Journal of Advanced Research in Defense and Security Studies
Vol. 1, No. 1, April 2022, pp. 19-34
Available online at: https://ejournal.hakhara-institute.org/index.php/JARDS

PENGEMBANGAN *CYBER SECURITY* DALAM MENGHADAPI *CYBER WARFARE* DI INDONESIA

Bram Ronald Sanjaya[1*], Dian Efrianti[2], Mohammad Ali[3], Taufiq Prasetyo[4], M Mukhtadi[5], Yuniar Kurnia Widasari[6], Zahrotul Khumairoh[7]

[1] Universitas Pertahanan Republik Indonesia, Bogor, Indonesia
[2] Universitas Pertahanan Republik Indonesia, Bogor, Indonesia
[3] Universitas Pertahanan Republik Indonesia, Bogor, Indonesia
[4] Universitas Pertahanan Republik Indonesia, Bogor, Indonesia
[5] Universitas Pertahanan Republik Indonesia, Bogor, Indonesia
[6] Universitas Pertahanan Republik Indonesia, Bogor, Indonesia
[7] Universitas Pertahanan Republik Indonesia, Bogor, Indonesia

Keywords

Cyber Crime; Cyber Security; Cyber Warfare; Policy; Technology.

Abstract

The rapid development of technology in this millennial era has brought various positive and negative impacts. There are several abuses in the use of technology so that it can pose a threat of crime in the field of information technology known as cyber crime. Therefore, this study aims to. The research method used is a literature study with content analysis techniques. The findings of this study are that there are several abuses in the use of technology, giving rise to crimes in the field of information technology which, if carried out continuously, will become cyber warfare. The emergence of cyber warfare threats encourages the awareness of all parties in Indonesia to pay more attention to Indonesia's technology-based defense system. Synergy in dealing with the threat of cyber warfare is a necessity and a necessity for Indonesia. The strengthening of the legal basis for cyber crime is carried out thoroughly in various aspects, both legally and statutory, as well as non-legal through special approaches such as soft skills training efforts related to information technology for relevant agencies and public education. In addition, strengthening the legal basis of cyber crime also requires the development of cooperation between regions, between islands, and between countries through harmonization of substantive crimes, considering that cyber crime is a crime with a very broad and unlimited scope.

Kata Kunci

Cyber Crime; Cyber Security; Cyber Warfare; Kebijakan; Teknologi.

Abstrak

Perkembangan teknologi yang semakin pesat di era milenial ini telah membawa berbagai dampak baik positif maupun negatif. Terdapat beberapa penyalahgunaan dalam pemanfaatan teknologi sehingga dapat menimbulkan ancaman kejahatan di bidang teknologi informasi yang dikenal dengan kejahatan siber (*cyber crime*). Oleh karena itu, penelitian ini bertujuan untuk. Adapun

metode penelitian yang digunakan adalah studi literatur dengan teknik analisis isi. Adapun temuan dari penelitian ini adalah terdapat beberapa penyalahgunaan dalam pemanfaatan teknologi sehingga menimbulkan kejahatan di bidang teknologi informasi yang jika terus menerus dilakukan akan menjadi *cyber warfare.* Munculnya ancaman *cyber warfare* mendorong kesadaran semua pihak di Indonesia untuk memberikan perhatian lebih terhadap sistem pertahanan Indonesia yang berbasis teknologi. Sinergitas dalam menghadapi ancaman *cyber warfare* merupakan sebuah keniscayaan dan keharusan bagi Indonesia. Penguatan dasar hukum *cyber crime* dilakukan secara menyeluruh dalam berbagai aspek, baik secara hukum dan perundang-undangan, maupun non-hukum melalui pendekatan-pendekatan khusus semisal upaya pelatihan *softskill* terkait teknologi informasi bagi instansi terkait dan edukasi masyarakat. Selain itu, penguatan dasar hukum *cyber crime* juga memerlukan pengembangan kerjasama antar wilayah, antar pulau, hingga antar negara melalui harmonisasi pidana subtantif, mengingat *cyber crime* merupakan kejahatan dengan cakupan yang sangat luas dan tak terbatas.

e-ISSN: 2830-3571

*Corresponding Author:
Bram Ronald Sanjaya
Email: bram.sanjaya@idu.ac.id

PENDAHULUAN

Perkembangan zaman yang terjadi pada saat ini telah memberikan perubahan yang signifikan pada tatanan kehidupan manusia (Prasetyo & Trisyanti, 2018). Peradaban manusia perlahan tapi pasti telah mengalami pergeseran ke arah modernisasi yang mempengaruhi seluruh aspek kehidupan manusia. Perkembangan zaman saat ini salah satunya ditandai dengan adanya kemajuan teknologi dan informasi yang kemudian diaplikasikan oleh manusia untuk mempermudah pekerjaan mereka. Internet merupakan salah satu produk kemajuan teknologi dan informasi. Banyak kemudahan-kemudahan yang dirasakan akibat dari kemajuan teknologi dan informasi ini, salah satunya dapat diterapkan dalam bidang pertahanan negara sebagai salah satu komponen yang mendukung dalam upaya penyelenggaraannya. Kecepatan dalam mengakses informasi,

konektivitas antar subsistem, dan modernisasi sarana prasarana merupakan manfaat yang dapat dikembangkan dalam bidang pertahanan berbasis teknologi dan informasi (Aprilia, 2020).

