e-ISSN: 2550-0813 | p-ISSN: 2541-657X | Vol 12 No 3 Tahun 2025 Hal. : 1194-1206

NUSANTARA: Jurnal Ilmu Pengetahuan Sosial

available online http://jurnal.um-tapsel.ac.id/index.php/nusantara/index

PERANG CYBER SEBAGAI BENTUK PEPERANGAN ASIMETRIS: PERSPEKTIF FILSAFAT KEAMANAN DIGITAL DAN NIST CYBERSECURITY FRAMEWORK

Ahmad Jufri Lubis, Fauzia G Cempaka T, Suhirwan

Peperangan Asimetris, Fakultas Strategi Pertahanan, Universitas Pertahanan

Abstrak

Keamanan nasional dalam era digital menghadapi tantangan baru yang muncul dari ancaman perang siber sebagai bentuk peperangan asimetris. Penelitian ini mengkaji bagaimana aktor non-negara dan negara dengan sumber daya terbatas memanfaatkan teknologi untuk menyerang infrastruktur kritis, seperti sistem keuangan dan komunikasi, tanpa keterlibatan fisik langsung. Menggunakan teori keamanan nasional dan peperangan asimetris, penelitian ini menjelaskan dinamika dan kompleksitas perang siber dalam mengancam stabilitas negara. Studi ini berfokus pada penerapan NIST Cybersecurity Framework, yang terdiri dari lima fungsi utama: Identify, Protect, Detect, Respond, dan Recover, sebagai model untuk memperkuat pertahanan siber nasional. Melalui analisis kasus serangan terhadap Pusat Data Nasional dan Bank Syariah Indonesia, penelitian ini menyoroti pentingnya kolaborasi lintas sektor antara pemerintah, sektor swasta, dan masyarakat dalam membangun sistem keamanan digital yang tangguh dan inklusif. Penelitian ini juga merumuskan strategi untuk mempertahankan integritas negara, yang mencakup penguatan regulasi siber, peningkatan kapasitas teknologi dan sumber daya manusia (SDM), serta kesadaran masyarakat terkait keamanan digital. Hasil penelitian ini diharapkan memberikan rekomendasi strategis bagi pengambil kebijakan dalam merespons ancaman perang siber yang terus berkembang dan menjaga keseimbangan antara keamanan nasional dan hak asasi manusia.

Kata Kunci: Keamanan nasional, perang siber, peperangan asimetris, NIST Cybersecurity Framework, keamanan digital, kolaborasi lintas sektor.

*Correspondence Address : ahmadjufrilubis22@gmail.com
DOI : 10.31604/jips.v12i3.2025. 1194-1206

PENDAHULUAN

Keamanan nasional merupakan salah satu aspek krusial yang menentukan stabilitas suatu negara. Secara konseptual, keamanan nasional dapat dijelaskan sebagai kondisi di mana warga negara tidak menghadapi ancaman, baik militer, non-militer, maupun hibrida, baik dari luar negeri maupun dalam negeri (Larosa, 2019). Ancaman tersebut bisa bersifat laten, tersembunyi, maupun terlihat jelas, yang mencakup berbagai dimensi seperti konflik sosial, politik, ekonomi, budaya, agama, serta ancaman ekologis (Dewan Ketahanan Nasional, 2010).

Keamanan nasional tidak hanya mencakup kondisi aman dalam negeri, tetapi juga stabilitas keamanan global. Kekuatan negara, perkembangan senjata, teknologi digital, dan senjata nuklir memengaruhi keamanan internasional (Turner, 1960). Banyak negara merasa perlu berperang demi menjaga kedaulatan, dengan prinsip "Si vis Pacem, para bellum" menekankan pentingnya kesiapan menghadapi konflik. Perang, sejatinya, didefinisikan sebagai konflik bersenjata antara dua atau lebih pemerintah atau negara (Clausewitz, 1984.).

Dalam perkembangan terkini, peperangan asimetris dapat dibagi menjadi tiga jenis utama, yaitu strategic asymmetry, tactical asymmetry dan proxy war (Khan, 2005). Asimetri strategis terjadi ketika kedua pihak menggunakan pasukan serupa, tetapi hasil ditentukan oleh kualitas dan kuantitas pasukan, termasuk komando dan kendali. Asimetri taktis muncul saat satu pihak memiliki keunggulan teknologi yang dapat mengatasi keunggulan jumlah lawan. Perang proksi melibatkan aktor non-pemerintah yang bertindak atas nama negara. Dinamika ini menambah kompleksitas peperangan modern yang perlu dipahami lebih mendalam (Lele, 2014).

Di era digital, perang cyber sebagai bentuk peperangan asimetris menjadi semakin relevan. Setelah peristiwa 9/11, aktor non-negara mulai memanfaatkan taktik non-konvensional untuk mengeksploitasi kerentanan negara (Lele, 2014). Seiring dengan kemajuan teknologi, serangan siber tidak hanya bersifat teknis, tetapi juga melibatkan strategi cerdas untuk merusak sistem vital. Sebagai contoh, serangan oleh kelompok hacker Brain Cipher terhadap Pusat Data Nasional Indonesia pada Juni 2024 (Kompas.com, 2024) hal ini menyingkap betapa rentannya infrastruktur vital terhadap serangan terencana, yang berdampak pada layanan pemerintah, keamanan nasional, dan stabilitas ekonomi.

