebanyak kurang lebih 2 juta, akun dan password Remote Desktop Protocol (RDP), SMTP dan C Panel dari grup Facebook SIXTEEN MARKET. Dengan alamat email, SMTP Google, RDP dan C Panel yang sudah diperoleh, terdakwa I memulai aksi menggunakan metode phising yang mana *script web phising* sudah terlebih dahulu dibuat oleh terdakwa I. Email yang dikirimkan terdakwa kepada calon korban nantinya tampak sebagai email yang seolah-olah adalah email asli dari Platform Coinbase yang berisi berita bahwa akun Coinbase calon korban mengalami masalah dan perlu diverifikasi kembali. Salah satu korban dari aksi tersebut adalah Melody June Royalty dengan alamat email melody_sturgill@hotmail.com . Korban mengklik tombol palsu yang kemudian mengarah pada web phising yang telah dibuat terdakwa I. Pada halaman tersebut, korban mengisi user dan password akun Coinbase yang berisikan mata uang digital miliknya. Akun dan password tersebut pun tertampung dalam kotak pandora yang nantinya diakses oleh terdakwa I melalui RDP.

Setelah mendapatkan akses ke dalam akun Coinbase milik korban, terdakwa I pun memindahkan mata uang digital berupa Bitcoin dan Ethereum milik korban ke *wallet* Binance milik Fahri Fauzi (terdakwa II) dan beberapa wallet Indodax yang dikuasai terdakwa I dalam 5 kali transaksi. Total mata uang digital yang dipindahkan tersebut apabila dikonversikan ke mata uang fiat pada saat itu jumlahnya kurang lebih senilai Rp19.330.191.926,00. Terdakwa I juga memberikan mata uang digital berupa USDT kepada terdakwa II karena telah meminjamkan wallet Binance kepada terdakwa I yang apabila dikonversikan pada saat itu ke mata uang fiat jumlahnya kurang lebih senilai Rp2.500.000.000,00. Sementara itu wallet Indodax yang dikuasai oleh terdakwa I dibuat atas nama terdakwa I, Ahmad Sururi, Ahmad Kumaedi, dan Muhammad Rizki. Mata uang digital yang telah berada di penguasaan terdakwa I kemudian oleh terdakwa I dikonversikan ke mata uang fiat dalam bentuk rupiah. Uang

tersebut oleh terdakwa I dibelanjakan sejumlah aset (rumah, pakaian, tas, jam dan kendaraan mewah) dan jasa (renovasi rumah, asuransi jiwa) serta transfer (ibu, istri, mertua). Terdakwa II turut mengkonversikan mata uang di bawah penguasaannya ke dalam mata uang fiat rupiah yang kemudian dibelanjakan sejumlah aset (rumah, toko vape, kendaraan) serta jasa (umroh, modifikasi kendaraan) dan melakukan transfer (istri).

Terdakwa I dan II dinyatakan terbukti secara sah dan menyakinkan bersalah melakukan tindak pidan membantu dengan sengaja dan melawan hukum memindahkan atau mentransfer informasi elektronik dan/ atau dokumen elektronik kepada sistem elektronik orang lain yang tidak berhak, yang menimbulkan kerugian bagi orang lain dan pencucian uang. Terdakwa I dan II dijatuhi pidana penjara masing-masing selama 6 (enam) tahun dan masing-masing denda sebesar Rp2.000.000.000,00 (dua miliar rupiah).



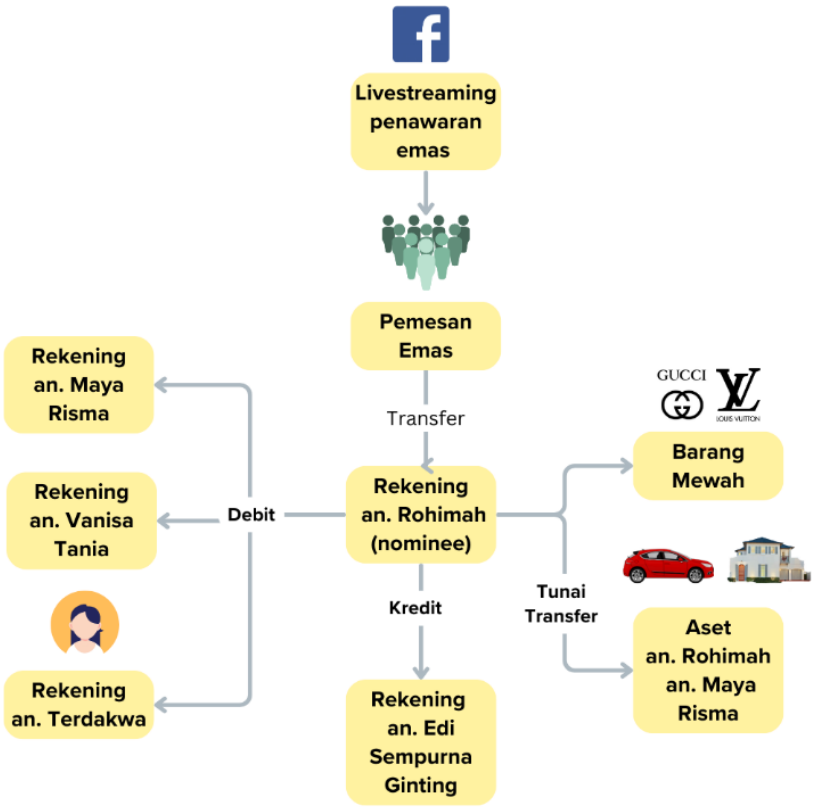
Gambar 19 Gambaran Kasus Muhammad Fauji Alfariz dan Fahri Fauzi

Kasus 5

TPA Penipuan

Berdasarkan Putusan no. 205/PID.SUS/2021/PT.DKI

Drelia Wangsih menggunakan akun Facebook miliknya untuk untuk menawarkan logam mulia emas yang didapatkan dari PT. Antam Tbk dengan harga yang relatif murah. Penawaran dilakukan melalui *Livestreaming*/siaran langsung dengan membacakan/menayangkan list harga emas antam terbaru serta menunjukan logam mulia emas antam yang terdakwa jual dengan mengatakan bahwa emas selalu tersedia dan siap dikirim. Padahal emas tersebut dibeli terdakwa dari Toko Emas Mulia ITC Cempaka Emas Mega Grosir, Toko Emas Singa Emas dan toko emas di Pasar Koja Jakarta Utara. Emas tersebut kemudian dikirim kepada para pembeli sehingga pembeli merasa yakin dan tertarik untuk membeli kembali. Padahal terdakwa tidak memiliki ijin sebagai penjual emas. Terdakwa menyediakan nomor rekening atas nama Rohimah untuk memudahkan transaksi pembayaran bagi para pembeli. Namun setelah pemesanan berikutnya dalam jumlah uang yang lebih besar terdakwa tidak mengirimkan emas pesanan walaupun para pemesan sudah mentransferkan uang dan uang yang telah ditransfer tersebut tidak dikembalikan oleh terdakwa.



Gambar 20 Gambaran Kasus Drelia Wangsih

Uang atas pembayaran emas yang tertampung di rekening atas nama Rohimah kemudian dipindahkan ke rekening milik terdakwa. Transaksi yang telah dilakukan terdakwa dari uang yang diperoleh antara lain sebagai berikut:

1. Membeli barang berharga dengan merek Louis Vuitton, Gucci, Christian Dior, dan Off White;
2. Transaksi debit dari rekening an. Rohimah ke rekening an. Maya Risma, an. Vanisa Tania, dan an. Terdakwa;
3. Transaksi kredit dari rekening an. Rohimah ke rekening an. Edi Sempurna Ginting; dan
4. Pembelian tanah dan bangunan serta kendaraan baik secara tunai maupun kredit.

Terdakwa dinyatakan terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana penipuan dan pencucian uang. Terdakwa dijatuhi pidana penjara selama 4 (empat) tahun dan denda sebesar Rp500.000.000,00 (lima ratus juta rupiah).

Kasus 6

TPA Penjualan Fiktif Alat Kesehatan melalui *Website*

Berdasarkan Putusan no. 492/Pid.Sus/2019

Sdr. James Bangun (DPO) menghubungi Aldaf Risia (Terdakwa I) untuk dicarikan rekening bank dengan menggunakan data palsu (*nominee*) untuk menampung pembayaran jual beli fiktif *online* alat kesehatan di *website* www.bastmed.com milik Sdr. James Bangun, dan Terdakwa I akan mendapatkan imbalan sebesar 20% dari uang yang masuk ke dalam rekening tersebut. Selanjutnya, Terdakwa I menghubungi Jamaluddin Garinging (Terdakwa II) untuk meminta nomor rekening palsu sesuai dengan permintaan Sdr. James Bangun dan Terdakwa II akan mendapatkan imbalan 20% dari uang yang masuk ke rekening tersebut. Terdakwa II berhasil mendapatkan nomor rekening palsu dengan cara membelinya dari Sdr. Adi Sucipto dengan harga sekitar Rp3.000.000,00 dan mendapatkan buku tabungan Bank BNI, kartu ATM dengan nomor rekening 0721835260 atas nama Mashuri. Kemudian Terdakwa II memberitahukan kepada Terdakwa I dan informasi tersebut diteruskan oleh Terdakwa I ke Sdr. James Bangun.

