ISSN: 2614-6754 (print)
ISSN: 2614-3097(online)

Halaman 23934-23943
Volume 8 Nomor 2 Tahun 2024

Tantangan Pertahanan dan Keamanan *Data Cyber* dalam Era Digital: Studi Kasus dan Implementasi

Balqis Tsabitah Azzahrah[1], Muhammad Naufal Razzan Hamdi[2], Rasheesa Ryash Raynee[3], Zulfa Layla Ni'matussa'idah[4], Subakdi[5]

[1,2,3,4,5] Program Studi Hukum, Fakultas Hukum, Universitas Pembangunan Nasional "Veteran" Jakarta

e-mail: 2310611147@mahasiswa.upnvj.ac.id[1], 2310611129@mahasiswa.upnvj.ac.id[2], 2310611122@mahasiswa.upnvj.ac.id[3], 2310611146@mahasiswa.upnvj.ac.id[4], subakdi@upnvj.ac.id[5]

Abstrak

Kriminalitas di ranah maya semakin canggih dalam mengeksploitasi celah keamanan dalam sistem digital. Cara untuk memperkuat pertahanan siber adalah dengan analisis komprehensif terhadap ancaman yang ada di ekosistem digital dan solusi yang tepat untuk dapat diterapkan. Ancaman cybercrime di Indonesia meliputi serangan peretasan, pemecahan keamanan, sabotase siber, dan perangkat lunak mata-mata. Manajemen risiko melibatkan proses identifikasi, penilaian, penanganan, dan pengendalian risiko. Antisipasi ancaman yang dapat dilakukan adalah dengan adanya keberadaan tenaga ahli teknologi untuk mendukung pengembangan sistem pertahanan negara yang canggih serta pendirian pusat komando keamanan siber. Dalam konteks era digital yang terus berkembang, keamanan siber menjadi perhatian utama dalam menjaga keutuhan data dan infrastruktur komputer. Artikel ini membahas tantangan dalam mengamankan data di ranah siber, dengan menitikberatkan pada pemahaman, metode penelitian, temuan hasil penelitian, dan diskusi terkait situasi keamanan siber di Indonesia. Pendahuluan menguraikan pentingnya keamanan siber menghadapi ancaman digital yang semakin kompleks. Tinjauan pustaka mengeksplorasi teori-teori terkait keamanan siber dan sumber-sumber referensi yang digunakan. Metode penelitian yang digunakan adalah pendekatan kualitatif dengan fokus studi kasus untuk mendapatkan pemahaman yang dalam tentang tantangan keamanan siber. Temuan hasil penelitian menunjukkan bahwa mahasiswa telah mempunyai pemahaman yang memadai tentang keamanan siber, namun masih ada kekurangan dalam tingkat keamanan siber di Indonesia. Beberapa langkah pencegahan terhadap kejahatan siber telah diidentifikasi, termasuk praktik penggunaan kata sandi yang kuat, kehati-hatian dalam mengonsumsi informasi, dan upaya edukasi terkait keamanan siber. Diskusi menekankan kompleksitas tantangan yang dihadapi dalam mengatasi kejahatan siber, serta pentingnya langkah-langkah yang lebih efektif dari instansi terkait dan kesadaran masyarakat untuk meningkatkan keamanan data. Dengan demikian, artikel ini memberikan gambaran menyeluruh tentang tantangan keamanan siber di era digital, dengan harapan

mampu memberikan kontribusi positif dalam meningkatkan kesadaran dan perlindungan terhadap keamanan data di Indonesia.

