INNOVATIVE: Journal Of Social Science Research
Volume 5 Nomor 3 Tahun 2025 Page 4465-4485
E-ISSN 2807-4238 and P-ISSN 2807-4246
Website: https://j-innovative.org/index.php/Innovative

Advanced Persistent Threat (APT) sebagai Ancaman Perang Siber Asimetris Terhadap Pemerintah Indonesia

Sahnan Sulaiman Harahap[1✉], Mhd. Halkis[2], Rudy Sutanto[3]
Universitas Pertahanan
Email: sahnanharahap98@gmail.com[1✉]

Abstrak

Perkembangan teknologi digital yang pesat telah mendorong transformasi layanan publik di Indonesia, namun juga membawa risiko signifikan berupa ancaman siber. Salah satu ancaman utama adalah Advanced Persistent Threat (APT), kelompok penyerang siber yang terorganisir dengan tujuan mencuri data penting, melakukan spionase, dan sabotase terhadap infrastruktur pemerintah. Penelitian ini menggunakan metode kualitatif melalui studi pustaka untuk menganalisis peran APT dalam konteks perang siber asimetris. Hasil penelitian menunjukkan bahwa serangan APT bersifat canggih, sulit dideteksi, dan sering kali didukung oleh entitas negara untuk kepentingan strategis atau politis. Dampak serangan ini meliputi gangguan layanan publik, kerugian finansial, dan penurunan kepercayaan masyarakat. Untuk menghadapi ancaman ini, diperlukan penguatan kebijakan keamanan siber, peningkatan kesadaran publik, dan kolaborasi internasional. Penelitian ini menyoroti pentingnya pendekatan holistik untuk melindungi stabilitas nasional di era digital.

Kata Kunci: *Perang Asimetris, Transformasi Digital, Serangan Siber, APT*

Abstract

The rapid development of digital technology has driven the transformation of public services in Indonesia, but also brings significant risks in the form of cyber threats. One of the main threats is Advanced Persistent Threat (APT), an organized group of cyber attackers with the aim of stealing important data, conducting espionage, and sabotaging government infrastructure. This study uses a qualitative method through a literature study to analyze the role of APT in the context of asymmetric cyber warfare. The results show that APT attacks are sophisticated, difficult to detect, and often supported by state entities for strategic or political interests. The impacts of these attacks include disruption of public services, financial losses, and decreased public trust. To deal with this threat, strengthening cybersecurity policies, increasing public awareness, and international collaboration are needed. This study highlights the importance of a holistic approach to protecting national stability in the digital era.

Keywords: *Asymmetric Warfare, Digital Transformation, Cyber Attacks, APT*

PENDAHULUAN

Saat ini tercatat lebih dari 200 juta masyarakat Indonesia telah terhubung dengan internet, sehingga teknologi digital menjadi sebuah komponen dasar bagi kehidupan masyarakat (Lebang dkk., 2023). Data tersebut diperkuat juga oleh data (APJII, 2024) yang menunjukkan tingkat penetrasi internet di Indonesia mencapai 79.50% dari total populasi penduduk. APJII menyampaikan bahwa penetrasi internet di Indonesia mengalami peningkatan setiap tahunnya. Dilihat dari sebaran wilayah Indonesia, data APJII menunjukkan bahwa 89,96% wilayah Indonesia telah tersedia infrastruktur untuk mengakses internet. Dengan sebaran infrastruktur internet yang hampir menyeluruh, (Lebang dkk., 2023) berpendapat bahwa hal tersebut dimanfaatkan pemerintah Indonesia menjadi sebuah dasar andalan sebagai kekuatan transformatif digital yang bisa dimanfaatkan menjadi sarana untuk memperkuat pertumbuhan, peningkatan pelayanan publik dalam berbagai sektor seperti ekonomi dan keamanan nasional, menutup kesenjangan pembangunan, serta kualitas hidup masyarakat Indonesia dapat ditingkatkan.

Dengan tingkat pengguna internet yang besar dan akan terus bertumbuh, (Syalman, 2023) menyatakan hal tersebut berpotensi terhadap serangan siber atau dunia maya. Ia menuturkan beberapa serangan berpotensi antara lain *phishing*, *malware*, dan *ransomware* yang menimbulkan kerugian finansial hingga kerusakan reputasi individu, institusi, maupun organisasi. Dalam Laporan Monitoring Lanskap Keamanan Siber Nasional Tahunan BSSN, menunjukkan bahwa Indonesia menjadi Top 10 sumber dan tujuan serangan siber (BSSN, 2021, 2022, 2023). Laporan tersebut juga menyatakan bahwa serangan siber yang terjadi di

Indonedia mengalami peningkatan setiap tahunnya dan menarget beberapa sektor. BSSN menyebutkan salah satu sektor yang menjadi target utama para hacker adalah sektor Pemerintahan.

Serangan siber di Indonesia pada beberapa tahun belakang, menunjukkan sektor pemerintah masuk dalam sepuluh besar target utama penyerang. Kondisi ini terlihat dalam laporan BSSN tentang Lanskap Keamanan Siber Tahunan yang dirilis setiap tahunnya. Salah satu serangan yang sangat dikenal dan menjadi pusat perhatian publik yaitu munculnya Bjorka dan menyebarkan beberapa dokumen pemerintahan (Llewellyn & Aisyah, 2022). Insiden ransomware di pusat data nasional sementara Indonesia juga terjadi dan menyebabkan gangguan layanan imigrasi, termasuk layanan pengelolaan dokumen imigrasi di bandara, dan menghapus informasi yang tidak dicadangkan (CSIS, 2024). BSSN menyatakan bahwa munculnya beberapa serangan siber di Indonesia diduga dilakukan oleh sekelompok penyerang yang dinamakan advanced persistent threat (APT) yang terafiliasi dengan entitas tertentu ataupun tidak terafiliasi.

Dalam peperangan asimetris, keberadaan suatu entitas selain negara dapat diberdayakan sebagai aktor lain untuk melakukan kegiatan tertentu seperti halnya melakukan serangan siber ke target yang telah ditentukan (Devore & Lee, 2017). Selanjutnya Devore & lee menyatakan APT dapat mengganggu suatu stabilitas negera karena karakteristiknya yang sangat ofensif. Peperangan asimetris merupakan sebuah perang yang berkembang dan spektrumnya bertambah luas hingga mencakup astagata (geografi, demografi, sumber daya alam, idelologi, politik, ekonomi, sosial dan budaya) (Anjelika dkk., 2023).

Oleh karena itu, berdasarkan fenomena serangan siber yang terjadi terhadap pemerintah Indonesia dan munculnya kelompok hacker atau penyerang yang disebut dengan APT, maka dalam penelitian ini akan membahas serangan yang dilakukan oleh APT sebagai ancaman dalam dimensi perang asimetris. Adapun hasil dari penelitian ini nantinya diharapkan dapat memberikan pengetahuan dan perhatian akan pentingnya untuk meningkatkan keamanan sibernya guna mengantisipasi serangan dari aktor perang asimetris yaitu APT bagi pemerintah Indonesia. Sehingga pemerintah Indonesia dapat menghadirkan dan memastikan adanya rasa aman dan mendapat kepercayaan dari masyarakat.