Sdr. James Bangun Kembali menghubungi Terdakwa I bahwa akan ada calon pembeli yang akan membayar atas nama Andrea Martinez ke Bank BNI. Kemudian, Terdakwa I diminta untuk membalas *e-mail* dari calon pembeli menggunakan *e-mail* sales@bastmed.com mengenai pembelian produk kesehatan VERSA-TRAC Lumbar Retractor Master Set sebanyak

2 buah sebesar USD 8.400 dan setelah terjadi kesepakatan harga, Terdakwa I mengedit *invoice company profile* menjadi Bastmed d/h MASHURI supaya korban menjadi lebih percaya.

Terdakwa II menginformasikan kepada Terdakwa I bahwa terdapat uang masuk dari Andrea Martinez ke rekening penampung sebesar USD 8.400 atau Rp123.302.480,00. Adapun dari uang tersebut, Terdakwa II mendapatkan imbalan sebesar 20% yakni Rp24.000.000,00 dan sisanya Terdakwa II transfer ke rekening Bank BCA atas nama Aldaf Risia dengan nomor rekening 0080852983 secara bertahap yakni melalui setoran teller di KCP Nagoya Bank BCA sebesar Rp45.000.000.- (empat puluh lima juta rupiah), kedua sebesar Rp47.250.000.- (empat puluh tujuh juta dua ratus lima puluh ribu rupiah) melalui setoran teller di KCP PENUIN Bank BCA Batam, dan ketiga sebesar Rp9.000.000.- (sembilan juta rupiah) melalui mobile Banking Bank Mandiri. Kemudian Terdakwa I mentransfer uang yang telah dikirimkan Terdakwa II, kepada Sdr. James Bangun dengan nomor rekening 8200283563 (bank BCA) setelah dipotong sebesar Rp16.000.000,00 (enam belas juta rupiah) sebagai imbalan untuk Terdakwa I sehingga uang yang ditansfer kepada Sdr. JAMES BANGUN sebesar Rp74.000.000,00 (tujuh puluh empat juta rupiah).

Terdakwa I dan Terdakwa II terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana penipuan dan permufakatan jahat pencucian uang mentransfer harta kekayaan yang diketahui merupakan hasil tindak pidana dengan tujuan menyamarkan harta kekayaan. Para terdakwa dijatuhi pidana penjara masing-masing selama 1 (satu) tahun dan 8 (delapan) bulan serta denda sejumlah Rp50.000.000,00.

Gambar 21 Gambaran Kasus Aldaf Risia dan Jamaluddin Garinging

Kasus 7

TPA Penipuan dan Penggelapan Investasi Robot Trading

Berdasarkan Putusan Nomor 24/Pid-Sus/2023/PT.DKI.

Terdakwa Hendry Susanto bekerja sama dengan Dylan Velio untuk membuat usaha robot trading. Hendry Susanto bertindak sebagai pendiri sekaligus direktur PT. FSP Akademi Pro, sedangkan Dylan Velio bertindak sebagai pendiri PT. Lotus Global Buana. PT FSP Akademi Pro bertindak sebagai penjual aplikasi *robot trading* Fahrenheit, sedangkan PT Lotus Global Buana bertindak sebagai *broker robot trading*.

Izin usaha yang didaftarkan dimuat pada lampiran Perizinan Berusaha Berbasis Risiko PT. FSP Akademi Pro Nomor: 12770007304210003 sebagai Piranti Lunak Pencatatan Keuangan dengan 3 (tiga) jenis merk barang, yaitu Catat Basic, Catat Pro, dan Catat Premium. Adapun pelanggaran yang dilakukan terdakwa adalah karena tidak melakukan kegiatan usaha yang sesuai dengan perizinan yang dimiliki. Penyebaran informasi penjualan Robot Trading Fahrenheit dilakukan melalui media sosial dengan cara mengunggah video di Youtube, Tiktok, Instagram, Twitter, dan Facebook, serta penyebaran *digital flyer* melalui unggahan cerita Whatsapp yang dibuat oleh Inton Luando Yohanes.

Adapun PT. Lotus Global Buana sebagai broker bagi member robot trading Fahrenheit tidak memiliki izin dari Bappepti untuk penjualan usaha sebagai Bursa Berjangka, Lembaga Kriling Berjangka, Pialang Berjangka, Penasihat Berjangka, Pengelola Sentra Dana Berjangka, sertifikat pendaftaran sebagai Pedagang Berjangka, Calon Pedagang Fisik Aset Kripto maupun perizinan lainnya atas nama PT. Lotus Global Buana. Skema bisnis yang digunakan oleh terdakwa adalah Multi Level Marketing (MLM). Adapun skema investasi robot trading yang ditawarkan Fahrenheit menjanjikan keuntungan sebesar 1 persen per hari atau sebesar 20 persen hingga 25 persen per bulan. Setiap member diperolehkan memiliki 2 (dua) akun atau lebih dengan 1 (satu) identitas yang sama ataupun email yang sama.

Akun robot trading yang digunakan akan diverifikasi menggunakan ID akun dan password pada aplikasi Meta Trader 4 (MT4). Biaya untuk mendapatkan robot atau *script* trading Fahrenheit dijual dengan harga 10 persen dari biaya investasi dengan menggunakan kurs Rp15.000 per 1 (satu) dolar AS dan dikemas dengan paket penjualan sebagai berikut.

1. **Newbie** sebesar USD500 atau senilai Rp7.500.000,00 (tujuh juta lima ratus ribu rupiah), nilai Robot 10% atau sebesar $ 50 (lima puluh dollar amerika). Keuntungan trading untuk investor sebesar 50% dan untuk perusahaan 50%.
2. **Premium** sebesar USD1.000 atau senilai Rp15.000.000,00 (lima belas juta rupiah), nilai Robot 10% atau sebesar $100 (seratus dollar amerika). Keuntungan trading untuk investor sebesar 60% dan untuk perusahaan 40%.
3. **Profesional** sebesar USD5.000 atau senilai Rp. 75.000.000,00 (tujuh puluh lima juta rupiah), nilai Robot 10% atau sebesar $500 (lima ratus dollar amerika). Keuntungan trading untuk investor sebesar 70% dan untuk perusahaan 30%.
4. **Expert** sebesar USD10.000 atau senilai Rp150.000.000,00 (seratus lima puluh juta rupiah), nilai Robot 10% atau sebesar $ 1.000 (seribu dollar amerika). Keuntungan trading untuk investor sebesar 75% dan untuk perusahaan 25%.
5. **Advance** sebesar USD 25.000 atau senilai Rp375.000.000,00 (tiga ratus tujuh puluh lima juta rupiah), nilai Robot 10% atau sebesar $2.500 (dua ribu lima ratus dollar amerika). Keuntungan trading untuk investor sebesar 80% dan untuk perusahaan 20%.
6. **Legend** sebesar USD 50.000 atau senilai Rp750.000.000,00 (tujuh ratus lima puluh juta rupiah), nilai Robot 10% atau sebesar $5.000 (lima ribu dollar amerika). Keuntungan trading untuk investor sebesar 90% dan untuk perusahaan 10%.

Terdakwa menjanjikan 3 (tiga) keuntungan yang akan diperoleh member apabila berinvestasi di Robot Trading Fahrenheit, yaitu bagi hasil keuntungan, keuntungan *trading downline* dan bonus grup penjualan berdasarkan peringkat penjualan dalam skema MLM. Bonus yang dijanjikan kepada para member yang berhasil mencari member di bawah jaringannya (*downline*) akan mendapatkan beragam tambahan keuntungan seperti logam mulia, mobil, laptop, handphone, motor dan keutungan komisi yang ternyata merupakan hasil dari dana yang disetor member sendiri, dan bukan dari hasil keuntungan trading.

Pembagian menurut level jaringan member dalam skema MLM yang dijanjikan oleh PT FSP Akademi Pro sebagai berikut.

1. Level 1 sebesar 50%;
2. Level 2 Sebesar 20%;
3. Level 3 sebesar 15%;
4. Level 4 sebesar 10%;

5. Level 5 sebesar 5%.

Saksi-saksi atas nama Maria Fransiska, David, dan terdakwa Hendry Susanto tidak memiliki izin, sertifikasi ataupun pengetahuan yang mumpuni sebagai penyedia *exchanger*, melainkan hanya mengendalikan rekening penampungan dana investasi para member PT. FSP Akademi Pro. Terdakwa menggunakan dana investasi yang berasal dari para member untuk melakukan kegiatan usahanya serta membayarkan operasional perusahaan maupun untuk membagi keuntungan dan bonus para member. Artinya, uang yang disetor oleh member diputar kembali melalui skema ponzi.

