Jurnal Strategi Pertahanan Udara
Volume 11 Nomor 1, 2025 E-ISSN 2830-3490

PENINGKATAN KEMAMPUAN *CYBER ESPIONAGE* DALAM MENGHADAPI ANCAMAN SIBER DI LINGKUNGAN TNI

(ANALYSIS OF ORGANIZATIONAL AND HUMAN RESOURCE POLICIES IN STRENGTHENING THE CYBER INTELLIGENCE CAPABILITIES OF THE INDONESIAN AIR FORCE)

[1]Auriawan Wisnu Broto, [2]Rudy A.G. Gultom, [3]Sigit Purwanto
wiznoe.leo1@gmail.com

Abstrak. Ancaman siber, khususnya cyber espionage, menjadi salah satu tantangan besar yang dihadapi berbagai sektor di Indonesia, termasuk sektor pertahanan. Bagi Tentara Nasional Indonesia (TNI), ancaman ini dapat menyerang sistem komunikasi, intelijen, serta infrastruktur militer yang berpotensi mengancam kedaulatan negara. Cyber espionage biasanya melibatkan aktivitas peretasan dan pengumpulan informasi strategis secara ilegal melalui serangan siber. Oleh sebab itu, peningkatan kemampuan TNI dalam menghadapi ancaman tersebut sangat krusial untuk menjaga kerahasiaan dan keutuhan data strategis negara. Penelitian ini bertujuan untuk menganalisis langkah-langkah penguatan kemampuan menghadapi cyber espionage di lingkungan TNI serta mengidentifikasi strategi yang diperlukan untuk meningkatkan kesiapsiagaan dan ketahanan sistem pertahanan nasional terhadap ancaman siber. Metode yang digunakan mencakup studi literatur, analisis kebijakan, dan wawancara dengan para ahli di bidang keamanan siber. Hasil penelitian menunjukkan bahwa TNI perlu memperkuat sistem pertahanan sibernya melalui peningkatan kapasitas personel, pelatihan yang berkelanjutan, serta pemanfaatan teknologi modern dalam deteksi dan penanggulangan serangan siber. Selain itu, kerja sama dengan lembaga keamanan siber baik di tingkat nasional maupun internasional menjadi faktor penting untuk menciptakan sistem pertahanan yang lebih tangguh, adaptif, dan responsif terhadap ancaman yang terus berkembang. Penelitian ini diharapkan dapat memberikan kontribusi nyata terhadap pengembangan kebijakan dan strategi pertahanan siber yang lebih efektif di lingkungan TNI guna menjaga keamanan dan stabilitas nasional di tengah eskalasi ancaman cyber espionage yang semakin kompleks.

Kata kunci: Ancaman *cyber*, *Cyber espionage*, TNI

Abstract. *Cyber threats, particularly cyber espionage, pose a significant challenge to various sectors in Indonesia, including the defense sector. For the Indonesian National Army (TNI), these threats encompass potential attacks on communication networks, intelligence systems, and military infrastructure, all of which can endanger national sovereignty. Cyber espionage typically involves the unauthorized acquisition of sensitive information through targeted cyberattacks on strategic national data. Consequently, enhancing the TNI's capability to counter such threats is crucial to safeguarding the confidentiality and integrity of vital state information. This study aims to examine efforts to strengthen the TNI's cyber espionage defense capabilities and to identify measures necessary to improve the preparedness and resilience of Indonesia's defense systems against cyber threats. Employing a methodology that includes literature review, policy analysis, and interviews with cybersecurity experts, the research reveals that the TNI must build greater capacity by reinforcing its cyber defense infrastructure, conducting personnel training, and adopting advanced technologies for cyber threat detection and response. Furthermore, cooperation with both national and international cybersecurity institutions is essential to establish a more adaptive and responsive cyber defense system. Overall, this research contributes to the formulation of more effective cyber defense policies and strategies within the TNI to ensure national security and stability in the face of increasingly sophisticated cyber espionage activities.*

Keywords: *Cyber espionage, Cyber Threat,* TNI

1. Pendahuluan

Indonesia sebagai suatu negara yang memiliki cita-cita untuk hidup bersama dengan rakyatnya dan memiliki sistem pemerintahan yang berdaulat, maka Indonesia harus mampu mewujudkannya melalui kekuasaan yang dimiliki yaitu kedaulatan sehingga dalam melaksanakan jalannya pemerintahan suatu negara dapat terlaksana melalui pemerintahan yang berdaulat (Asshidiqie, 1994). Hal tersebut melalui kekuasaan yang dimiliki oleh Indonesia berupa kedaulatan, maka untuk menghadapai persaingan global bisa menggunakannya sebagai bentuk proteksi diri dari ancaman/serangan luar yang dapat mengancam pertahanan dan keamanan Negara. Ancaman yang hadir selalu semakin kompleks sesuai perkembangan teknologi digital.