Peperangan asimetris, yang ditandai dengan perbedaan kekuatan dan strategi antara pihak yang terlibat menimbulkan pertanyaan mengenai legitimasi tindakan dan dampaknya pada masyarakat sipil (Lele, 2014). Serangan siber terhadap infrastruktur vital tidak hanya memengaruhi aspek militer, tetapi juga kehidupan masyarakat. (Kim & Solomon, 2018).

Perkembangan teknologi digital meningkatkan ancaman perang cyber sebagai bentuk peperangan asimetris, di mana aktor non-negara memanfaatkan taktik non-konvensional yang merusak infrastruktur vital dan mengancam keamanan nasional. Penelitian ini bertujuan untuk mengkaji dinamika perang cyber yang merupakan bagian dari peperangan asimetris serta merumuskan strategi keamanan nasional dan keamanan digital yang melibatkan kolaborasi pemerintah, sektor swasta, dan masyarakat sipil. Kolaborasi ini esensial untuk membangun sistem keamanan digital serta pertahanan siber yang tangguh dan inklusif.

TINJAUAN PUSTAKA

Perang siber, sebagai bentuk peperangan asimetris, telah menjadi ancaman signifikan bagi keamanan nasional modern. Aktor non-negara atau aktor dengan kekuatan militer terbatas menggunakan teknologi untuk menyerang infrastruktur penting tanpa keterlibatan konflik fisik langsung. Hal ini semakin relevan di era digital, di mana banyak negara bergantung pada infrastruktur digital untuk operasional sosial, ekonomi, dan politik. Penelitian ini menyoroti dua studi terkait ancaman perang siber terhadap keamanan nasional.

Penelitian yang dilakukan oleh Lele (2014) mengenai Asymmetric Warfare: A State vs Non-State Conflict berfokus pada bagaimana perang asimetris memungkinkan aktor non-negara atau aktor yang lebih lemah secara militer untuk memanfaatkan teknologi guna menyeimbangkan kekuatan dengan pihak yang lebih kuat. Lele menjelaskan bahwa serangan siber menjadi salah satu taktik utama yang digunakan dalam perang asimetris, di mana teknologi digunakan untuk menyerang kerentanan dalam sistem infrastruktur negara tanpa melibatkan kekuatan fisik secara langsung. Dalam temuan utama penelitiannya, Lele mengungkapkan bahwa perang siber dapat merusak stabilitas negara dengan menargetkan infrastruktur kritis seperti jaringan komunikasi dan sistem keuangan, yang dalam konteks modern semakin bergantung pada teknologi digital. Pendekatan metodologi Lele bersifat analitis dan berfokus pada studi kasus peperangan asimetris yang telah terjadi, menunjukkan bagaimana teknologi menjadi senjata utama dalam konflik asimetris.

Larosa (2019) dalam artikelnya Redefining Indonesia's National Security in Ensuring the Survival of the Nation menyoroti pentingnya memperluas definisi keamanan nasional untuk mencakup ancaman non-militer, termasuk serangan siber. Larosa berpendapat bahwa keamanan nasional Indonesia tidak hanya harus melindungi dari ancaman fisik, tetapi juga harus mengantisipasi serangan yang bersifat non-konvensional, seperti serangan siber yang semakin relevan dalam dunia yang semakin terhubung secara digital. Temuan utama penelitian ini menekankan bahwa keamanan siber harus menjadi prioritas nasional, dengan pemerintah berperan sebagai penggerak utama dalam memperkuat pertahanan siber melalui kolaborasi lintas sektor antara pemerintah, sektor swasta, dan masyarakat sipil.

Meskipun penelitian Lele (2014) dan Larosa (2019) memberikan landasan kuat dalam memahami ancaman siber dan perang asimetris, terdapat kesenjangan yang perlu dieksplorasi lebih lanjut,. Lele berfokus pada perang siber sebagai bagian dari perang asimetris, sementara Larosa menitikberatkan pada kebijakan keamanan nasional. Namun, keduanya belum secara khusus membahas bagaimana perang siber didefinisikan sebagai perang asimetris dan bagaimana keamanan digital mendukung keamanan nasional.

Penelitian ini menggunakan teori keamanan nasional sebagai grand theory, dengan keamanan digital sebagai aspek pentingnya. Teori peperangan asimetris diposisikan sebagai middle-range theory, yang menjelaskan peran proxy digital dalam unconventional war. Metz dan Johnson (2001) menjelaskan bahwa aktor yang lebih lemah menggunakan strategi tidak konvensional, seperti teknologi dan inovasi, untuk menghadapi kekuatan yang lebih besar.

Sebagai applied theory, digunakan model NIST Cybersecurity Framework, yang dikembangkan oleh National Institute of Standards and

Technology (NIST) di Amerika Serikat. Kerangka ini berfokus pada lima fungsi utama: Identify, Protect, Detect, Respond, dan Recover, yang membantu negara dan organisasi membangun keamanan siber yang tangguh dengan pendekatan kolaboratif antara pemerintah, sektor swasta, dan masyarakat, serta memberikan pedoman untuk menghadapi ancaman siber yang kompleks.