Kronologi awal mula *scam* yang dilakukan terdakwa Hendry Susanto adalah dengan membuat video yang diunggah di akun media sosial milik PT. FSP Akademi Pro dan mengumumkan adanya perbaikan regulasi dari pemerintah. Terdakwa menyatakan bahwa pemerintah mengharuskan para penyedia robot trading untuk mengurus perizinan perdagangan robot trading. Pernyataan ini merupakan alasan yang diungkapkan oleh terdakwa yang membuat PT. FSP Akademi Pro menghentikan kegiatan trading dan proses penarikan uang investasi (*withdraw*) para *member*. Pada tanggal 25 Februari 2022, Robot Trading Fahrenheit seolah-olah kembali melakukan kegiatan trading, akan tetapi para member belum bisa melakukan penarikan uang (*withdraw*) dan dijanjikan dapat melakukan penarikan kembali uang dana investasi maupun komisi trading pada tanggal 7 Maret 2022. Trading fiktif ini digunakan untuk meyakinkan para member bahwa PT. FSP Akademi Pro sedang berupaya untuk memenuhi regulasi terbaru yang ditetapkan oleh pemeritah sehingga member tidak merasa panik atau tertipu.

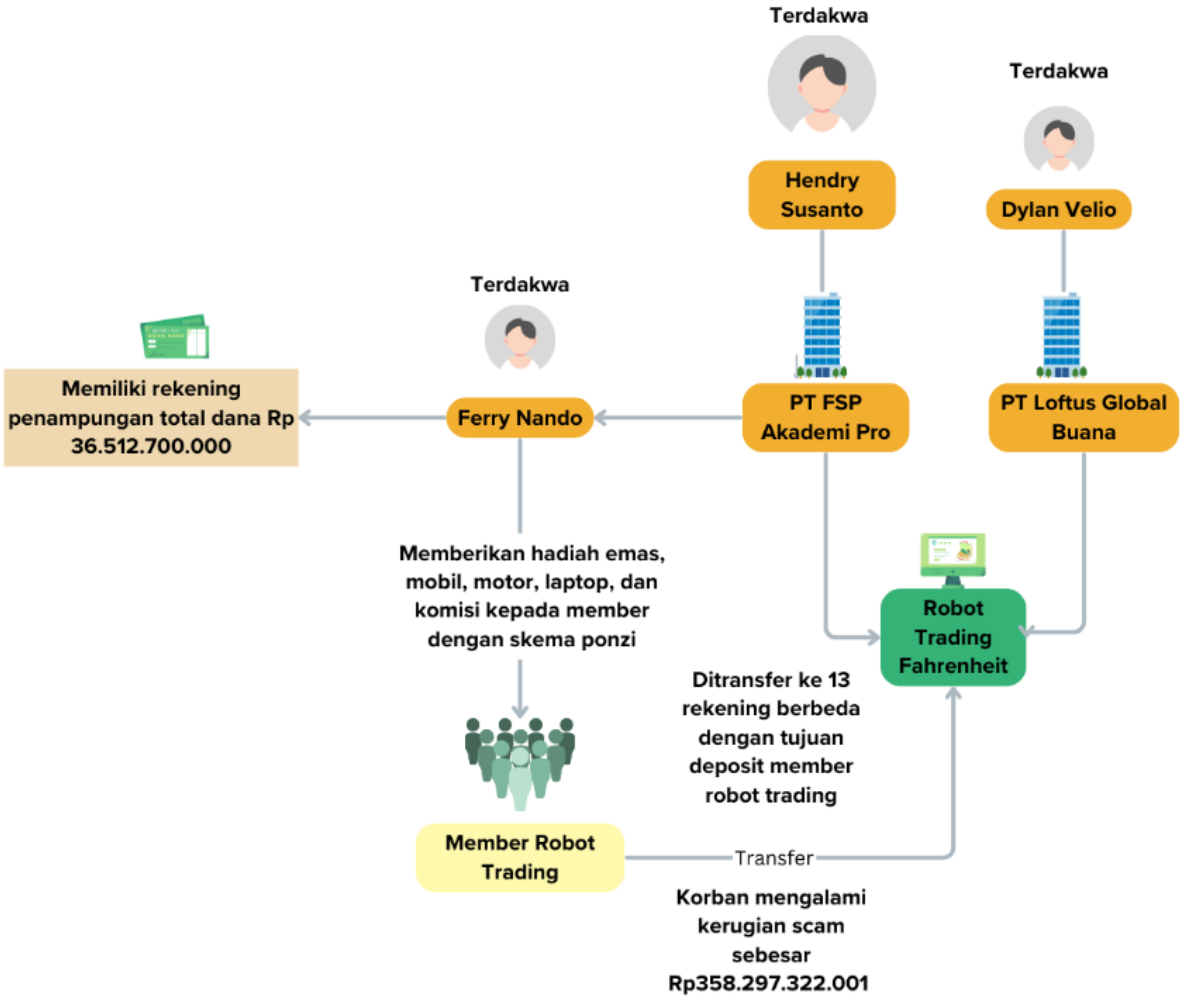
Sejak tanggal 25 Februari 2022 sampai dengan tanggal 7 Maret 2022, terjadi kerugian investasi yang dialami oleh para member robot trading Fahrenheit yang mengakibatkan semua modal para member habis dengan skema yang dibuat seolah *margin call*. Terdakwa Hendry Susanto dan Dylan Velio membuat kondisi kerugian ini seolah-olah sebagai konsekuensi dari transaksi trading yang nyata, padahal transaksi tersebut hanya merupakan transaksi fiktif yang sengaja dibuat margin call sebagai *exit plan*.

Berdasarkan hasil audit terhadap member, sebanyak 1.449 yang telah melapor dari kurang lebih 20.000 *member robot trading* Fahrenheit. Diketahui 1.449 *member* tersebut mengalami kerugian kurang lebih sebesar Rp. 358.297.322.001 (tiga ratus lima puluh delapan milyar dua ratus sembilan puluh tujuh juta tiga ratus dua puluh dua ribu satu rupiah).

Menurut pendapat ahli ITE, Dr. Ronny, S.Kom, M.Kom, M.H., robot trading yang diperdagangkan oleh PT. FSP Akademi Pro adalah ilegal karena belum mendapatkan ijin dari Pemerintah, khususnya dari Lembaga BAPPEBTI (Badan Pengawas Perdagangan Berjangka Komoditi) dan Otoritas Jasa Keuangan (OJK). Tawaran keuntungan investasi dengan potensi keuntungan yang tinggi oleh Fahrenheit dapat mempengaruhi masyarakat untuk ikut dan bergabung menjadi member. Padahal dalam transaksi elektronik perdagangan, terdapat peluang yang sama antara keuntungan dan risiko kerugian. Terlebih lagi bahwa Fahrenheit menawarkan robot trading yang terbukti melakukan transaksi fiktif dan hanya menjalankan skema ponzi dalam skema bisnisnya.

Tindakan yang dilakukan oleh PT. FSP Akademi Pro dengan terdakwa Hendry Susanto, Dylan Velio dan Ferry Nando merupakan tindak pidana sebagaimana diatur dan diancam pidana karena terbukti melanggar Pasal 45A ayat (1) Jo 28 ayat (1) Undang-Undang Nomor 19 Tahun 2016 Tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) jo Pasal 55 ayat (1) ke-1 KUHP DAN pada Dakwaan Kedua Pasal 3 Jo Pasal 10 Undang-Undang Nomor 8 Tahun 2010 tentang Pencegahan dan Pemberantasan Tindak Pidana Pencucian Uang. Terdakwa dinyatakan terbukti melakukan penyembunyian hasil kejahatan dengan menggunakan perusahaan yang berada di bawah pengendalian pelaku. Terdakwa juga terbukti melakukan permufakatan jahat kepada pihak lain sebagai saksi untuk menyediakan rekening penampung untuk menempatkan dana hasil tindak kejahatan.

Para terdakwa terbukti secara sah dan meyakinkan bersalah melakukan tindak pidana dengan sengaja dan Tanpa Hak menyebarkan berita Bohong dan Menyesatkan yang merugikan Konsumen dalam Transaksi Elektronik dan Tindak Pidana Pencucian Uang. Vonis yang dijatuhkan kepada terdakwa adalah pidana penjara terhadap Terdakwa selama 10 (sepuluh) Tahun dan Denda sebesar Rp3.000.000.000,00 (tiga miliar rupiah) dengan ketentuan apabila tidak bisa dibayar diganti dengan kurungan selama 6 (enam) bulan.



