BAB I

PENDAHULUAN

1.1 Latar Belakang

Segala bentuk kejahatan di dunia maya disebut sebagai *cyber crime* yang pada dasarnya merupakan dampak dari kecanggihan teknologi sehingga merubah kebiasaan masyarakat, awalnya kegiatan hanya bersifat konvensional kini dengan kemajuan dan fasilitas teknologi tinggi dapat menyelesaikan atau berinteraksi secara online tanpa harus berinteraksi secara langsung. Menurut Susan W. Brenner, *cybercrime* terdiri dari tindakan yang dilarang karena mengancam ketertiban. *Cybercrime* berbeda dari kejahatan biasa dalam cara melakukannya, penjahat menggunakan senjata, sedangkan pelaku *cybercrime* menggunakan teknologi komputer. Sebagian besar *cybercrime* yang kita lihat saat ini hanya mewakili migrasi kejahatan dunia nyata ke dunia maya. Dunia maya menjadi alat yang digunakan para penjahat untuk melakukan kejahatan lama dengan cara-cara baru (Brenner, 2010).

Kasus pertama yang dipublikasikan tentang komputer yang digunakan untuk melakukan kejahatan muncul pada tahun 1960-an, ketika komputer merupakan sistem mainframe yang besar. Sejarah komputasi modern sudah ada sejak abad kesembilan belas, tetapi pengembangan komputer bisnis mainframe baru dimulai setelah Perang Dunia II. Pada tahun 1946, beberapa perusahaan mulai mengerjakan mainframe komersial, dan pada tahun 1951, UNIVAC

(*Universal Automatic Computer*), yang dibuat oleh perusahaan dengan nama yang sama, digunakan oleh Biro Sensus. Pada tahun 1951, Biro Sensus menggunakan UNIVAC untuk memprediksi hasil pemilihan presiden, yang membantu mempopulerkan teknologi baru ini. Pada tahun 1960, 5.000 mainframe digunakan di Amerika Serikat; pada tahun 1970, hampir 80.000 mainframe digunakan di Amerika Serikat dan 50.000 mainframe digunakan di luar negeri. Mengingat peningkatan jumlah komputer yang luar biasa, tidak mengherankan jika *cybercrime* mulai menjadi masalah pada tahun 1960-an. *Cybercrime* pada tahun 1960-an dan 1970-an berbeda dengan kejahatan dunia maya yang kita hadapi saat ini. Tidak ada internet mainframe tidak terhubung dengan jaringan ke komputer lain. Pada tahun 1960, sebuah mainframe biasa berharga beberapa juta dollar yang mana membutuhkan seluruh ruangan untuk menampungnya, dan membutuhkan sistem pendingin udara khusus untuk memastikan bahwa tabung vakumnya tidak akan terlalu panas dan membakar data di dalam komputer. Sebuah mainframe membutuhkan sekelompok teknisi spesialis untuk memastikan bahwa bagian dalam komputer tidak akan meleleh jika pendingin udaranya mati. Hanya sekelompok peneliti tertentu yang diizinkan untuk menggunakan mainframe. Untuk mengakses mainframe, seorang peneliti memberikan data yang ingin dianalisis oleh komputer kepada operator pemegang kunci. Karena satu-satunya cara untuk mengakses mainframe adalah dengan menggunakan proses yang rumit ini, hanya beberapa orang yang berada dalam posisi untuk melakukan *cybercrime*. Mereka adalah "orang dalam"

yang pekerjaannya memberi mereka akses ke komputer mainframe. Hal ini mempengaruhi jenis *cybercrime* yang dilakukan di era ini. Orang dalam terkadang memata-matai karyawan lain dengan membaca file rahasia mereka dan mereka mungkin menyabotase komputer atau data yang ada di dalamnya sebagai pembalasan karena dipecat atau didisiplinkan. Kejahatan-kejahatan ini terjadi, namun jenis *cybercrime* yang paling umum terjadi di era ini adalah kejahatan finansial memperkaya diri mereka sendiri.