Peningkatan kasus kejahatan siber (cyber crime) dipengaruhi oleh berbagai faktor, seperti anonimitas di ruang digital, kemajuan teknologi yang mempermudah aksi kejahatan, kesenjangan sosial yang mendorong individu melakukan tindak kriminal, serta motif keuntungan finansial yang tinggi. Faktor-faktor tersebut memberikan dampak signifikan terhadap stabilitas keamanan nasional. Di sisi lain, upaya penegakan

hukum terhadap kejahatan siber masih menghadapi hambatan akibat keterbatasan sumber daya dan kemampuan teknologi di lembaga penegak hukum. Ancaman siber kini menjadi isu serius yang memengaruhi berbagai sektor, termasuk sektor pertahanan. Bagi Tentara Nasional Indonesia (TNI), Ancaman ini tidak hanya datang dari individu atau kelompok tertentu, tetapi juga dari negara-negara yang memiliki kapasitas untuk melakukan serangan siber secara terencana dan terorganisir. Serangan semacam ini dapat menargetkan sistem komunikasi, jaringan intelijen, dan infrastruktur vital yang menopang operasi militer. Oleh karena itu, TNI perlu meningkatkan kapasitasnya dalam menghadapi ancaman tersebut, Salah satunya dengan memperkuat kapasitas di bidang *cyber espionage* sebagai elemen penting dalam strategi pertahanan siber nasional.

Cyber espionage Merupakan salah satu jenis ancaman siber yang dilakukan dengan cara mengakses dan mengumpulkan data atau informasi secara tidak sah dari sistem komputer atau jaringan tanpa izin. Dalam konteks militer, *Cyber espionage* sering digunakan oleh pihak asing untuk memperoleh informasi strategis yang berkaitan dengan doktrin, strategi, serta teknologi militer yang dimiliki. Untuk itu, peningkatan kemampuan TNI dalam menghadapi ancaman ini sangat penting agar dapat menjaga kerahasiaan informasi yang bersifat vital dan mengurangi potensi kerugian akibat kebocoran informasi.

Sebagai komponen utama pertahanan nasional, TNI dituntut memiliki kemampuan untuk mendeteksi, mengidentifikasi, dan menanggulangi serangan siber, khususnya yang bertujuan mencuri data dan informasi strategis. Upaya ini mencakup penguatan sistem keamanan siber, peningkatan kompetensi personel melalui pelatihan, serta pemanfaatan teknologi mutakhir guna memperkuat kemampuan deteksi dan penanganan ancaman siber. Langkah-langkah tersebut tidak hanya berfokus pada aspek teknis, tetapi juga mencakup penyusunan kebijakan dan prosedur yang mendukung pelaksanaan operasi keamanan siber di lingkungan militer. Peningkatan kapasitas dalam bidang spionase siber menjadi bagian penting dari strategi pertahanan siber yang terpadu dan berkelanjutan. Seiring perkembangan teknologi yang pesat, bentuk serangan siber semakin canggih dan sulit dideteksi, sehingga diperlukan sistem yang

lebih adaptif dan tanggap dalam menghadapi berbagai ancaman. Salah satu faktor kunci dalam memperkuat ketahanan siber TNI adalah memperluas kerja sama dengan berbagai lembaga, baik di tingkat nasional maupun internasional, guna meningkatkan pertukaran informasi dan pengalaman dalam menghadapi ancaman siber yang terus berkembang.

