* [](https://i0.wp.com/informatika.uc.ac.id/wp-content/uploads/2022/01/CyberCrime.jpeg?fit=1920%2C1080&ssl=1)

**Cyber Crime di Era Industri 4.0**

Menurut Organization of European Community Development (OECD) cyber crime adalah semua bentuk akses ilegal terhadap suatu transmisi data. Itu artinya, semua bentuk kegiatan yang tidak sah dalam suatu sistem komputer termasuk dalam suatu tindak kejahatan. Sedangkan revolusi industri 4.0 atau juga yang biasa dikenal dengan istilah “cyber physical system” merupakan sebuah fenomena dimana terjadinya kolaborasi antara teknologi siber dengan teknologi otomatisasi.

Era revolusi industri 4.0 sangat berpengaruh terhadap tingkat kejahatan yang semakin modern. Bahkan, kejahatan manual sudah banyak ditinggalkan dan beralih kepada kejahatan yang sifatnya kejahatan dunia maya atau yang dikenal dengan istilah Cyber Crime. Memasuki era revolusi industri 4.0, aktivitas di dunia maya semakin meningkat, sehingga banyak juga kejahatan yang lebih besar di dunia maya. Meski kejahatan-kejahatan tersebut bersifat khusus, namun hal tersebut masih dijumpai di sekitar lingkungan masyarakat sendiri. Namun secara problematik,  kejahatan ini lebih banyak yang terjadi di dunia maya.

Kejahatan dalam revolusi industri 4.0 akan dianggap sebagai kejahatan ekonomi atau bisnis. Terminologi revolusi industri 4.0 terkait erat dengan aktivitas produksi bisnis. Oleh karena itu, kejahatan akan menciptakan kerugian yang menyebabkan kerugian ekonomi atau keuangan bagi para korban. Kerugian ekonomi atau keuangan tersebut harus nyata dan dapat dihitung. Para korban adalah perusahaan yang melakukan kegiatan bisnis dan produksi.

Kekhawatiran awal terkait dengan akses tidak sah ke informasi pribadi diperluas menjadi kekhawatiran bahwa komputer juga dapat digunakan untuk kejahatan ekonomi. Informasi adalah kunci dalam era informasi saat ini, semua perintah berbeda yang diketik oleh seorang programmer perangkat lunak yang memerintahkan komputer untuk melakukannya adalah instruksi yang memungkinkan era informasi. Kehilangan informasi dapat mengganggu atau menghentikan operasi bisnis dan produksi yang menyebabkan hilangnya manfaat.

[](https://i0.wp.com/informatika.uc.ac.id/wp-content/uploads/2022/01/pexels-mati-mango-6330644-scaled.jpeg?ssl=1)

Photo by Mati Mango from Pexels

Niat pelaku kejahatan siber tidak selalu didasarkan pada motivasi ekonomi. Tidak semua penjahat siber mencari untung, ada yang berniat menyebabkan kerusakan dan menghancurkan jaringan komputer karena alasan jahat. Menciptakan vandalisme teknologi tinggi berkontribusi terhadap motivasi. Beberapa penjahat dunia maya yang melakukan kejahatan sebagai bagian dari keberadaan mereka, kemampuan dan pernyataan politik.

Ada tujuh jenis kejahatan yaitu meretas (*hacking*), Intersepsi illegal, mengotori (*Defacing*), pencurian elektonik, *Interference*, Memfasilitasi tindak pidana terlarang dan Pencuri Identitas Identitas. konten ilegal dengan menggunakan internet, komputer dan teknologi terkait untuk melakukan kejahatan, seperti pornografi, judi, firnah, ujaran bencian dan lainnya juga termasuk kejahatan dunia maya.

Pelaku kejahatan siber dapat dihukum jika serangan itu menyebabkan kerusakan di komputer atau jaringan internet bahkan sulit, kerusakan tidak menyebabkan kerugian ekonomi atau finansial. Ketika serangan itu menyebabkan kerusakan pada jaringan komputer atau internet dan juga membuat kerugian ekonomi atau finansial, maka hukuman untuk kejahatan dunia maya lebih parah.

Pada akhirnya, konsep yang lebih luas dalam Undang-Undang Informasi dan Transaksi Elektronik tidak sepenuhnya cocok dengan kejahatan dunia maya dalam revolusi industri 4.0 yang mengklasifikasikan kejahatan dunia maya sebagai bagian dari kejahatan ekonomi dan bisnis. Oleh karena itu, konsep tersebut akan direvisi pada amandemen Informasi dan UU Transaksi Elektronik berikutnya. Di masa depan, diperlukan penelitian yang lebih empiris tentang kejahatan dunia maya di Indonesia. Tujuannya adalah untuk memahami jenis, motivasi dan pengembangan kejahatan dunia maya di Indonesia, sehingga negara dan pemerintah dapat membuat dan merencanakan pencegahan kejahatan dunia maya.

PERTANYAAN

1. Apa yang dimaksud dengan cyber crime dan cyber law ?
2. kasus dari cyber crime di Indonesia dan dikenakan pasal UU ITE berapa ?
3. langkah penanggulangan dari cybercrime ?
4. **Apa yang dimaksud dengan hacking?**
5. **Apa yang dimaksud dengan Malware?**

JAWABAN

1. **#Cyber Crime** adalah sebuah bentuk kriminal yang mana menggunakan internet dan komputer sebagai alat atau cara untuk melakukan tindakan kriminal.  
   **#Cyber Law** adalah hukum yang digunakan di dunia cyber ( dunia maya ), yang umumnya diasosiasikan dengan internet. Cyber law dibutuhkan karena dasar atau fondasi dari hukum di banyak negara adalah “ruang dan waktu”.
2. **Undang-Undang ITE Pasal 27 ayat 2;**

**“Setiap Orang dengan sengaja dan tanpa hak mendistribusikan dan/atau mentransmisikan dan/atau membuat dapat diaksesnya Informasi Elektronik dan/atau Dokumen Elektronik yang memiliki  muatan  perjudian”.**

**Ketentuan Pidana pada UU ITE sesuai UU ITE pasal 45 ayat (1);**

**“Setiap Orang yang memenuhi unsur sebagaimana dimaksud dalam Pasal 27 ayat (1), ayat (2), ayat (3), atau ayat (4) dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp1.000.000.000,00 (satu miliarrupiah). “**

1. IDCERT (Indonesia Computer Emergency Response Team)  
   Salah satu cara untuk mempermudah penanganan masalah keamanan adalah dengan membuat sebuah unit untuk melaporkan kasus keamanan. Masalah keamanan ini di luar negeri mulai dikenali dengan munculnya “sendmail worm” (sekitar tahun 1988) yang menghentikan sistem email Internet kala itu. Kemudian dibentuk sebuah Computer Emergency Response Team (CERT) Semenjak itu di negara lain mulai juga dibentuk CERT untuk menjadi point of contact bagi orang untuk melaporkan masalah kemanan. IDCERT merupakan CERT Indonesia.
2. Hacking adalah usaha memasuki secara ilegal sebuah jaringan dengan maksud bisa hanya sekedar mengamati, menyadap, mencuri data, dan sebagainya.
3. Malware merupakan program yang dibuat untuk melakukan suatu tindak kejahatan tertentu oleh suatu pihak sehingga akan merugikan pengguna yang komputernya terjangkit program ini.