METODE PENELITIAN

Penelitian ini disusun menggunakan pendekatan penelitian kualitatif. Metode penelitian kualitatif adalah cara penelitian yang digunakan untuk mempelajari objek dalam keadaan alami, di mana peneliti berperan penting dalam prosesnya. Teknik pengumpulan data dilakukan dengan berbagai cara untuk memastikan keakuratan, analisis data dilakukan secara induktif, dan hasil penelitian lebih fokus pada pemahaman makna daripada pembuatan kesimpulan umum (Abdussamad, 2021). Data penelitian kualitatif adalah data yang disajikan dalam bentuk kata-kata, kalimat, cerita, atau gambar (Nasution, 2023). Melalui pendekatan kualitatif, penelitian ini fokus pada serangan APT yang menjadi ancaman dalam perang siber asimetris terhadap pemerintah Indonesia. Untuk mengumpulkan data, peneliti menggunakan metode studi pustaka, yaitu mencari informasi dari berbagai sumber seperti buku, jurnal, artikel, dan dokumen. Data yang dikumpulkan akan digunakan sebagai dasar teori untuk menjawab tujuan penelitian dan masalah yang dibahas. Selain itu, data juga akan digunakan untuk memperkuat argumen dalam penelitian ini.

HASIL DAN PEMBAHASAN

Transformasi Digital Indonesia

Transformasi digital adalah sebuah rangkaian proses yang dilakukan dengan pendekatan secara holistik dan strategis (Meiyani & Hardi, 2024). Dalam bukunya, Meiyani & Hardi juga menjelaskan bahwa proses transformasi digital saat telah menjadi perhatian berbagai sektor salah satunya adalah sektor pemerintah. Pemerintah Indonesia telah melakukan transformasi digital secara serius dan dapat dilihat dari adanya 27.000 aplikasi atau sistem yang dimiliki oleh pemerintah pusat maupun pemerintah daerah (Kompas, 2024). Hal ini dilakukan dalam rangka memanfaatkan internet pada era revolusi industri 4.0 dan masyarakat 5.0 (Susilawati dkk., 2023). Pemanfaatan teknologi internet diharapkan dapat meningkatkan kualitas pelayanan publik dalam penyelenggaraan pemerintahan.

Susilawati dkk menyampaikan bahwa ada dua faktor yang mendasari pemerintah melakukan transformasi pelayanan berbasis digital yaitu untuk memujudkan pelayanan publik dan administrasi yang lebih baik, serta membangun pemerintah yang siap dalam menghadapi arus perubahan dalam industri 4.0 dan masyarakat 5.0. Sebuah pemerintahan yang responsif merupakan dambaan bagi masyarakat untuk memenuhi kebutuhan secara cepat, tepat, dan adil (Meiyani & Hardi, 2024). Sementara menurut (Andriyan dkk., 2024) transformasi digital pada pemerintahan bersumber dari beberapa faktor seperti

peningkatan efisiensi, peningkatan pelayanan, menghemat biaya, dan keterlibatan partisipasi masyarakat. Saat ini bentuk digitalisasi yang telah dilaukan pemerintah diwujudkan dengan membuat portal, website, layanan whatsapp, layanan virtual, integrasi sistem yang mempermudah, terjangkau, dan akuntabel (Taswin, 2024).

Cita-cita mewujudkan transformasi digital yang baik ini didukung dengan tingkat pengguna dan penetrasi internet yang tinggi sebagaimana yang disampaikan oleh APJII. Tingkat penggunaan internet dan penyebaran infrastrukturnya menunjukkan di atas angka 80 persen (APJII, 2024). Tentunya hal ini akan menjadi solusi ketika adanya keterbatasan dan hambatan berupa bentuk negara kepulauan yang geografis dan demografinya beragam dan luas (Nurlaila dkk., 2024). Perlu ditekankan bahwa transformasi digital dalam pelayanan publik yang dilakukan oleh pemerintah sebagai upaya menghadirkan kepuasan dan pemenuhan harapan yang diingankan oleh masyarakat (Harahap, 2023). Tingkat penetrasi, jumlah pengguna, sebaran ketersediaan infratruktur internet yang ada saat ini adalah sebuah potensi. Potensi ini menjadi peluang bagi pemerintah dalam era revolusi industri 4.0 dan masyarakat 5.0 untuk meningkatkan pelayanan publik. Pemenuhan pelayanan publik yang berkualitas dapat memberikan kepuasan dan harapan serta mengatasi tantangan sosial yang kompleks.

Peperangan Asimetris

Perang asimetris adalah salah satu jenis dari perang modern yang merupakan perkembangan dari bentuk perang konvensional (Anjelika dkk., 2023). Selanjutnya diterangkan bahwa perang ini memiliki karakter berupa lingkup spektrumnya yang luas mencakup Astagata (delapan aspek kehidupan). Karena sifat spektrumnya yang luas, maka dapat dikatakan bahwa dampak dari perang ini bisa meliputi aspek geografi, sumber daya alam, ideologi, ekonomi, politik, demogradi, dan sosial budaya. Sementara (Suhirwan, 2023) mengatakan perang asimetris merupakan sebuah jenis perang lain berintensitas baru, namun berasal dari era kuno. Ia juga menuturkan bahwa peperangan ini bisa saja menuntut sebuah strategi baru, kekuatan yang harus berbeda, atau melakukan jenis pelatihan militer yang baru dan bisa saja berbeda juga. Selanjutnya ia menambahkan bahwa istilah perang asimetris pertama kali muncul di lingkungan pemerintah Amerika Serikat pada tahun 1990-an. Perang ini tentunya berbeda dengan konsep perang konvensional. Menurut Suhirwan, perang konvensional seperti Perang Duni II, dapat dirincikan, terukur, teratur, dan terikat dengan sebuah konvensi.

Pendapat (Pratama dkk., 2023) menyampaikan bahwa perang asimetris adalah sebuah ancaman yang menonjol melibatkan kompleksitas strategi dan tidak terduga. Selanjutnya disampaikan, ancaman ini dapat dilakukan oleh aktor konvensional yang lebih rentan secara kekuatan yang memanfaatkan kelompok tertentu untuk mengganggu keamanan nasional suatu negara. Kewaspadaan nasional akan hadirnya ancaman perang ini adalah penting. Dalam arus global dan kompleks, kewaspadaan adalah fondasi untuk menjaga keamanan suatu negara dan integritasnya. Pratama dkk juga berpendapat adanya peningkatan ancaman perang asimetris dalam berbagai dimensi termasuk dimensi serangan atau keamanan siber. Pendapat lain memberikan definisi perang asimetris yaitu perang antara dua entitas yang kekuatannya tidak berimbang (TNI AD, 2018). Kekuatan yang tidak berimbang ini akhirnya menuntut entitas tersebut untuk mencari taktik maupun strategi mengalahkan musuhnya. Perang ini juga dikembangkan secara tidak lazim, tidak terikat pada aturan tertentu, terbuka, spektrum perang yang luas, bahkan mencakup semua aspek kehidupan. Aktor peran ini berupa pihak yang tidak terlihat dengan jelas keberadaan, aturan, bahkan peralatan yang digunakan.

Saat ini, perang siber dalam dunia maya adalah sebuah keniscayaan bentuk perang asimetris (Fauzi dkk., 2022). Perang ini didasari konflik berbasis internet yang dapat menimbulkan kerusakan dan terganggunya layanan suatu negara. Melalui perang ini sangat memungkinkan suatu entitas mendapatkan informasi rahasia, melakukan spionase, sabotase infrastruktur, black out jaringan listrik bahkan merenggut nyawa tanpa invasi militer secara fisik. Secara teknis, perang ini dilakukan melibatkan afiliasi negara atau kelompok yang didukung, bahkan ini adalah sebuah strategi suatu kombatan tertentu (Fa'izi, 2024).