METODE PENELITIAN

Metode penelitian ini menggunakan desain studi kasus kualitatif untuk mendalami strategi dan tantangan keamanan digital dalam konteks perang siber sebagai bentuk peperangan asimetris, dengan perspektif filsafat keamanan digital. Penelitian ini dilakukan dengan langkah-langkah sebagai berikut: pertama, mengumpulkan data sekunder dari literatur yang relevan, termasuk jurnal akademik, laporan pemerintah, dan dokumentasi terkait kebijakan keamanan nasional dan keamanan digital; kedua, analisis data menggunakan pendekatan analisis wacana untuk memahami bagaimana ancaman siber diposisikan dalam diskursus keamanan nasional; dan ketiga, mengeksplorasi studi kasus dari serangan siber yang signifikan untuk menganalisis bagaimana proxy digital digunakan sebagai strategi asimetris. Pendekatan ini diharapkan dapat memberikan wawasan yang mendalam terkait implikasi strategis dan etis dari perang siber terhadap keamanan nasional.

HASIL DAN DISKUSI

1. Pendahuluan

Bab ini menyajikan hasil penelitian mengenai perang siber sebagai bentuk peperangan asimetris dan implikasinya terhadap keamanan digital. Penelitian ini menemukan bahwa perang siber menjadi ancaman signifikan bagi keamanan nasional, terutama ketika aktor non-negara dan pihak dengan keterbatasan sumber daya dapat memanfaatkan teknologi untuk menciptakan dampak signifikan terhadap lawan yang lebih kuat. Dalam konteks ini, perang siber digunakan sebagai alat untuk mengeksploitasi kerentanan infrastruktur kritis, seperti sistem keuangan, energi, dan komunikasi, yang semakin bergantung pada teknologi digital.

Tujuan penelitian ini adalah untuk mengkaji dinamika perang siber sebagai bagian dari peperangan asimetris serta implikasinya terhadap keamanan nasional. Pendekatan yang digunakan dalam analisis ini mencakup teori keamanan nasional sebagai landasan konseptual, dengan fokus pada keamanan digital dan studi kasus serangan siber Korea Utara untuk memberikan gambaran empiris yang relevan.

2. Analisis Berdasarkan Grand Theory: Keamanan Nasional

2.1 Keamanan Nasional dalam Konteks Perang Cyber

Perang siber telah muncul sebagai ancaman signifikan bagi keamanan nasional, khususnya dalam konteks perang asimetris di mana perbedaan sumber daya sangat terlihat. Sebagai bentuk peperangan asimetris, perang siber memungkinkan pihak inferior untuk mengurangi kelemahan mereka dan memberikan dampak strategis terhadap infrastruktur kritis lawan. Dalam konteks ini, keamanan nasional harus beradaptasi untuk melindungi infrastruktur kritis, seperti sistem keuangan, energi, dan komunikasi, yang semakin rentan terhadap serangan siber.

Pendekatan analitis dalam penelitian ini mengacu pada teori yang dikembangkan oleh Professor Dorothy E.

Denning, yang mengidentifikasi ancaman siber sebagai hasil dari tiga faktor utama: niat (intent), kapabilitas (capability), dan kesempatan (opportunity) (Denning, 1999). Dalam penelitian ini, kerentanan yang telah banyak dipublikasikan dalam infrastruktur elektronik AS dianggap sebagai bentuk "kesempatan" yang dapat dimanfaatkan oleh aktor negara maupun non-negara. Niat untuk meluncurkan serangan siber diidentifikasi dari dokumen resmi atau pernyataan publik pemerintah asing terkait adopsi program atau doktrin perang siber. Sementara itu, kapabilitas teknis dan institusional memungkinkan negara-negara, terutama yang memiliki sumber daya besar, untuk meningkatkan efektivitas serangan siber yang diluncurkan.

Serangan siber oleh aktor negara, seperti yang dilakukan Korea Utara terhadap Sony Pictures dan jaringan SWIFT, menunjukkan bahwa serangan tersebut dapat memberikan efek strategis penting jika dilakukan pada skala besar oleh layanan intelijen negara. Analisis ini juga mengungkap bahwa tantangan untuk menilai kapabilitas siber negara tertentu, seperti Korea Utara, sangat besar karena sifat masyarakat tertutup yang membatasi akses informasi. Sumber dari negara rival, seperti Korea Selatan, juga sering kali tidak dapat diandalkan sepenuhnya karena bias dan kesalahan faktual yang disengaja (Denning, 1999; Kuehl, 2000).

2.2 Tantangan dan Implikasi bagi Keamanan Nasional

Tantangan utama dalam menghadapi perang siber adalah kemampuan untuk melakukan atribusi terhadap pelaku serangan. Kesulitan dalam melacak identitas penyerang menjadi hambatan besar dalam memberikan respons yang tepat terhadap ancaman siber. Selain itu, sifat serangan siber yang dapat dilancarkan dari berbagai lokasi dan dengan pola serangan yang beragam membuat upaya pencegahan menjadi semakin kompleks. Negara-negara dengan masyarakat tertutup, seperti Korea Utara, memberikan tantangan khusus bagi para peneliti karena minimnya informasi resmi yang tersedia dan sering kali harus bergantung pada sumber-sumber dari negara rival yang mungkin memiliki bias (Denning, 1999).

Implikasi dari meningkatnya serangan siber adalah pentingnya keamanan digital sebagai komponen utama dalam strategi keamanan nasional. Perang siber, seperti yang terlihat dalam kasus serangan Korea Utara, memperlihatkan bahwa keamanan digital tidak lagi menjadi isu sekunder, melainkan menjadi bagian integral dari pertahanan nasional. Oleh karena itu, penguatan kapasitas pertahanan siber, peningkatan kesadaran digital, dan kolaborasi internasional menjadi langkah penting dalam menjaga stabilitas keamanan nasional di era digital ini.

