Jurnal
ILMU KEPOLISIAN
ISSN : 2620-5025

Volume 17 / Nomor 3 / Desember 2023

DIGITAL POLICING; STUDI PEMANFAATAN TEKNOLOGI DALAM PELAKSANAAN TUGAS INTELIJEN KEPOLISIAN UNTUK MENCEGAH KEJAHATAN SIBER (*CYBERCRIME*)

Marzuki Ismail
Program Studi Doktor Ilmu Kepolisian, Sekolah Tinggi Ilmu Kepolisian, Jakarta 12160
e-mail: ahmadmarzuq2021@gmail.com

Abstrak

Pasca transformasi sosiologis masyarakat menuju masyarakat digital dengan dukungan jaringan internet, sebagian besar kebiasaan perilaku, budaya pun ikut berubah, termasuk transaksi keuangan yang dulunya dilakukan secara konvensional sejak satu dekade terakhir dengan menggunakan berbagai platform aplikasi. Kejahatan penipuan online, semakin mengancam dan meningkat secara signifikan dengan berbagai modus operandi yang berubah dan terus berkembang. Perkembangan teknologi digital belum maksimal dimanfaatkan oleh intelijen kepolisian untuk mencegah berbagai bentuk kejahatan (crime Prevention). teknologi digital secara maksimal untuk mengumpulkan informasi dan melakukan pendataan secara digital, hal ini mengakibatkan lambatnya antisipasi terhadap berbagai potensi kejahatan siber. Perpolisian digital dalam pelaksanaan tugas intelijen kepolisian perlu terus dikembangkan dengan melakukan investasi pada peralatan teknologi terkini agar dapat mewujudkan kepolisian yang prediktif, responsif, transparan, berkeadilan, dan mampu melakukan pencegahan kejahatan. Pendekatan dalam penelitian ini adalah penelitian kualitatif dengan metode studi literatur dengan menganalisis buku, jurnal, berita media terkait pemanfaatan teknologi dalam tugas intelijen kepolisian.

Kata kunci: perpolisian digital; teknologi; kejahatan siber; pencegahan kejahatan; intelijen

Abstract

After the sociological transformation of society to a digital society with the support of the internet network, most behavioural habits, culture have also changed. Including financial transactions that used to be carried out conventionally since the last decade using various application platforms. Various crimes, especially online fraud crimes, are increasingly threatening and increasing significantly with various modus operandi that change and continue to develop. The development of digital technology has not been maximally utilised by police intelligence to prevent various forms of crime (crime prevention). Police intelligence has not used digital technology to the fullest to collect information and conduct digital data collection. This has resulted in slow anticipation of various potential cyber crimes. Digital policing in the implementation of police intelligence tasks needs to be continuously developed by investing in the latest technological equipment in order to realise a predictive, responsive, transparent police force with justice and could accur the prevention of crime. The approach in this research is qualitative research with a literature study method by analysing books, journals, media news related to the use of technology in police intelligence tasks.

Keywords: digital policing; technology; cybercrime; crime prevention; intelligence

Pendahuluan

Sejak beberapa dekade terakhir, komunikasi, dan transaksi sektor keuangan ditransformasikan ke dalam sistem teknologi jaringan internet dan digital, maka peluang pelaku kejahatan menggunakan jaringan internet untuk melakukan kejahatan semakin meningkat secara signifikan. Berdasarkan data Kemenkominfo, selama tahun 2022 ada 130 Ribu korban kasus penipuan online (*Online Fraud, Phishing, Scamming*). Menurut Direktur Jenderal Aplikasi Informatika (Aptika) Semuel Abrijan, masyarakat Indonesia paling mudah ditipu secara *online* dan penipuan *online* sangat tinggi di Indonesia (https://infopublik.id/kategori/). Data tersebut baru kasus penipuan online, belum termasuk kasus-kasus pencurian data pribadi, pecemaran nama baik, dan lain-lain.

Tidak hanya di Indonesia, di Amerika Serikat berdasarkan *Internet Crime Report* (ICR) tahun 2020 terdapat 791.790 kasus laporan kejahatan internet di Amerika Serikat dengan total kerugian diperkirakan $ 4,1 Milyar atau sekitar Rp 59,5 Triliyun. Jumlah laporan ini naik 69% dibanding tahun 2019 dengan penipuan online merupakan laporan yang paling menonjol berjumlah 241.342 kasus. Jumlah kasus *ransomware* juga terus meningkat dengan 2474 laporan pada tahun 2020 (IC3, 2021: 3). Pergeseran jenis tindak pidanan dari konvensional ke kejahatan siber merupakan dampak negatif dari transformasi masyarakat tradisional ke masyarakat digital.
Perubahan sosial merupakan perubahan dari interaksi dan bagaimana masyarakat menyikapi setiap perkembangan yang terjadi. Perubahan sosial meliputi struktur, nilai, norma, pranata, dan fungsi masyarakat. Perubahan sosial masyarakat yang cepat akibat perkembangan ilmu dan teknologi dapat berakibat pada kondisi apa yang disebut oleh Emile Durkheim (1893) sebagai *anomie.* *Anomie* diartikan sebagai disfungsi sebuah sistem yaitu suatu keadaan masyarakat yang berubah dari masyarakat tradisional ke masyarakat modern di mana terjadi kondisi *normlessness*. Kondisi *normlessness* diartikan tidak berfungsinya norma dalam masyarakat serta nilai yang selama ini hidup dalam masyarakat terjadi kehilangan makna sebagai akibat munculnya banyak jenis kejahatan. Durkheim termasuk ilmuan yang memiliki keperihatinan tentang dampak modernitas terhadap masyarakat kontemporer (Stewart, John, 2023: 1).

Salah satu perubahan sosial yang terjadi dalam masyarakat adalah terjadinya transformasi dari masyarakat tradisional ke masyarakat digital. Saat ini kita hidup pada era yang sangat dinamis yang terus berubah dengan cepat. Teknologi informasi telah mengubah struktur kehidupan manusia. Pengaruh teknologi digital saat ini terhadap kehidupan individu dan sosial diyakini belum pernah terjadi sebelumnya (Levin dan Mamlok, 2021). Pola dan pengalaman hidup kita saat ini telah jauh berubah dibandingkan dengan pengalaman hidup kita 20 atau 30 tahun yang lalu. Transformasi teknologi informasi berdampak pada hampir seluruh aspek kehidupan manusia, mulai kebiasaan sehari hari, pola hubungan sosial, budaya masyarakat, pendidikan, ekonomi, politik, keamanan, pertahanan dan lain-lain.