Berdasarkan beberapa paragraf di atas, peneliti mengambil kesimpulan tentang definisi perang asimetris adalah jenis perang modern yang berkembang dari perang konvensional, dengan karakteristik spektrum yang luas yang mencakup berbagai aspek kehidupan. Dampak dari perang ini dapat memengaruhi geografi, sumber daya alam, ideologi, ekonomi, politik, demografi, dan sosial budaya. Perang asimetris juga memerlukan strategi baru dan pelatihan militer yang berbeda dari perang konvensional, yang terukur dan terikat pada konvensi. Ancaman dari perang ini bisa melibatkan aktor konvensional yang lebih lemah, yang memanfaatkan kelompok tertentu untuk mengganggu keamanan negara. Peningkatan ancaman perang asimetris, termasuk dalam serangan siber, menjadi perhatian penting dalam menjaga keamanan nasional. Dalam konteks ini, perang siber

menjadi bentuk nyata dari perang asimetris yang dapat menyebabkan kerusakan dan gangguan besar pada layanan negara tanpa invasi fisik.

Serangan Siber

Penemuan dan perkembangan teknologi ternyata turut diikuti dengan munculnya ancaman serangan siber (Luthfah, 2021). Ancaman serangan siber juga mengalami peningkatan yang mengikuti meningkatnya angka pengguna internet dalam ruang siber. Serangan siber merupakan sebuah rangkaian proses sistematis dilakukan oleh perorangan maupun kelompok dengan maksud mencuri, merusak, bahkan menghancurkan sistem atau jaringan komputer target tertentu. Serangan siber biasanya menyebabkan tidak terjaganya salah satu dari domain keamanan informsi yang dikenal dengan tiga serangkai CIA (*confidetiality, integrity, availability*).

Dalam dunia keamanan informasi, terdapat tiga domain keamanan yaitu confidentiality (kerahasiaan), integrity (keutuhan), dan availability (ketersediaan) yang biasanya disebut tiga serangkai CIA (Fauzi dkk., 2022). Confidentiality ditujukan sebagai kerahasiaan atas akses terhadap suatu informasi atau dokumen. Integrity adalah terjaganya keutuhan dokumen atau informasi. Avalability merupakan sebuah kondisi di mana sebuah dokumen atau informasi dapat diakses saat dibutuhkan. Dalam bukunya Introduction Cyber Security, (Fauzi dkk., 2022) dan penelitian (Goswami dkk., 2021) menyebutkan beberapa jenis serangan siber yaitu denial of service (DoS), distributed denial of service (DDoS), malware, phishing, data breach, ransomware, web defacement, zero-day attack, direct-access Attack, backdoor, Eavesdropping, Spoofing, Tampering, Repudiation Attack, information disclosure, Privilege Escalation Attack, Social Engineering, bots, rootkits, spyware, trojan horses, worm, keylogger, password attack, bluejacking, dan bluesnarfing.

Selanjutnya, serangan siber yang terjadi pada suatu sistem menimbulkan beberapa dampak teknis dan nonteknis. Data breach, pencurian kredensial, pelanggaran, kerugian finansial, dan kehancuran reputasi. Di sisi lain, (Bendovschi, 2015) menuturkan bahwa dampak serangan siber sulit dihitung karena perusahaan sering tidak membagikan semua informasi. Namun, serangan ini biasanya menyebabkan hilangnya data, gangguan bisnis, kerugian uang, dan kerusakan perangkat. Serangan yang paling umum mencuri informasi pribadi seperti nama, tanggal lahir, nomor identitas, alamat, catatan medis, nomor telepon, data keuangan, email, nama pengguna, kata sandi, dan informasi asuransi. (Falowo dkk., 2022) juga menambahkan dampak dari serangan siber dapat berupa kerugian uang,

masalah hukum, kehilangan privasi, rusaknya reputasi, data penting yang dicuri, dan gangguan pada keamanan negara.

Dalam buku tersebut disebutkan pula bahwa secara umum ada tiga kategori motif serangan siber yaitu hacktivisme, kejahatan dunia maya (cyber crime) dan spionase dunia maya (cyber-espionage). Hacktivisme adalah aktivitas meretas sistem komputer yang bertujuan mendukung agenda politik, sosial, atau ideologis tertentu. Kegiatan ini digunakan untuk menyampaikan pesan atau memengaruhi opini. Pelaku hacktivisme biasanya melakukan serangan seperti DoS (denial-of-service), DDoS (distributed denial of service), pencurian data, pelanggaran informasi, perusakan situs, pembajakan URL (typosquatting), dan berbagai bentuk sabotase digital lainnya. Kejahatan dunia maya (cyber crime) mencakup berbagai aktivitas ilegal yang menggunakan teknologi digital, khususnya untuk meraih keuntungan finansial. Contohnya meliputi penipuan perbankan secara langsung atau penjualan barang curian secara tidak langsung. Spionase siber (cyber espionage) adalah upaya mencuri informasi rahasia tanpa izin, baik dari individu, organisasi, pemerintah, maupun pihak lain, untuk kepentingan pribadi, ekonomi, politik, atau militer. Kegiatan ini memanfaatkan jaringan internet, komputer, atau perangkat lunak berbahaya seperti trojan dan spyware. Aksi ini bisa dilakukan secara daring oleh profesional dari lokasi yang jauh, oleh mata-mata terlatih, atau bahkan oleh peretas amatir.

Menurut (Paraskevas, 2022), pelaku serangan siber adalah individu atau kelompok yang memanfaatkan kelemahan keamanan di jaringan komputer dan kurangnya perhatian terhadap keamanan di organisasi untuk mengakses sistem secara ilegal dan mencuri atau merusak data. Serangan siber biasanya dibagi menjadi empat jenis: perang untuk tujuan politik, aktivisme dengan tujuan ideologi, kejahatan untuk uang, dan sabotase karena alasan emosional. Karena itu, pelaku ancaman ini dapat digolongkan sebagai pihak yang didukung negara, aktivis, penjahat siber, atau orang dalam.

Berdasarkan beberapa teori dan definisi diatas, peneliti mendapatkan sebuah konklusi bahwasanya perkembangan teknologi menyebabkan ancaman serangan siber yang semakin besar. Seiring dengan banyaknya pengguna internet, risiko serangan untuk mencuri atau merusak sistem juga meningkat. Serangan ini dapat mengganggu kerahasiaan, keutuhan, dan ketersediaan informasi yang disebut tiga serangkai CIA. Beberapa jenis serangan siber seperti DoS, DDoS, malware, dan phishing bisa menyebabkan kerugian uang, pencurian data, bahkan kerusakan reputasi. Motif serangan siber biasanya terkait dengan hacktivisme, kejahatan dunia maya (cyber crime), atau spionase siber (cyber

espionage). Pelaku serangan ini bisa datang dari individu atau kelompok dengan berbagai tujuan, seperti politik, ideologi, atau keuntungan finansial.

Advanced Persistent Threat (APT)

Menurut (Alshamrani dkk., 2019) Advanced Persistent Threat (APT) ialah sebuah kelompok yang umumnya didukung oleh suatu organisasi atau pemerintah untuk mendapatkan informasi penting dari target yang telah ditentukan. Selanjutnya (Alshamrani dkk., 2019) menyatakan bahwa istilah APT sebenarnya sebuah istilah yang biasa digunakan dalam lingkungan militer, namun kemudian istilah tersebut digunakan dalam lingkup keamanan informasi karena serangan-serangan yang terjadi atau dilakukan oleh negara-negara. Sedangkan menurut (Chen dkk., 2018) APT adalah sekelompok musuh atau penyerang yang kompeten serta memiliki sumber daya yang cukup untuk mendukung mereka mencapai tujuan dengan berbagai metode serangan. Kelompok ini mempunyai alat-alat sesuai kebutuhan operasi yang akan mereka lakukan.