Bab ini menunjukkan bahwa keamanan nasional harus berkembang sejalan dengan perkembangan teknologi dan ancaman yang ditimbulkan. Pendekatan tradisional dalam mempertahankan kedaulatan negara harus dilengkapi dengan strategi yang efektif dalam menghadapi ancaman siber yang semakin kompleks dan tidak terduga.

3. Analisis Berdasarkan Middle-Range Theory: Peperangan Asimetris

3.1 Perang Siber sebagai Bentuk Peperangan Asimetris

Perang siber merupakan bentuk signifikan dari peperangan asimetris, di mana aktor non-negara memanfaatkan teknologi untuk mengeksploitasi kerentanan negara yang lebih kuat. Hal ini menjadi sangat efektif ketika aktor yang lebih lemah menggunakan taktik yang melemahkan struktur kekuatan tradisional yang terpusat, sehingga

memperoleh keuntungan strategis yang signifikan meskipun keterbatasan sumber daya konvensional mereka (Freedman, 2006; Arquilla & Ronfeldt, 1993). Sifat dunia siber—yang sangat bergantung pada infrastruktur dan sistem yang saling terhubung—menyediakan peluang besar untuk mengganggu jaringan penting, sistem komunikasi, dan infrastruktur vital lainnya (RAND Corporation, 1996). Serangan siber ini bertujuan untuk menciptakan gangguan berskala besar tanpa harus melibatkan konfrontasi militer langsung, menjadikannya cara yang efisien bagi aktor yang lebih lemah untuk menyerang lawan yang lebih kuat.

Perang siber dengan demikian menantang definisi tradisional mengenai perang dan kekuatan seperti yang dikemukakan oleh Clausewitz, yang memandang perang sebagai kelanjutan dari interaksi politik dengan cara lain. Berbeda dengan peperangan konvensional yang mengandalkan kekuatan militer untuk secara fisik menghadapi dan menghancurkan musuh, perang siber melibatkan serangan non-kinetik yang berfokus pada menonaktifkan komponen vital keamanan nasional tanpa secara langsung membahayakan nyawa manusia (Nye, 2011). Hal ini tidak hanya menyetarakan medan pertempuran bagi aktor-aktor asimetris, tetapi juga menyoroti ketidakpastian dan saling ketergantungan dalam keterlibatan militer modern.

3.2 Kehadiran Proxy Digital sebagai Perang Non-Konvensional

Munculnya proxy digital merupakan karakteristik kunci dalam perang siber, yang memposisikan jenis konflik ini sebagai bentuk peperangan non-konvensional. Proxy digital sering kali berupa kelompok atau individu yang tidak secara langsung terafiliasi dengan negara tetapi bertindak untuk kepentingan negara tersebut, menggunakan alat siber untuk mencapai tujuan strategisnya. Hal ini menambah dimensi baru dalam konflik asimetris, di mana batas antara aktor negara dan non-negara menjadi semakin kabur (Dunn Cavealty, 2015). Proxy ini dapat digunakan untuk melancarkan operasi siber, menjaga penyangkalan yang masuk akal bagi negara sponsor, dan mencapai tujuan politik tanpa memicu respons militer langsung.

Keunggulan asimetris dari proxy digital terletak pada kemampuannya untuk beroperasi tanpa kekuatan militer konvensional, namun tetap menciptakan gangguan yang signifikan. Dalam konteks perang siber, negara dapat memanfaatkan aktor non-negara untuk melancarkan serangan terhadap infrastruktur kritis, seperti yang terlihat dalam berbagai insiden global baru-baru ini di mana aktor menargetkan jaringan energi, sistem pemerintahan, dan jaringan komunikasi (Liff, 2013). Sifat non-konvensional dari serangan ini mencerminkan tujuan strategisnya: melemahkan lawan yang lebih kuat dengan menargetkan kerentanan kritis tanpa harus terlibat dalam konfrontasi militer terbuka.

Melalui taktik ini, baik aktor negara maupun non-negara membentuk ulang medan pertempuran modern, yang tidak lagi terbatas pada batas-batas geografis melainkan meluas ke jaringan digital yang dapat diakses dari seluruh penjuru dunia. Peperangan asimetris, termasuk perang siber dan penggunaan proxy digital, telah mengubah dinamika kekuatan, memberi aktor yang lebih lemah kemampuan untuk secara signifikan mempengaruhi hasil dalam hubungan internasional dan keterlibatan militer.

4. Cybercrime dan Perang Cyber sebagai Bentuk Peperangan

Asimetris: Kasus-Kasus Signifikan di Indonesia

Beberapa kasus serangan siber yang signifikan di Indonesia tidak hanya berdampak pada individu dan lembaga tertentu, tetapi juga mencerminkan bagaimana ancaman siber dapat digunakan sebagai taktik dalam perang asimetris. Salah satu kasus besar terjadi pada 15 Juni 2024, ketika Pusat Data Nasional (PDN) diserang oleh kelompok hacker Brain Cipher, yang menggunakan ransomware Lockbit 3.0. Serangan ini menyebabkan kebocoran data dari 230 lembaga publik, termasuk kementerian, dan berlangsung selama beberapa hari sebelum akhirnya dihentikan. Brain Cipher menuntut tebusan sebesar 8 juta USD, namun pemerintah Indonesia menolak untuk bernegosiasi. Serangan ini menyoroti kelemahan infrastruktur digital nasional, terutama dalam aspek identifikasi risiko dan deteksi ancaman.