Gambar 22 Gambaran Kasus Hendry Susanto

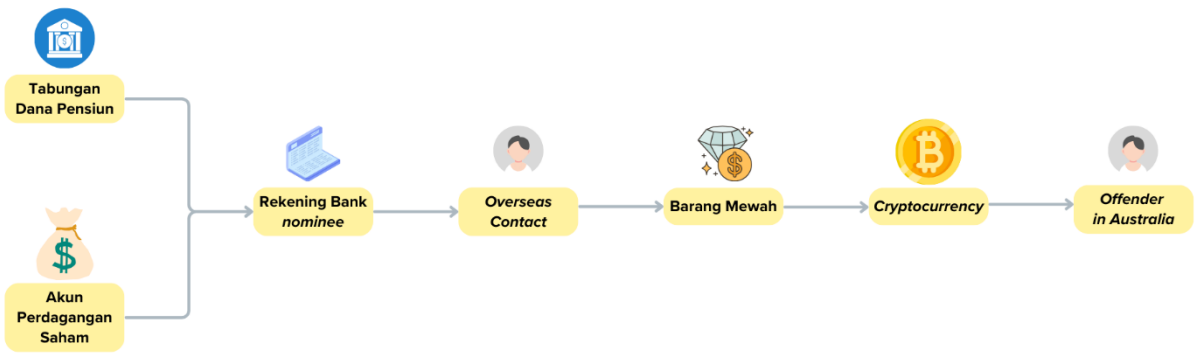
Kasus 8

TPA *Phishing* (Kasus di Australia)

Seorang wanita berusia 24 tahun dari Melbourne telah dijatuhi hukuman karena perannya yang penting dalam sindikat kriminal internasional besar yang mencuri jutaan dolar dari tabungan dana pensiun dan perdagangan saham milik korban yang tidak bersalah dengan menggunakan penipuan dan pencurian identitas. Jumlah yang dicuri melalui skema penipuan ini diperkirakan melebihi $3,3 juta. Upaya juga dilakukan untuk mencuri tambahan $7,5 juta dari tabungan dana pensiun dan perdagangan saham korban. Kelompok ini juga mencuci tambahan $2,5 juta melalui pembelian dan penjualan kembali barang-barang mewah di Hong Kong. Pada 30 April 2019, penyidik AFP dan ASIC melakukan penggeledahan di kediaman wanita tersebut dan melakukan pemeriksaan terhadap komputer laptop dan ponsel miliknya serta mengidentifikasi rincian dan gambar dari ratusan dokumen identitas yang dicuri.

Penyelidikan yang diberi nama Operasi Birks menunjukkan bahwa wanita tersebut bekerja sebagai bagian dari sindikat kriminal internasional yang menggunakan identitas yang diperoleh secara curang untuk melakukan kejahatan siber berskala besar dan canggih. Informasi identitas yang dicuri dibeli dari pasar *darknet*, bersama dengan kartu SIM telepon sekali pakai dan akun email palsu, digunakan untuk melakukan 'pengambilalihan identitas' dari korban yang tidak menyadari hal tersebut. Identitas palsu ini dibuat untuk meniru individu asli yang tanpa sadar identitasnya telah dikompromikan dan kemudian digunakan untuk membuka rekening bank di berbagai lembaga di Australia. Penyidik menemukan setidaknya 60 rekening bank yang dibuat menggunakan identitas palsu ini.

Setelah identitas palsu dan rekening bank dibuat, sindikat tersebut secara ilegal mengakses dan mencuri uang dari tabungan dana pensiun dan perdagangan saham milik korban. Pelaku bekerja dengan orang lain untuk membuat situs *web* kloning yang meniru situs *web* sah dari tabungan dana pensiun, menggunakan nama *domain* yang hampir identik dengan situs asli. Iklan online digunakan untuk mempromosikan situs *web* kloning ini agar muncul di bagian atas mesin pencari. Tujuannya adalah untuk mengambil nama pengguna dan kata sandi anggota saat mereka mengunjungi situs *web* kloning tersebut (*phishing*). Informasi anggota yang dicuri kemudian digunakan untuk mendapatkan akses tidak sah ke akun anggota. Sindikat ini menarik dana tabungan dana pensiun dari korban dan menyetorkannya ke rekening bank palsu. Dana yang dicuri kemudian dicuci dengan mengirimkannya ke kontak di luar negeri, yang menggunakan dana tersebut untuk membeli aset yang tidak dapat dilacak seperti perhiasan dan barang-barang mewah di Hong Kong. Barang-barang ini kemudian dijual dan uangnya dikirim kembali kepada pelaku di Australia melalui *cryptocurrency*.



Gambar 23 Gambaran Kasus Phishing Australia

BAB V
KESIMPULAN DAN STRATEGI MITIGASI RISIKO

5.1. KESIMPULAN

Berdasarkan hasil identifikasi, analisis, dan evaluasi risiko TPPU dan TPPT dari TP Siber, diperoleh hasil sebagai berikut:

1. Berdasarkan hasil analisis dan evaluasi risiko sektoral dari TP Siber, perkembangan kejahatan siber saat ini terhadap risiko nasional perlu dipertimbangkan. Hal ini disebabkan pelaku kejahatan semakin memanfaatkan sarana siber atau teknologi canggih untuk melakukan pencucian uang yang berasal dari berbagai jenis tindak pidana. Putusan TPPU dari TP Siber masih rendah dibandingkan Tindak Pidana Asalnya sehingga penanganan TPPU dari TP Siber perlu ditingkatkan, terutama dari judi *online*.
2. Berdasarkan jenis TP Siber, penipuan dalam jaringan (*online fraud*) dan perjudian *online* (*online gambling*) dinilai berisiko tinggi TPPU.
3. Berdasarkan profil, pengusaha/wiraswasta dan pegawai swasta dinilai menjadi profil berisiko tinggi TPPU hasil TP Siber. Warga Negara Indonesia/WNI dinilai berisiko tinggi TPPU hasil TP Siber. Hasil TP Siber cenderung dilakukan pencucian uang oleh pelaku TP Siber sendiri.
4. Berdasarkan wilayah, DK Jakarta dinilai berisiko tinggi terjadi TPPU hasil TP Siber.
5. Berdasarkan sektor industri pihak pelapor, bank dinilai berisiko tinggi.
6. Berdasarkan tipologi TPPU, yang dinilai berisiko tinggi adalah penggunaan mata uang virtual dan perjudian *online*.
7. Berdasarkan pola transaksi, yang dinilai berisiko tinggi adalah transfer dan tarik/setor tunai
8. Singapura, Amerika Serikat, Hong Kong, Republik Rakyat Tiongkok, India, dan Malaysia dinilai para responden sebagai negara-negara yang berpotensi menjadi sumber, tujuan, dan transit dana TPPU dari TP Siber.
9. Tingkat risiko TPPT belum dapat diukur dalam kajian ini karena keterbatasan data kasus. Namun dengan adanya kasus penipuan siber sebagai sumber dana TPPT di luar negeri, potensi tersebut perlu diwaspadai.

10. Penyalahgunaan teknologi keuangan (misalnya aset kripto) dan ruang siber dalam rangka komunikasi, propaganda, dan perekrutan telah nyata terjadi dan perlu diwaspadai aparat penegak hukum.

Ancaman baru atau *emerging threat* TPPU dan TPPT dari hasil TP Siber antara lain:

1. Penyalahgunaan AI
2. Penyalahgunaan *e-wallet*
3. Penggunaan layanan percampuran koin/*coin mixer*
4. Pengiriman tautan/berkas yang berisi virus atau untuk percobaan mengambil alih data pengguna
5. Penggunaan *private wallet address*
6. Eksploitasi Web3 dan Aset Kripto

5.2. STRATEGI MITIGASI RISIKO

Berdasarkan hasil identifikasi ancaman, kerentanan dan dampak serta risiko tindak pidana pencucian uang dan tindak pidana pendanaan terorisme dari TP Siber, telah dilakukan evaluasi risiko dan ditentukan langkah-langkah strategi mitigasi risiko yang dapat dilakukan oleh seluruh pihak pemangku kepentingan terkait, di antaranya:

a. Bidang Pencegahan

No	Strategi Bidang Pencegahan	Jangka Waktu	Penanggung Jawab
1.	Meningkatkan kesadaran Masyarakat mengenai TP Siber, misalnya bahaya TP Siber dan dampak jual beli rekening	Menengah	1. Kementerian Komunikasi dan Digital 2. Badan Siber dan Sandi Negara 3. POLRI
2.	Menyusun indikator TKM terkait TP Siber	Menengah	1. PPATK 2. POLRI 3. LPP 4. Kementerian Komunikasi dan Digital 5. Badan Siber dan Sandi Negara
3.	Meningkatkan pemanfaatan teknologi dalam pencegahan TP Siber, terutama terhadap serangan siber dan deteksi transaksi TP Siber	Pendek	1. PPATK 2. POLRI 3. LPP