Menurut (Rani dkk., 2024) menyatakan, memahami tentang apa dan bagaimana APT merupakan sebuah tantangan yang kritikal dan penting dalam konteks keamanan siber karena berdampak terhadap proses identifikasi pelaku secara akurat dibalik terjadinya sebuah serangan siber. Mereka juga menyatakan bilamana APT melakukan sebuah serangan, maka serangan tersebut adalah sebuah kampanye yang terorganisir, didukung sebuah entitas, beroperasi secara rahasia dan metodenya dilakukan dalam rentang waktu yang cukup lama.

Insiden serangan siber yang dilakukan oleh APT telah terbukti nyata. Di awali dengan terdeteksinya sebuah kelompok yang bernama Titan Rain (Alshamrani dkk., 2019). Kelompok ini melakukan modus operandinya pada tahun 2003 hingga akhirnya terungka pada tahun 2015 dan terafiliasi dengan US Defence Constractors. Kemudian sebuah APT yang bernama Hydraq terdeteksi pada tahun 2009 menargetkan google, adobe reader, dan aplikasi acrobat sebagai korbannya. Selanjutnya sebuah APT yang sangat dikenal pada tahun 2009 yaitu Stuxnet, berhasil menginfeksi fasilitas pengelolaan nuklir uranium milik Iran dan menghambat proses pembuatan senjata nuklir. Beberapa kasus serangan siber oleh APT dapat dilihat pada tabel 1.

Tabel 1. Beberapa Kasus Serangan Siber oleh APT

Serangan APT	Waktu	Tujuan	Vektor serangan yang digunakan
Titan Rain	2003-2015	Mencuri Data Perusahaan	*Social Engineering, Backdoors*

Hydraq	2009-2011	Mencuri Data Perusahaan	*Social Engineering, Phishing, Bakcdoors, Zero-Day Exploit*
Stuxnet	2009-2012	Melumpuhkan komponen kritikal	*Malware viaUSB devices, Zero-Day Exploits, Backdoors*
RSA SecureID Attack	2011-2011	Mencuri Data Perusahaan	*Spear-Phishing, Zero-Day Exploits, Backdoors*
Carbanak	2013-2015	Mendapatkan Uang	*Social Engineering, Spear-Phishing, Backdoors, Key Loggers, Form Grabbers, Video Captures of Victim's Activities, Remote Administration Tools*

Dari tabel diatas bisa dipahami operasi serangan yang dilakukan oleh APT bersifat jangka panjang. APT melakukan serangan siber menggunakan berbagai vector serangan. Sehingga mereka mendapatkan tujuan berupa data penting, uang, bahkan membuat kerusakan sistem. Dari tabel di atas, peneliti juga berpendapat bagaimana APT menyusupi jaringan korban dalam waktu yang lama dan serangan akan berakhir ketika mereka telah ketahuan oleh korban dan mendapatkan targetnya berupa data organisasi. Sehingga mereka menimbulkan kerusakan yang cukup besar pada korbannya. Bahkan sikorban dihakimi gagal kerana tidak dapat mendeteksi walaupun mereka memiliki sistem kemanan siber yang mumpuni. Tujuan serangan yang dilakukan APT tidak hanya mengumpulkan data entitas target saja, akan tetapi juga mengumpulkan detail tentang organisasi, aplikasi yang dihosting, antivirus yang digunakan, sistem deteksi yang digunakan (IDS), sistem pencegahan yang digunakan (IPS), bahkan mereka mengidentifikasi kelemahan semua alat yang dimiliki oleh korban sehingga mereka dapat mengirimkan malware yang tidak terdeteksi. Jika dilihata lebih jauh lagi, mereka menghabiskan waktu untuk mengidentifikasi kerentanan di semua alat korban dan membuat malware yang akan mengeksploitasi kerentanan tersebut. Mereka kemudian mengirimkan malware yang dibuat ini, sering kali melalui upaya phishing/spear-phishing, untuk mendapatkan akses ke jaringan organisasi (Alshamrani dkk., 2019). Oleh karena itu menjadi sesuatu yang menarik untuk mengetahui bagaimana kelompok APT melakukan serangan terhadap korbannya.

Tahapan yang dilakukan oleh APT dimulai dengan memantau, memindai jaringan internal, bergerak dari satu sistem ke sistem lain dalam jaringan, lalu melakukan tindakan utamanya. Setelah mencapai tujuannya, APT akan meninggalkan korban tanpa jejak atau bahkan meninggalkan pintu belakang (backdoor) untuk dapat kembali masuk di lain waktu. Ini menunjukkan bahwa APT berbeda dari serangan yang dilakukan oleh hacker individu. (Chen dkk., 2018) mengatakan beberapa tahapan yang dilakukan oleh APT dengan

menginfeksi untuk mencoba mengeksploitasi celah sistem atau jaringan target, kemudian melakukan discovery berupa mengumpulkan informasi berupa topologi jaringan, alokasi sumber daya, kerawanan perangkat keras, dan tahap terakhir adalah melakukan capture dan transmission, pada tahapan ini APT telah berhasil mengakses informasi sensitif dan telah menanamkan atau membuat pintu belakang (backdoor) di sistem yang dapat digunakan sewaktu-waktu jika mereka ingin mencari informasi lain lagi. Dalam penelitian ini disampaikan bahwa fenomena kehilangan data selalu menjadi masalah karena terjadinya pelanggaran keamanan informasi.

Dampak dari serangan yang dilakukan menyebabkan berbagai kerusakan jauh sebelum suatu organisasi menemukannya dan pemerintah serta perusahaan komersial tidak kebal terhadap serangan APT, dan pencegahan saat ini masih jauh dari cukup untuk melindunginya. Tindakan yang dilakukan oleh sebuah kelompok APT merupakan ancaman yang ditakuti oleh berbagai negara (Alshamrani dkk., 2019). Hal tersebut disampaikan oleh Alshamrani dkk karena status sebuah APT yang kadang dilindungi oleh negara sponsornya, peralatan yang canggih dan susah untuk dideteksi oleh korban. Peneliti menyimpulkan, Advanced Persistent Threat (APT) adalah kelompok yang didukung oleh organisasi atau pemerintah untuk mencuri informasi penting dari target mereka. APT menggunakan berbagai cara untuk menyerang, seperti memanfaatkan celah keamanan dan membuat pintu belakang. Serangan APT biasanya berlangsung lama dan dilakukan secara diam-diam agar tidak terdeteksi. Beberapa contoh serangan APT yang terkenal adalah Titan Rain, Hydraq, dan Stuxnet, yang menargetkan data dan sistem penting. APT juga pandai menemukan kelemahan dalam sistem dan membuat virus yang sulit dideteksi. Serangan APT dapat menyebabkan kerusakan besar sebelum korban menyadari adanya ancaman.