Cybercrime mengacu pada aktivitas kriminal yang dilakukan dengan menggunakan komputer atau internet yang mana hal ini mencakup berbagai aktivitas ilegal, termasuk peretasan, pencurian identitas, phishing, distribusi malware, penipuan online, *cyberbullying*, dan banyak lagi (Dwily Hamana et al., 2023a). Kejahatan ini dilakukan oleh individu atau kelompok dengan niat jahat untuk mendapatkan akses tidak sah ke informasi sensitif, mengganggu sistem, mencuri uang, atau menyebabkan kerugian (Furnell, 2001). Salah satu tantangan dalam menangani *cybercrime* adalah sifat teknologi yang terus berkembang, yang memberikan peluang baru bagi para penjahat untuk mengeksploitasi kerentanan dalam sistem digital. Penjahat *cyber* sering kali menggunakan teknik canggih untuk melewati langkah-langkah keamanan dan tetap tidak terdeteksi. Mereka dapat menargetkan individu, bisnis, lembaga pemerintah, atau infrastruktur penting, yang menimbulkan ancaman signifikan terhadap keamanan *cyber* di seluruh dunia.

Cybercrime mencakup sejumlah besar tindakan, kejahatan, atau perilaku

terlarang yang dilakukan baik oleh individu maupun kelompok menggunakan perangkat yang berhubungan dengan komputer, atau jaringan informasi, serta kejahatan tradisional yang difasilitasi atau dipelihara oleh penggunaan internet atau teknologi informasi. Secara luas diakui bahwa istilah ini digunakan untuk menjelaskan berbagai kejahatan dan perilaku berbahaya yang mana mendefinisikan kejahatan dunia maya sebagai kejahatan apa pun yang difasilitasi atau yang dilakukan dengan menggunakan komputer, jaringan, atau perangkat keras" (Phillips et al., 2022a)

Globalisasi telah memudahkan setiap orang untuk mengakses berbagai jenis informasi, bahkan dari belahan dunia lain, karena teknologi telah berkembang seiring dengan itu. Hal ini terutama terjadi di bidang informasi dan telekomunikasi. Di sisi negatifnya, globalisasi dan kemajuan teknologi sering kali disalahgunakan untuk tujuan yang tidak benar. Melajunya akses informasi yang sangat signifikan ini membuka peluang kepada mereka yang ingin melakukan kejahatan. Kemajuan teknologi yang pesat seiring dengan munculnya globalisasi telah memunculkan masalah kejahatan serta penyalahgunaan teknologi. Hal ini membuat orang lebih mudah mendapatkan akses melalui jaringan, yang meningkatkan risiko berbagai ancaman yang menyusup dan merusak perangkat lunak, aplikasi, dan data. Ancaman terhadap keamanan *cyber* dapat terjadi dalam berbagai bentuk, tetapi biasanya merupakan hasil dari suatu entitas yang ingin atau berniat melanggar hukum, aturan, dan regulasi, serta kontrol atas keamanan informasi dan aset fisik

lainnya, untuk mendapatkan keuntungan yang berwujud dan tidak berwujud (Yusgiantoro, 2014).

Motivasi di balik *cybercrime* dapat bervariasi, dengan beberapa individu mencari keuntungan finansial, sementara yang lain terlibat dalam *cybercrime* untuk alasan politik, ideologi, atau pribadi. Peretas, istilah umum yang terkait dengan *cybercrime*, dapat diklasifikasikan ke dalam berbagai kategori berdasarkan niat dan keterampilan mereka. Memahami motivasi dan karakteristik pelaku *cybercrime* sangat penting untuk mengembangkan strategi guna mencegah dan merespons *cybercrime.* Pemerintah, lembaga penegak hukum, pakar keamanan *cyber*, dan organisasi di seluruh dunia terus berupaya memerangi kejahatan *cyber* melalui undang-undang, langkah-langkah keamanan *cyber*, kampanye kesadaran, dan kerja sama internasional. Kolaborasi antara berbagai pemangku kepentingan sangat penting untuk mengatasi lanskap ancaman *cyber* yang kompleks dan terus berubah(Andrian & Santoso, 2023) .

Di antara berbagai macam *cybercrime* ini adalah serangan kriptografi, yang mana menggunakan pragmatisme untuk memecahkan kriptografi dan mengidentifikasi kelemahan dalam kode, protokol, atau sandi yang melampaui apa yang diperlukan untuk menguraikan teks biasa tanpa kunci. Lalu ada serangan akses, di mana penyerang memasuki mesin host yang tidak diizinkan untuk digunakan dengan tujuan memanipulasi data. Lalu ada serangan pengintaian, di mana penyerang memetakan sistem yang mereka targetkan dan mencari kelemahan pada perangkat untuk mendapatkan data (Suharto & Apriyani, 2021). Jenis