Berkaitan dengan bidang pertahanan, pemanfaatan teknologi informasi dapat dilakukan dengan meningkatkan kapasitas komponen negara baik dalam hal fasilitas dan sumber daya manusianya dalam upaya mencapai tujuan nasional dan menangkal setiap ancaman, tantangan, hambatan, dan gangguan yang datang baik dari dalam maupun luar (Widodo, 2011). Paradigma tentang perang kini sudah bergeser, perang bukan lagi tentang pertempuran angkat senjata namun perang modern akan terjadi dengan cara perang dagang, perang informasi, *cyber war, proxy war*, dan peperangan asimetris lainnya (Legionosuko, 2019). Hal tersebut dapat menimbulkan adanya celah baru yang dapat mengancam keutuhan dan kedaulatan Negara Kesatuan Republik Indonesia. *Cyber war* merupakan salah satu celah yang sejak terbentuknya pola-pola komunikasi melalui internet dengan batas-batas konvensional yang dianut dan dipatuhi secara konsensus nasional kini menjadi semu, karena sekarang perang tidak lagi memperhitungkan kondisi geografis suatu negara, jarak tidak menjadi masalah dalam perang siber (Tampubolon, 2019).

Hal yang perlu diperhatikan adalah pengguna fasilitas teknologi informasi dan *cyber* ini tidak lagi hanya dimiliki oleh dunia sosial dan bisnis, tetapi mulai merambat pada semua bidang termasuk militer. Dalam dunia militer sebagai contohnya, teknologi informasi juga digunakan sebagai bagian dari sistem komando dan kendali (siskodal) (Allim, 2020). Fakta kondisi dari perkembangan informasi tersebut merupakan perang cangih *cyber war* yang terjadi saat ini di dunia, sedangkan kegiatan komunikasi melalui fasilitas jejaring sosial sebenarnya hanyalah visualisasi dari sebagian kecil kemampuan dalam *cyber warfare* (Ardiwidha & Rusfiana, 2018). *Cyber warfare* atau perang teknologi yang mengunakan jaringan komputer dan internet atau dunia maya *cyber space* dalam bentuk strategi pertahanan atau penyerangan sistem informasi. *Cyber warfare* dengan pengguna fasilitas www (*world, wide, web*) dan jaringan internet untuk melakukan perang di dunia maya. Saat ini *cyber warfare* dimasukkan ke dalam model perang informasi berskala rendah (*low level information warfare*), tetapi pada beberapa tahun mendatang *cyber warefare* akan berpotensi menjadi perang yang sebenarnya (Rahmah, 2018).

Tanpa kita sadari, *cyber warfare* saat ini telah menjadi medan baru bagi negara dalam menghadapi peperangan yang telah bertransformasi mengikuti perkembangan zaman pada saat ini (Djaya, 2021). Kepala Badan Telekomunikasi PBB, Toure Hamadoun, pada Oktober 2009 telah memperingatkan bahwa perang dunia bisa terjadi di dunia maya. Pelaku-pelaku dalam *cyber war* dapat berupa negara, NGO maupun perorangan yang sering disebut dengan *hacker.* Menurut Hastri (2021), perang siber mempunyai tujuan yang tidak jauh berbeda dengan perang konvensional yaitu untuk menaklukkan kemauan dan kemampuan para pengambil keputusan baik pemimpin politik maupun militer melalui operasi yang salah satunya disebut sebagai *Computer Network Operations* (CNO) yang meliputi:

1. *Computer Network Attack* merupakan satu operasi yang dirancang untuk mengganggu bahkan merusak data atau informasi yang disimpan dalam komputer atau jaringan komputer atau bahkan untuk merusak jaringannya.
2. *Computer Network Exploitation* merupakan satu operasi yang tujuannya mengambil data atau informasi yang sangat penting dan bernilai intelijen dari satu jaringan komputer mengunakan sarana teknologi informasi dan komunikasi (TIK).
3. *Computer Network Defense* merupakan satu operasi yang melindungi semua sarana TIK dan infrastrukturnya terhadap *Computer Network Attack* dan *Computer Network Exploitation* lawan.

Dalam perkembangannya, serangan *cyber* makin sering dirasakan. Beberapa kalangan mengingatkan bahwa serangan *cyber* juga mulai beralih dari mendapatkan keuntungan ekonomi ke kepentingan politik. Oleh karena itu, pengamanan akses dan data perlu ditingkatkan. Kementerian Komunikasi dan Informatika menyebutkan serangan yang berdampak pada 10 juta lebih identitas terus meningkat, dimana pada tahun 2014, serangan berdampak pada 11 juta identitas, 2015 naik menjadi 13 juta identitas, dan 2016 naik lagi menjadi 15 juta identitas (Pratiwi, 2022). Kementerian Komunikasi dan Informatika menyatakan bahwa Indonesia merupakan salah satu dari 10 besar negara-negara di dunia yang masuk dalam target perang *cyber*. Dari 10 negara sasaran, Indonesia berada di urutan kelima atau keenam. *Symantec*, sebuah perusahaan perangkat lunak dalam *Internet Security Threat Report* tahun ini melaporkan serangan terhadap jaringan internet secara global.