Transformasi Digital Pemerintah Indonesia dan Tantangannya

Pada era revolusi industri 4.0 dan masyarakat 5.0 saat ini, manusia sudah terbiasa untuk mengumpulkan data dari dunia nyata, memprosesnya dengan komputer, dan menerapkannya kembali ke dunia nyata. Konsep ini sudah ada sebelumnya. Ruang siber adalah tempat di mana data dunia nyata dikumpulkan dan dianalisis untuk menemukan solusi. Ini adalah ruang virtual di mana data mentah diubah menjadi informasi yang berguna dan dibagikan. Infrastruktur ruang ini terdiri dari berbagai jaringan komputer. Dalam Society 5.0, dunia maya tidak hanya digunakan untuk bertukar data, tetapi juga untuk menganalisis masalah dan menemukan solusi yang bisa diterapkan langsung di dunia nyata. Saat

menganalisis data, sistem komputer menggunakan struktur yang mencerminkan dunia fisik (Wibowo, 2023).

Teknologi informasi digunakan dalam berbagai aspek kehidupan, seperti bisnis, pendidikan, dan kegiatan sosial. Sistem informasi tidak hanya mencakup perangkat keras dan perangkat lunak, tetapi juga cara menggunakan informasi dalam bisnis, termasuk pengetahuan, metode, dan teknik. Dalam bisnis, teknologi informasi membawa perubahan besar dalam persaingan, produksi, pemasaran, manajemen sumber daya manusia, serta dalam transaksi antara perusahaan dengan pelanggan, perusahaan lain, pemasok, pemegang saham, pemerintah, dan pihak terkait lainnya (Wulandari dkk., 2016).

Meningkatkan efisiensi layanan publik dengan teknologi digital menjadi fokus utama banyak pemerintah dan lembaga. Teknologi membantu memperbaiki cara administrasi, komunikasi, dan pemberian layanan kepada masyarakat. Contohnya, dengan digitalisasi administrasi dan membuat portal layanan publik yang mudah, masyarakat bisa lebih cepat mendapatkan layanan dan informasi. Pengembangan aplikasi yang mudah digunakan dan penerapan sistem e-government juga bagian dari proses mengubah layanan menjadi digital (Wiranti & Frinaldi, 2023).

Pemerintah Indonesia terus mendorong perubahan dalam layanan publik untuk mengatasi berbagai tantangan. Dengan perubahan yang tepat, layanan publik di Indonesia bisa menjadi lebih baik, efisien, dan memuaskan masyarakat, sehingga Indonesia dapat maju dan sejahtera. Transformasi layanan publik di era digital mencakup penggunaan teknologi, digitalisasi, dan lebih banyak partisipasi masyarakat. Perubahan ini membawa manfaat seperti kemudahan akses, efisiensi, transparansi, dan akuntabilitas. Namun, ada juga beberapa tantangan, seperti kesenjangan digital, masalah keamanan data, keterbatasan sumber daya manusia, dan perubahan budaya (Natika, 2024).

Indonesia memiliki peran penting dalam perkembangan dunia siber. Di awal 2023, sekitar 77% dari total populasi Indonesia sudah menggunakan internet. Angka ini membuka peluang bagi Indonesia untuk terus berkembang sebagai produsen di dunia maya. Namun, hal ini juga membuat Indonesia rentan terhadap persaingan global dan ancaman siber. Dengan semakin luasnya penetrasi internet di seluruh Indonesia, tantangan konektivitas global menjadi perhatian penting bagi negara (Alfi dkk., 2023).

Serangan siber adalah tindakan yang menggunakan peralatan, jaringan komputer, atau kode komputer untuk merusak, mengganggu, menutup akses, atau merusak file dan sistem komputer secara sengaja dan ilegal. Serangan ini bisa membuat kinerja komputer atau jaringan menjadi lebih buruk, atau merusak data yang ada. Tindakan ini jelas

mengancam hak seseorang dalam menggunakan teknologi komputer dan bisa merusak kerahasiaan, keutuhan, dan ketersediaan informasi, yang dikenal dengan prinsip CIA (confidentiality, integrity, availability) (Suharto & Apriyani, 2021).

Beberapa serangan siber pada pemerintah Indonesia. Dalam kurun waktu dari 2020 hingga 2023, Pemerintah Indonesia telah mengalami insiden keamanan yang diakibatkan oleh serangan siber. Peneliti telah mengumpulan beberapa kejadian serangan siber terhadap pemerintah Indonesia dalam tabel 2.

Tabel 2. Insiden Serangan Siber Pemerintah Indonesia

NO	Insiden	Tahun	Dampak
1	Malware	2020	Serangan ini mengakibatkan penyerang dapat mengakses perangkat yang digunakan dari jarak jauh.
2	*Data Breach*	2021	Data pribadi masyarakat terekspos dan beredar di platform media sosial.
3	*Data Breach*	2021	Data nasabah dari sebuah asuransi milik pemerintah bocor sebanyak 2 juta nasabah yang setara dengan 250GB.
4	*Data Breach*	2022	Beberapa dokumen rahasia milik Istana Kepresidenan bocor ke publik
5	Ransomware Brain Chiper	2023	Menyebabkan Pusat Data Nasional sementara Indonesia tidak beroperasi dan menyebabkan berbagai aktifitas pelayanan publik terganggu.
6	*Web Defacement*	Hingga saat ini	Beberapa situs pemerintah pusat dan daerah Indonesia sering terjasi perubahan tampilan yang mengakibatkan masyarakat tidak dapat mengakses informasi.

Dari tabel di atas, dapat dilihat dalam beberapa tahun terakhir, Indonesia menghadapi sejumlah insiden siber yang berdampak signifikan. Pada 2020, sebuah serangan malware memungkinkan penyerang mengakses perangkat secara jarak jauh. Kemudian, pada 2021, dua insiden data breach mengakibatkan data pribadi masyarakat dan 2 juta nasabah asuransi pemerintah bocor, yang menyebar di platform media sosial dan mencapai ukuran 250GB. Pada 2022, sejumlah dokumen rahasia dari Istana Kepresidenan juga terungkap ke publik. Serangan ransomware Brain Chiper pada 2023 menyebabkan Pusat Data Nasional Indonesia tidak berfungsi, mengganggu pelayanan publik. Selain itu, hingga saat ini, insiden web defacement terjadi pada beberapa situs pemerintah pusat dan daerah, menyebabkan gangguan akses informasi bagi masyarakat.

Pada Mei 2021, FBI dan Australia Cyber Security Center memberikan peringatan ke beberapa negara termasuk Indonesia, karenda terdeteksi adanya aktifitas ransomware yang menargetkan multisektor termasuk sektor pemerintah (CSIS, 2024). Selain berdampak pada CIA, serangan siber menyebabkan kerugian yang tidak sedikit (Sari, 2024). Dalam laporan pada lama web cisrt.or.id menuturkan sebuah fakta bahwa serangan siber yang terjadi di Inggris menimbulkan kerugian sebanyak 879 miliar rupiah. Sementara insiden serangan siber di Indonesia, yaitu lumpuhnya Pusat Data Nasional sementara, menimbulkan kerugian finansial sebanyak USD 5.600 per harinya (Lucretie, 2024). Selain kerugian finansial, seragan siber dapat menganggu layanan pemerintahan dan menurunnya kepercayaan masyarkat. Insiden Bjorka pada tahun 2022 menjadi sebuah fenomena dramatisasi dengan upaya doxing menyerang pemerintah sehingga masyarakat tidak percaya dengan pemerintah (Harahap, 2023).

Dilansir dari Laporan Monitoring Keamanan Siber Nasional yang dirilis oleh BSSN dari tahun 2021 hingga 2023, peneliti menemukan bahwa adanya keterlibatan kelompok APT pada fenomena insiden keamanan siber di Indonesia. Beberapa APT yang terdeteksi melakukan aksinya di Indonesia ditampilkan pada tabel 3.