No	Strategi Bidang Pencegahan	Jangka Waktu	Penanggung Jawab
			4. Kementerian Komunikasi dan Digital 5. Badan Siber dan Sandi Negara
4.	Meningkatkan kapasitas pengawas dan penyidik TP Siber dalam hal teknologi keuangan dan aset kripto	Menengah	1. PPATK 2. POLRI 3. LPP 4. Kementerian Komunikasi dan Digital 5. Badan Siber dan Sandi Negara
5.	Menyosialisasikan hasil penilaian risiko	Pendek	1. PPATK 2. POLRI 3. LPP 4. Kementerian Komunikasi dan Digital 5. Badan Siber dan Sandi Negara
6.	Meningkatkan kapasitas petugas APU-PPT pihak pelapor	Menengah	1. PPATK 2. POLRI 3. LPP 4. Kementerian Komunikasi dan Digital 5. Badan Siber dan Sandi Negara

b. Bidang Pemberantasan

No	Strategi Bidang Pemberantasan	Jangka Waktu	Penanggung Jawab
1.	Meningkatkan penanganan perkara TPPU dari TP Siber, terutama judi *online*	Menengah	1. POLRI 2. Kejaksaan Agung
2.	Memperkuat regulasi TP Siber	Panjang	Pemerintah RI
3.	Menyusun panduan/SOP untuk penyitaan Aset Kripto	Menengah	3. POLRI 4. Kejaksaan Agung
4.	Membuat *single government wallet* untuk penanganan barang bukti Aset Kripto	Pendek	1. POLRI 2. Kejaksaan Agung
5.	Menyusun panduan khusus dalam penyidikan TPPU dan TPPT Siber	Menengah	1. POLRI 2. Kejaksaan Agung

c. Bidang Kerja Sama

No	Strategi Bidang Pemberantasan	Jangka Waktu	Penanggung Jawab
1.	Memperkuat kerja sama penanganan perkara baik dalam maupun luar negeri	Pendek	1. PPATK 2. POLRI 3. Kejaksaan Agung 4. Otoritas MLA 5. LPP
2.	Meningkatkan kerja sama pertukaran informasi baik dalam maupun luar negeri	Pendek	1. PPATK 2. POLRI 5. Kejaksaan Agung 6. LPP 7. K/L terkait 8. Asosiasi industri pihak pelapor 9. Pihak Pelapor 10. Lokapasar/*e-commerce*
3.	Meningkatkan kerja sama Pendidikan dan pelatihan baik dalam maupun luar negeri	Pendek	1. PPATK 2. POLRI 3. Kejaksaan Agung 4. LPP 5. K/L terkait 6. Asosiasi industri pihak pelapor 7. Pihak Pelapor
4.	Meningkatkan pemanfaatan *platform Public Private Partnership* (PPP) dalam pertukaran informasi dan penyusunan *operational alert* (OA) terkait TP Siber	Pendek	1. PPATK 2. POLRI 3. Kejaksaan Agung 4. LPP 5. K/L terkait 6. Pihak Pelapor

DAFTAR PUSTAKA

Anjelina, C. D., & Afifah, M. N. (2024, Juni 29). *Kilas Balik Ransomware WannaCry, Pernah Serang 150 Negara Termasuk Indonesia 7 Tahun Lalu*. Retrieved November 28, 2024, from Kompas: https://www.kompas.com/tren/read/2024/06/29/063000065/kilas-balik-ransomware-wannacry-pernah-serang-150-negara-termasuk-indonesia#google_vignette

Aswara, Dani (2024, November 7). *PPATK: Transaksi Judi* Online *2024 Tembus Rp283 Triliun*. Diakses 28 November 2024, dari https://www.tempo.co/hukum/ppatk-transaksi-judi-online-2024-tembus-rp-283-triliun-1164927

Australian Strategic Policy Institute. (2021). *Counterterrorism Yearbook 2021*.

Australian Strategic Policy Institute. (2022). *Counterterrorism Yearbook 2022*.

Aziz, M. A. (2019). Pengembangan Satuan Unit Cyber Crime. *Jurnal Litbang Polri, 22*(1), 408-459.

Dimila, M. (2019, Mei 25). *Cerita Irdam Tangani Kasus Cybercrime Pertama di Indonesia*. Retrieved November 28, 2024, from Dialeksis: https://www.dialeksis.com/soki/cerita-irdam-tangani-kasus-cybercrime-pertama-di-indonesia/#:~:text=Saat%20itu%20Irdam%20bertugas%20di,1946%

Humas Polri. (2024, Juni 21). Bareskrim Polri Ungkap 318 Kasus Judi Online, 464 Tersangka Diringkus. Diakses 28 November 2024, dari https://mediahub.polri.go.id/image/detail/69221-bareskrim-polri-ungkap-318-kasus-judi-online-464-tersangka-diringkus

Indonesia. *Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara RI Tahun 2008 Nomor 58, Tambahan Lembaran Negara RI Nomor 4843. Sekretariat Negara. Jakarta

___. *Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara RI Tahun 2016 Nomor 251, Tambahan Lembaran Negara RI Nomor 5952. Sekretariat Negara. Jakarta

___. *Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua Atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik*. Lembaran Negara RI Tahun 2024 Nomor 1, Tambahan Lembaran Negara RI Nomor 6905. Sekretariat Negara. Jakarta

Interpol. (2021). *ASEAN Cyberthreat Assessment 2021*. Diakses dari https://www.interpol.int/content/download/16106/file/ASEAN%20Cyberthreat%20Assessment%202021%20-%20final.pdf

__. (2023). *Interpol's 2023 Global Crime Report*. Diakses dari https://www.interpol.int/How-we-work/Criminal-intelligence-analysis/Our-analysis-reports

Kantor Imigrasi Khusus Kelas 1 TPI Batam. (2024, Juni 28). *Kantor Imigrasi Amankan 103 WNA yang Menyalahgunakan Izin Tinggal dan Diduga Melakukan Kejahatan Siber*. Retrieved November 28, 2024, from Kantor Imigrasi Khusus Kelas 1 TPI Batam: https://kanimbatam.kemenkumham.go.id/berita/2024/06/imigrasi-amankan-103-wna-yang-menyalahgunakan-izin-tinggal-dan-diduga-melakukan-kejahatan-terkait-siber#:~:text=Berita%20Utama-, Imigrasi%20Amankan%20103%20WNA%20yang%20Menyalahgunakan%20Izin,Diduga%20Me

Malik, N. (2018). *Terror In The Dark: How Terrorists Use Encryption, The Darknet, And Cryptocurrencies*. London: The Henry Jackson Society.

Pusiknas Bareskrim Polri. (n.d.). *Kejahatan Siber di Indonesia Naik Berkali-kali Lipat*. Diakses November 22, 2024, dari https://pusiknas.polri.go.id /detail_artikel/kejahatan_siber_di_indonesia_naik_berkali-kali_lipat

R, M. A. (2024, September 21). *Resmi, Kini Ada DIrektorat Reserse Siber di Polda*. Diakses dari Detik News: https://news.detik.com/berita/d-7551640/resmi-kini-ada-direktorat-reserse-siber-di-8-polda

Sa'diyah, H. (2017, Januari 10). *Bahrun Naim Kirim Dana Lewat Paypal*. Retrieved November 28, 2024, Diakses dari Republika: https://www.republika.co.id/berita/koran/hukum-koran/17/01/10/ojjy4633-bahrun-naim-kirim-dana-lewat-paypal

Tribratanews.polri.go.id. (2023, Desember 27). *Polri: Kasus Kejahatan Siber di 2023 Turun hingga 1.075 Perkara dari 2022*. Retrieved November 28, 2024, Diakses dari Tribratanews.polri.go.id: https://tribratanews.sulut.polri.go.id/polri-kasus-kejahatan-siber-di-2023-turun-hingga-1-075-perkara-dari-2022/

U.S. Immigration and Customs Enforcement. (2020, Agustus 13). *Global Disruption of 3 terror finance cyber-enabled campaigns*. Diakses 22 November 2024 dari U.S. Immigration and Customs Enforcement: https://www.ice.gov/news/releases/global-disruption-3-terror-finance-cyber-enabled-campaigns

United Nations Office of Counter-Terrorism & United Nations Interregional Crime and Justice Research Institue. (2024). *Beneath The Surface: Terrorist And Violet Extremist Use of The Dark Web and Cybercrime As a Service For Cyber-Attacks*. United Nations Office of Counter-Terrorism & United Nations Interregional Crimw and Justice Research Institue.

Wolf, A. (2024, April 19). *A Brief History of Cybercrime*. Retrieved November 22, 2024, from Arctic Wolf: https://arcticwolf.com/resources/blog/decade-of-cybercrime/

Wu, Jiajing et. al. (2023). J. Wu, K. Lin, D. Lin, Z. Zheng, H. Huang and Z. Zheng, "Financial Crimes in Web3-Empowered Metaverse: Taxonomy, Countermeasures, and Opportunities," in IEEE Open Journal of the Computer Society, vol. 4, pp. 37-49, 2023, doi: 10.1109/OJCS.2023.3245801.

LAMPIRAN

Tabel 4 Tingkat Risiko TPPU Hasil TP Siber Berdasarkan Jenis TP Siber

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
1	Peretasan sistem elektronik (*hacking*)	4.93	Rendah	6.84	Menengah	11.77	5.84	Menengah	5.92	Menengah	34.57	5.12	Menengah
2	Intersepsi atau penyadapan ilegal (*illegal interception*)	3.00	Rendah	3.70	Rendah	6.70	3.04	Rendah	3.00	Rendah	9.12	3.00	Rendah
3	Pengubahan tampilan situs web (*web defacement*)	3.82	Rendah	4.37	Rendah	8.20	3.87	Rendah	3.78	Rendah	14.64	3.46	Rendah
4	Gangguan sistem (*system interference*)	3.63	Rendah	3.00	Rendah	6.63	3.00	Rendah	4.07	Rendah	12.21	3.26	Rendah
5	Manipulasi data (*data manipulation*)	4.62	Rendah	5.65	Menengah	10.27	5.01	Menengah	5.52	Menengah	27.68	4.55	Rendah
6	Pornografi dalam jaringan (*online pornography*)	5.17	Menengah	7.03	Tinggi	12.20	6.08	Menengah	4.93	Rendah	29.99	4.74	Rendah