serangan berikutnya disebut serangan aktif, yang terjadi ketika transfer data memodifikasi konten dan mengganggu operasi hingga bertindak sebagai perantara dan menyebabkan kerusakan serius. Mengenai serangan pasif, penyerang tidak mengubah atau mengkompromikan basis data; sebaliknya, ia hanya mengawasi target untuk mengakses data ketika sedang ditransmisikan. Dengan kata lain, tujuan utama penyerang adalah untuk mengumpulkan informasi dengan cara mendengarkan percakapan tuan rumah dengan menggunakan berbagai metode (Kaur & Ramkumar, 2022). Sedangkan pada phishing, yang mana jenis penipuan online lainnya yang dilakukan dengan menyamar sebagai situs web yang sah dengan URL yang identik. Pada malware sendiri terjadi ketika fungsi reguler sistem komputer terganggu oleh program jahat atau sepotong kode. Program-program malware biasanya dibuat dengan tujuan moneter atau tujuan-tujuan lain yang telah ditentukan sebelumnya. Serangan malware menjadi masalah yang sangat signifikan karena jumlahnya terus meningkat. Malware telah menyebar ke seluruh masyarakat dan sekarang berdampak pada orang-orang di semua bidang usaha (Yusgiantoro, 2014).

Adapun beberapa jenis *cybercrime* lainnya yaitu seperti:

1. *Denial of Service* (DoS), *Distributed Denial of Service* (DDoS), dan *Advanced Persistent Threats* (APT) membebani kapasitas sistem dan melarang pengguna yang sah untuk mengakses dan menggunakan sistem atau sumber daya yang diserang. Dengan mengekspos sistem untuk mengakses permintaan dan proses yang jauh lebih besar daripada yang dapat dikelola, serangan ini berusaha

mengganggu fungsi sistem normal. agar sistem menjadi terlalu sibuk dan macet, membuatnya tidak dapat digunakan atau tidak dapat dioperasikan.

2. Serangan malware, yang melibatkan penggunaan perangkat lunak atau program berbahaya untuk mengganggu operasi reguler sistem komputer. Program malware biasanya dibuat dengan tujuan moneter atau tujuan lain yang telah ditentukan sebelumnya.

3. Serangan vandalism, serangan ini melibatkan pengubahan atau pengubahan situs web korban sehingga konten situs web korban bergeser agar sesuai dengan tujuan penyerang.

4. Mengawasi lalu lintas transmisi data, data yang tidak terenkripsi yang dikirim melalui jaringan menggunakan protokol komunikasi akan dapat didengar oleh para penyadap. Mereka menggunakan PC untuk mengoperasikan, mengendus dan menganalisis lalu lintas jaringan sebelum mendapatkan kredensial yang dikirim pengguna dalam bentuk terenkripsi.

5. Spam, yaitu email massal yang tidak diminta kepada penerima dengan tujuan menginfeksi sistem dengan malware dan perangkat lunak berbahaya lainnya.

6. Penyalahgunaan protokol komunikasi. Karena *Transmission Control Protocol* (TCP) menciptakan hubungan logis antara dua sistem akhir untuk memfasilitasi transmisi data, serangan spoofing pada TCP bergantung pada fitur ini. Sambungan TCP dibuat dengan menggunakan nomor port, yang merupakan identitas logis.

7. Scam/fraud, mengacu pada aktivitas penipuan yang dilakukan melalui atau dengan bantuan sistem komputer atau internet.

Hal ini mencakup berbagai macam praktik penipuan, seperti penyalahgunaan kartu kredit, skema investasi yang menipu, barang yang tidak dikirim, dan penyalahgunaan dana. Kegiatan penipuan ini sering dilakukan dengan menggunakan berbagai platform online seperti situs web, email, dan ruang obrolan (Verma & Bajaj, 2008). Penipuan ini lebih berorientasi pada "orang" seringkali menggunakan metode manipulasi psikologis atau teknis untuk menipu korban agar memberikan informasi sensitif atau melakukan tindakan tertentu yang merugikan mereka (Furnell, 2001). Menurut jurnal yang berjudul "*Mapping the Terrain of Cybercrime" scam* terdiri dari kasus-kasus penipuan yang melibatkan perencanaan dan detail yang rumit, yang mana menargetkan individu dalam artian bahwa mereka mencari partisipasi dari para korban atau penipuan yang melibatkan korban 'pekerjaan' di mana korban berpartisipasi dalam sebuah skema yang biasanya penipuan pencucian uang, dan untuk partisipasi mereka, mereka diberi imbalan finansial. Penipuan ini sering kali dapat mengarah pada pencurian identitas dan kejahatan berbasis identitas lainnya karena dengan terlibat dalam salah satu penipuan ini, korban mungkin adalah seorang "pelamar" untuk apa yang mereka yakini sebagai kesempatan kerja (Stabek et al., 2010).