Tabel 3. APT yang terdeteksi di Indoensia

NO	APT	Tujuan
1	Lazarus	Kelompok ini bertujuan mencuri data dan informasi bernilai tinggi, dengan alasan finansial, spionase, sabotase, dan untuk mengancam keamanan serta stabilitas politik. Keterlibatan pemerintah Korea Utara memberikan pengaruh politik pada aktivitas Lazarus. Selain menargetkan sektor keuangan, lembaga pemerintah, dan industri, kelompok ini juga melakukan serangan besar seperti meretas bank dan mencuri mata uang kripto.
2	Winnti	Kelompok ini mencuri informasi dan melakukan spionase. Winnti terlibat dalam serangan siber yang rumit, terutama pada industri dan lembaga pemerintah, dengan menggunakan cara-cara canggih seperti eksploitasi perangkat lunak dan spear-phishing. Mereka mencuri data penting, terutama yang berkaitan dengan kekayaan intelektual dan informasi industri, serta menyerang penyedia perangkat lunak dan perusahaan pemasaran.
3	Kimsuky	Kelompok ini bertujuan untuk mencuri informasi dan melakukan spionase. Mereka juga terlibat dalam berbagai serangan yang

		menargetkan sektor pemerintah, militer, dan lembaga penelitian di berbagai negara.
4	Anchor Panda	Anchor Panda terkenal karena tujuannya yang berhubungan dengan intelijen dan ekonomi. Ancaman dari kelompok ini tidak hanya mencakup pencurian data penting, tetapi juga spionase industri yang dapat merusak sektor teknologi dan ekonomi, serta mengancam kerahasiaan negara.
5	APT40	Ancaman dari APT40 melibatkan pencurian data penting, kerahasiaan teknologi, dan dapat mempengaruhi keamanan negara. Selain mencuri data dari sektor pelayaran dan energi, APT40 juga terlibat dalam spionase industri yang dapat mengancam stabilitas keamanan nasional.

Berdasarkan data dari tabel di atas, bisa disimpukan bahwa kelompok-kelompok APT (Advanced Persistent Threat) yang disebutkan memiliki tujuan utama untuk mencuri data dan melakukan spionase, dengan berbagai motif seperti finansial, sabotase, dan ancaman terhadap keamanan dan stabilitas politik. Lazarus, yang terkait dengan pemerintah Korea Utara, terlibat dalam serangan besar yang menargetkan sektor keuangan, lembaga pemerintah, dan industri, termasuk meretas bank dan mencuri mata uang kripto. Winnti, dengan serangan canggih, fokus pada industri dan lembaga pemerintah, serta mencuri data kekayaan intelektual dan informasi industri. Kimsuky berfokus pada sektor pemerintah, militer, dan lembaga penelitian di berbagai negara untuk melakukan spionase dan pencurian informasi. Anchor Panda terlibat dalam spionase industri yang dapat merusak sektor teknologi dan ekonomi, serta mengancam kerahasiaan nasional. APT40 juga terlibat dalam pencurian data dari sektor pelayaran dan energi, serta spionase industri yang dapat memengaruhi stabilitas keamanan nasional.

Berdasarkan uraian fenomena, serta data yang telah disampaikan di atas, peneliti dapat memberikan sebuah pandangan bahwa transformasi digital telah menjadi bagian integral dari perkembangan teknologi di berbagai sektor, termasuk layanan publik, bisnis, dan keamanan siber. Indonesia, sebagai negara dengan tingkat penetrasi internet yang tinggi, menghadapi tantangan dan ancaman yang signifikan terkait serangan siber, baik yang disebabkan oleh malware, kebocoran data, maupun serangan ransomware. Dalam konteks ini, beberapa kelompok APT (Advanced Persistent Threat) seperti Lazarus, Winnti, dan Kimsuky berperan dalam serangan yang menyasar sektor-sektor penting, termasuk keuangan, militer, dan industri. Meskipun ada banyak manfaat dari transformasi digital

seperti kemudahan akses dan efisiensi, ancaman terhadap keamanan data dan kerahasiaan informasi tetap menjadi masalah yang harus diatasi. Oleh karena itu, penting bagi Indonesia untuk terus mengembangkan infrastruktur digital yang aman dan meningkatkan kesadaran tentang ancaman siber, serta memperkuat kerja sama internasional untuk mengatasi tantangan global ini. Dengan langkah yang tepat, Indonesia dapat memanfaatkan peluang digital dan mengurangi risiko ancaman yang ada.

Tinjauan Perang Asimetris Terhadap Serangan Siber oleh APT

Definisi perang asimetris. Perang asimetris adalah jenis perang modern yang berkembang dari perang konvensional. Perang ini memiliki ciri khas dengan spektrum yang luas, mencakup delapan aspek kehidupan yang dikenal sebagai Astagata. Karena cakupannya yang luas, dampak perang ini dapat memengaruhi berbagai bidang, seperti geografi, sumber daya alam, ideologi, ekonomi, politik, demografi, serta sosial dan budaya. Ancaman asimetris mencakup terorisme, pemberontakan, penyebaran informasi yang menyesatkan, gangguan, dan ancaman yang belum diketahui (Buffaloe, 2006). Aktivitas yang dilakukan oleh APT sangat beragam, seperti pencurian uang, spionase, serangan merusak, dan pemerasan siber. Hal ini menunjukkan bahwa ancaman siber memiliki banyak bentuk dan menjadi tantangan bagi keamanan nasional. Kasus ini menegaskan pentingnya pendekatan menyeluruh dalam keamanan siber yang mencakup kerentanan teknis dan faktor manusia (Perdana dkk., 2024).

Keterkaitan antara aktifitas APT dan entitas yang mendukungnya dengan karakteristik gigih dalam melakukan operasinya, kecanggihan alat yang digunakan maupun dukungan lain yang dimiliki adalah sebuah fakta. Salah satu negara yang diketahui mendukung dan mendanai aktifitas APT adalah Korea Utara. Korea Utara sering melakukan serangan siber strategis yang berhasil meretas dan mengganggu sistem keuangan penting di Amerika Serikat (Kim dkk., 2020). Insiden serangan siber yang terjadi di Indonesia juga dilakukan oleh sekelompok APT. Fakta tersebut telah dipaparkan oleh BSSN yang dituliskan pada laporan tahunan mereka. Jika kita merujuk kembali pada tabel yang menunjukkan beberapa aktifitas APT yang ada di Indonesia, beberapa negara memberikan dukungan nyata atas aktifitas tersebut. Kelompok APT mengumpulkan informasi untuk tujuan strategis atau politis. Umumnya, mereka tidak memilih target secara acak, melainkan bertindak atas perintah baik langsung maupun tidak langsung dari lembaga pemerintah. Lembaga ini bisa berupa badan intelijen, militer, penegak hukum, kementerian luar negeri, atau kementerian ekonomi, tergantung negara asalnya. Tugas mereka bisa terkait dengan rencana pertumbuhan

ekonomi, situasi politik terkini untuk keputusan jangka pendek, atau strategi jangka panjang untuk perencanaan masa depan (Steffens, 2020).