Transformasi perkembangan teknologi ini tidak hanya membawa manfaat besar tetapi juga risiko besar. Kejahatan digital (*digital crime*) adalah salah satu aktivitas kriminal dengan pertumbuhan tercepat (Rakhmanova dan Pinkevich, 2020: 193). Pada saat bersamaan orang di berbagai belahan dunia bisa menjadi korban kejahatan yang sama. Kejahatan digital memiliki karakteristik tersendiri. Ia tidak memiliki batas geografis; kejahatan digital dapat dilakukan di suatu negara atau wilayah sementara korbannya ada di negara lain. Terlepas dari kenyataan bahwa dunia digital memunculkan anonimitas dan impunitas ketika melakukan kejahatan menggunakan

teknologi digital, penjahat tetap meninggalkan jejak digital. Tempat terjadinya kejahatan digital adalah lingkungan virtual; data komputer, sistem digital, atau media sosial yang digunakan untuk melakukan kejahatan (Rakhmanova: 195).

Transformasi masyarakat yang cukup signifikan adalah ketika penemuan Komputer, tetapi yang menjadi katalisator dalam transformasi yang besar dan cepat mulai terjadi ketika penemuan internet pada tahun 1969. Karena internet inilah yang dapat menkoneksikan jaringan komputer global. Internet adalah jaringan komputer yang saling terhubung dan memiliki kemampuan untuk membaca dan menkoneksikan, memfasilitasi berbagai aplikasi. Perkembangan jaringan internet semakin berkembang pesat, apalagi setelah Amerika Serikat membentuk *National Science Foundation Network* (NSFNet) pada tahun 1986. NSFNet menghubungkan jaringan komputer yang ada di berbagai negara. Dari sinilah kemudian pada tahun 1993 semua komputer yang menggunakan internet harus memiliki alamat *Internet Protocol* (IP *address*) atau nama domain berupa simbol numerik atau bentuk tertentu sebagai tanda pengenal. Jadi sampai saat ini setiap komputer, laptop atau *notebook* dan *device* lainnya yang terhubung dengan internet pasti memiliki IP *address*.

Kemudian secara perlahan jaringan internet ini mulai dikomersialkan pada awal tahun 1990-an dengan dilakukannya restrukrisasi NSFNet dan membuat entitas nirlaba untuk pengembangan komersial jaringan. Sejak saat itulah lahir berbagai pengembangan mulai *dot kom*, mesin pencari *mozilla firefox browser, Chrome browser, bitcoin, windows* dan istilah lain yang membuat masyarakat dapat mengakses berbagai informasi dan menghubungkannya dengan berbagai komunitas, produk dan juga ilmu pengetahuan di berbagai belahan dunia. Saat ini kita dapat mengetahui secara mudah apa yang terjadi di berbagai belahan dunia pada detik yang sama. Termasuk perkembangan mutakhir beberapa tahun belakangan adalah kita dapat melakukan belanja secara online dengan aplikasi bukalapak.com, shopee, tokopedia tanpa kita harus datang ke pusat perbelanjaan atau ke toko tempat barang yang kita butuhkan di jual. Atau kita juga dapat memesan tiket pesawat, tiket kereta api, memesan hotel hanya melalui sebuah peralatan yang ada dalam genggaman kita. Kita benar-benar sudah berada dalam percaturan dunia digital.

Kemudahan tersebut pada satu sisi dimanfaatkan oleh pelaku untuk melakukan kejahatan dengan memanfaatkan tekhnologi (*cybercrime*). Semua kemudahan dari revolusi teknologi ini awalnya dipandang sebagai sebuah peluang baru karena membawa kemudahan yang sangat signifikan. Namun dibalik semua kemudahan juga dengan segera menjadi sebuah ancaman. Diketahui bahwa revolusi industri telah menyumbangkan banyak kekayaan, tetapi juga banyak ketimpangan dan banyak masalah ekonomi. Hal yang sama berlaku untuk periode teknologi digital dan perubahan sosial saat ini (Hilbert, Martin, 2020: 189).

Dengan mudahnya pelaku kejahatan melancarkan misinya di dunia digital, maka ini merupakan tantangan bagi negara dan aparat penegak hukum untuk dengan serius memberantasnya untuk menghindari korban kejahatan digital semakin banyak. Salah satu yang perlu dilakukan adalah peningkatan sumberdaya teknologi yang digunakan oleh intelijen kepolisian untuk mengantisipasi dan mencegah kejahatan siber dan kecepatan dalam menanggapi suatu insiden kejahatan siber.

Yang menjadi permasalahan dalam artikel ini adalah dengan semakin tingginya kasus kejahatan di ruang digital (*cybercrime*) belum direspon secara maksimal oleh Intelijen kepolisian untuk mengantisipasi perkembangan teknologi yang begitu pesat. Pelaku kejahatan siber terus

mengembangkan modus operandinya dalam melakukan kejahatan tanpa upaya maksimal dari intelijen kepolisian untuk melakukan uapaya-upaya pencegahan.

Tinjauan Literatur

Digital

Digital berasal dari Bahasa Yunani yaitu *digitus* yang berarti jemari. Maksudnya adalah hitungan jari yang berjumlah 10 (Sepuluh). Dalam Kamus Besar Bahasa Indonesia (KBBI) arti digital adalah angka-angka. Digital merupakan penggambaran dari keadaan bilangan. Semua sistem komputer menggunakan sistem digital sebagai basis datanya atau disebut juga dengan istilah Bit (*Binary digit*). Era digital terlahir dengan kemunculan digital, jaringan internet khususnya teknologi informasi komputer (Wikipedia.org). Media baru era digital memiliki karakteristik dapat dimanipulasi, bersifat jaringan atau internet. Semakin canggihnya teknologi digital masa kini membuat perubahan besar terhadap dunia, Berbagai kalangan telah dimudahkan dalam mengakses suatu informasi melalui banyak cara, serta dapat menikmati fasilitas dari teknologi digital dengan bebas.

Era digital sebenarnya dimulai sejak lahirnya sistem komputer. Tetapi Ketika itu data yang ada dalam memori komputer belum dapat bergerak cepat. Baru setelah munculnya internet, data-data komputer dapat bergerak cepat, seperti pengiriman data melalui surat elektronik (email). Belakangan setelah muncul era *smart phone* maka pergerakan data jauh lebih cepat. Seiring munculnya *smart phone* muncul pula berbagai aplikasi media digital yang digunakan untuk keperluan *chatting* seperti *yahoo massanger, short massage service, face book, whataps, istagram, twitter, youtube,* dan lain-lain. Media jurnalistik *online*pun bermunculan sangat banyak.