Fenomena *cyber scam* yang baru – baru ini terjadi dapat dilihat pada kasus penipuan pekerja wni di kamboja. Dengan meningkatnya angka kemiskinan dan gangguan di dunia kerja setelah pandemi COVID-19, diperparah dengan krisis

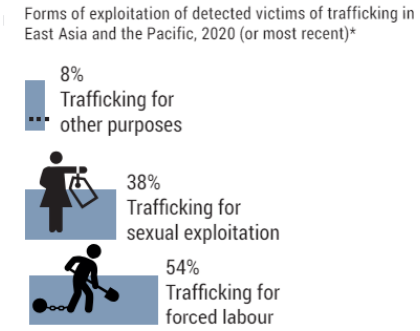
biaya hidup dan kerawanan kebutuhan pangan membuat banyak masyarakat mau tak mau harus segera mendapatkan pekerjaan baru. Media sosial merupakan faktor penting yang berkontribusi terhadap tindak pidana perdagangan orang, karena memungkinkan pengguna untuk mengakses informasi tanpa batas dan menciptakan komunitas dan jaringan virtual. Bentuk komunikasi elektronik ini memungkinkan terjadinya interaksi dan pertukaran informasi antar pengguna. Beberapa situs media yang banyak digunakan oleh masyarakat untuk melakukan interaksi dengan jarak tidak terbatas, diantaranya seperti WhatssApp, Facebook, Instagram, Twitter, Telegram, dan platfom lain sebagainya. Kementerian Luar Negeri Indonesia melaporkan adanya peningkatan kasus TPPO, di mana para korban direkrut melalui media sosial untuk pekerjaan di bidang layanan pelanggan atau pemasaran investasi, namun dipaksa untuk menjual investasi palsu atau bentuk lainnya secara online. Para calo TPPO juga digunakan sebagai penipu judi online di Kamboja. (Dwily Hamana et al., 2023).

Para pelaku *cyber scam* seringkali tidak memenuhi janji pekerjaan yang diiklankan, banyak dari perusahaan-perusahaan ini mulai memaksa para rekrutan untuk melakukan penipuan melalui internet yang diarahkan pada target internasional dan membuat mereka mengalami berbagai macam penyiksaan dan pelanggaran-termasuk penahanan dokumen perjalanan dan identitas dokumentasi perjalanan dan identitas, pengenaan utang sewenang-wenang, akses terbatas terhadap makanan, air, obat-obatan, komunikasi, dan pergerakan; dan ancaman, pemukulan, dan sengatan listrik. Operasi penipuan termasuk penjualan penipuan

berbasis kuota, skema perjudian dan investasi online ilegal dan penipuan percintaan, di mana korban dipaksa untuk menjalin hubungan online palsu dengan dan mengambil uang dari target yang tidak menaruh curiga. Para pelaku perdagangan orang memaksa korban untuk bekerja hingga 15 jam sehari dan, dalam beberapa kasus, "menjual kembali" korban ke operasi penipuan lainnya atau menjadikan mereka sebagai korban perdagangan seks jika mereka tidak setuju untuk merekrut anggota tambahan secara curang, atau jika para korban tidak memenuhi kuota pendapatan yang sangat tinggi. Larangan perjalanan terkait pandemi telah digunakan sebagai alasan untuk menahan para korban dengan kedok kepatuhan terhadap langkah-langkah kesehatan masyarakat. Bahkan ada laporan tentang operator penipuan *cyber* berbasis kasino yang secara brutal membunuh pekerja yang mencoba untuk melarikan diri.

Menurut data dari Laporan Perdagangan orang 2020 oleh Departemen Luar Negeri AS tahun 2023, kerja paksa adalah bentuk eksploitasi yang paling banyak terdeteksi di Asia Tenggara. Korban pelacakan kerja paksa meningkat hampir dua kali lipat antara tahun 2018 dan 2020, meningkat dari 29 persen menjadi 54 persen (U.S. DEPARTMENT of STATE, 2020). Namun penurunan deteksi korban pada tahun 2020 akibat merebaknya pandemi wabah pandemi COVID-19 dan mungkin telah dipengaruhi oleh langkah-langkah pencegahan yang dilakukan yang diterapkan di banyak negara di kawasan ini.