Kata Kunci: *Keamanan Siber, Era Digital, Peran Mahasiswa.*

Abstract

Cybercrime in the digital realm is becoming increasingly sophisticated in exploiting security vulnerabilities within digital systems. The way to strengthen cyber defense with a comprehensive analysis of the threats that exist in the digital ecosystem and the appropriate solutions that can be implemented. Cybercrime threats in Indonesia include hacking attacks, security breaches, cyber sabotage, and spy software. Risk management involves the process of identifying, assessing, handling, and controlling risks. Anticipation of threats can be done by having technological experts support the development of a sophisticated national defense system and the establishment of a cyber security command center. In the evolving landscape of the digital era, cybersecurity is paramount in safeguarding data integrity and computer infrastructure. This article discusses the challenges of securing data in the cyber realm, focusing on understanding, research methods, research findings, and discussions regarding the cybersecurity landscape in Indonesia. The introduction highlights the importance of cybersecurity in facing increasingly complex digital threats. The literature review explores theories related to cybersecurity and the referenced sources. The research methodology employed is a qualitative approach with a case study focus to gain a profound understanding of cybersecurity challenges. Research findings indicate that students have adequate understanding of cybersecurity, yet there are still shortcomings in Indonesia's cybersecurity level. Several prevention measures against cybercrime have been identified, including the practice of using strong passwords, cautious consumption of information, and cybersecurity education efforts. The discussion emphasizes the complexity of the challenges faced in combating cybercrime, as well as the importance of more effective measures from relevant authorities and public awareness to enhance data security. Thus, this article provides a comprehensive overview of cybersecurity challenges in the digital era, with the hope of making a positive contribution to increasing awareness and protection of data security in Indonesia.

Keywords: *Cybersecurity, Digital Era, Role of Students.*

PENDAHULUAN

Keamanan siber (*cybersecurity*) merupakan serangkaian aktivitas dan pengukuran melalui elemen-elemen *cyberspace* (*hardware*, *software*, *computer network*) sebagai defensif dari serangan, disrupsi, atau ancaman lainnya. Sebagai bidang praktek, keamanan siber ini bertujuan untuk melindungi komputer, jaringan, aplikasi perangkat lunak, sistem kritis, dan data-data dari potensi ancaman digital.

Pada era digital saat ini yang berkembang dengan pesat, keamanan siber berperan penting yang sangat berpengaruh karena sebagian besar seluruh aspek kehidupan,

termasuk bisnis, pemerintahan, dan kehidupan pribadi, bergantung pada teknologi informasi. Pendekatan terhadap era keamanan siber untuk mencapai tujuan yang ditetapkan dengan melibatkan berbagai strategi serta kebijakannya.

Perkembangan era digital yang semakin pesat menyebabkan peningkatan volume dan kompleksitas data yang dihasilkan dan dipertukarkan di dunia maya. Dalam konteks ini, keamanan data siber menjadi isu krusial yang tidak bisa diabaikan. Serangan siber, seperti peretasan, pencurian data, dan *ransomware*, menjadi ancaman nyata yang dapat merugikan berbagai pihak.

Dengan berkembangnya teknologi di era digital ini, maka diperlukan keamanan siber yang efektif untuk menjaga data pribadi, data perusahaan, maupun data negara. Tantangan utama yang akan dihadapi dalam era digital ini adalah menerapkan pertahanan dan keamanan data siber.

Kejahatan siber telah marak terjadi di Indonesia yang menjadi ancaman bagi pertahanan dan keamanan negara. Akibat dari permasalahan ini adalah bocornya data pribadi, data perusahaan, maupun data negara yang ditampilkan secara umum oleh pihak-pihak yang tidak bertanggung jawab. Berdasarkan permasalahan tersebut, kelompok akan melakukan kegiatan penelitian mengenai pertahanan dan keamanan siber di era digital dengan para mahasiswa.

Melalui penelitian yang dilakukan oleh kelompok, diharapkan dapat mendapatkan pengetahuan dan pemahaman yang lebih dalam mengenai tantangan menghadapi keamanan siber di Indonesia. Dengan penelitian ini juga diharapkan kelompok beserta para responden yang berisi mahasiswa dapat mendapatkan pemahaman mengenai upaya dalam mengatasi tantangan keamanan siber tersebut dan dapat menemukan solusi yang efektif untuk mencapai tujuan dari ditingkatkannya pertahanan dan keamanan siber.