Teknologi digital, termasuk keterhubungannya yang ada di mana-mana dan kecerdasan buatannya (*Artificial Intelligence*) yang kuat, adalah gelombang panjang terbaru dari evolusi sosial ekonomi umat manusia (Hilbert, 2020; 189). Inovasi teknologi informasi terus berkembang tanpa henti, bahkan transaksi ekonomi dan bisnis, pertemuan bisnis semuanya dapat dilakukan secara online atau *virtual*. Pembelian saham sebuah perusahaan atau emiten dapat dilakukan tanpa harus datang ke perusahaan atau bursa efek. Dengan membaca profile perusahaan dan jenis saham yang dijualnya Indonesia dapat langsung membeli saham sebuah perusahaan dan langsung masuk dalam portofolio Indonesia. Tidak hanya sampai di situ, pada saat ini apabila masyarakat membutuhkan dana dalam keadaan mendesak, tanpa harus bergerak dari tempat duduknya dapat melakukan pinjaman secara online (Pinjol) melalui *platform* digital.

Policing

Istilah '*policing*' dalam bahasa Indonesia diartikan 'pemolisian', ada juga yang memberi makna 'perpolisian'. Dalam penelitian ini peneliti menggunakan makna 'pemolisian'. Awalnya, menurut Johnston (Dalam Button, 2002; 4-5) sebelum pertengahan abad ke 18 istilah *policing* mencakup regulasi pemerintahan, moral, dan ekonomi. Baru kemudian istilah *policing* dikaitkan dengan pemeliharan ketertiban dan pencegahan kejahatan. Penting untuk membedakan istilah '*police*' dan '*policing*'. Istilah '*police*' mengacu pada sebuah organisasi tertentu, sedangkan '*policing'* mengacu pada proses sosial di mana fenomena-fenomena menjadi bagiannya, walaupun sebagian

besar *'policing*' dilaksanakan oleh organisasi polisi. *Policing* atau pemolisian merupakan fungsi masyarakat yang berkontribusi pada tatanan sosial tertentu yang dilakukan oleh berbagai badan dan lembaga yang berbeda.

Policing merupakan profesi yang sangat lama sekaligus baru. Kelahiran polisi modern pada awal abad ke 19 secara bersamaan dengan lahirnya birokrasi modern, industrialisasi, dan pembagian sosial. Kepolisian Metropolitan Robert Peel dianggap sebagai departemen kepolisian modern pertama, karena fokus pada birokrasi dalam menetapkan domain yang dapat diprediksi, yaitu kejahatan dan kekacauan publik, serta penekanan mereka pada pembangunan konsensus (Bielejewski, 2021: 11) Menurut Sparrow Pemolisian modern telah menjadi semakin "ilmiah," dengan penekanan pada cara terbaik untuk mencapai tujuan kelembagaan profesi tersebut.

Menurut Newburn (2008: 1) dalam literatur-literatur ilmu sosial modern, istilah yang dominan dibicarakan adalah globalisasi, resiko, bentuk baru modernitas dan lain-lain. Hal-hal yang dibahas tersebut merupakan hal-hal yang signifikan mempengaruhi kehidupan kita yang menembus semua aspek kehidupan, tidak terkecuali masalah pemolisian (*policing*). Maksudnya diskursus tentang *policing* merupakan masalah yang ikut didiskusikan oleh para sarjana sosial dalam literatur-literatur mereka. Bahkan banyak ilmuan sosial, kriminologi menaruh perhatian khusus pada masalah *policing* sebagai subyek penelitian mereka. Karena harus diakui bahwa *policing* merupakan suatu sub sistem dalam menata ketertiban masyarakat, penjaga moral, sebagai kontrol sosial dan juga kontrol kejahatan serta merupakan bagian yang dapat memberikan kampanye atau pendidikan tentang kejahatan dan dampaknya, pelaku kejahatan dan bagaimana agar masyarakat tidak menjadi korban kejahatan.

Dalam Collins *Dictionary* (www.collinsdictionary.com) ada dua makna *policing*: pertama, *the activities carried out by police officers in order to preserve law and order the policing of public places* artinya kegiatan yang dilakukan oleh aparat kepolisian dalam rangka menjaga keamanan dan ketertiban di tempat umum. Makna yang ke dua lebih moderat yaitu: *the actions of a person or group in authority in order to ensure fairness and legality in an area of public life* artinya tindakan seseorang atau kelompok yang berwenang untuk memastikan keadilan dan legalitas di bidang kehidupan publik. Makna yang pertama hanya dilaksanakan oleh polisi saja, tetapi makna yang ke dua dapat saja dilaksanakan oleh seseorang atau kelompok masyarakat dan makna ini lebih fokus pada pengawasan.

Intelijen Kepolisian

Intelijen sendiri berasal dari Bahasa Inggris *intelligence* yang bermakna kecerdasan. Pengertian intelijen dapat dibagi dalam tiga bagian, yaitu: *pertama*, Intelijen sebagai kegiatan; *kedua*, Intelijen sebagai organisasi; dan Intelijen sebagai produk, yaitu bahan keterangan yang sudah diolah yang selanjutnya disampaikan kepada pimpinan untuk bahan pertimbangan dalam pengambilan keputusan. *Core* dari tugas intelijen adalah *early warning system* atau sistem peringatan dini yang dapat memberikan informasi, peringatan atau pencegahan sebelum terjadi suatu insiden, terutama tindak pidana siber.

Intelijen Kepolisian merupakan intelijen penegakan hukum (*law enforcement intelligence*) atau juga sering ditemukan istilah intelijen kriminal (*criminal intellgence*) yang merupakan tugas kepolisian untuk menjaga keamanan dalam negeri. Pengertian intelijen penegakan hukum salah satunya dikemukakan oleh David L. Carter, dari *School of Justice, Minchigan State University* yaitu produk akhir dari sebuah proses analitik yang mengumpulkan dan menilai informasi tentang

kejahatan dengan tujuan untuk membuat penilaian dan kesimpulan tentang kondisi masyarakat, masalah potensial, dan aktivitas kriminal dengan tujuan untuk melakukan penuntutan pidana atau memproyeksikan tren kejahatan (Carter, 1990: 2).

Intelijen kepolisian juga sering disebut intelijen keamanan yang bertugas melakukan penyelidikan dalam rangka memelihara keamanan dan ketertiban masyarakat dengan metode mengumpulkan informasi (bahan keterangan) mengolah informasi, membuat analisa dan kemudian menyampaikan rekomendasi kepada pimpinan untuk penentuan kebijakan.