Memperhatikan data tersebut, pengembangan teknologi informasi beserta dengan sinergisitas antar instansi menjadi sangat penting dalam menghadapi *cyber warfare.* Terutama di Indonesia sendiri dianggap sebagai ancaman nyata yang dapat merusak kedaulatan Negara Kesatuan Republik Indonesia. Belum hilang dari ingatan kita mengenai penyadapan yang dilakukan oleh Australia kepada pejabat-pejabat Negara Indonesia beberapa tahun yang lalu dan pada akhirnya hal tersebut merupakan *warning* tersendiri bagi Indonesia agar memikirkan apa yang harus dilakukan kedepannya. Berdasarkan uraian di atas, maka tujuan dari penelitian ini adalah untuk mendeskripsikan pengembangan *cyber security* dalam menghadapi *cyber warfare* di Indonesia.

METODE PENELITIAN

Tulisan ini menggunakan studi literatur sebagai pendekatan dalam penelitiannya. Studi literatur merupakan suatu rangkuman artikel dari jurnal, buku, maupun dokumen lain yang ditulis untuk mengkonsepkan dan mendeskripsikan suatu teori tertentu dengan cara mengorganisasikan literatur tersebut sesuai dengan topik yang diperlukan (Alawiyah et al., 2020; Basri et al., 2019; Bastian et al., 2021; Muara et al., 2021; Rahmanisa et al., 2021; Rahmat & Budiarto, 2021). Dalam penelitian, peneliti mengelaborasi berbagai konsep tentang *cyber security* sebagai bentuk pertahanan dari ancaman *cyber warfare*. Selain itu, pada tulisan ini juga menjelaskan mengenai perkembangan teknologi di bidang *cyber* (*trend cyber*) dan dasar hukum yang mengatur *cyber*. Sumber data yang digunakan dalam penelitian ini yakni literatur tentang perang dagang, perkembangan industri semen di Indonesia, dan ancaman pertahanan negara. Sedangkan, untuk analisis datanya menggunakan teknik analisis isi (Nurmalasari et al., 2022; Rahmat et al., 2022a; Rahmat et al., 2022b; Yuliarta & Rahmat, 2021; Yurika et al., 2022).

HASIL DAN PEMBAHASAN

Di era digital sekarang ini, teknologi memainkan peran yang sangat penting. Perangkat teknologi komputer dan internet telah menjadi alat kehidupan sehari-hari sehingga menjadikan setiap negara harus mampu menguasai, mengendalikan, dan

mengawasi pergerakan manusia di dalam dunia maya (Subagyo, 2018). Teknologi komputer dan internet telah menciptakan dunia baru yang bernama dunia maya atau *cyber space* yang didalamnya terdapat warga negara dunia maya dengan sebutan "*netizen*" dan melakukan berbagai komunikasi, interaksi, dan gerakan melalui media sosial sehingga sangat penting untuk diperhatikan setiap negara. Dunia maya telah melahirkan berbagai hal yang serba elektronik, seperti *e-commerce, e-procurement, e-bisnis, e-trade, e-service, e-life style,* dan lain-lain. Bahkan, saat ini banyak sekali berbagai aplikasi yang berbasis elektronik di berbagai komunitas bisnis, perbankan, pemerintahan, kementerian, kampus, dan lain-lain.

Hal ini menunjukkan bahwa dunia maya telah menjadi ranah baru dalam kehidupan politik global. Perkembangan dunia maya telah melahirkan kejahatan dunia maya (*cyber crime). Cyber crime* adalah salah satu jenis kejahatan transnasional karena melibatkan pelaku yang berasal dari dua negara atau lebih, korbannya bisa lebih dari satu negara, modus operasinya di dunia maya dengan menggunakan perangkat komputer dan internet, dan alat buktinya berupa alat bukti elektronik sehingga memerlukan proses penegakan hukum yang modern dan canggih (Sinaga, 2022).

Kualifikasi *cyber crime* oleh Barda Nawawi Arief berdasarkan *Convention on Cyber Crime* 2001 di Budapest, Hungaria membatasinya dalam sembilan kegiatan utama, yaitu (a) *illegal access* (mengakses sistem komputer secara ilegal), (b*) illegal interception* (penggunaan alat bantu teknis dalam penyadapan sistem pengiriman dan pemancaran data komputer), (c) *data interference* (melakukan perusakan, penghapusan secara sengaja dan ilegal), (d) *system interference* (melakukan gangguan serius atas fungsi sistem komputer secara sengaja dan ilegal), (e) *missues of devices* (penyalahgunaan perlengkapan komputer), (f) *computer related forgerry* (pemalsuan data autentik melalui perubahan, pemalsuan hingga penghapusan), dan (g) *computer related fraud* (penipuan dengan tujuan pemerasan dan pemerolehan keuntungan secara ilegal) (Alfian, 2017). Oleh karena itu, *cyber crime* disebut sebagai salah satu ancaman terbesar bagi Indonesia di era globalisasi ini sebagai dampak negatif dari perkembangan ilmu pengetahuan dan teknologi.