1. Keamanan Siber

Berdasarkan konsep, keamanan siber memiliki dua macam yaitu siber (*cyber*) dan keamanan (*security)*. Menurut beberapa ilmuwan sosial, keamanan merupakan absennya ancaman terhadap ‘nilai yang didapatkan’ (Wolvers dalam Baldwin, 1997). Menurut Ghernaouti-Helie (2009), kata “Keamanan” didefinisikan sebagai perlindungan terhadap beberapa hal yang kemungkinan akan dihadapi dan terjadi di masa depan. Konsep keamanan siber berkaitan dengan perlindungan terhadap potensi bahaya yang mungkin terjadi pada sumber daya teknologi informasi (TIK).

Keamanan siber ialah sebuah alat kebijakan, konsep keamanan, perlindungan keamanan, peraturan, pedoman, pendekatan manajemen risiko, tindakan, pelatihan, praktik terbaik, jaminan, dan teknologi yang berfungsi untuk melindungi pengguna ruang siber dari berbagai ancaman serta resiko yang ada (Fitri, hal.28). Menurut Buzan (1998), terdapat tiga model keamanan yang mengkaji bidang siber yakni *Hyper Securitization, Everyday Security Practice,* serta *Technotification* yang menggunakan ahli dalam bidang siber. Menurut McLeod dan Schell, terdapat tiga tujuan utama yang dapat dicapai dalam keamanan informasi, yaitu kerahasiaan, ketersediaan, dan integritas (Raymond & George P, 2008).

2. Era Digital

Era digital merupakan suatu periode dimana mayoritas masyarakat menggunakan teknologi digital dalam aktivitas sehari-harinya. Teknologi informasi dan komunikasi pada era saat ini banyak mengalami perkembangan yang sangat signifikan sehingga mempengaruhi masyarakat dalam bekerja, berkomunikasi, dan menjalani kehidupan sehari-hari (Castells, 2010). Menurut Tapscott (1996), menyebutkan era digital sebagai era informasi yang menjadi komoditas utama guna menggerakkan ekonomi dan masyarakat.

Kelly (1998) menggambarkan era digital sebagai masa di mana informasi dapat diakses secara instan dan global melalui internet. Kelly menyatakan bahwa era digital dicirikan oleh keterbukaan, kolaborasi, dan aksesibilitas informasi, yang semuanya didukung oleh teknologi digital yang terus berkembang.

Menurut Musnaini, Suherman, Wijoyo, dan Indrawan (2020), teknologi digital ialah teknologi yang berjalan sendiri dan tidak lagi bergantung pada tenaga manusia atau manual. Sehingga era digital saat ini, teknologi digital banyak digunakan oleh masyarakat. Kemajuan dari teknologi ini telah meningkatkan kualitas dan efisiensi kapasitas data yang dihasilkan dan dikirimkan.

3. Peran Mahasiswa

Mahasiswa adalah sebutan bagi orang yang belajar di perguruan tinggi (KBBI,2016). Seseorang dapat disebut sebagai mahasiswa apabila ia aktif sebagai pelajar dan terdaftar perguruan tinggi (Damar Adi Hartaji, 2012). Mahasiswa adalah masyarakat intelektual yang lebih memahami permasalahan yang sedang terjadi dan memiliki peran untuk menganalisa problematika yang ada dalam masyarakat kemudian disuarakan sebagai aspirasi kepada pemerintah (Ilhafa dkk., 2022).

Mahasiswa merupakan orang yang menuntut ilmu dan menempuh pendidikan yang terdaftar di perguruan tinggi, seperti di universitas, institut ataupun akademik. Mahasiswa tergolong manusia yang memiliki dua sifat, yaitu manusia muda dan calon intelektual. Pada kenyataan sosial, mahasiswa diharuskan untuk mencoba kritis dalam berpikir, sedangkan secara sifat manusia muda sebagian besar tidak dapat memprediksi berbagai risiko yang akan terjadi pada dirinya sendiri (Djojodibroto, 2004).

Mahasiswa dikenal sebagai agen pembawa perubahan (*agen of change*). Besarnya tanggung jawab yang dimiliki mahasiswa menjadi suatu hal yang membanggakan dikalangan masyarakat. Hal ini karena adanya predikat *agen of change* tersebut, mahasiswa dianggap mampu menyelesaikan masalah yang sedang dihadapi masyarakat dengan memberikan solusi yang tepat dan informatif (Haringsih Fitri S., 2019).