Secara struktural Intelijen kepolisian berada pada Badan Intelijen Keamanan (BIK) Polri yang bertanggung jawab kepada Kepala Kepolisian Negara Republik Indonesia (Kapolri). Di samping intelijen kepolisian, ada juga fungsi bahkan institusi intelijen melekat pada berbagai lembaga negara seperti Badan Intelijen Negara (BIN), Badan Intelijen Strategis (TNI), Intelijen Kejaksaan, Intelijen Imigrasi, Intelijen pertahanan, Intelijen keuangan, dan lain-lain.

Pencegahan Kejahatan

Pencegahan kejahatan (*Crime Prevention*) terdiri dari strategi dan tindakan yang bertujuan untuk mengurangi risiko terjadinya kejahatan, dan potensi dampak buruknya terhadap individu dan masyarakat, termasuk rasa takut akan kejahatan, dengan mengintervensi berbagai penyebabnya (The Prevention of Crime ECOSOC Resolution 2002/13, Annex). Di dalam *Action to promote effective crime prevention* disebutkan bahwa diatara prinsip dasar dalam strategi pencegahan kejahatan antara lain adanya peran semua level pemerintahan untuk membangun strategi yang efektif dalam pencegahan kejahatan.

Lab (1992: 31-32) mendefinisikan pencegahan kejahatan merupakan sebuah tindakan untuk menghilangkan kejahatan sebelum terjadi atau sebelum kejahatan berkembang lebih jauh. Lab juga membedakan antara pencegahan kejahatan dengan pengendalian kejahatan. Model pencegahan kejahatan dibagi tiga yaitu pertama, pencegahan kejahatan primer merupakan tindakan yang diambil untuk menghindari pengembangan tingkat masalah; Kedua, pencegahan kejahatan sekunder bergerak dan fokus pada masyarakat dan situasi yang memperlihatkan tanda-tanda awal suatu masalah atau kejahatan; ketiga pencegahan kejahatan tersier berhubungan dengan pelanggar hukum yang nyata dan melibatkan intervensi setelah terjadi kejahatan agar tidak terjadi kejahatan berulang.

Untuk melaksanakan ketiga model pencegahan di atas harus adanya kerjasama antara berbagai *stakeholders* juga sangat menentukan pengembangan strategi pencegahan kejahatan. Konsep pemolisian modern yang yang dicetuskan oleh Sir Robert Peel di Inggris sejatinya menekankan pada pencegahan kejahatan dengan model patroli polisi berseragam (Rainer, 2016: 114). Di samping upaya-upaya dari kepolisian, pencegahan kejahatan dapat dilakukan oleh masyarakat dan *stakeholders* lainnya dalam perspektif tradisional sebagaimana dalam Teori *Situasional Crime Prevention*, yaitu dengan menciptakan lingkungan masyarakat untuk mengurangi kesempatan bagi pelaku untuk melakukan kejahatan, terutama pada situasi lingkungan, waktu, dan modus operandi. Pendekatan pencegahan seperti ini berupaya membuat target kurang memiliki potensi dan meningkatkan resiko bagi pelaku serta meningkatkan kesukaran bagi pelaku untuk melakukan kejahatan atau *target hardening*. Menciptakan lingkungan dalam konteks kejahatan siber dengan memasang end-point antara lain *Instrusion Detection Systems* (IDS), *Instrusion Prevention Systems* (IPS) yang mengambil tindakan otomatis untuk menghentikan serangan potensial, *Authentication and Access Control* dan peralatan lainnya.

Kejahatan Siber (*Cybercrime*)

Casey (2000) mendefinisikan *cybercrime* sebagai kejahatan yang melibatkan komputer dan jaringan (Kyung-Shick Choi, 2008: 2). Dalam kejahatan siber, alat yang digunakan adalah komputer, *smartphone* atau peralatan lainnya yang difasilitasi oleh jaringan internet dan antara korban dengan pelaku rata-rata tidak pernah bertemu, mereka hanya berkomunikasi secara virtual. Ada berbagai macam jenis kejahatan siber antara lain: *Unauthorized Acces to Computer System and Service*; *Hacking dan Cracking ; Cyber Fraud/Online Fraud; spoofing*; *credit card fraud*; *identity theft* (Vadza, 2013: 1) *Data Forgery , Cyber Espionage; Cyber Sabotage and Extortion; Offense Against Intellectual Property; Infrengments of Privacy; Gambling; Cyber Porn/Cyber Sex; Cyber Stalking* (Burhansyah, 2016: 41), *Cyber terrorism, Cyberbullying, Child Pornography* (Ibrahim, Samira dkk, 2021: 1-2).

Jenis kejahatan siber ini terus berkembang dan berubah dengan berbagai modus operandinya. Maka dalam pencegahan kejahatan siber sangat dibutuhkan strategi yang efektif oleh intelijen kepolisian untuk dapat mendeteksi potensi ancaman kejahatan siber dan juga dapat mendeteksi potensi masyarakat yang akan menjadi korban, sehingga dapat diberikan *early warning* dari awal.

Metodologi Penelitian

Penelitian ini menggunakan pendekatan penelitian kualitatif dengan strategi studi kepustakaan dengan menganalisis buku, jurnal, dan berita media yang terkait dengan penggunaan teknologi dalam tugas intelijen kepolisian. Metode penelitiannya adalah studi kasus. Teknik pengumpulan data yaitu: dengan wawancara, observasi, dan studi dokumen. Teknik analisis data yaitu: dengan triangulasi data, sebelumnya dilakukan validitas data.

Hasil dan Pembahasan

Polisi dan Teknologi

Dalam penelitian-penelitian sebelumnya menunjukkan bahwa polisi merupakan pengadopsi awal penggunaan teknologi baru dan dapat memprediksi perkembangan teknologi baru. Karena adanya kemajuan tekhnologi, maka polisi menerapkan *cyber-policing* dengan pembentukan unit khusus *cybercrime* (Dale Willits dan Nowacki, 2016: 12-13). Penggunaan teknologi oleh kepolisian, karena polisi berada paling depan dalam penggunaan teknologi untuk merespon kejahatan siber. Hal ini menunjukkan bahwa polisi secara eksperimental menggunakan teknologi canggih sebagai bentuk keterlibatan dalam teknologi sosial dan berada di garis depan. Dalam penelitian lain, tentang inovasi kepolisian akan ada manfaat antara keterlibatan teknologi dan kemajuan lainnya dalam strategi teknologi kepolisian (Dale, 2016: 25).