Urgensi pertahanan siber ditujukan untuk mengantisipasi datangnya ancaman-ancaman dan serangan siber yang terjadi dan menjelaskan posisi ketahanan saat ini sehingga diperlukan kesiapan dan ketanggapan dalam menghadapi ancaman serta

memiliki kemampuan untuk memulihkan akibat dampak serangan yang terjadi di ranah siber (Herlia, 2019). Sumber ancaman adalah entitas yang berkeinginan atau memiliki niat dan benar-benar secara nyata akan melakukan kegiatan yang melanggar norma, hukum, aturan, ketentuan, kaidah, dan kontrol keamanan informasi serta aset fisik lainnya dengan tujuan untuk mendapatkan keuntungan yang bersifat materiel dan immateriel.

Ancaman dan serangan tersebut dapat dilakukan oleh pelaku yang mewakili pemerintah (*state actor*) atau non pemerintah (*non state actor*) sehingga pelaku bisa bersifat perorangan, kelompok, golongan, organisasi atau bahkan sebuah negara. Secara umum, unsur-unsur yang dapat diidentifikasi memiliki potensi sebagai sumber ancaman terdiri atas sumber internal dan eksternal, kegiatan intelijen, kekecewaan, investigasi, organisasi ekstrimis, *hacktivists,* grup kejahatan terorganisir, persaingan, permusuhan dan konflik serta teknologi (Putra et al., 2018). Sistem informasi pertahanan negara memiliki perangkat utama yang terdiri atas delapan komponen dasar, yaitu Sumber Daya Manusia (SDM) sebagai pengguna dan pengelola, organisasi, perangkat lunak (*software)*, perangkat keras (*hardware)*, data dan informasi, tata kelola Teknologi Informasi dan Komunikasi (TIK), jaringan serta keamanan (Swastanto, 2018).

Banyak kasus di sektor perusahaan yang kehilangan data rahasia perusahaan oleh para *hacker* dan *cracker*. Selain itu, komunitas perbankan juga merasa terancam karena pengamanan jaringannya seringkali jebol oleh ulah para *hacker* dan *cracker* yang melakukan aksi kriminal di dunia maya. Bahkan, seringkali para *hacker* menyebarkan virus untuk merusak jaringan yang dimiliki oleh situs-situs pemerintahan sehingga sangat membahayakan kedaulatan negara di dunia maya. Hal ini mengindikasikan bahwa setiap negara di dunia harus mampu mengembangkan kekuatan pertahanan *cyber* agar dapat menahan serangan dunia maya dari berbagai pihak yang akan melakukan peretasan, penyadapan, dan perusakan terhadap berbagai sistem, *software,* maupun perangkat lunak lainnya. Semua negara harus menyadari bahwa ancaman keamanan global sekarang ini tidak hanya bersifat fisik semata, melainkan ancaman yang bersifat virtual, digital, dan dunia maya berupa aksi kejahatan yang menyerang situs, *website* maupun berbagai instalasi dunia maya lainnya. Inilah yang kemudian melahirkan ancaman baru dalam dunia internasional, berupa ancaman perang *cyber* (*cyber warfare*).

Munculnya ancaman perang siber harus mendorong kesadaran semua pihak di Indonesia untuk memberikan perhatian lebih terhadap sistem pertahanan Indonesia. Seperti diketahui bahwa sistem pertahanan Indonesia adalah sistem pertahanan semesta (sishanta) dengan komponen utama adalah TNI dan komponen pendukungnya adalah rakyat. Dalam konteks ini, sistem pertahanan semesta yang tertuang dalam Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara, harus mampu dimaknai sebagai semesta yang bersifat tidak hanya fisik semata, melainkan non fisik, khususnya digital dan dunia maya.

Faktanya kini, penangganan kejahatan *cyber* yang masih berjalan masing-masing dan tersebar serta tidak adanya koordinasi yang baku dalam penanganan masalah *cyber security*. Badan Pertahanan *Cyber* Nasional atau badan yang berkaitan harus segera dibentuk agar terwujud mekanisme koordinasi, komunikasi, dan sinergi antar berbagai aktor keamanan dan pertahanan dalam melindungi kedaulatan dunia maya Indonesia dari berbagai ancaman serangan *cyber*. Kementerian Pertahanan, TNI, POLRI, BIN, Kominfo, Lembaga Sandi Negara, dan berbagai instansi terkait lainnya harus mampu bersinergi untuk menangkis, menangkal, dan mencegah serangan *cyber* dari pihak tertentu atau dari negara lain yang mencoba untuk menganggu kedaulatan dunia maya Indonesia saat ini dan di masa depan (Sumarwani, 2014).