Mahasiswa memiliki tugas yang sangat penting yaitu belajar pada saat perkuliahan. Kepribadian dan intelektual dapat berkembang melalui perkuliahan tersebut. Mahasiswa mampu beradaptasi terhadap kurikulum yang menawarkan wawasan dan cara berpikir yang baru, juga pandangan serta penilaian terhadap sesuatu (Papalia, et.al., 2001:34).

METODE

Metode penelitian merupakan sebuah ilmu atau cara yang digunakan untuk mendapatkan sebuah informasi serta data yang nantinya akan digabungkan dengan sejumlah informasi serta data lainnya yang kemudian akan diproses kembali untuk dianalisis dan dipelajari.

Metode yang digunakan pada penelitian kami ialah kualitatif jenis pendekatan studi kasus, metode dan pendekatan ini memiliki sifat deskriptif namun lebih menggunakan analisis yang berpusat pada penggalian informasi yang mendalam. Meskipun metode kualitatif dan pendekatan studi kasus mempunyai perbedaan dalam beberapa cakupan, namun hal ini dapat menghasilkan suatu pandangan baru terhadap fenomena atau peristiwa yang luas dan terperinci dari berbagai sudut pandang. Dengan melakukan pengumpulan data melalui penyebaran angket atau kuesioner kepada para narasumber, observasi dan mencari informasi dari sosial media kami dapat dengan mudah memperoleh berbagai sumber informasi yang akan digunakan untuk kepentingan data artikel ilmiah ini.

Metode penelitian kualitatif jenis pendekatan studi kasus ini karena metode serta pendekatan ini mempunyai sifat deskriptif berdasarkan pada fakta-fakta yang terjadi. Dengan meneliti informasi melalui sosial media, melakukan observasi dan menyebarkan kuesioner kepada beberapa narasumber sekiranya hal tersebut dapat mempermudah kami dalam memperoleh sumber informasi yang akurat dari berbagai sudut pandang seputar “Tantangan Pertahanan dan Keamanan Data Cyber dalam Era Digital: Studi Kasus dan Implementasi” guna memenuhi kepentingan data yang akan dianalisis dan dituang kembali kedalam sebuah susunan paragraf yang baru.

HASIL DAN PEMBAHASAN

Hasil Penelitian

Pada penelitian kali ini menunjukan bahwa para mahasiswa atau narasumber sudah mengetahui apa itu keamanan siber. Mayoritas berpendapat bahwa keamanan siber itu merupakan upaya untuk melindungi keamanan data pribadi. Dari hasil penelitian tersebut dapat dilihat bahwa para mahasiswa berpendapat jika di Indonesia pada era saat ini keamanan siber masih belum dalam kategori yang aman dan masih diperlukan keamanan dan pertahanan siber yang efektif.

Dalam penelitian yang dilakukan melalui kuesioner kepada para mahasiswa dapat diketahui bahwa sudah banyak mahasiswa yang telah mengetahui terkait isu kejahatan siber yang meningkat di era digital pada saat ini. Kejahatan siber ini juga telah dialami oleh para narasumber kami. Hal itu dapat meresahkan para narasumber kami dalam menggunakan media sosial. Menurut para mahasiswa yang menjadi narasumber kami isu terkait permasalahan keamanan siber yang dialami pada era digital saat ini ada beberapa pendapat mengenai penanggulangan dalam pencegahan kasus kejahatan siber yang marak terjadi, seperti:

- Menggunakan password yang kuat dan unik untuk menjaga agar akun pribadi maupun perusahaan sukar diretas oleh pihak-pihak yang tidak bertanggung jawab.
- Berhati-hati dalam menerima sebuah informasi yang belum jelas sumbernya agar tidak terjerumus dalam tindak pidana penipuan.