Sebelumnya, pada Mei 2023, Bank Syariah Indonesia menjadi korban serangan ransomware yang diluncurkan oleh grup hacker Lockbit, yang berhasil mencuri 1,5 terabyte data nasabah dan pegawai. Serangan ini menyebabkan kelumpuhan layanan mobile banking selama lima hari, yang tidak hanya merugikan secara operasional, tetapi juga merusak reputasi bank. Insiden ini menjadi peringatan penting bagi sektor keuangan di Indonesia tentang pentingnya memperkuat proteksi data dan memastikan sistem mampu merespons ancaman dengan lebih cepat.

Pada 2022, hacker yang dikenal dengan nama Bjorka berhasil membobol data dari berbagai institusi, termasuk Kementerian Komunikasi dan Informatika (Kominfo) dan Bank Indonesia. Bjorka mencuri dan menyebarkan data-data pribadi, termasuk data registrasi kartu SIM dan nasabah. Kasus ini memicu kekhawatiran serius tentang lemahnya proteksi privasi di Indonesia, terutama dalam pengelolaan data di sektor pemerintahan.

Pada tahun 2021, situs web Kejaksaan Agung RI diretas oleh hacker Indonesia yang menggunakan nama samaran Gh05t666nero. Serangan ini mengakibatkan pencurian lebih dari tiga juta data pribadi yang kemudian dijual di pasar gelap. Selain mencuri data, peretas juga mengubah tampilan situs dengan pesan protes, menunjukkan bahwa sistem keamanan digital pemerintah masih rentan terhadap serangan. Kasus ini menggarisbawahi kelemahan dalam proteksi digital sektor publik.

Tahun yang sama, Kementerian Kesehatan juga menjadi korban kebocoran data melalui aplikasi Electronic Health Alert (e-HAC), yang mengakibatkan bocornya data kesehatan lebih dari 1,3 juta orang. Data tersebut termasuk informasi terkait tes Covid-19 dan informasi kesehatan pegawai. Insiden ini menunjukkan urgensi peningkatan keamanan dalam pengelolaan data kesehatan, yang bersifat sangat sensitif dan bernilai tinggi di dunia digital.

Salah satu serangan siber yang paling dikenal adalah penyebaran virus WannaCry pada Mei 2017, yang menyerang jaringan komputer di seluruh dunia, termasuk Indonesia. Virus ini mengunci ribuan komputer di sektor pemerintah dan kesehatan, meminta tebusan dalam bentuk Bitcoin. Kasus ini menunjukkan lemahnya pembaruan keamanan sistem operasi di berbagai institusi, yang membuka celah bagi serangan ransomware global ini. Dampaknya tidak hanya menyebabkan kerugian finansial yang besar, tetapi juga menghentikan operasional berbagai lembaga vital selama beberapa waktu.

Kasus-kasus ini memperlihatkan bagaimana ancaman siber tidak hanya menyebabkan kerusakan pada sistem digital, tetapi juga merupakan bagian dari strategi perang asimetris. Dalam era modern, perang tidak selalu

menggunakan kekuatan fisik, tetapi juga melalui serangan digital yang mampu melemahkan infrastruktur nasional, ekonomi, dan keamanan suatu negara.

4.1 Model Keamanan Sibernetika NIST

Model NIST Cybersecurity Framework terdiri dari lima fungsi utama yang saling berkaitan: Identify, Protect, Detect, Respond, dan Recover. Setiap fungsi memberikan pendekatan sistematis dalam meningkatkan keamanan digital dan membangun sistem pertahanan siber yang tangguh, sebagaimana yang diperlukan dalam menghadapi berbagai kasus cybercrime yang telah terjadi di Indonesia.

1. Identify (Mengidentifikasi)

Fungsi ini berfokus pada pengidentifikasian aset, risiko, dan kerentanan yang ada dalam sistem. Dalam kasus Pencurian Data Pusat Data Nasional (PDN) pada tahun 2024, lemahnya identifikasi terhadap ancaman ransomware yang digunakan oleh kelompok hacker Brain Cipher memperlihatkan bagaimana kegagalan mengidentifikasi risiko dapat menyebabkan kebocoran data skala besar. Pendekatan NIST dalam mengidentifikasiaset penting dan kerentanan sistem akan membantu organisasi mencegah akses tidak sah dan memberikan pemetaan yang lebih baik terhadap risiko siber.

2. Protect (Melindungi)

Pada kasus Bank Syariah Indonesia yang terkena serangan ransomware pada 2023, terlihat perlunya perlindungan lebih baik terhadap data nasabah dan infrastruktur digital. Fungsi Protect dalam model NIST menekankan perlunya kontrol akses yang kuat, enkripsi, dan tindakan pencegahan seperti pembaruan sistem secara berkala untuk mengurangi peluang terjadinya serangan. Jika fungsi perlindungan telah diterapkan dengan baik, seperti menggunakan enkripsi data atau segmentasi jaringan, maka pencurian data dalam jumlah besar dapat dihindari.