Terkait dengan pengembangan strategi nasional dalam membangun *cyber-security* di Indonesia ke depan dilakukan dengan memenuhi empat pondasi yang mendukung perkembangan teknologi informasi termasuk didalamnya pengembangan *cyber-security*, yaitu pengembangan perangkat lunak (*software)* seperti sistem dan aplikasi, pengembangan alat keras (*hardware)*, pengembangan sarana dan prasarana teknologi informasi, manajemen isi (*content management*), *telecommunication and networking*, pengembangan keamanan transaksi *online* (Ardiyanti, 2014).

Saat ini, perkembangan teknologi informasi di seluruh dunia berlangsung dengan sangat cepat, termasuk perkembangan teknologi dalam bidang *cyber*. Perkembangan *cyber* semakin meningkat dari tahun ke tahun, baik dalam jumlah maupun variasi serangan yang semakin maju seiring perkembangan teknologi. Sebagai contoh, yang pada awalnya internet hanya bisa untuk mengirimkan pesan singkat dan email saja sehingga kejahatan *cyber* yang muncul pada saat itu hanya sebatas kejahatan via pesan singkat atau *e-mail*.

Berbeda dengan saat ini, internet digunakan di seluruh bidang pekerjaan dan kehidupan masyarakat dengan kemudahan aksesnya sehingga muncul kejahatan *cyber* yang semakin bervariasi.

Tren kejahatan *cyber* menurut *Territory Channel Manager Kaspersky Indonesia*, Doni Koesmandarin, menyebutkan bahwa mereka tidak segan mencantumkan nama dan email, bahkan ada yang mencantumkan nomor telepon yang bisa dihubungi. Para pelaku *cyber crime* sudah berani melakukan kejahatannya secara terang-terangan. Tren serangan *malware* masih menduduki peringkat teratas karena memiliki kelebihan dari *malware* yang akan hilang setelah pengguna melakukan *reboot* pada komputer. Sebutan untuk *malware* ini dikenal dengan *Project Sauron* yang memiliki kemampuan untuk menghapus data dari memori dengan kemampuan menyembunyikan diri, *malware* ini dapat mengetahui kebiasaan sang korban dalam lima tahun terakhir. Tren yang kedua adalah serangan lewat *open source program* dengan celah kelengahan para pengguna yang merasa percaya dengan aplikasi *open source*, bahkan di aplikasi berbasis *android* (Danuri, 2017).

Kejahatan *cyber crime* tidak hanya dalam lingkup nasional, tetapi bersifat global yang dapat menembus ruang dan waktu, tidak ada batas negara, tidak mengenal yuridiksi, dan dapat dilakukan kapanpun dan dimanapun. Pada bidang perbankan, penggunaan transaksi *e-banking* yang meningkat menimbulkan kejahatan *cyber crime* pun meningkat, hal ini dipengaruhi oleh meningkatnya penggunaan *mobile wallet*. Pada bidang pemerintahan, serangan *cyber crime* ini menargetkan web dan situs-situs pemerintahan yang memang kadang membuka akses penuh kepada semua *user* agar masyarakat dapat mengakses dengan maksimal, tetapi dimanfaatkan oleh para pelaku *cyber* untuk menyerang. Pada bidang pendidikan, serangan *cyber* tidak terjadi secara langsung, namun banyak situs-situs yang berbau pornografi yang bebas di akses oleh anak-anak dan remaja masa kini jika tanpa adanya proteksi dan pengawasan dari orang tua. Pada bidang bisnis, serangan *cyber* muncul pada perkembangan pesat *e-commerce*, salah satunya toko online dengan penipuan terhadap konsumen dan pemalsuan data-data milik seseorang untuk mengelabui *user*.

Rendahnya *awarenees* atau kesadaran terhadap adanya ancaman *cyber attack* yang berdampak melumpuhkan infrastruktur vital, contohnya adalah sistem radar penerbangan di Bandara Internasional Soekarno Hatta yang beberapa kali mengalami

gangguan. Tidak menutup kemungkinan *cyber attack* menyerang infrastruktur vital negara seperti itu. Terkait dengan kebijakan *cyber-security* di Indonesia perlu diatur sebuah kebijakan yang mengatur tentang berbagai elemen yang terkait dengan *cyber-security* dalam berbagai kebijakan.

Pemerintah Indonesia melalui beberapa kebijakan hukum dan perundang-undangan yang berkaitan dengan masalah komputer dalam *cyber crime*, diantaranya adalah sebagai berikut:

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.
2. Undang-Undang Nomor 15 Tahun 2002 tentang Pencucian Uang. Pencucian uang dilakukan untuk mengubah dana ilegal menjadi dana legal, semisal dana hasil korupsi, penjualan narkotika, pencurian mobil, dan perampokan. Proses pelaksanaan penyidikan pencucian uang dilakukan dengan mudah oleh aparatur negara atau polisi, namun faktanya tidak dapat mengurangi tingkat kejahatan korupsi di Indonesia.
3. Undang-Undang Nomor 19 Tahun 2002 tentang Hak Cipta. Pembajakan *software* adalah salah satu kasus yang paling banyak terjadi di Indonesia dengan alasan mahalnya harga *software* asli. Meski tindak pembajakan sudah dikategorikan sebagai tindak pidana pada pasal 72 ayat (3) dengan pidana penjara paling lama 5 tahun dan atau denda paling banyak sebanyak lima ratus juta rupiah, nyatanya pembajakan dianggap sebagai hal biasa di Indonesia.
4. Undang-Undang Nomor 28 Tahun 2014 tentang Telekomunikasi.
5. Undang-Undang Nomor 32 Tahun 2002 tentang Penyiaran.