Perkembangan kontemporer lain bidang pemolisian, dalam tugasnya polisi juga menggunakan teknologi baru dan selalu mengubah metode dan strategi mereka (Michael Gelles dkk, 2019: 4). Tantangan tugas yang berhadapan dengan perkembangan teknologi informasi. Kejahatan-kejahatan yang terjadi, modus operandi atau polanya terus berubah. Kejahatan siber secara kuantitas dan kualitas meningkat pesat, sehingga menuntut Polri untuk membentuk satuan khusus untuk menangani kejahatan siber, yaitu dengan dibentuk Direktorat Tindak Pidana Siber (Dit Tipidsiber) yang berada di bawah Bareskrim Polri. Direktorat Siber harus memanfaatkan teknologi Informasi secara maksimal, terutama melakukan patroli siber (*cyber patrol*) terhadap media-media sosial. Pembentukan Dittipidsiber Bareskrim Polri tidak diimbagi oleh pembentukan

cyber intelligence yang kuat di Badan Intelijen Keamanan (Baintelkam) Polri. Dalam tugasnya Dit Tipidsiber melaksanakan penyelidikan dan penyidikan untuk menentukan suatu tindak pidana kemudian memproses secara hukum di sisi lain penyelidikan intelijen melaksanakan penyelidikan untuk meniadakan (mencegah) suatu potensi kejahatan siber.

Walaupun teknologi informasi terus berubah secara cepat, fungsi, dan tugas pokok aparatur hukum adalah tetap menegakkan hukum dengan tantangan dan peralatan yang semakin berkembang. Fungsi penegakan hukum, khususnya terhadap kasus siber, selama ini dirasakan belum efektif terutama pada aspek pencegahan dan juga penindakan. Karena kompleksitas dari kasus siber mulai dari sifatnya yang virtual, trans-nasional, dan sulitnya mengikuti uang hasil kejahatan (*follow the money*). Tetapi kurangnya perhatian yang diberikan pada kejahatan siber tidak sesuai dengan tingkat kerugian yang ditimbulkan. Padahal kerugian akibat kejahatan siber tidak sama dengan yang dialami oleh korban kekerasan, terutama mengalami trauma emosional dan psikologis (Cross dan Blackshaw, 2015: 4-5).

Kemunculan kejahatan siber dan banyaknya tersebar informasi yang salah serta informasi negatif memerlukan aparat penegak hukum yang dapat menanggulangi dan dapat memprediksi kejahatan serta dapat mencegah menyebarnya informasi negatif kepada masyarakat di dunia maya, sehingga model-model pemolisian di berbagai negara mengalami perubahan yang signifikan seperti di Amerika Serikat, Eropa, Australia, dan lain-lain yang sudah mencari solusi terhadap sebuah pemolisian yang berlomba dengan perkembangan kemajuan TI yaitu *Digital Policing*, *Predictive Policing* atau Pemolisian prediktif. Pemolisian digital dapat menganalisis isu dan permasalahan yang berpotensi menjadi gangguan keamanan. Hal ini menunjukkan Pemolisian digital dan prediktif memerlukan penerapan teknik kuantitatif untuk menganalisis data untuk menentukan perkiraan potensi di mana kegiatan kriminal mungkin terjadi dalam waktu dekat (Meijer dan Wessels, 2019: 1033). Dalam perkembangan pemolisian, tidak dapat diimplementasi satu model pemolisian saja, tetapi beberapa model pemolisian berjalan secara simultan. Di samping ada model pemolisian yang modern, model pemolisian lama juga tidak dapat ditinggalkan seluruhnya. Hal ini tentu saja ditujukan untuk menemukan pola pencegahan yang efektif terhadap kejahatan siber.

Dalam menghadapi tantangan tugas kepolisian yang semakin kompleks, terutama kejahatan siber, perlu dibangun "pusat keunggulan" (*Center of Excellent*) sebagai representasi dari seluruh penegakan hukum. Seperti yang dilakukan di Kepolisian Australia, mereka membangun "*Center of Excellent*" dan "*Sigle Point of Contact*" yang mewakili seluruh penegakan hukum yang efektif untuk seluruh spektrum kejahatan yang serius/menonjol. Dengan adanya pusat keunggulan ini dapat memastikan peningkatan yang terus menerus di bidang forensik, intersepsi dan kemampuan teknis lainnya. *Center of Excellent* ini sebentuk kemlompok ahli di bidang intelijen dan juga para penyidik yang berkolaborasi untuk mengantisipasi kejahatan siber.

Penggunaan Teknologi oleh Intelijen Kepolsian

Tugas-tugas intelijen sejatinya dapat memanfaankan Teknologi Informasi (TI) secara lebih cerdas dan masif. Karena pemanfaatan TI merupakan konsekuensi logis atau sesuatu yang niscaya. Tugas intelijen salah satunya adalah mendeteksi isu-isu yang berkembang dalam masyarakat di bidang ideologi, politik, ekonomi, sosial, budaya, dan keamanan. Tekhnologi informasi telah memberikan banyak kemudahan bagi umat manusia, tetapi di sisi lain tekhnologi informasi juga memunculkan

kejahatan dengan menggunakan tekhnologi. Kejahatan yang menggunakan teknologi informasi sebagai media, modusnya juga bermacam-macam dan cepat sekali berubah.

Intelijen kepolisian adalah intelijen penegakan hukum yang bekerja sebagai bagian dari penegakan hukum. Tugas-tugas kepolisian dibidang *law enforcement* memerlukan aktifitas intelijen. Karena proses penegakan hukum membutuhkan data-data spesifik yang dibutuhkan oleh pimpinan (*User*). *Data Collecting* dilakukan oleh fungsi intelijen melalui aktifitas *early detection* yang secara sistematis mengikuti *intelligency cycle* yang meliputi *planning, collection, processing, analysis, dissemination.* Siklus intelijen ini merupakan metode kerja intelijen yang terencana yang diharapkan dapat menghasilkan data yang akurat dan dapat mendukung upaya-upaya penegakan hukum (Chryshnanda, 2020: 157).

Dalam pelaksanaan penyelidikan terdapat beberapa tantangan yang dihadapi oleh penyelidik diantaranya terkait masalah praktis, teknis, dan sosial seperti ketersediaan sistem dan kerja kolaboratif serta didukung dengan perangkat komputer (Nouh, Mariam dkk, 2019: 1) Dalam pelaksanaan penyelidikan dengan berbagai model, pengumpulan data intelijen merupakan proses untuk mendukung penegakan hukum. Meskipun model-model pengumpulan informasi seperti berbeda, tetapi model proses pengumpulan informasi intelijen memiliki proses yang sama, seperti yang terlihat dalam gambar siklus intelijen di bawah ini (Nouh, 2019: 2).