3. Detect (Mendeteksi)

Deteksi dini terhadap ancaman siber adalah kunci untuk meminimalisir dampak serangan. Pada kasus Kejaksaan Agung RI yang diretas pada 2021, lemahnya sistem deteksi menyebabkan hacker berhasil mencuri jutaan data pribadi sebelum serangan tersebut dapat dihentikan. Dalam kerangka kerja NIST, teknologi pemantauan dan deteksi real-time terhadap aktivitas mencurigakan dapat membantu organisasi mendeteksi potensi ancaman lebih awal dan mengambil langkah mitigasi sebelum kerusakan meluas.

4. Respond (Merespons)

Merespons secara cepat dan efektif terhadap insiden siber adalah salah satu kunci dalam meminimalkan dampak dari serangan. Pada serangan terhadap PDN, meskipun pemerintah menolak untuk bernegosiasi dengan hacker, penanganan dan tanggapan yang cepat akan membantu membatasi kerugian. Fungsi Respond dalam NIST menekankan perlunya memiliki rencana respons insiden yang jelas, dengan tim yang siap menangani situasi darurat dan memitigasi dampak serangan.

5. Recover (Memulihkan)

Setelah serangan siber, memulihkan sistem dan layanan yang terkena dampak adalah langkah penting untuk kembali ke operasi normal. Dalam kasus Bank Syariah Indonesia, lumpuhnya layanan selama lima hari menunjukkan bahwa mekanisme pemulihan yang lebih tangguh perlu diterapkan. Fungsi Recover dalam NIST membantu organisasi merancang

strategi pemulihan yang mencakup backup data secara berkala dan rencana pemulihan bencana untuk memastikan operasi dapat dilanjutkan secepat mungkin setelah serangan.

Dengan mengikuti kelima fungsi dalam NIST Cybersecurity Framework, organisasi dapat memperkuat sistem mereka terhadap ancaman siber yang terus berkembang.

4.2 Kolaborasi Pemerintah, Sektor Swasta, dan Masyarakat

Penerapan NIST Cybersecurity Framework tidak hanya mengandalkan upaya individu dari satu organisasi, tetapi juga memerlukan kolaborasi lintas sektor. Kasus serangan terhadap PDN dan Bank Syariah Indonesia menunjukkan bahwa sektor pemerintah dan swasta sama-sama rentan terhadap ancaman siber, sehingga kolaborasi antara kedua sektor ini menjadi penting.

1. Kolaborasi Pemerintah

Pemerintah memiliki peran penting dalam menetapkan kebijakan dan regulasi keamanan siber. Dalam menghadapi serangan terhadap PDN, pemerintah Indonesia menolak untuk bernegosiasi dengan hacker, menunjukkan sikap tegas dalam menanggapi kejahatan siber. Selain itu, regulasi yang lebih ketat serta upaya peningkatan kesadaran siber di lembaga-lembaga pemerintahan perlu ditingkatkan.

2. Kolaborasi Sektor Swasta

Sektor swasta, seperti perbankan dan layanan kesehatan, juga memegang peran penting dalam memperkuat infrastruktur digital. Kasus Bank Syariah Indonesia dan e-HAC Kemenkes menunjukkan bahwa serangan terhadap lembaga-lembaga ini dapat berdampak pada kepercayaan publik. Penerapan NIST Cybersecurity Framework dalam sektor ini harus melibatkan perencanaan kolaboratif dengan pemerintah dan komunitas keamanan siber, sehingga standar keamanan dapat diterapkan secara merata.

3. Peran Masyarakat

Masyarakat juga perlu lebih sadar akan pentingnya keamanan digital. Pada kasus Bjorka yang berhasil mencuri data pribadi dari beberapa institusi, banyak dari serangan tersebut melibatkan kelemahan pada sisi pengguna, seperti penipuan phishing atau penggunaan kata sandi yang lemah. Edukasi masyarakat mengenai langkah-langkah keamanan dasar, seperti penggunaan kata sandi yang kuat dan waspada terhadap penipuan online, akan membantu mengurangi risiko serangan yang melibatkan faktor manusia.

Kolaborasi antara pemerintah, sektor swasta, dan masyarakat akan menciptakan lingkungan yang lebih siap dalam menghadapi serangan siber, memastikan bahwa protokol keamanan yang diterapkan dapat menangkal ancaman dengan lebih efektif.

4.3 Evaluasi Keberhasilan dan Tantangan Implementasi

Dalam penerapan NIST Cybersecurity Framework di Indonesia, terdapat beberapa keberhasilan yang dapat diidentifikasi, tetapi juga ada tantangan besar yang masih harus diatasi.

1. Keberhasilan

NIST Cybersecurity Framework telah memberikan panduan yang jelas dan terstruktur bagi organisasi di seluruh dunia, termasuk Indonesia, untuk meningkatkan keamanan siber mereka. Implementasi yang berhasil dapat dilihat dari kesadaran yang meningkat di sektor-sektor penting, seperti perbankan dan pemerintah, untuk memperkuat perlindungan data. Meskipun ada insiden seperti pada PDN, tanggapan pemerintah yang tegas menunjukkan pemahaman akan

pentingnya tata kelola keamanan siber yang baik.