Pemerintah dibantu aparatur negara terus mengupayakan optimalisasi pelaksanaan kebijakan tersebut, namun implementasinya menghadapi beberapa kendala, diantaranya keterbatasan perangkat dan penegak hukum dalam proses pengusutan pelaku dan alat-alat bukti dari kasus *cyber crime*, perangkat komputer forensik belum dimiliki oleh aparatur negara, dan kurang optimalnya pemberdayaan AWAR (Asosiasi Warnet Indonesia).

Implementasi penguatan dasar hukum *cyber crime* dapat dilakukan melalui beberapa metode, yaitu (a) kalibrasi ulang konsepsi Undang-Undang Hukum Pidana (KUHP) untuk disesuaikan dengan ranah perkembangan ilmu pengetahuan dan teknologi

sehingga secara dinamis mampu mencakup segala kasus kejahatan *cyber crime*, (b) penegakan hukum *cyber crime* tidak terbatas pada pendekatan yuridis atau penal (hukum utama yang berlaku di Indonesia), namun melalui pendekatan non-penal, sosialisasi pencegahan *cyber crime* kepada masyarakat secara lebih luas atau pengajaran penggunaan komputer melalui kurikulum informatika, (c) peningkatan kualitas *hardware* dan *software* untuk keperluan militer sebagai bagian dari evaluasi perangkat keamanan untuk menghadapi ancaman, tantangan, hambatan, dan gangguan ranah *cyber*, (d) pembentukan divisi khusus dalam institusi POLRI atau militer yang terdiri atas prajurit-prajurit dengan *good-skill* dalam menangani kejahatan dunia maya, dan (e) kerja sama dengan penyedia jasa internet atau ISP (*Internet Service Provider*) melalui program pemberdayaan AWARI (Asosiasi Warnet Indonesia) sebagai bagian dari realisasi tindakan komponen cadangan serta komponen pendukung dalam menghadapi *cyber crime*.

Selain itu, pengembangan ranah tinjauan yuridis pemidanaan *cyber crime* melalui prespektif hukum pidana positif dalam kategori-kategori khusus. Hal ini dilakukan sebagai bagian dalam penerapan pasal-pasal KUHP yang terkait dengan perkara yang menjadikan komputer sebagai objek sekaligus subjek sarana kejahatan dengan tujuan untuk mempermudah pengambilan keputusan dan pelaksanaan kebijakan atas *cyber crime cases*. Menurut Sumarwarni (2014), kategori-kategori tersebut terbagi atas empat macam yang terdiri atas:

1. Kategori perusakan barang sebagai alat bukti yang sah dalam hukum Indonesia;
2. Kategori pencurian, contohnya *unauthorized transfer payment case* pada tahun 1986, setoran wakaf fiktif PT Bank Bali tahun 1989 ataupun kasus manipulasi data saldo *master file* Bank Danamon pada tahun 1990;
3. Kategori persaingan curang; dan
4. Kategori pemalsuan.

Penguatan dasar hukum *cyber crime* dilakukan secara menyeluruh dalam berbagai aspek, baik secara hukum (penal) yang diatur dalam pasal-pasal KUHP dan perundang-undangan, maupun non-hukum (non-penal) melalui pendekatan-pendekatan khusus, contohnya upaya pelatihan *softskill* bagi masyarakat. Selain itu, penguatan dasar hukum *cyber crime* juga memerlukan pengembangan kerjasama antar wilayah, antar pulau,

hingga antar negara melalui harmonisasi pidana subtantif, mengingat *cyber crime* merupakan kejahatan dengan cakupan yang sangat luas dan tak terbatas. Penguatan peran intelijen untuk kepentingan mencegah terjadinya *cyber warfare* dan mengembangkan kemampuan artifisial intelijen.

Selanjutnya perlu dijalankan program *capacity building* dalam bentuk pelatihan dan peningkatan keahlian bidang *cyber security* yang dilakukan secara terpusat. Langkah tersebut dilakukan sebagai upaya meningkatkan kapasitas SDM untuk memahami dan mampu menetukan langkah-langkah preventif dalam menangkal segala tindakan *cyber crime. Capacity building* yang selanjutnya teknologi yang canggih dalam mendeteksi dan menangani serangan siber ini.