Melalui peningkatan kemampuan *Cyber espionage*, Tentara Nasional Indonesia (TNI) diharapkan dapat meningkatkan kesiapsiagaan dan ketahanan sistem pertahanan negara dalam menghadapi ancaman siber. Lebih lanjut, hal ini merupakan langkah krusial dalam menjaga kedaulatan negara di dunia siber dan memastikan sistem pertahanan dan keamanan negara tetap beroperasi secara aman dan efektif meskipun serangan siber semakin canggih. Berdasarkan perbandingan dengan penelitian sebelumnya, para peneliti menyimpulkan bahwa belum ada penelitian yang dilakukan untuk meningkatkan kapabilitas Tentara Nasional Indonesia (TNI). *cyber security* dalam mendukung tugas TNI Angkatan Udara di era digital, berdasarkan hal tersebut dirasa perlu untuk melaksanakan penelitian ini dengan judul "Peningkatan Kemampuan *Cyber espionage* dalam menghadapi ancaman siber di lingkungan TNI".

2. Tinjauan Pustaka

a. Teori Keamanan Nasional.

Menurut Alan Collins (2005), keamanan nasional merupakan kebutuhan fundamental untuk menjamin kelangsungan hidup suatu negara melalui pemanfaatan kekuatan ekonomi, militer, dan politik serta pelaksanaan diplomasi yang efektif. Dalam konteks persaingan global, keamanan nasional suatu negara, terutama yang memiliki sumber daya besar, sangat bergantung pada penerapan langkah teknis dan operasional yang tepat, termasuk perlindungan terhadap informasi rahasia, sistem persenjataan militer, dan strategi diplomasi antarnegara. Konsep keamanan nasional mencakup lima bidang utama, yaitu militer, politik, ekonomi, sosial, dan lingkungan, di mana sektor militer tetap penting namun bukan satu-satunya faktor penentu. Seiring berkembangnya dinamika hubungan internasional, ancaman terhadap keamanan negara tidak lagi

terbatas pada aspek militer, melainkan juga meluas ke bidang ekonomi, politik, hukum, sosial budaya, ideologi, demografi, serta pengelolaan sumber daya alam. Bagi Indonesia, sebagai negara kepulauan dengan posisi geografis yang strategis, tantangan menjaga kedaulatan dan keutuhan wilayah menjadi semakin kompleks, meliputi isu seperti konflik perbatasan, separatisme, terorisme, penyalahgunaan narkoba, dan kejahatan transnasional. Di era modern, ancaman juga muncul dalam bentuk serangan siber, propaganda digital, serta perang informasi yang berpotensi menggoyahkan stabilitas nasional. Selain itu, kemajuan teknologi menghadirkan tantangan baru dalam bidang pertahanan, seperti penggunaan drone, sistem persenjataan otomatis, dan peperangan berbasis kecerdasan buatan (AI). Oleh karena itu, strategi pertahanan nasional harus beradaptasi dengan memperkuat ketahanan siber, penguasaan teknologi, serta kolaborasi lintas sektor untuk memastikan keamanan negara yang berkelanjutan dan komprehensif informasi. Indonesia menghadapi berbagai ancaman yang bersifat kompleks dan dinamis. Beberapa tantangan utama yang dihadapi antara lain:

1) Konflik Perbatasan. Perselisihan wilayah dengan negara-negara tetangga masih menjadi tantangan yang memerlukan pendekatan diplomasi dan pertahanan yang seimbang.

2) Separatisme di Papua. Perkembangan gerakan separatis menuntut adanya strategi pertahanan yang tidak semata-mata berfokus pada kekuatan militer, melainkan juga mencakup upaya pembangunan di bidang sosial dan ekonomi.

3) Kejahatan Siber. Peningkatan serangan siber berpotensi mengancam keamanan informasi negara, sehingga diperlukan sistem pertahanan siber yang tangguh dan terintegrasi.

4) Ketegangan di Laut Cina Selatan. Konflik geopolitik di kawasan ini berpotensi berdampak pada stabilitas Indonesia, sehingga diperlukan kebijakan luar negeri dan pertahanan yang adaptif.

5) Terorisme dan Radikalisme. Perkembangan ideologi ekstrem yang mengancam persatuan nasional menuntut adanya kebijakan pencegahan yang efektif.

b. Teori *Cyber Crime* Menurut Aep S. Hamidin (2010).

Menurut Aep S. Hamidin "Tips dan Trik Penggunaan Kartu Kredit: Maksimalkan Manfaat dan Mengelola Risiko Kartu Kredit" (2010): berdasarkan jenis kegiatannya, *cyber crime* dapat dibagi menjadi beberapa jenis, yaitu:

1) Unauthorized access merupakan jenis kejahatan siber yang terjadi ketika seseorang memperoleh akses ilegal atau tidak sah ke sistem atau jaringan komputer. Contohnya termasuk pemindaian port dan peretasan Contohnya tindakan *probing* dan *port*.