Gambar 1. Siklus Intelijen (*Departement of Defence)*

Siklus Intelijen terdiri dari Enam langkah utama: Perencanaan dan Pengarahan, Pengumpulan, Pemrosesan dan Eksploitasi, Analisis dan Produksi, Penyebarluasan dan Integrasi, serta Evaluasi dan Umpan Balik. Dalam pengumpulan data dan informasi siklus ini akan terus berputar. Apabila ada suatu misi atau target yang hendak dicapai maka selalu dimulai dari perencanaan pengumpulan informasi yang terdiri dari menentukan personil yang akan melaksanakan misi, rencana anggaran, rencana limit waktu, rencana *safe house*, rencana *emergency* dan rencana *escape* apabila terjadi situasi emergensi untuk tindakan penyelamatan personil dan informasi yang telah didapat. Dan yang sangat penting dalam pelaksanaan pengumpulan informasi ini adalah penggunaan teknologi digital pada setiap tahap siklus intelijen tersebut. Proses pengumpulan informasi yang dilakukan selama ini kurang dibarengi dengan

penggunaan teknologi informasi berupa peralatan khusus (Alsus) yang seharusnya melekat pada setiap langkah siklus intelijen untuk membantu dan memetakan serta pendataan yang akurat dalam membuat analisis, prediksi, dan rekomendasi intelijen.

Pemanfaatan model pemolisian digital dalam bidang intelijen kepolisian belum maksimal. Padahal model pemolisian digital ini sebagai salah satu bentuk *e-policing* dan merupakan salah satu bentuk pemolisian era digital yang berupaya menerobos sekat-sekat ruang dan waktu sehingga pelayanan kepolisian dapat terselenggara secara cepat, tepat, akurat, transparan, akuntabel, informatif dan mudah diakses. Model pemolisian ini dapat menjadi terobosan kreatif atau *creative breakthrough* (Chryshnanda, 2020: 39).

Pelaksanaan tugas intelijen Kepolsian masih sangat minim pemanfaatan teknologi informasi sehingga intelijen kepolisian dalam pelaksanaan tugasnya masih dominan dengan *human intelligence* atau metode konvensional yang mengandalkan kemampuan agen (petugas) intelijen yang kurang dikombinasikan dengan peralatan teknologi canggih untuk membantu tugas intelijen kepolisian. Karena masih belum optimalnya pemanfaatan TI maka kehadiran anggota Polri secara fisik dalam rangka mengumpulkan informasi (*gather of Information*) masih sangat dominan. Padahal kalau TI dimanfaatkan secara maksimal, maka akan memudahkan kerja-kerja intelijen kepolisian yang berujung juga pada pelayanan masyarakat yang lebih cepat, mudah dan akurat serta dapat melakukan *crime prevention* secara simultan.

Bagi dunia intelijen, secara tradisional petugas intelijen (agen) berhadapan dengan suatu sasaran yaitu manusia. Tetapi di era digital, sasaran operasi atau penyelidikan intelijen bukan hanya manusia, tetapi perangkat tekhnologi yang digunakan manusia. Perangkat seperti *smart phone*, komputer, aplikasi dan vitur-viturnya dengan media internet maka akan sangat efektif dalam mengirim pesan kepada orang lain. Tekhnologi intelijen seharusnya dapat mendeteksi pesan atau lalu lintas pesan dan gerak media sosial yang merupakan sebuah dunia tersendiri (dunia maya) tetapi dapat memberikan dampak dalam dunia nyata. Karena melalui lalu lintas pesan di dunia maya yang sangat banyak itulah berisi potensi dan rencana melakukan kejahatan.

Pola-pola pemolisian di bidang intelijen selama ini belum jauh berubah sejak bergulirnya reformasi Polri. Artinya pola pemolisian di bidang intelijen masih sangat mengandalkan human (tenaga manusia), selama ini personil bekerja mirip seperti pekerjaan fungsi Binmas, sehingga muncul *anekdot*, intelijen itu ada dua, yaitu Intel yang berseragam yaitu Binmas atau Babinkamtibmas dan Intel tidak berseragam (*Ununiform*) yaitu fungsi intelijen, karena memang pola kerjanya hampir sama. Padahal kemajuan TI seharusnya dapat dimanfaatkan untuk mempercepat dalam pengumpulan bahan keterangan (informasi) dan juga dapat secara cepat disampaikan (diseminasi) kepada pengambil kebijakan atau kepada *stakeholders* yang membutuhkan.

Pemolisian era digital di bidang intelijen sangat luas. Intelijen harus dapat mendeteksi potensi ancaman di bidang ideologi, politik, ekonomi, sosial, budaya dan keamanan (Ipoleksosbudkam). Bidang-bidang tersebut kalau di*break down* sangat luas, mulai dari politik, dampak otonomi daerah, sengketa batas daerah, konflik antara masyarakat dengan investor, dampak pelaksanaan Pilkada, kenaikan harga bahan kebutuhan pokok, masalah buruh, tenaga kerja, masalah investasi, pelaksanaan ujian nasional, dampak inflasi, dampak pembangunan, masalah sumber daya alam, kejahatan konvensional, Kejahatan bidang ekonomi, korupsi, Narkoba, terorisme, radikalisme, aliran kepercayaan, konflik Suku, Agama, Ras dan Antar golongan (SARA). Dalam semua bidang yang disebut di atas semuanya dapat berpotensi terjadi

kejahatan siber. Maka dengan bidang tugas yang sangat luas seperti itu, pemanfaatan teknologi informasi dan sarana elektronik yang maksimal sangat membantu pelaksanaan tugas-tugas intelijen agar lebih modern, cepat, akurat, tepat, dan akuntabel untuk dapat menjaga kepentingan dan keamanan nasional, termasuk serangan dari kejahatan siber.

Untuk dapat mendukung misi-misi intelijen dalam pengumpulam informasi, maka diperlukan juga Unit *Intellgence Cyber Cops* (ICC). Unit ini dibutuhkan untuk menjawab tantangan era digital yang serba cepat. Dalam unit ini diisi oleh polisi intelijen yang muda dan memiliki kemampuan TI yang mempuni sehingga dapat menyajikan data 24 jam sehari, Tujuh hari dalam seminggu dengan standar kualitas yang tinggi dengan kemampuan analisis intelijen yang kuat. Mereka harus dilatih secara khusus dan serius tentang analisa intelijen, sehingga mereka dapat membuat sebuah analisa intelijen yang kuat, tajam dengan prediksi dan rekomendasi yang dapat digunakan oleh pimpinan (*User*) untuk mendukung pengambilan keputusan bidang pencegahan kejahatan siber.