- Selalu berperilaku bijak dalam setiap aktivitas yang dilakukan dalam menggunakan internet.
- Tidak menyebarluaskan data pribadi dan selalu menjaga keamanan data untuk memastikan privasi tetap terjaga di tengah meningkatnya ancaman kejahatan siber.
- Tidak sembarangan mengklik tautan yang mencurigakan dan tidak mengunduh aplikasi yang tidak resmi.
- Memberikan edukasi terkait pentingnya keamanan siber kepada masyarakat untuk lebih peduli terhadap keamanan data pribadi serta agar terhindar dari kejahatan siber.

Berdasarkan pendapat para mahasiswa dalam mengisi kuesioner kami yang telah memberikan opini mengenai penanganan kasus kejahatan siber yang marak terjadi pada era digital saat ini oleh instansi terkait bahwa penanganan yang telah dilakukan oleh instansi terkait mayoritas narasumber kami memiliki pandangan bahwa instansi terkait masih dirasa kurang dalam menangani kasus tersebut. Namun, ada beberapa narasumber yang memiliki pandangan bahwa instansi terkait telah melaksanakan tugasnya dengan baik dalam menjaga keamanan data. Maka dari itu, kami berharap agar instansi terkait dapat meningkatkan keamanannya dalam melindungi data-data pribadi, perusahaan, dan negara serta dapat lebih baik dalam menangani kasus kejahatan siber. Kami juga berharap kepada masyarakat itu sendiri dapat memahami pentingnya menjaga data pribadi guna terhindar dari kejahatan siber.

Pembahasan

Pada era digital yang semakin canggih, tantangan pertahanan dan keamanan *data cyber* merupakan salah satu masalah yang paling kompleks dihadapi oleh masyarakat dan suatu organisasi. Dalam perkembangan teknologi dan informasi yang sangat pesat, timbul ancaman *cyber crime* dan *cyber warfare* yang meningkat drastis pula, sehingga dengan fenomena tersebut diperlukan adanya upaya yang lebih efektif untuk melindungi data dan sistem komputer dari serangan *cyber.*

Melihat respon dari para responden mahasiswa mengenai pemahaman kejahatan siber itu sendiri dapat disimpulkan bahwa kejahatan siber merupakan suatu kejahatan yang ruang lingkupnya merupakan sistem-sistem komputer yang mengancam data-data yang terdapat pada komputer itu sendiri. Hal tersebut sesuai dengan definisi kejahatan siber sendiri atau biasa disebut *cybercrime* yang merupakan kejahatan dengan memanfaatkan teknologi informasi dan tidak sesuai dengan kebijakan ditetapkan sehingga dapat ditindak pidana lebih lanjut. Kejahatan siber juga dapat disebut dengan *computer crime,* menurut The U.S. Department of Justice, kejahatan siber dapat didefinisikan *"...any illegal act requiring knowledge of computer technology for its preparation, investigation, or prosecution".* Maka dapat diartikan sebagai kejahatan siber merupakan kejahatan yang memerlukan pemahaman mengenai komputer itu sendiri dan pelaksanaannya menggunakan komputer.

Tidak hanya perkembangan teknologi dan informasi saja yang berkembang pesat, kejahatan siber atau *cyber crime* ini sendiri juga mengalami perkembangan seiring dengan waktu ke waktu dan informasi yang tersedia. Kejahatan siber tentu saja dapat menyerang berbagai kalangan selama pengguna komputer atau internet, sesuai dengan sifat dari

kejahatan siber itu sendiri bersifat global sehingga sulit untuk dideteksi, kemudian pelaku kejahatan siber yang tidak memandang usia serta bersifat universal, dan yang terakhir kejahatan siber ini tidak menimbulkan suatu kekacauan yang terlihat karena ruang lingkupnya yang berada pada dunia maya. Kejahatan siber ini lebih khas dibandingkan dengan kejahatan lainnya karena perbuatan kejahatan terjadi di dunia maya (*cyberspace*) tanpa hak dan tidak etis, sehingga pemberlakuan yurisdiksi hukum Negara tidak dapat dipastikan, mengingat wilayah maya tersebut cakupannya sangat luas dan memungkinkan pelaku memang dari negara lain.