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
7	Perjudian dalam jaringan (*online gamble*)	7.52	Tinggi	9.00	Tinggi	16.52	8.47	Tinggi	8.32	Tinggi	70.45	8.12	Tinggi
8	Pencemaran nama baik (*online defamation*)	3.49	Rendah	3.47	Rendah	6.96	3.18	Rendah	3.00	Rendah	9.55	3.04	Rendah
9	Penipuan dalam jaringan (*online fraud*)	9.00	Tinggi	8.48	Tinggi	17.48	9.00	Tinggi	9.00	Tinggi	81.00	9.00	Tinggi
10	Pengancaman dan Pemerasan online	4.60	Rendah	3.93	Rendah	8.53	4.05	Rendah	4.47	Rendah	18.13	3.75	Rendah
11	Akses ilegal (*illegal access*)	5.60	Menengah	5.65	Menengah	11.25	5.55	Menengah	5.29	Menengah	29.36	4.69	Rendah
12	pencurian data (*data theft*)	5.23	Menengah	5.65	Menengah	10.88	5.35	Menengah	5.20	Menengah	27.82	4.56	Rendah

Tabel 5 Tingkat Risiko TPPU Hasil TP Siber Berdasarkan Profil Pelaku

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
1	Buruh, Pembantu Rumah Tangga dan Tenaga Keamanan	4,48	Rendah	4,71	Rendah	9,19	4,64	Rendah	4,69	Rendah	21,75	4,06	Rendah
2	Ibu Rumah Tangga	4,78	Rendah	6,20	Menengah	10,97	5,56	Menengah	4,24	Rendah	23,59	4,22	Rendah
3	Pedagang	5,10	Menengah	7,06	Tinggi	12,16	6,18	Menengah	5,73	Menengah	35,39	5,20	Menengah
4	Pegawai Bank	5,17	Menengah	7,25	Tinggi	12,42	6,31	Menengah	5,30	Menengah	33,45	5,04	Menengah
5	Pegawai BUMN/BUMD (termasuk pensiunan)	4,45	Rendah	6,40	Menengah	10,85	5,50	Menengah	4,77	Rendah	26,20	4,43	Rendah
6	Pegawai Money Changer	4,65	Rendah	6,61	Menengah	11,25	5,71	Menengah	4,83	Rendah	27,55	4,55	Rendah
7	Pegawai Swasta	7,79	Tinggi	9,00	Tinggi	16,79	8,57	Tinggi	7,42	Tinggi	63,58	7,55	Tinggi
8	Pejabat Lembaga Legislatif dan Pemerintah	4,62	Rendah	6,87	Menengah	11,49	5,83	Menengah	5,83	Menengah	33,96	5,08	Menengah

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
9	Pelajar/Mahasiswa	6,51	Menengah	8,33	Tinggi	14,84	7,56	Tinggi	6,05	Menengah	45,75	6,06	Menengah
10	Pengajar dan Dosen	4,11	Rendah	5,92	Menengah	10,02	5,07	Menengah	4,27	Rendah	21,68	4,06	Rendah
11	Pengrajin	3,00	Rendah	4,23	Rendah	7,23	3,62	Rendah	3,21	Rendah	11,65	3,22	Rendah
12	Pengurus dan pegawai yayasan/lembaga berbadan hukum lainnya	4,14	Rendah	5,48	Menengah	9,62	4,86	Rendah	4,34	Rendah	21,12	4,01	Rendah
13	Pengurus Parpol	4,68	Rendah	6,61	Menengah	11,28	5,72	Menengah	4,86	Rendah	27,80	4,57	Rendah
14	Pengurus/Pegawai LSM/organisasi tidak berbadan hukum lainnya	4,50	Rendah	5,77	Menengah	10,28	5,20	Menengah	4,51	Rendah	23,46	4,20	Rendah
15	Pengusaha/Wiraswasta	9,00	Tinggi	8,62	Tinggi	17,62	9,00	Tinggi	9,00	Tinggi	81,00	9,00	Tinggi
16	Petani dan Nelayan	3,02	Rendah	3,00	Rendah	6,02	3,00	Rendah	3,00	Rendah	9,00	3,00	Rendah
17	PNS (termasuk pensiunan)	4,96	Rendah	5,99	Menengah	10,94	5,55	Menengah	5,26	Menengah	29,20	4,68	Rendah

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
18	Profesional dan Konsultan	5,04	Menengah	6,40	Menengah	11,44	5,80	Menengah	5,86	Menengah	34,01	5,08	Menengah
19	TNI/Polri (termasuk pensiunan)	4,40	Rendah	5,84	Menengah	10,24	5,18	Menengah	5,29	Menengah	27,43	4,54	Rendah
20	Ulama/Pendeta/Pimpinan organisasi dan kelompok keagamaan	3,12	Rendah	4,63	Rendah	7,75	3,90	Rendah	3,54	Rendah	13,79	3,40	Rendah

Tabel 6 Tingkat Risiko TPPU Hasil TP Siber Berdasarkan Wilayah

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
1	Aceh	3,49	Rendah	3,69	Rendah	7,18	3,57	Rendah	3,60	Rendah	12,86	3,32	Rendah
2	Bali	5,26	Menengah	6,39	Menengah	11,65	5,82	Menengah	6,51	Menengah	37,84	5,40	Menengah

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
3	Banten	5,66	Menengah	5,65	Menengah	11,31	5,65	Menengah	6,96	Menengah	39,29	5,52	Menengah
4	Bengkulu	3,37	Rendah	3,43	Rendah	6,80	3,38	Rendah	3,43	Rendah	11,61	3,22	Rendah
5	DI Yogyakarta	4,45	Rendah	5,65	Menengah	10,11	5,04	Menengah	4,46	Rendah	22,51	4,13	Rendah
6	DKI Jakarta	9,00	Tinggi	9,00	Tinggi	18,00	9,00	Tinggi	9,00	Tinggi	81,00	9,00	Tinggi
7	Gorontalo	3,43	Rendah	3,77	Rendah	7,20	3,58	Rendah	3,50	Rendah	12,54	3,30	Rendah
8	Jambi	3,40	Rendah	3,60	Rendah	7,00	3,48	Rendah	3,50	Rendah	12,19	3,27	Rendah
9	Jawa Barat	6,35	Menengah	7,13	Tinggi	13,48	6,74	Menengah	7,71	Tinggi	51,94	6,58	Menengah
10	Jawa Tengah	5,05	Menengah	6,45	Menengah	11,50	5,74	Menengah	5,58	Menengah	32,05	4,92	Rendah
11	Jawa Timur	5,31	Menengah	6,71	Menengah	12,02	6,00	Menengah	5,88	Menengah	35,26	5,19	Menengah
12	Kalimantan Barat	3,90	Rendah	4,41	Rendah	8,31	4,14	Rendah	3,70	Rendah	15,31	3,53	Rendah
13	Kalimantan Selatan	3,49	Rendah	3,77	Rendah	7,26	3,61	Rendah	3,53	Rendah	12,77	3,31	Rendah

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
14	Kalimantan Tengah	3,43	Rendah	3,77	Rendah	7,20	3,58	Rendah	3,53	Rendah	12,66	3,31	Rendah
15	Kalimantan Timur	3,88	Rendah	4,01	Rendah	7,90	3,93	Rendah	4,52	Rendah	17,77	3,73	Rendah
16	Kalimantan Utara	3,30	Rendah	3,43	Rendah	6,74	3,35	Rendah	3,40	Rendah	11,39	3,20	Rendah
17	Kep. Bangka Belitung	3,60	Rendah	3,69	Rendah	7,29	3,63	Rendah	4,37	Rendah	15,87	3,57	Rendah
18	Kep. Riau	4,46	Rendah	4,41	Rendah	8,88	4,42	Rendah	6,64	Menengah	29,39	4,70	Rendah
19	Lampung	4,26	Rendah	4,33	Rendah	8,59	4,28	Rendah	4,13	Rendah	17,67	3,72	Rendah
20	Maluku	3,20	Rendah	3,26	Rendah	6,47	3,22	Rendah	3,36	Rendah	10,82	3,15	Rendah
21	Maluku Utara	3,27	Rendah	3,18	Rendah	6,45	3,21	Rendah	3,33	Rendah	10,67	3,14	Rendah
22	Nusa Tenggara Barat	3,69	Rendah	3,60	Rendah	7,30	3,63	Rendah	3,40	Rendah	12,34	3,28	Rendah
23	Nusa Tenggara Timur	3,40	Rendah	3,43	Rendah	6,83	3,40	Rendah	3,36	Rendah	11,43	3,20	Rendah
24	Papua	3,27	Rendah	3,69	Rendah	6,96	3,46	Rendah	3,47	Rendah	12,00	3,25	Rendah