2. Tantangan

Tantangan utama dalam penerapan NIST di Indonesia adalah kurangnya infrastruktur teknologi yang memadai dan kesadaran yang masih rendah di banyak organisasi. Kasus kebocoran data di e-HAC Kemenkes dan POLRImenunjukkan bahwa masih banyak lembaga yang belum memiliki sistem deteksi dan respon yang efektif terhadap ancaman siber. Selain itu, kekurangan tenaga ahli keamanan siber di Indonesia juga merupakan hambatan yang signifikan, mengingat meningkatnya frekuensi dan kompleksitas serangan siber.

3. Peran Keamanan Digital dalam Hak Asasi Manusia

Penerapan keamanan siber juga harus memperhatikan keseimbangan antara keamanan dan hak asasi manusia, terutama dalam elindungi privasi individu. Kasus-kasus seperti WannaCry dan pencurian data PDN menunjukkan bagaimana serangan siber dapat mengganggu kehidupan pribadi dan melanggar hak-hak dasar. Oleh karena itu, upaya keamanan tidak boleh dilakukan dengan cara yang mengorbankan privasi individu, dan organisasi harus memastikan bahwa langkah-langkah keamanan yang diambil juga menghormati hak-hak dasar pengguna.

Secara keseluruhan, meskipun NIST Cybersecurity Framework telah membantu banyak organisasi memperkuat sistem keamanan mereka, tantangan dalam hal infrastruktur, tenaga ahli, dan kesadaran akan tetap menjadi fokus utama dalam meningkatkan ketahanan siber di Indonesia.

5. Pembahasan tentang Adaptasi Strategi Keamanan Nasional

5.1 Pendekatan Holistik terhadap Keamanan Nasional

Hasil analisis atas kasus-kasus cybercrime di Indonesia menunjukkan bahwa ancaman siber telah berkembang menjadi ancaman yang signifikan terhadap keamanan nasional. Oleh karena itu, penting bagi pemerintah untuk mengadopsi pendekatan holistik dalam menjaga keamanan nasional, yang mencakup berbagai aspek tidak hanya dari segi teknologi, tetapi juga sosial, ekonomi, dan politik. Pendekatan ini menuntut koordinasi yang erat antara berbagai sektor untuk melindungi infrastruktur vital, seperti sistem keuangan, layanan kesehatan, dan data pemerintah.

Pendekatan holistik mengakui bahwa keamanan siber tidak dapat ditangani secara terpisah atau sektoral. Ancaman yang terus berkembang, seperti pencurian data di Pusat Data Nasional (PDN) atau serangan terhadap Bank Syariah Indonesia, menunjukkan bahwa infrastruktur siber bersifat saling terhubung dan kerentanannya bisa berdampak luas ke berbagai sektor. Oleh karena itu, perlindungan harus dirancang secara sistemik dan inklusif, melibatkan berbagai lapisan masyarakat dan industri, bukan hanya institusi pemerintah.

Selain itu, keamanan nasional tidak hanya soal melindungi aset digital negara, tetapi juga harus menjaga stabilitas sosial dan ekonomi yang semakin bergantung pada teknologi digital. Kasus-kasus besar seperti WannaCry dan pencurian data di Kemenkes mengindikasikan bahwa dampak serangan siber bisa meluas ke kehidupan masyarakat umum, mengganggu layanan penting seperti kesehatan dan keamanan publik. Dengan demikian, pendekatan holistik juga harus mempertimbangkan aspek-aspek

perlindungan data pribadi dan hak asasi manusia dalam upaya meningkatkan keamanan digital nasional.

5.2 Rekomendasi Strategi

Untuk menjaga integritas negara sekaligus menjunjung tinggi nilai-nilai demokrasi dan hak asasi manusia, beberapa rekomendasi strategis perlu dipertimbangkan dalam membangun sistem keamanan digital yang kuat namun inklusif:

1. Penguatan Kerangka Regulasi yang Menyeimbangkan Keamanan dan Privasi

Pemerintah harus memperkuat regulasi siber yang mendukung keamanan nasional tetapi tidak mengorbankan privasi warga negara. Pengalaman dari kasus Bjorka dan Kejaksaan Agung RI menegaskan perlunya perlindungan data pribadi yang lebih baik, tanpa menimbulkan ancaman bagi kebebasan sipil. Regulasi keamanan siber harus dirancang untuk menutup celah keamanan, tetapi tetap sejalan dengan prinsip-prinsip demokrasi dan menghormati hak asasi manusia.

2. Kolaborasi Lintas Sektor: Pemerintah, Sektor Swasta, dan Masyarakat

Serangan siber sering kali menargetkan sektor-sektor penting, seperti Bank Syariah Indonesia dan e-HAC Kemenkes, menunjukkan bahwa kerjasama antara pemerintah, sektor swasta, dan masyarakat sangat penting. Strategi yang direkomendasikan adalah membangun mekanisme kolaborasi yang lebih formal dan terstruktur antara sektor-sektor ini, termasuk berbagi informasi tentang ancaman siber dan praktik terbaik untuk mitigasi risiko. Dengan kolaborasi yang kuat, setiap sektor dapat saling mendukung untuk membangun sistem keamanan digital yang lebih tangguh.