SIMPULAN

Perkembangan teknologi yang semakin pesat di era milenial ini telah membawa berbagai dampak baik positif maupun negatif. Terdapat beberapa penyalahgunaan dalam pemanfaatan teknologi tersebut sehingga menimbulkan kejahatan di bidang teknologi informasi (*cyber crime*). Terdapat beberapa tren perkembangan *cyber* di Indonesia, baik pada bidang perbankan, pemerintahan, pendidikan, dan bisnis. *Cyber security* ke depan hendaknya dibangun atas lima bidang dasar yaitu kepastian hukum (undang-undang *cyber crime*), teknis dan tindakan prosedural (pendekatan langsung dan penyedia layanan dan perusahaan perangkat lunak), struktur organisasi (struktur organisasi sangat berkembang, menghindari tumpang tindih), *capacity building* dan pendidikan pengguna (kampanye publik dan komunikasi terbuka dari ancaman *cyber crime* terbaru), dan kerjasama internasional (termasuk didalamnya kerjasama timbal balik dalam upaya mengatasi ancaman *cyber*).

Sinergitas dalam menghadapi ancaman *cyber warfare* merupakan sebuah kepastiaan dan keharusan bagi Indonesia. Kementerian Pertahanan harus mampu menjadi ujung tombak dalam mempelopori sinergitas antar berbagai komponen bangsa untuk melawan ancaman *cyber warfare*. Mekanisme pembangunan jalinan komunikasi, koordinasi, jaringan, dan kerja sama teknis harus dicanangkan oleh Kementerian Pertahanan untuk membentuk komunitas pertahanan *cyber (cyber defence community)* yang dapat menangkal,

mendeteksi, menangkis, dan mencegah secara dini berbagai potensi serangan ancaman *cyber warfare*.

DAFTAR PUSTAKA

Ardiyanti, H. (2014). Cyber-security dan Tantangan Pengembangannya di Indonesia. *Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional, 5*(1).

Danuri, M. (2017). Trend Cyber Crime dan Teknologi Informasi di Indonesia. *Jurnal INFOKAM, XIII*(2).

Alfian, M. (2017). Penguatan Hukum Cyber Crime di Indonesia dalam Perspektif Peraturan Perundang-Undangan. *Jurnal Kosmik Hukum, 17*(2).

Sumarwani, S. (2014). Tinjauan Yuridis Pemindanaan Cybercrime dalam Perspektif Hukum Pidana Positif. *Jurnal Pembaharuan Hukum, 1*(1).

Swastanto, Y. (2018). *Monograf Pengembangan Kompetensi SDM Pusat Data Informasi (PUSDATIN) Kementerian Pertahanan dalam Rangka Menghadapi Cyber War*. Universitas Pertahanan.

Prasetyo, B., & Trisyanti, U. (2018). Revolusi industri 4.0 dan tantangan perubahan sosial. *IPTEK Journal of Proceedings Series*, (5), 22-27.

Aprillia, A. A. (2020). Implementasi E-Tilang Dalam Meningkatkan Pelayanan Publik Oleh Satuan Lalu-Lintas Polres Banyumas. *Advances in Police Science Research Journal*, *4*(1), 209-280.

Widodo, S. (2011). Implementasi bela negara untuk mewujudkan nasionalisme. *CIVIS*, *1*(1).

Legionosuko, T., Madjid, M. A., Asmoro, N., & Samudro, E. G. (2019). Posisi dan strategi indonesia dalam menghadapi perubahan iklim guna mendukung ketahanan nasional. *Jurnal Ketahanan Nasional*, *25*(3), 295-312.

Tampubolon, K. E. A. (2019). Perbedaan Cyber Attack, Cybercrime, dan Cyber Warfare. *Jurist-Diction*, *2*(2), 539-554.

Allim, T. Y., Supartono, S., & Gultom, R. A. (2020). DESAIN KONSEPTUAL SISTEM PENGAWASAN KAPAL SELAM ASING BERBASIS TEKNOLOGI AKUSTIK TOMOGRAFI UNTUK MENDUKUNG SISTEM PERTAHANAN NEGARA. *Teknologi Penginderaan*, *1*(2).

Ardiwidha, D., & Rusfiana, Y. (2018). PENGARUH KEBEBASAN BEREKSPRESI DAN PENGGUNAAN MEDIA SOSIAL TERHADAP KEAMANAN INFORMASI DI KODAM XIII/MERDEKA. *Strategi Pertahanan Darat*, *4*(2).

Djaya, S. (2021). Dakwah Moderat dan Jihad Modern: Belajar Menganalisa Informasi dan Materi Dakwah dari Sokrates. *Dakwah: Jurnal Kajian Dakwah dan Kemasyarakatan*, *25*(2), 116-133.

Rahmah, Y. N. (2018). Pengaruh Penggunaan Internet Banking Dan Perlindungan Nasabah Pengguna Fasilitas Internet Banking Terhadap Cyber Crime Di Daerah Istimewa Yogyakarta. *Jurnal Pendidikan dan Ekonomi*, *7*(6), 579-588.

Hastri, E. D. (2021). Cyber Espionage Sebagai Ancaman Terhadap Pertahanan dan Keamanan Negara Indonesia. *Law & Justice Review Journal*, *1*(1), 12-25.