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
25	Papua Barat	3,14	Rendah	3,35	Rendah	6,49	3,23	Rendah	3,11	Rendah	10,04	3,09	Rendah
26	Papua Tengah	3,07	Rendah	3,26	Rendah	6,33	3,15	Rendah	3,15	Rendah	9,92	3,08	Rendah
27	Papua Pegunungan	3,21	Rendah	3,18	Rendah	6,38	3,17	Rendah	3,11	Rendah	9,88	3,07	Rendah
28	Papua Selatan	3,00	Rendah	3,09	Rendah	6,09	3,03	Rendah	3,00	Rendah	9,08	3,01	Rendah
29	Papua Barat Daya	3,03	Rendah	3,00	Rendah	6,03	3,00	Rendah	3,00	Rendah	9,00	3,00	Rendah
30	Riau	4,09	Rendah	4,41	Rendah	8,51	4,24	Rendah	3,86	Rendah	16,34	3,61	Rendah
31	Sulawesi Barat	3,54	Rendah	3,60	Rendah	7,15	3,56	Rendah	3,53	Rendah	12,57	3,30	Rendah
32	Sulawesi Selatan	4,23	Rendah	4,41	Rendah	8,64	4,31	Rendah	4,67	Rendah	20,11	3,93	Rendah
33	Sulawesi Tengah	3,64	Rendah	4,01	Rendah	7,66	3,81	Rendah	3,60	Rendah	13,72	3,39	Rendah
34	Sulawesi Tenggara	3,43	Rendah	3,69	Rendah	7,12	3,54	Rendah	3,43	Rendah	12,16	3,26	Rendah
35	Sulawesi Utara	3,58	Rendah	3,93	Rendah	7,52	3,74	Rendah	3,63	Rendah	13,59	3,38	Rendah

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
36	Sumatera Barat	3,73	Rendah	4,01	Rendah	7,74	3,86	Rendah	4,49	Rendah	17,32	3,69	Rendah
37	Sumatera Selatan	4,93	Rendah	5,72	Menengah	10,65	5,31	Menengah	5,30	Menengah	28,17	4,60	Rendah
38	Sumatera Utara	4,99	Rendah	5,45	Menengah	10,44	5,21	Menengah	5,27	Menengah	27,47	4,54	Rendah

Tabel 7 Tingkat Risiko TPPU Hasil TP Siber Berdasarkan Kewarganegaraan Pelaku

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
1	WNI	9,00	Tinggi	9,00	Tinggi	18,00	9,00	Tinggi	9,00	Tinggi	81,00	9,00	Tinggi
2	WNA	3,00	Rendah	3,00	Rendah	6,00	3,00	Rendah	3,00	Rendah	9,00	3,00	Rendah

Tabel 8 Tingkat Risiko TPPU Berdasarkan Apakah Pelaku TPPU Juga Pelaku TP Siber

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
1	Pelaku TP Siber juga Pelaku TPPU	9,00	Tinggi	9,00	Tinggi	18,00	9,00	Tinggi	9,00	Tinggi	81,00	9,00	Tinggi
2	Pelaku TP Siber bukan Pelaku TPPU	3,00	Rendah	3,00	Rendah	6,00	3,00	Rendah	3,00	Rendah	9,00	3,00	Rendah

Tabel 9 Tingkat Risiko TPPU Hasil TP Siber Berdasarkan Sektor Industri Pihak Pelapor

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
1	Bank	9,00	Tinggi	9,00	Tinggi	18,00	9,00	Tinggi	9,00	Tinggi	81,00	9,00	Tinggi
2	Perusahaan Pembiayaan	4,06	Rendah	5,51	Menengah	9,57	4,75	Rendah	4,04	Rendah	19,23	3,85	Rendah
3	Perusahaan Asuransi dan Perusahaan Pialang Asuransi	3,72	Rendah	4,73	Rendah	8,45	4,19	Rendah	3,60	Rendah	15,08	3,51	Rendah

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
4	Dana Pensiun Lembaga Keuangan	3,42	Rendah	4,21	Rendah	7,63	3,78	Rendah	3,47	Rendah	13,11	3,34	Rendah
5	Perusahaan Efek	4,27	Rendah	5,72	Menengah	9,98	4,96	Rendah	4,38	Rendah	21,72	4,06	Rendah
6	Manajer Investasi	4,21	Rendah	5,58	Menengah	9,80	4,87	Rendah	4,29	Rendah	20,91	3,99	Rendah
7	Kustodian	3,51	Rendah	3,98	Rendah	7,49	3,71	Rendah	3,69	Rendah	13,68	3,39	Rendah
8	Wali Amanat	3,42	Rendah	3,66	Rendah	7,08	3,50	Rendah	3,24	Rendah	11,35	3,20	Rendah
9	Perposan sebagai penyedia jasa giro	3,30	Rendah	3,42	Rendah	6,72	3,32	Rendah	3,24	Rendah	10,76	3,15	Rendah
10	Pedagang Valuta Asing	5,69	Menengah	6,69	Menengah	12,38	6,17	Menengah	4,66	Rendah	28,76	4,65	Rendah
11	Penyelenggara Alat Pembayaran Menggunakan Kartu	4,34	Rendah	5,38	Menengah	9,72	4,83	Rendah	4,07	Rendah	19,67	3,89	Rendah
12	Penyelenggara E-Money dan/atau E-Wallet	6,01	Menengah	7,06	Tinggi	13,07	6,52	Menengah	4,69	Rendah	30,54	4,79	Rendah
13	Koperasi yang Melakukan Kegiatan Simpan Pinjam	3,51	Rendah	4,66	Rendah	8,17	4,05	Rendah	3,50	Rendah	14,19	3,43	Rendah
14	Pegadaian	3,26	Rendah	4,05	Rendah	7,32	3,62	Rendah	3,10	Rendah	11,24	3,19	Rendah

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
15	Perusahaan yang Bergerak di Bidang Perdagangan Berjangka Komoditi	4,77	Rendah	5,02	Menengah	9,79	4,87	Rendah	6,02	Menengah	29,28	4,69	Rendah
16	Pedagang Fisik Aset Kripto	5,97	Menengah	8,10	Tinggi	14,06	7,02	Tinggi	5,41	Menengah	37,95	5,41	Menengah
17	Penyelenggara Kegiatan Usaha Pengiriman Uang	5,34	Menengah	6,37	Menengah	11,71	5,83	Menengah	4,76	Rendah	27,77	4,56	Rendah
18	Perusahaan Properti/Agen Properti	4,53	Rendah	5,58	Menengah	10,11	5,03	Menengah	4,07	Rendah	20,47	3,96	Rendah
19	Pedagang Kendaraan Bermotor	4,57	Rendah	5,58	Menengah	10,16	5,05	Menengah	4,04	Rendah	20,42	3,95	Rendah
20	Pedagang Permata dan Perhiasan/Logam Mulia	4,67	Rendah	6,31	Menengah	10,98	5,47	Menengah	4,58	Rendah	25,06	4,34	Rendah
21	Pedagang Barang Seni dan Antik	3,91	Rendah	4,73	Rendah	8,64	4,29	Rendah	3,66	Rendah	15,69	3,56	Rendah
22	Balai Lelang	3,30	Rendah	4,13	Rendah	7,43	3,68	Rendah	3,44	Rendah	12,64	3,30	Rendah
23	Perusahaan Modal Ventura	3,39	Rendah	3,90	Rendah	7,29	3,61	Rendah	3,53	Rendah	12,74	3,31	Rendah

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
24	Perusahaan Pembiayaan Infrastruktur	3,17	Rendah	3,74	Rendah	6,91	3,41	Rendah	3,34	Rendah	11,40	3,20	Rendah
25	Lembaga Keuangan Mikro	3,33	Rendah	3,98	Rendah	7,30	3,61	Rendah	3,21	Rendah	11,59	3,22	Rendah
26	Lembaga Pembiayaan Ekspor	3,20	Rendah	4,21	Rendah	7,41	3,67	Rendah	3,47	Rendah	12,72	3,31	Rendah
27	Penyelenggara layanan pinjam meminjam uang berbasis teknologi informasi	4,14	Rendah	5,85	Menengah	9,99	4,97	Rendah	4,27	Rendah	21,19	4,02	Rendah
28	Penyelenggara layanan urun dana melalui penawaran saham berbasis teknologi informasi	4,19	Rendah	5,02	Menengah	9,22	4,58	Rendah	4,18	Rendah	19,15	3,85	Rendah
29	Penyelenggara layanan Transaksi Keuangan berbasis teknologi informasi	4,19	Rendah	5,85	Menengah	10,04	4,99	Rendah	4,21	Rendah	21,03	4,00	Rendah
30	Advokat	3,17	Rendah	3,58	Rendah	6,75	3,33	Rendah	3,21	Rendah	10,69	3,14	Rendah
31	Notaris	3,64	Rendah	4,13	Rendah	7,77	3,85	Rendah	3,53	Rendah	13,61	3,38	Rendah

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
32	Pejabat Pembuat Akta Tanah	3,51	Rendah	4,05	Rendah	7,57	3,75	Rendah	3,44	Rendah	12,88	3,32	Rendah
33	Akuntan	3,20	Rendah	3,25	Rendah	6,45	3,18	Rendah	3,07	Rendah	9,78	3,06	Rendah
34	Akuntan Publik	3,00	Rendah	3,08	Rendah	6,08	3,00	Rendah	3,00	Rendah	9,00	3,00	Rendah
35	Perencana Keuangan	3,17	Rendah	3,00	Rendah	6,17	3,04	Rendah	3,21	Rendah	9,75	3,06	Rendah