Dampak komunikasi di dunia maya dengan teknologi digital dari sisi positifnya sangat banyak, seperti pengiriman data atau file melalui media yang cepat dengan kapasitas besar. Tetapi Perkembangan teknologi juga memiliki dampak negatif seperti provokasi melalui media sosial yang menyebabkan kerusuhan, penculikan, penipuan, penghasutan, transaksi *illegal*, dan lain-lain. Sehingga sangat berpengaruh terhadapat keamanan dan ketertiban masyarakat (*social order*). Kalau sudah berpengaruh terhadap keamanan dan ketertiban masyarakat, artinya masalah ini sudah menjadi tugas dan tanggung jawab Polri sebagai penjaga ketertiban masyarakat dan penegakan hukum. Polisi yang bertugas sebagai *law enforcement officer* tidak bisa tiba-tiba langsung dapat menangkap pelaku kejahatan di dunia maya apabila tidak ada kemampuan untuk mendeteksi dan menelusuri jejak pelaku yang juga ada di dunia maya dengan menggunakan berbagai aplikasi digital.

Intelijen polisi yang bertugas sebagai investigator di dunia maya harus memiliki kemampuan *cyber patrol*, harus dapat membongkar sebuah akun, *ip address*, *mobile number* yang digunakan dan sebagainya. Gunanya adalah untuk mengetahui pemilik akun yang digunakan untuk menipu atau menghasut, provokasi dan lain-lain. Kalau sudah sampai pada tahap ini polisi dapat merencanakan Langkah-langkah selanjutnya dalam rangka penegakan hukum.

Kemampuan dan jenis media yang digunakan oleh Lembaga kepolisian juga perlu menjadi perhatian, karena pesatnya kemajuan teknologi informasi, maka masyarakatpun menggunakan berbagai jenis media sosial dalam berinteraksi. Dalam organisasi Polri belum ada data tentang jenis-jenis media sosial yang digunakan oleh departemen di kepolisian. Misalnya Badan Intelijen Keamanan (BIK) Polri yang di dalamnya terdapat beberapa direktorat dan bagian, secara official menggunakan media sosial apa saja untuk memonitor dan menjalin kemitraan dengan masyarakat. Di Amerika Serikat, berdasarkan penelitian yang dilakukan oleh *Police Exsecutive Research Forum* (PERF) pernah melakukan penelitian tentang persentase jenis media sosial yang digunakan oleh badan/bagian kepolisian. Bahkan 98 % dari badan-badan kepolisian yang disurvey akan meningkatkan penggunaan media sosial dalam dua sampai lima tahun yang akan datang (PERF, 27).

Tujuan penggunaan media sosial oleh kepolisian diantaranya adalah untuk desiminasi pesan kepada masyarakat dan juga dapat mengumpulkan informasi dari media sosial untuk mencegah dan dalam rangka penyelidikan kejahatan (PERF). Dalam even-even besar media sosial dapat memandu bagian operasi kepolisian untuk memonitor isu-isu atau *trending topics* yang

menjadi pembicaraan di kalangan masyarakat atau mengguna media sosial. Bahakan di *Los Angeles Police Departement* (LAPD) telah memasukkan Bagian Sosial Media dalam struktur organisasi operasi dalam banyak even yang bertanggung jawab untuk memberikan pengarahan tentang aktivitas yang sedang dibicarakan di media sosial (PERF, 28).

Peralatan Teknologi Intelijen Kepolisian

Intelijen kepolisian sejatinya memiliki peralatan khusus (Alsus) yang memiliki kualitas dan berteknologi tinggi untuk dapat digunakan dalam pelaksanaan tugas-tugas intelijen untuk mencegah kejahatan siber. Secara Umum peralatan intelijen terdiri dari alat deteksi, alat keamanan dan alat komunikasi. Berdasarkan Surat Keputusan Kapolri Nomor : Skep / 992 / XII / 2005 tanggal 30 Desember 2005, tentang Standarisasi Alat Khusus Intelijen, ada tiga belas kegunaan peralatan khusus intelijen yaitu untuk observasi, merekam suara, merekam gambar bergerak (video) dan tidak bergerak (photo), menyadap suara, menyadap video, komunikasi, pengamanan, deteksi barang-barang berbahaya, membuka pintu dan tas koper, transportasi, pengolah data, menjam / mengacau alat penyadap lawan, melacak alat penyadap lawan (Sumarjiyo, 2018: 150).

Pada saat ini dengan perkembangan teknologi informasi yang sangat cepat peralatan intelijen kepolisian juga harus menyesuaikan dengan perkembangan peralatan terbaru, agar dapat berfungsi efektif dalam mencegah kejahatan siber. Standar produk yang digunakan untuk pelaksanaan tugas intelijen kepolisian harus mempertimbangkan kelayakan, kehandalan, spesifikasi dari material dan juga struktur penggunan (Sumarjiyo, 158). Pengadaan peralatan intelijen kepolisian sangat perlu memperhatikan kualitas dan fungsionalisasinya agar dapat dioperasionalkan secara maksimal. Oleh sebab itu dibutuhkan pelatihan bagi personil yang mengawaki peralatan tersebut untuk dapat mengetahui secara detail penggunaan dan pemeliharannya.

Kesimpulan dan Saran

Perkembangan teknologi informasi, terutama teknologi digital tidak dapat dihindari oleh semua komponen masyarakat dan lembaga pemerintah. Yang terpenting bagi masyarakat adalah bagaimana memanfaatkan teknologi tersebut untuk tetap menjaga dan membangun peradaban yang dicita-citakan. Bagi Polri, terutama intelijen kepolisian harus memaksimalkan peran pengawasan untuk mencegah terjadinya penyalahgunaan teknologi dalam bentuk kejahatan siber (*Cybercrime*) dan apabila sudah terjadi penyalahgunaan atau adanya unsur tindak pidana yang merugikan orang lain atau bahkan merugikan negara. Polri harus dapat mengatasi bentuk-bentuk kejahatan yang dapat merusak peradaban umat manusia dengan cara Intelijen kepolisian melakukan *collecting data base* terhadap kelompok masyarakat, residivis, kelompok pelaku kejahatan, aktivitas masyarakat yang menonjol. *Collecting data* dapat dilakukan secara konvensional dan juga secara digital (*online)* dengan memanfaatkan teknologi untuk mengimbagi para pelaku kejahatan yang juga menggunakan teknologi digital dalam menjalankan aksinya. Polri juga melaksanakan investigasi atau penyelidikan secara digital dan *online* seperti penggunaan media sosial untuk ketepatan dan kecepatan penyajian data dan hasil investigasi kepada *user* agar dapat diambil Langkah-langkah antisipatif dan preventif.