Gambar 1.1 Bentuk-bentuk eksploitasi terhadap korban perdagangan orang yang terdeteksi di Asia Timur dan Pasifik, 2020



Sumber: Global Report on Trafficking in Persons 2022

Menurut data statistik dari otoritas Kamboja, diperkirakan terdapat sekitar 100 ribu warga negara Indonesia yang tinggal di Kamboja. Hal tersebut merupakan peningkatan drastis, jika dibandingkan dengan sebelum Covid-19 hanya ada sekitar 2.000 orang Indonesia tinggal di Kamboja. Mereka bekerja di berbagai pekerjaan antara lain sebagai staf hotel, insinyur *cyber* hingga pemilik restoran (Kemlu RI, 2024). Menurut *Director General of Immigration of the Indonesian Ministry of Law and Human Rights* Silmy Karim, pun mengatakan saat ini terdapat lebih dari 73.000 warga negara Indonesia yang tinggal di Kamboja. Jumlah tersebut termasuk 58.307 WNI yang memiliki izin kerja resmi di Kamboja dan selebihnya merupakan pekerja ilegal yang mana perdagangan orang di Kamboja umumnya melibatkan penipuan online dan kerja paksa (Indonesiana, 2024). Direktur Pelindungan Warga Negara Indonesia Judha Nugraha mengatakan, kasus *online scam* di asia tenggara sejak tahun 2021 sampai 2023 tercatat ada 3.347. Dalam rentang waktu tersebut, negara Kamboja menjadi

negara terbanyak di asia tenggara yang memiliki kasus online scam.

Calon korban direkrut melalui iklan di media sosial atau broadcast di grup-grup chatting untuk lowongan pekerjaan sebagai customer service atau marketing investasi (Indonesiana, 2024; Zarbiyani & Djaja, n.d.). Indonesia dan Kamboja termasuk dalam Tier-2 dalam Laporan Perdagangan orang 2020 oleh Departemen Luar Negeri AS (U.S. DEPARTMENT of STATE, 2020). Laporan tersebut menyatakan bahwa meskipun Indonesia dan Kamboja telah melakukan upaya yang signifikan dalam memerangi perdagangan orang, Indonesia dan Kamboja gagal memenuhi standar minimum untuk menghapuskan kejahatan tersebut. Maka dari itu, dalam penelitian ini penulis akan melihat sebuah isu *cyber scam* perdagangan orang menjadi sebuah pembahasan yang penting untuk dibahas. Penelitian ini akan membahas bagaimana kolaborasi antara Indonesia – Kamboja dalam mengatasi perdagangan orang dan menganalisis bagaimana kebijakan di dalam negeri maupun di Kamboja dalam upaya untuk menangani perdagangan orang.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah penulis jelaskan, maka didapatkan rumusan masalah yang akan dikaji yaitu "**Bagaimana kolaborasi *Cambodia-Indonesia Bilateral Meeting on Immigration Matters* dalam menangani *cyber scam* perdagangan orang ?"**

1.3 Pembatasan Masalah

Dengan penjelasan latar belakang yang telah penulis jelaskan, penulis akan membatasi permasalahannya dengan tujuan untuk memfokuskan penelitian.

Penelitian ini akan membahas permasalahan indonesia - Kamboja pada isu *cyber scam* perdaganan orang dalam jangka waktu pada tahun 2020 – 2024. Hal ini akan memberikan wawasan tentang langkah-langkah yang telah diambil untuk melindungi warga negara.

1.4 Tujuan dan Kegunaan Penelitian

1.4.1 Tujuan Penelitian

1. Untuk mengetahui bagaimana fenomena *cyber scam* perdagangan orang yang terjadi antara Indonesia – Kamboja.
2. Untuk mengetahui dampak yang di timbulkan dari adanya kejahatan *cyber scam* perdagangan orang.
3. Untuk mengetahui strategi kolaborasi antara Indonesia – Kamboja

1.4.2 Kegunaan Penelitian

1. Hasil penelitian ini diharapkan mampu memberikan pemahaman terhadap mahasiswa hubungan internasional mengenai *cyber scam* perdagangan orang di ranah internasional.
2. Memberikan sumbangsih terhadap pengembangan penelitian – penelitianyang berkaitan dengan tema dan topik pada penelitian ini.