Tujuan gerakan perang asimetris. Penggunaan strategi perang asimetris, tentunya hal tersebut memberikan sebuah dampak yang tidak kecil. Hal tersebut karena sifat dari perang asimetris dapat memberikan daya rusak yang dahsyat (ABN RI, 2015). Mari kita lihat salah satu dampak dari serangan siber yang terjadi di Indonesia. Insiden down nya Pusat Data Nasional sementara Indonesia memiliki tidak hanya menimbulkan dampak pada salah satu sistem (Irfan Adristi & Ramadhani, 2024). Dampak dari serangan tersebut menganggu berbagai layanan publik pemerintah yang tidak terbatas pada pemerintah pusat bahkan terjadi hingga ke daerah.

Berdasarkan berbagai penjelasan di atas, peneliti berpendapat Perang asimetris adalah bentuk perang modern yang mencakup berbagai aspek kehidupan, seperti geografi, ideologi, ekonomi, politik, dan budaya, dengan dampak yang sangat luas. Ancaman utama dalam perang ini adalah serangan siber yang dilakukan oleh kelompok APT, yang mencakup aktivitas seperti pencurian data, spionase, perusakan sistem, dan pemerasan. Serangan ini menjadi tantangan serius bagi keamanan nasional dan membutuhkan pendekatan yang menyeluruh, mencakup penguatan teknologi serta peningkatan kesadaran manusia. Kelompok APT sering bertindak atas perintah lembaga pemerintah, seperti badan intelijen atau militer, dengan tujuan strategis atau politis sesuai kepentingan negaranya. Korea Utara, misalnya, diketahui mendukung operasi APT untuk menyerang sistem keuangan negara lain, termasuk Amerika Serikat. Di Indonesia, serangan APT telah merusak infrastruktur penting, seperti insiden down-nya Pusat Data Nasional, yang menyebabkan gangguan pada layanan publik hingga ke daerah. Dampak serangan ini menunjukkan betapa besar kerugian yang ditimbulkan terhadap stabilitas nasional. Oleh karena itu, langkah strategis dalam keamanan siber sangat diperlukan untuk mengatasi ancaman tersebut.

SIMPULAN

Perang asimetris adalah bentuk perang modern yang mencakup berbagai aspek kehidupan, seperti geografi, ekonomi, politik, dan budaya. Salah satu ancaman utamanya adalah serangan siber, yang sering kali dilakukan oleh kelompok Advanced Persistent Threat (APT). Kelompok ini bekerja dengan strategi yang terorganisir, menggunakan metode seperti spionase, pencurian data, dan sabotase. Di Indonesia, transformasi digital yang pesat telah meningkatkan efisiensi layanan publik, tetapi juga membuka peluang bagi serangan siber yang menyasar infrastruktur penting, seperti Pusat Data Nasional.

Insiden-insiden ini menunjukkan kerentanan sistem digital pemerintah, sehingga perlindungan terhadap ancaman siber menjadi prioritas untuk menjaga stabilitas nasional.

Kelompok APT sering kali didukung oleh entitas negara untuk mencapai tujuan strategis atau politis. Serangan ini berlangsung dalam waktu lama, menggunakan teknik yang sulit dideteksi, dan sering kali meninggalkan dampak besar sebelum akhirnya teridentifikasi. Sebagai contoh, kelompok seperti Lazarus, Winnti, dan Kimsuky telah menyerang sektor keuangan, pemerintahan, dan industri, baik untuk keuntungan finansial maupun tujuan politik. Hal ini menegaskan pentingnya pendekatan holistik dalam keamanan siber, yang tidak hanya memperkuat teknologi tetapi juga meningkatkan kesadaran akan ancaman ini. Dengan langkah yang tepat, seperti penguatan kebijakan keamanan siber dan kolaborasi internasional, Indonesia dapat mengatasi ancaman ini sekaligus memanfaatkan potensi digital untuk kemajuan bangsa.

DAFTAR PUSTAKA

Abdussamad, Z. (2021). Buku Metode Penelitian Kualitatif (1 ed.; P. Rapanna, Ed.). Makassar: CV. Syakir Media Press.

ABN RI. (2015). Mengenal Perang Asimetris: Sifat, Bentuk, Pola dan Sumbernya. Diambil dari abnri.com website:https://abnri.com/2021/06/09/mengenal-perang-asimetris-sifat-bentuk-pola-dan-sumbernya-bagian-1-seri-perang-asimetris/

Alfi, M., Yundari, N. P., & Tsaqif, A. (2023). Analisis Risiko Keamanan Siber dalam Transformasi Digital Pelayanan Publik di Indonesia. Jurnal Kajian Stratejik Ketahanan Nasional, 6(2). https://doi.org/10.7454/jkskn.v6i2.10082

Alshamrani, A., Myneni, S., Chowdhary, A., & Huang, D. (2019). A Survey on Advanced Persistent Threats: Techniques, Solutions, Challenges, and Research Opportunities. IEEE Communications Surveys and Tutorials, 21(2), 1851–1877. https://doi.org/10.1109/COMST.2019.2891891

Andriyan, Y., Rajab, A. M., Pamungkas, A. C., Muhamad, S., & Rahakratat, R. (2024). Transformasi E-Government Menuju Good Governance di Pemerintah Kabupaten Sorong. Samakta: Jurnal Pengabdian Kepada Masyarakat, 1(2), 24–35. https://doi.org/10.61142/samakta.v1i2.127

Anjelika, F., Rahayu, J., Sari, T. P., & Ratmaningsih, N. (2023a). Analisis Perang Modern Pada Perang Ukrain. Jurnal Ilmu Sosial, Politik, dan Humaniora, 6(2), 2023.

Anjelika, F., Rahayu, J., Sari, T. P., & Ratmaningsih, N. (2023b). Analisis Perang Modern Pada Perang Ukrain. Jurnal Ilmu Sosial, Politik dan Humaniora, 6(2).

APJII. (2024). Survei Penetrasi Internet Indonesia 2024. Jakarta.

Bendovschi, A. (2015). Cyber-Attacks – Trends, Patterns and Security Countermeasures. Procedia Economics and Finance, 28, 24–31. https://doi.org/10.1016/s2212-5671(15)01077-1

BSSN. (2021). Laporan Tahunan Monitoring Keamanan Siber 2021. Jakarta.

BSSN. (2022). LANSKAP KEAMANAN SIBER INDONESIA 2022. Jakarta.

BSSN. (2023). LANSKAP KEAMANAN SIBER INDONESIA 2023. Jakarta.

Buffaloe, D. L. (2006). Defining Asymmetric Warfare. Virgina.

Chen, J., Su, C., Yeh, K. H., & Yung, M. (2018, Februari 1). Special Issue on Advanced Persistent Threat. Future Generation Computer Systems, Vol. 79, hlm. 243–246. Elsevier B.V. https://doi.org/10.1016/j.future.2017.11.005

CSIS. (2024). Significant Cyber Incidents Since 2006. Washington.

Devore, M. R., & Lee, S. (2017). APT(ADVANCED PERSISTENT THREAT)S AND INFLUENCE: CyBER WEAPONS AND THE CHANGING CALCULUS OF CONFLICT. Ther Journal of East Asian Affairs, 31(1).

Fa'izi, M. B. N. (2024, September). Apa itu Cyberwarfare? Metode dan Dampaknya. Diambil dari https://cyberhub.id/pengetahuan-dasar/apa-itu-cyberwarfare

Falowo, O. I., Popoola, S., Riep, J., Adewopo, V. A., & Koch, J. (2022). Threat Actors' Tenacity to Disrupt: Examination of Major Cybersecurity Incidents. IEEE Access, 10, 134038–134051. https://doi.org/10.1109/ACCESS.2022.3231847

Fauzi, A., Setiawan, A., Hasta, A. B., Maulana, A., & Permana, R. (2022). INTRODUCTION CYBER SECURITY (1 ed.). Bengkulu: Penerbit Elmarkazi.