Pratiwi, S. J. (2022). PENCEGAHAN TINDAK PIDANA KEKERASAN MELALUI MEDIA SOSIAL (CYBERBULLYING) BERDASARKAN PERSPEKTIF HUKUM POSITIF. *LEX CRIMEN*, *11*(3).

Subagyo, A. (2018). Sinergi Dalam Menghadapi Ancaman Cyber Warfare. *Jurnal Pertahanan & Bela Negara*, *5*(1), 89-108.

Sinaga, M. I. J. (2022). Penetapan Tersangka dalam Penyidikan Tindak Pidana Transnational Cybercrime Menurut Sistem Hukum di Indonesia. *Syntax Literate; Jurnal Ilmiah Indonesia*, *7*(3), 1229-1253.

Herlia, T. (2019). Model Sistem Peran Teknologi dan Informasi Terhadap Pertahanan Bisnis di Indonesia. *Majalah Ilmiah Bijak*, *16*(1), 38-47.

Putra, R. D., Supartono, S., & Deni, D. A. R. (2018). Ancaman Siber Dalam Persfektif Pertahanan Negara (Studi Kasus Sistem Pertahanan Semesta). *Peperangan Asimetris*, *4*(2).

Alawiyah, D., Rahmat, H. K., & Pernanda, S. (2020). Menemukenali konsep etika dan sikap konselor profesional dalam bimbingan dan konseling. *JURNAL MIMBAR: Media Intelektual Muslim dan Bimbingan Rohani*, *6*(2), 84-101.

Basri, A. S. H., Musyirifin, Z., Anwar, M. K., & Rahmat, H. K. (2019). Pengembangan Model Keilmuan Bimbingan dan Konseling Islam Melalui Jurnal Hisbah: Jurnal Bimbingan Konseling dan Dakwah Islam. *Al-Isyraq: Jurnal Bimbingan, Penyuluhan, dan Konseling Islam*, *2*(2), 136-158.

Bastian, O. A., Rahmat, H. K., Basri, A. S. H., Rajab, D. D. A., & Nurjannah, N. (2021). Urgensi Literasi Digital dalam Menangkal Radikalisme pada Generasi Millenial di Era Revolusi Industri 4.0. *Jurnal Dinamika Sosial Budaya, 23*(1), 126-133.

Muara, T., Prasetyo, T. B., & Rahmat, H. K. (2021). Psikologi Masyarakat Indonesia di Tengah Pandemi: Sebuah Studi Analisis Kondisi Psikologis Menghadapi COVID-19 Perspektif Comfort Zone Theory. *Ristekdik: Jurnal Bimbingan dan Konseling*, *6*(1), 69-77.

Nurmalasari, E., Rahmat, H. K., & Farozin, M. (2022). Motivasi Santri Tuli dalam Mengikuti Kegiatan Madrasah Diniyyah Daring di Madrasah Salafiyah III Pondok Pensantren Al-Munawwir Krapyak Yogyakarta. *The Indonesian Conference on Disability Studies and Inclusive Education, 2*, 103-117.

Rahmanisa, R., Rahmat, H. K., Cahaya, I., Annisa, O., & Pratiwi, S. (2021). Strategi Mengembangkan Resiliensi Individu di Tengah Masa Pandemi COVID-19 Menggunakan Islamic Art Therapy [Strategy to Develop Individual Resilience in The Middle of The COVID-19 Pandemic using Islamic Art Therapy]. *Journal of Contemporary Islamic Counselling*, *1*(1).

Rahmat, H. K., & Budiarto, A. (2021). Mereduksi Dampak Psikologis Korban Bencana Alam Menggunakan Metode Biblioterapi Sebagai Sebuah Penanganan Trauma Healing [Reducing The Psychological Impact of Natural Disaster Victims Using Bibliotherapy Method as a Trauma Healing Handler]. *Journal of Contemporary Islamic Counselling*, *1*(1).

Rahmat, H. K., Nurmalasari, E., Annisa, O., Hidayat, T., Fitriyani, N., & Pernanda, S. (2022a). The Influenced Factors of Gratitude: A Systematic Review. *International Conference on Islamic Guidance and Counseling, 2*, 9-16.

Rahmat, H. K., Salsabila, N. R., Nurliawati, E., Yurika, R. E., Mandalia, S., Pernanda, S., & Arif, F. (2022b). Bibliokonseling Berbasis Nilai-Nilai Sumbang Duo Baleh dalam Membangun Karakter Positif bagi Remaja di Minangkabau. *NCESCO: National Conference on Educational Science and Counseling, 2*(1).

Yuliarta, I. W., & Rahmat, H. K. (2021). Peningkatan Kesejahteraan Melalui Pemberdayaan Masyarakat Pesisir Berbasis Teknologi Sebagai Upaya Memperkuat Keamanan Maritim di Indonesia. *Jurnal Dinamika Sosial Budaya, 23*(1), 180-189.

Yurika, R. E., Rahmat, H. K., & Widyastuti, C. (2022). Integrasi Layanan Bimbingan dan Konseling dengan Kurikulum Berbasis Budaya Yogyakarta untuk Membangun Cultural Awareness. *NCESCO: National Conference on Educational Science and Counseling, 2*(1).