Kejahatan siber memiliki berbagai jenis, jenis kejahatan yang berkembang pada kejahatan siber itu sendiri terdiri atas:

a. *Unauthorized access,* yakni melakukan kejahatan dengan cara menyusup masuk kedalam sistem komputer tanpa seizin dan tidak diketahui pemilik sistem.
b. *Illegal contents,* yakni kejahatan yang menyebarluaskan sesuatu yang tidak valid, menyesatkan, tidak etis, dan melanggar norma-norma masyarakat.
c. Penyebaran virus, yakni kejahatan yang melakukan dengan mematikan, mencuri perangkat korban, serta data perusahaan.
d. *Cyber forgery,* yakni kejahatan yang biasanya dilakukan dalam perdagangan elektronik pada kesalahan pengetikan yang akan menguntungkan pelaku.
e. *Cyber espionage*, yakni kejahatan yang ada di jaringan internet sebagai alat utamanya.
f. *Cyber sabotage and extortion*, yakni kejahatan dengan melakukan gangguan, kerusakan, memusnahkan nama-nama data.
g. *Office against intellectual property,* yakni kejahatan yang dilakukan oleh seseorang di internet dengan cara mengajukan hak kekayaan intelektual.
h. *Infringements of privacy,* yakni kejahatan yang melakukan penyebaran informasi seseorang yang sangat privasi dan rahasia.

Berbagai macam kejahatan siber tersebut berdasarkan pada motif yang dapat diuraikan kembali menjadi beberapa cara seperti *Hacker* yang dalam artian luas adalah menyusup, kemudian *Cracker* yaitu seseorang yang dapat menembus dan mencuri serta merusak jaringan, *Hacking* berupa peretasan informasi, kemudian *Cyber Frand* yaitu penipuan melalui internet, dan yang terakhir adalah *Cyberporn* atau kejahatan melalui *website* dan media internet.

Secara hakikatnya keamanan siber adalah isu masih sangat baru dalam studi keamanan. Hal tersebut dapat terlihat saat seluruh aspek kehidupan yaitu politik, militer, ekonomi, sosial, dan budaya terhubung dengan dunia maya. Siber tersebut dapat menjadi ancaman diantaranya ialah *cyber terrorism*, *cyber crime* dan *cyber war*. Salah satu kawasan yang cukup tinggi tingkat pertumbuhan ekonomi dan adanya ancaman siber adalah Asia Tenggara. Pada penelitian ini bertujuan menjaga keamanan *cyber* di kawasan Asia Tenggara dengan cara menyusun strategi yang tepat (Ramadhan, 2019).

Adanya lonjakan kejahatan siber di Indonesia sehingga menjadi ancaman terhadap stabilitas keamanan dan ketertiban nasional. Intensifikasi tindak kejahatan di dunia maya mencapai level yang mengkhawatirkan. Penanganan pelanggaran hukum di ranah digital menjadi semakin kompleks dan tidak hanya mengandalkan hukum positif konvensional untuk

menyelesaikannya. Kompleksitas ini dipengaruhi oleh hubungan yang saling keterkaitan antara lima faktor utama, yakni pelaku kejahatan, korban, respons sosial terhadap tindak kejahatan, serta kerangka hukum yang berlaku.

Menurut Rahmawati (2017), ancaman kejahatan siber (*cyber crime*) dapat dihadapi dengan adanya tahapan proses manajemen risiko terbagi menjadi empat yang dapat diterapkan. Tahapan tersebut diuraikan yaitu:

1. *Identify*
   Identifikasi risiko kejahatan siber perlu dilakukan secara berkala. Hal ini tujuannya adalah mengidentifikasi penyebab dari kejahatan dapat terjadi. Pada proses ini, seluruh aspek perlu diidentifikasi secara seksama terhadap potensi yang nantinya akan menyebabkan kerugian. Selanjutnya seluruh risiko yang telah teridentifikasi kemudian dilakukan pengukuran yang mengacu pada probabilitas dan dampak.
2. *Assess*
   Tujuan dari *assess* atau penilaian risiko ini adalah evaluasi tingkat risiko dari kejahatan siber. Pada kejahatan siber tersebut dapat disebabkan pada aspek kehidupan, seperti pertahanan negara. Hal yang tidak dapat dilakukan secara langsung ini adalah dalam melakukan penilaian risiko kejahatan siber, untuk mengukur risiko tersebut dapat dilakukan dengan menggunakan tabel matriks. Tabel matriks ini memberikan gambaran dari tingkat probabilitas dan dampak yang akan terjadi setelah teridentifikasi.
3. *Treat*
   Treat ini dilakukan dengan cara memberhentikan secara paksa terhadap perbuatan dan respon yang terlibat dari risiko kejahatan siber. Adanya penentuan risiko tersebut nantinya akan diterima, dialihkan, diminimalisir, atau dihindari. Pada kasus pencurian informasi serta data tersebut terjadi secara individu ataupun secara lembaga, hal tersebut penting dalam upaya meminimalisir risiko.
4. *Control*
   Control dalam tahapan ini adalah melakukan pemantauan dan penyesuaian yang sangat penting dalam rangka mengevaluasi keberhasilan manajemen risiko. Mekanisme peringatan dini sangat penting diadakan dalam proses tersebut bagi pihak yang bertanggung jawab atas keamanan. Pihak tersebut seperti Kementerian Pertahanan Republik Indonesia, sehingga solusi yang diberikan dapat mencegah ancaman kejahatan siber.

Upaya dalam mencegah kejahatan siber tersebut dengan bantuan ahli teknologi yang didukung dengan kemampuan pengembangan sistem pertahanan negara yang canggih dan modern. Kerja sama sangat dibutuhkan, terutama pada industri pertahanan Indonesia karena untuk menciptakan program sistem informasi, serta komunikasi yang mempunyai daya saing dengan negara lain. Terdapat dua macam faktor dalam pengembangan sistem pertahanan siber di Indonesia, yakni regulasi dan keberadaan pusat komando siber. Pengembangan keamanan siber nasional perlu dibuatkan regulasi yang sesuai oleh pemerintah agar dapat teratur.

Dalam pandangan sifat kepemimpinan, seorang pemimpin harus mempunyai sifat yang teliti agar dapat menghindari kesalahan, hambatan dan tantangan yang ada serta agar dapat dipercaya oleh orang lain. Pemimpin juga harus dapat mengambil keputusan yang

bijak guna menangani berbagai masalah yang ada. Pemimpin juga perlu untuk mempunyai sifat yang kritis, logis dan berwawasan luas guna menyelesaikan suatu permasalahan dengan baik. Dengan adanya artikel mengenai kejahatan siber pada era modern saat ini diharapkan agar kedepannya nanti para pemimpin dapat lebih memperhatikan kejahatan siber di era modern pada saat ini yang sedang merebak atau di era pada masa yang akan datang nanti, juga diharapkan agar para pemimpin mampu mengatasi permasalahan mengenai kejahatan siber dan keamanan data pribadi serta perusahaan maupun negara.

SIMPULAN

Berdasarkan hasil penelitian, keamanan merupakan praktik melindungi sistem komputer, jaringan, perangkat, dan data dari ancaman digital seperti serangan siber, akses tidak sah, pencurian data, dan kerusakan. Tujuan dari keamanan siber adalah menjaga kerahasiaan, integritas, dan ketersediaan informasi, termasuk data pribadi, perusahaan, dan negara.

Di era digital ini, kejahatan siber semakin marak terjadi, menyebabkan kerugian yang signifikan bagi masyarakat yang kehilangan atau mengalami penyalahgunaan data pribadi. Kemajuan teknologi mempermudah pelaku kejahatan yang tidak bertanggung jawab dalam memanfaatkan teknologi untuk memperoleh data yang diinginkan. Meskipun tantangan dan ancaman sangat tinggi di era digital ini, seharusnya kita sebagai individu memanfaatkan perkembangan teknologi untuk menjaga kerahasiaan data dari pelaku kejahatan siber.