3. Pengembangan Kapasitas Teknologi dan SDM

Tantangan besar dalam keamanan siber di Indonesia adalah keterbatasan infrastruktur teknologi dan kurangnya tenaga ahli keamanan siber. Oleh karena itu, investasi besar dalam pengembangan teknologi keamanan siber, serta pelatihan dan peningkatan kapasitas tenaga kerja di bidang ini, sangat diperlukan. Pemerintah, dengan dukungan sektor swasta, harus berinvestasi dalam pendidikan dan pelatihan keamanan siber, sehingga dapat menutup kesenjangan keahlian yang ada.

4. Membangun Kesadaran Publik tentang Keamanan Siber

Selain memperkuat infrastruktur dan tenaga ahli, penting juga untuk meningkatkan kesadaran masyarakat tentang pentingnya keamanan digital. Sebagai contoh, banyak serangan seperti phishing yang melibatkan kelemahan dari sisi pengguna, sehingga masyarakat perlu diberikan edukasi tentang cara melindungi diri dari ancaman siber. Kampanye kesadaran keamanan siber, yang melibatkan sektor publik dan swasta, harus ditingkatkan untuk menciptakan budaya keamanan digital yang lebih kuat di seluruh lapisan masyarakat.

Dengan mengadopsi strategi-strategi ini, Indonesia dapat membangun sistem keamanan digital yang kuat, tangguh, dan inklusif, yang melindungi integritas negara sekaligus menjaga nilai-nilai demokrasi dan hak asasi manusia. Kolaborasi lintas sektor dan edukasi publik merupakan elemen kunci dalam menciptakan ekosistem keamanan digital yang berkelanjutan dan adaptif terhadap ancaman siber yang terus berkembang.

KESIMPULAN

Perang siber telah menjadi ancaman signifikan terhadap keamanan nasional, terutama melalui taktik

asimetris yang memungkinkan aktor non-negara maupun negara lemah untuk mengeksploitasi kerentanan infrastruktur kritis. Penerapan NIST Cybersecurity Framework menjadi langkah penting dalam membangun sistem keamanan digital yang tangguh, dengan fungsi-fungsi utama seperti Identify, Protect, Detect, Respond, dan Recover. Namun, keberhasilan strategi keamanan siber memerlukan pendekatan holistik yang melibatkan kolaborasi erat antara pemerintah, sektor swasta, dan masyarakat, serta harus tetap menjunjung tinggi hak asasi manusia. Dengan penguatan regulasi, peningkatan kapasitas teknologi dan SDM, serta kesadaran masyarakat, Indonesia dapat membangun sistem keamanan digital yang lebih inklusif dan berkelanjutan di tengah meningkatnya ancaman siber.

DAFTAR PUSTAKA

Buku

Brown, H. (1983). Technology, Military Equipment, and National Security. The US Army War College Quarterly: Parameters, 13(1), 3

Clausewitz, C. (1984). On War. "An act of violence intended to compel our opponent to fulfil our will." Princeton University Press.

Denning, D. E. (1999). Information Warfare and Security. Addison-Wesley.

Freedman, L. (2006). The Transformation of Strategic Affairs. Routledge.

Kim, P., & Solomon, M. (2018). Digital security and ethical implications in the age of cyber warfare. Oxford University Press.

Nye, J. S. (2011). The Future of Power. PublicAffairs.

Susanto, H. (2011). Pertahanan siber dan tantangan nasional dalam era digital. Bandung: ITB Press.

Jurnal

Dunn Cavelty, M. (2015). Cybersecurity in the national security discourse: The case of the United States. International Studies Review, 17(2), 191–209. https://doi.org/10.1111/misr.12232

Turner, H. (1982). Britain, the United States and scandinavian security problems 1945-1949. University of Aberdeen (United Kingdom).

Lele, A. (2014). Asymmetric warfare in the contemporary strategic environment. Defence Studies Journal, 10(2), 123-145.

Lele, A. (2014). Asymmetric Warfare: A State vs Non-State Conflict. OASIS, (20), 97-111.

Liff, A. P. (2013). Cyberwar: A new "absolute weapon"? The proliferation of cyberwarfare capabilities and interstate war. Journal of Strategic Studies, 36(1), 33–62. https://doi.org/10.1080/01402390.2012.742014

Raharjo, D. (2017). Partisipasi masyarakat dalam keamanan digital: Perspektif etika dan keamanan. Jurnal Teknologi Informasi dan Komunikasi, 12(3), 221-236.

Dokumen Resmi/Undang-Undang

Khan, A. A. (2005). Asymmetric warfare: A theory for fighting complex threats. War College Research Papers.

McKenzie, K. (2000). Types of asymmetric warfare. [Publication details unavailable].

RAND Corporation. (1996). The Advent of Netwar (Revisited). RAND Corporation. Retrieved from https://www.rand.org/pubs/monograph_reports/MR1382.html

Sumber Daring

Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is Coming!. RAND Corporation. Retrieved from https://www.rand.org/pubs/reports/R3991.html

Kompas. (2024). "Brain Cipher Telah Berikan Kunci Enkripsi Ransomware PDN, Apakah Sudah Bisa Dipakai?". Kompas. Retrieved from https://www.kompas.com/tren/read/2024/07/04/121500065/brain-cipher-telah-berikan-kunci-enkripsi-ransomware-pdn-apakah-sudah-bisa?page=all

Kompas.com. (2024). Serangan hacker Brain Cipher terhadap Pusat Data Nasional

Indonesia. Kompas. Retrieved from https://www.kompas.com

Kuehl, D. (2000). The Information Revolution and the Transformation of Warfare. Parameters, 30(3), 30–39.