Tabel 10 Tingkat Risiko TPPU Hasil TP Siber Berdasarkan Tipologi TPPU

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
1	Penggunaan identitas palsu	7,19	Tinggi	8,31	Tinggi	16	7,63	Tinggi	5,83	Menengah	44,51	6,57	Menengah
2	Properti/real estate, termasuk peran agen properti	4,26	Rendah	5,61	Menengah	10	4,56	Rendah	4,22	Rendah	19,23	4,00	Rendah

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
3	Penggunaan nominees (nama pinjaman), trusts, anggota keluarga atau pihak ketiga	7,59	Tinggi	7,49	Tinggi	15	7,40	Tinggi	5,30	Menengah	39,20	6,03	Menengah
4	*Smurfing*	6,56	Menengah	8,31	Tinggi	15	7,29	Tinggi	5,74	Menengah	41,86	6,30	Menengah
5	*Structuring*	6,90	Menengah	7,90	Tinggi	15	7,25	Tinggi	5,57	Menengah	40,38	6,15	Menengah
6	Penggunaan Jasa Profesi	3,11	Rendah	3,91	Rendah	7	3,00	Rendah	3,12	Rendah	9,35	3,00	Rendah
7	Penggunaan metode/sistem pembayaran baru	6,53	Menengah	6,63	Menengah	13	6,35	Menengah	4,63	Rendah	29,38	5,03	Menengah
8	Pemanfaatan Korporasi (legal person)	4,32	Rendah	4,90	Rendah	9	4,20	Rendah	3,58	Rendah	15,02	3,58	Rendah
9	Pemanfaatan Sektor Yang Tidak Teregulasi Dengan Baik	5,07	Menengah	8,21	Tinggi	13	6,42	Menengah	5,06	Menengah	32,48	5,35	Menengah
10	Penggunaan Sektor Non Keuangan	3,69	Rendah	4,66	Rendah	8	3,73	Rendah	3,63	Rendah	13,53	3,42	Rendah
11	Penukaran uang asing	5,68	Menengah	6,29	Menengah	12	5,71	Menengah	4,32	Rendah	24,67	4,56	Rendah

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
12	Mingling (penyatuan uang haram dalam bisnis legal)	6,42	Menengah	7,17	Tinggi	14	6,59	Menengah	5,16	Menengah	33,96	5,50	Menengah
13	Penggunaan kartu kredit, cek, surat perjanjian utang	3,44	Rendah	4,41	Rendah	8	3,46	Rendah	3,58	Rendah	12,35	3,30	Rendah
14	Trade-based money laundering dan transfer pricing	3,87	Rendah	5,38	Menengah	9	4,21	Rendah	3,90	Rendah	16,45	3,72	Rendah
15	Perdagangan perhiasan dan logam mulia	3,87	Rendah	5,84	Menengah	10	4,47	Rendah	6,66	Menengah	29,75	5,07	Menengah
16	Penggunaan Mata Uang Virtual	7,33	Tinggi	8,11	Tinggi	15	7,60	Tinggi	9,00	Tinggi	68,40	9,00	Tinggi
17	Bank ilegal/jasa pengiriman dana alternatif/hawala	4,46	Rendah	5,49	Menengah	10	4,60	Rendah	4,58	Rendah	21,07	4,19	Rendah
18	Penggunaan offshore banks, perusahaan bisnis internasional dan trusts lepas pantai	4,75	Rendah	6,41	Menengah	11	5,26	Menengah	4,58	Rendah	24,06	4,49	Rendah
19	Pembelian aset berharga (barang	3,72	Rendah	3,53	Rendah	7	3,12	Rendah	3,12	Rendah	9,73	3,04	Rendah

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
	seni, barang antik, dll)												
20	Penggunaan perusahaan cangkang (shell companies)	6,53	Menengah	5,61	Menengah	12	5,80	Menengah	4,38	Rendah	25,36	4,63	Rendah
21	Aktivitas perjudian online	9,00	Tinggi	9,00	Tinggi	18	9,00	Tinggi	6,00	Menengah	54,03	7,54	Tinggi
22	Transfer internasional/penggunaan rekening bank asing	5,79	Menengah	5,02	Menengah	11	5,07	Menengah	8,29	Tinggi	41,99	6,32	Menengah
23	Penggunaan internet (enkripsi, akses terhadap identitas, perbankan internasional, dll)	5,83	Menengah	7,59	Tinggi	13	6,49	Menengah	5,39	Menengah	34,99	5,60	Menengah
24	Pertukaran komoditas (barter, misalnnya reinvestasi dalam obat-obatan terlarang)	3,00	Rendah	4,04	Rendah	7	3,01	Rendah	3,46	Rendah	10,42	3,11	Rendah

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
25	Investasi di pasar modal, penggunaan perantara	3,70	Rendah	3,66	Rendah	7	3,18	Rendah	3,52	Rendah	11,19	3,19	Rendah
26	Penyelundupan manusia	6,04	Menengah	3,00	Rendah	9	4,10	Rendah	3,00	Rendah	12,31	3,30	Rendah

Tabel 11 Tingkat Risiko TPPU Hasil TP Siber Berdasarkan Pola Transaksi

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
1	Tarik/Setor Tunai	7,65	Tinggi	7,66	Tinggi	15	7,86	Tinggi	8,57	Tinggi	67,35	7,84	Tinggi
2	Cek	5,60	Menengah	3,91	Rendah	10	4,82	Rendah	3,76	Rendah	18,10	3,66	Rendah
3	Transfer	9,00	Tinggi	8,49	Tinggi	17	9,00	Tinggi	9,00	Tinggi	81,00	9,00	Tinggi
4	Internet Banking/mobile banking	6,59	Menengah	7,82	Tinggi	14	7,38	Tinggi	5,94	Menengah	43,85	5,84	Menengah

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
5	Virtual Account	6,64	Menengah	7,11	Tinggi	14	7,04	Tinggi	5,52	Menengah	38,83	5,42	Menengah
6	Jual/Beli Valas	5,20	Menengah	6,28	Menengah	11	5,85	Menengah	4,67	Rendah	27,34	4,44	Rendah
7	Pembelian Aset Properti	5,48	Menengah	6,28	Menengah	12	6,00	Menengah	4,52	Rendah	27,13	4,42	Rendah
8	Pembelian Aset Kendaraan Bermotor	4,77	Rendah	6,28	Menengah	11	5,62	Menengah	4,29	Rendah	24,12	4,17	Rendah
9	Pembelian Barang Lainnya (selain aset)	5,08	Menengah	5,59	Menengah	11	5,42	Menengah	3,93	Rendah	21,30	3,93	Rendah
10	Pemanfaatan Layanan Teknologi Finansial	5,47	Menengah	6,37	Menengah	12	6,04	Menengah	4,86	Rendah	29,33	4,61	Rendah
11	Pembawaan Uang Tunai Lintas Batas	3,78	Rendah	4,68	Rendah	8	4,27	Rendah	3,80	Rendah	16,21	3,50	Rendah
12	Pembelian Barang Antik	3,49	Rendah	4,96	Rendah	8	4,26	Rendah	3,67	Rendah	15,64	3,45	Rendah
13	Pembelian Barang Lelang	3,44	Rendah	4,30	Rendah	8	3,89	Rendah	3,41	Rendah	13,27	3,25	Rendah
14	Pembelian Perhiasan Emas/Logam Mulia	4,26	Rendah	6,03	Menengah	10	5,22	Menengah	4,21	Rendah	21,99	3,99	Rendah

POINT OF CONCERN		Skala Ancaman	Tingkat Ancaman	Skala Kerentanan	Tingkat Kerentanan	Kecenderungan		Tingkat Kecenderungan	Skala Dampak	Tingkat Dampak	Risiko		Tingkat Risiko
						Total	Skala Kecenderungan				Kecenderungan x Dampak	Skala Risiko	
15	Pembelian Polis Asuransi	3,00	Rendah	3,91	Rendah	7	3,45	Rendah	3,00	Rendah	10,36	3,00	Rendah
16	Pembelian Produk Pasar Modal	4,49	Rendah	5,59	Menengah	10	5,12	Menengah	4,13	Rendah	21,13	3,91	Rendah
17	Pembelian Produk Aset Kripto	7,71	Tinggi	9,00	Tinggi	17	8,59	Tinggi	5,84	Menengah	50,21	6,38	Menengah
18	Pemanfaatan Alat Pembayaran Baru: Uang Elektronik, Dompet Elektronik	5,70	Menengah	7,58	Tinggi	13	6,79	Menengah	5,11	Menengah	34,69	5,07	Menengah
19	Pembawaan Bearer Negotiable Instrument Lintas Batas (contoh: bilyet giro; warkat atas bawa berupa cek; cek perjalanan; surat sanggup bayar; dan sertifikat deposito,)	3,05	Rendah	3,00	Rendah	6	3,00	Rendah	4,71	Rendah	14,13	3,32	Rendah
20	Transaksi uang tunai antar para pihak	4,63	Rendah	6,62	Menengah	11	5,73	Menengah	4,52	Rendah	25,89	4,32	Rendah

PUSAT PELAPORAN DAN ANALISIS TRANSAKSI KEUANGAN

Jl. Ir. H Juanda No. 35 Jakarta 10120 Indonesia
Phone: (+6221) 3850455, 3853922
Fax: (+6221) 3856809 - 3856826
Website: http://www.ppatk.go.id