Saran yang diberikan dalam artikel ini berupa saran praktis, bukan saran teoristis, dengan maksud agar dapat dilaksanakan oleh pengambil kebijakan di bidang pelaksanaan intelijen

kepolisian. Adapun saran-saran tersebut sebagai berikut: (1) Untuk dapat mengantisipasi dan mencegah kejahatan siber, intelijen kepolisian perlu menggunakan dan memanfaatkan teknologi mutakhir untuk mendukung data *collecting*, analisis dan prediktif, sehingga dapat diambil langkah antisipatif dan kebijakan oleh pimpinan; (2) dalam pelaksanaan tugas intelijen era digital, maka perlu dibentuk Direktorat *Cyber-Intelligence* untuk secara maksimal dapat melakukan pencegahan kejahatan siber dengan memanfaatkan Unit *Intellgence Cyber Cops* (ICC); (3) Intelijen kepolisian perlu secara terus menerus meng-*upgrade* peralatan intelijen khusus untuk mendukung pelaksanaan pencegahan kejahatan siber yang sangat luas sebarannya; dan (4) perlu melatih personel khusus intelijen kepolisian yang memiliki kompetensi bidang teknologi informasi. Pelatihan yang dilaksanakan secara berkala dan insidentil untuk mengantispasi perkembangan teknologi baru. Di samping memiliki kemampuan TI, personel intelijen kepolisian juga memiliki kemampuan analisis yang kuat dalam bidang kejahatan siber agar dapat memberikan rekomendasi yang akurat.

Daftar Pustaka

Albert Meijer and Martijn Wessels, 2019. *Predictive Policing: Review of Benefits and Drawbacks*, International Jounal of Public Administration, Vol 42 No 12.

Bielejewski, Aaron, 2021. *Policing Communities and Community-Oriented Policing in Rural Germany*, a Doctoral Dissertation to the University of Kassel, Department of Social Sciences, Germany.

Burhansyah A, Encik Muhammad, 2016. *Kerja Sama Polri dan Australian Federal Police (AFP) Sektor Capacity Building Dalam Penanggulangan Tindak Pidanan Cybercrime Di Indonesia Periode 2012-2014*, Journal of International Relations, Volume 2, Nomor 1, p. 38-46.

Button, Mark, 2002. *Private Policing*, UK: Willan Publishing.

David L. Carter, David L, 1990. *Law Enforcement Intelligence Operations*, School of Justice, Michigan: Michigan State University.

Chryshnanda DL, 2020. *Polisi dan Pemolisian*, Jakarta: YPKIK.

Cross, Cassandra dan Dom Blackshaw, 2015. *Improving the Police Response to Online Fraud*, Policing, Oxford: Oxford Press.

Dale Willits and Jeffrey Nowacki, 2016. *The Use of Specialized Cybercrime Policing Units: An Organizational Analysis*, Criminal Justice Studies, Vol. 29, No. 2, Southern Illinois University, Departement of Criminology and Criminal Justice.

Federal Bureau of Investigation (Internet Crime Complaint Center, IC3), *Internet Crime Report 2020*, 2021. Linglay, USA.

Hilbert, Martin, 2020. *Digital Technology and Social Change: The Digital Transformation of Society from a Historical Perspective*, Dialogues in Clinical Neuroscience, Vol 22 No. 2.

Ibrahim, Samira, Ojeifoh Okosun, Daniel Nnamani, 2021. *Types of Cybercrime and Approaches of Detection*, IOSR Journal of Computer Engineering 23(5):24-26, DOI:10.9790/0661-2305022426.

Kyung-Shick Choi, 2008. *Computer Crime Victimization and Integrated Theory: An Empirical Assessment*, International Journal of Cyber Criminology, (IJCC) ISSN: 0974 – 2891 January-June 2008, Vol 2 (1).

Lab, Steven P, 1992. *Crime Prevention: Approaches, Practices, and Evaluations*, Anderson Publishing, Edisi Terjemahan Bahasa Indonesia 2017.

Levin, Ilya, dan Mamlok, Dan, 2021. *Culture and Society in the Digital Age*, MDPI, Information, https://doi.org/10.3390/info12020068

Michael Gelles, Alex Mircow and Joe Mariani, 2019. *The Future of Law Enforcement*, The Deloitte Center for Government Insights.

Newburn, Tim, 2008. *Introduction: Understanding Policing* (dalam buku *Handbook of Policing*), Willan Publishing.

Nouh, Mariam, Jason R.C. Nurse, Helena Webb, dan Michael Goldsmith, 2019. *Cybercrime Investigators are Users Too! Understanding the Socio-Technical Challenges Faced by Law Enforcement*, Cornell University, Published in the Proceeding of 2019 Workshop on Usable Security 24-27, San Diego, USA. https://arxiv.org/abs/1902.06961.

Police Executive Research Forum (PERF), 2014. *Future Trends in Policing.* Washington, D.C.: Office of Community Oriented Policing Services.

Rainer, Robert, 2016. *Policing, popular culture and political economy: towards a social democratic criminology*, Routledge Punlising, London and New York.

Rakhmanova E.N, Pinkevich T.V, 2020, *Digital Crime Concept*, Advances in Economics, Business and Management Research, volume 138, Atlantic Press SARL, Russian State University of Justice, Saint Petersburg -http://creativecommons.org/ licenses/by-nc/4.0/.

Stewart, John, 2023. *The Crisis of Modern Society: Richard Titmuss and Emile Durkheim*, History of the Human Sciences, Sage Journal, https://doi.org/ 10.1177 /09526951231169399.

Sumarjiyo, 2018. *Efektifitas Peralatan Intelijen Polri Dalam Rangka Deteksi Dini Guna Mencegah Tindak Pidana*, Jurnal Litbang Polri, Vol 21, No1.

The Prevention of Crime ECOSOC Resolution 2002/13, Annex, Action to Promote Effective Crime Prevention.

Vadza, Kejal Chintan, 2013. *Cyber Crime and its Categories*, Computer Science, Volume: 3 | Issue: 5 | May 2013 | ISSN - 2249-555X.

Weeber, Stan C, 2004. *Durkheim on Crime and Societal Development: The Durkheim School of Comparative Criminology Reconsidered*, Free Enquiry of Creative Sociology, Volume 32 No.1.