Goswami, R., Sharma, S., Chawla, C. S., Pande, J., Mallick, C., Paikaray, B. K., & Dash, G. P. (2021). Cyber Attacks and Counter Measures: User Perspective. Ahmedabad.

Harahap, M. N. (2023). Akselerasi Transformasi Digital Dalam Pelayanan Publik Guna Peningkatan Tata Kelola Pemerintahan. Jakarta.

Irfan Adristi, F., & Ramadhani, E. (2024). Analisis Dampak Kebocoran Data Pusat Data Nasional Sementara 2 (PDNS 2) Surabaya: Pendekatan Matriks Budaya Keamanan Siber dan Dimensi Budaya Nasional Hofstede (Vol. 02). Diambil dari https://journal.uii.ac.id/selma/index

Kim, Y.-K., Lee, J. J., Go, M.-H., & Lee, K. (2020). Analysis of the Asymmetrical Relationships between State Actors and APT Threat Groups. International Conference on Information and Communication Technology Convergence (ICTC), 695–700. IEEE. https://doi.org/10.1109/ICTC49870.2020.9289506

Kompas. (2024, Mei 27). Ada 27.000 Aplikasi Milik Pemerintah, Jokowi: Tidak Terintegrasi dan Tumpang Tindih. Diambil dari nasional.kompas.com website: https://nasional.kompas.com/read/2024/05/27/12282521/ada-27000-aplikasi-milik-pemerintah-jokowi-tidak-terintegrasi-dan-tumpang

Lebang, C. G., Priyandita, G., Wijaya, T., Zakaria, N. A., & Rasyid, A. K. (2023). TRANSFORMASI DIGITAL INDONESIA Kondisi Terkini dan Proyeksi. Jakarta.

Llewellyn, & Aisyah. (2022). Bjorka, the Online Hacker Trying To Take Down the Indonesia Government. The Diplomat.

Lucretie, A. (2024, Juni). Kerugian Negara Akibat Serangan Siber Terus Bertambah Hingga PDN Pulih Sepenuhnya. Diambil dari nasional.kontan.co.id website: https://nasional.kontan.co.id/news/kerugian-negara-akibat-serangan-siber-terus-bertambah-hingga-pdn-pulih-sepenuhnya

Luthfah, D. (2021). Serangan Siber Sebagai Penggunaan Kekuatan Bersenjata dalam Perspektif Hukum Keamanan Nasional Indonesia (Cyber Attacks as the Use of Force in the Perspective of Indonesia National Security Law). terAs Law Review : Jurnal Hukum Humaniter dan HAM, 3(1), 11–22. https://doi.org/10.25105/teras-lrev.v3i1.10742

Meiyani, E., & Hardi, R. (2024). TRANSFORMASI DIGITAL DAN PEMERINTAHAN RESPONSIF (1 ed.; M. R. Akbar, Ed.). Purbalingga: CV. Eureka Media Aksara.

Nasution, A. F. (2023). Metode Penelitian Kualitatif (1 ed.; M. Albina, Ed.). Bandung: CV. Harfa Creative.

Natika, L. (2024). TRANSFORMASI PELAYANAN PUBLIK DI ERA DIGITAL: MENUJU PELAYANAN MASA DEPAN YANG LEBIH BAIK. The World of Public Administration Journal (WPAJ, 6(1). Diambil dari http://ejournal.unsub.ac.id/index.php/publik

Nurlaila, N., Nurhasanah, N., & Bima, S. (2024). Transformasi Digital Pelayanan Publik: Tantangan dan Prospek dalam Implementasi E-Government di Kabupaten Bima. Public Service And Governance Journal, 5(2), 21–37.

Paraskevas, A. (2022). Cyber Threat Actors. Encyclopedia of Tourism Management and Marketing, 750–753. https://doi.org/10.4337/9781800377486.CYBER.THREAT.ACTORS

Perdana, A., Aminanto, M. E., & Anggorojati, B. (2024). Hack, heist, and havoc: The Lazarus Group's triple threat to global cybersecurity. Journal of Information Technology Teaching Cases, 0(0), 1–12. https://doi.org/10.1177/20438869241303941

Pratama, R., Timur, F. G. C., & Susanto, R. (2023). Revitalisasi Kewaspadaan Nasional

Melalui Sistem Pertahanan dan Keamanan Terhadap Ancaman Perang Asimetris. Nusantara : Jurnal Ilmu Pengetahuan Sosial, 10(9), 4548–4559.

Rani, N., Saha, B., & Shukla, S. K. (2024). A Comprehensive Survey of Advanced Persistent Threat Attribution: Taxonomy, Methods, Challenges and Open Research Problems. Diambil dari http://arxiv.org/abs/2409.11415

Sari, R. P. (2024, November). Serangan Siber di Inggris Sebabkan Kerugian Rp 879 Miliar. Diambil dari csirt.or.id website: https://csirt.or.id/berita/serangan-siber-di-inggris

Steffens, T. (2020). Attribution of Advanced Persistent Threats : How to Identify the Actors Behind Cyber-Espionage (1 ed.). Berlin: Spriger.

Suharto, M. A., & Apriyani, M. N. (2021). Konsep Cyber Attack, Cyber Crime, Dan Cyber Warfare Dalam Aspek Hukum Internasional. Risalah Hukum, 17(2), 98–107.

Suhirwan. (2023). Ilmu Pertahanan : Peperangan Asimetris (1 ed.; F. S. A. Uniawan, Ed.). Garut: CV. Aksara Global Akademia. Diambil dari www.aksaraglobal.com

Susilawati, F. E., Yanti, R., & Erni. (2023). Transformasi Digital Pemerintah (Studi Kasus: Implementasi e-Government dan Hambatannya). Journal Social Society, 3(2). https://doi.org/10.30605/jss.3.2.2023.338

Syalman, A. A. (2023). LANSKAP PENGGUNA INTERNET DAN PERAN ISP DALAM KEAMANAN SIBER INDONESIA. Jakarta. Diambil dari www.apjii.or.id

Taswin. (2024). Penguatan Digitalisasi Layanan Pemerintahan yang Terintegrasi Guna Mewujudkan Pembangunan Nasional. Jakarta.

TNI AD. (2018). Kajian Triwulan IV Kesiapan TNI AD dalam Menghadapi Ancaman Asimetris.

Wibowo, A. (2023). Revolusi Industri 4.0 dan Society 5.0 (1 ed.; J. T. Santoso, Ed.). Semarang: Yayasan Prima Agus Teknik.

Wiranti, N. E., & Frinaldi, A. (2023). Meningkatkan Efisiensi Pelayanan Publik dengan Teknologi di Era Digital. JIM: Jurnal Ilmiah Mahasiswa Pendidikan Sejarah, 8(2), 748–754. https://doi.org/10.24815/jimps.v8i2.24833

Wulandari, L. D., Falah, S., & Sanggenafa, M. (2016). PENGARUH TEKNOLOGI INFORMASI, SALING KETERGANTUNGAN, KESELARASAN TUJUAN DAN KOMUNIKASI TERHADAP KINERJA INDIVIDUAL (Studi Pada Perusahaan Yang Menerapkan Teknologi Informasi Di Jayapura). Jurnal Akuntansi & Keuangan Daerah, 11(1), 38–49.