Karena tingginya kejahatan siber yang terjadi saat ini, diperlukan beberapa tindakan untuk mengatasi masalah tersebut. Beberapa langkah yang dapat dilakukan untuk menjaga data pribadi antara lain membuat kata sandi yang sulit ditebak, berhati-hati dan bijaksana dalam menggunakan internet atau media sosial, tidak menyebarluaskan data pribadi, dan tidak sembarangan mengklik tautan dari sumber yang mencurigakan.

Selain upaya individu, pihak pemerintah maupun instansi terkait juga sudah seharusnya mengambil langkah untuk mencegah peningkatan kasus kejahatan siber di era digital saat ini. Pemerintah serta instansi terkait dapat melibatkan ahli teknologi untuk mengembangkan sistem pertahanan dan keamanan siber yang canggih sesuai dengan tuntutan era digital saat ini.

UCAPAN TERIMAKASIH

Terima kasih kami ucapkan kepada para narasumber yaitu para mahasiswa yang telah memberikan kami kesempatan untuk mengisi kuesioner di sela-sela kesibukan kegiatan sebagai mahasiswa dan juga telah meluangkan sebagian waktunya untuk menyampaikan beberapa pendapat, argumen serta saran yang dapat berguna untuk memenuhi kepentingan data penelitian kami. Proyek dan artikel ini dapat tersusun dengan baik karena bantuan dari para anggota kelompok kali yang tidak dapat disebutkan satu per satu namanya, berkat kontribusi yang luar biasa baik secara langsung maupun tidak langsung. Kami mengapresiasi dan mengucapkan terima kasih. Selain itu juga, kami mengucapkan terima kasih kepada dosen pengampu MKWU yaitu:

- Dosen Kepemimpinan, Bapak Drs. Subakdi, MM.

Berkat saran dan kritik yang diberikan oleh beliau, proyek maupun dalam penyusunan artikel ilmiah ini dapat diselesaikan dengan maksimal. Ucapan terima kasih juga kepada rekan sesama anggota kelompok penyusunan artikel ilmiah ini yang telah membantu menyusun dan menyelesaikan artikel ilmiah ini dengan dengan baik karena kerja keras dan kerja sama tim.

DAFTAR PUSTAKA

Andinia Azuraa A., Tinjauan Teoritis Tentang Efektivitas Kejahatan Siber serta Tindak Pidana Carding. *elibrary.unikom.ac.id*, diakses pada 28 Mei 2024.
Fischer, 2009.

Islami, Maulia J. (2017), Tantangan dalam Implementasi Strategi Keamanan Siber Nasional Indonesia Ditinjau dari Penilaian Global Cybersecurity Index. *Kemdikbud.go.id*, diakses pada 25 Mei 2024.

Issha Harruma (2022), *Kejahatan Siber: Pengertian, Karakteristik dan Faktor Penyebabnya.* https://nasional.kompas.com/read/2022/09/16/02400071/kejahatan-siber--pengertian-karakteristik-dan-faktor-penyebabnya, diakses pada 28 Mei 2024.

Penulis (2021), *Kejahatan Siber Memiliki Karakteristik yang Khas*, https://kilaskementerian.kontan.co.id/news/kejahatan-siber-memiliki-karakter-yang-khas, diakses pada 28 Mei 2024.

Rezky Yayang Y. (2023), *Waspada Kejahatan Siber di Era Serba Daring*. https://lan.go.id/?p=13415, diakses pada 28 Mei 2024.

Samudra, Y., Hidayat, A., & Wahyu, M. F. (2023). Pengenalan Cyber Security Sebagai Fundamental Keamanan Data Pada Era Digital. AMMA: Jurnal Pengabdian Masyarakat, 1(12), 1594-1601.

Si Protokol, *Tindak Pidana Cyber Crime*. https://www.hukumonline.com/klinik/a/tindak-pidana-cyber-crime-cl2824/, diakses pada 28 Mei 2024.

Soesanto, E., Romadhon, A., Mardika, B. D., & Setiawan, M. F. (2023). Analisis dan Peningkatan Keamanan Cyber: Studi Kasus Ancaman dan Solusi dalam Lingkungan Digital Untuk Mengamankan Objek Vital dan File. Sammajiva: Jurnal Penelitian Bisnis dan Manajemen, 1(2), 172-191.