2) *Illegal contents* merupakan tindakan mengirimkan data atau informasi yang tidak benar, cabul, dan mungkin ilegal melalui internet. Misalnya, mendistribusikan materi pornografi.

3) *Cyber espionage*, *sabotage and extortion* dalam kejahatan siber, *Cyber espionage* merupakan bentuk kejahatan siber. *Cyber espionage* dilakukan dilakukan dengan menggunakan internet untuk memata-matai atau menguping orang lain. Di sisi lain, sabotase dan pemerasan melibatkan gangguan atau kerusakan data, program, atau sistem jaringan komputer. Misalnya, spionase rahasia dagang dan kerusakan sistem jaringan yang digunakan untuk menyimpan rahasia tersebut.

c. Teori *Hybrid Warfare*.

Perang hibrida (*Hybrid Warfare*) merupakan strategi militer yang menggabungkan berbagai bentuk peperangan, baik konvensional maupun non-konvensional, serta ancaman dalam bentuk *cyber warfare*. Menurut Hoffman (2007), strategi ini melibatkan penggunaan senjata kimia, biologi, radiologi, nuklir, dan alat

peledak improvisasi (CBRNE), serta mencakup dimensi perang informasi dan teknologi siber. Bentuk peperangan ini mencerminkan karakter konflik modern yang fleksibel dan adaptif, di mana kekuatan konvensional digunakan ketika kondisi mendukung untuk mengalahkan musuh, sedangkan ketika situasi tidak menguntungkan, strategi alternatif seperti operasi siber, disinformasi, dan perang asimetris diterapkan untuk melemahkan lawan tanpa konfrontasi langsung. Secara umum langkah-langkah yang terlibat dalam strategi intelijen dalam hybrid warfare biasanya meliputi:

1) Pengumpulan informasi. Mengumpulkan informasi dari berbagai sumber, termasuk agen manusia, komunikasi yang disadap, citra satelit, platform online dan media sosial.

2) Analisis informasi. Menilai dan memproses informasi yang dikumpulkan untuk mengekstrak wawasan berharga, mengidentifikasi pola dan menentukan tindakan potensial.

3) Diseminasi. Berbagi intelijen yang dianalisis dengan pembuat keputusan, komandan militer dan pemangku kepentingan terkait lainnya untuk menginformasikan strategi dan tindakan mereka.

4) Eksploitasi. Memanfaatkan kecerdasan yang dikumpulkan untuk mengeksploitasi kerentanan, memanipulasi persepsi dan memengaruhi proses pengambilan keputusan musuh. Ini mungkin melibatkan serangan dunia maya, kampanye disinformasi, propaganda atau operasi rahasia.

5) Kontra Intelijen. Menerapkan langkah-langkah untuk melindungi kemampuan intelijen sendiri, mengidentifikasi dan menetralisir aktivitas intelijen yang bermusuhan dan melawan potensi ancaman atau upaya untuk mengeksploitasi kerentanan.

3. Metode Penelitian

Penelitian ini bertujuan untuk menganalisis peningkatan kemampuan dalam menghadapi ancaman *Cyber espionage* di lingkungan Tentara Nasional Indonesia (TNI). Metodologi yang digunakan dalam penelitian ini menggabungkan pendekatan kualitatif dengan analisis dokumen dan kajian literatur. Pendekatan ini dilakukan untuk menggali pemahaman yang mendalam mengenai ancaman *Cyber espionage* yang dihadapi oleh TNI serta bagaimana strategi dan upaya peningkatan kemampuan dalam menghadapi ancaman tersebut.

a. Studi Literatur. Studi literatur mengenai *Cyber espionage*, yang mencakup pemahaman dasar tentang definisi, dampak, serta contoh-contoh serangan *Cyber espionage* yang telah terjadi, baik di Indonesia maupun di negara lain. Data dikumpulkan dari berbagai sumber seperti jurnal, artikel, laporan penelitian, serta dokumen-dokumen resmi yang berkaitan dengan pertahanan siber dan keamanan informasi di Indonesia, khususnya yang berfokus pada TNI.
b. Analisis Kebijakan dan Strategi. Analisis dilakukan terhadap kebijakan-kebijakan yang ada di Indonesia, seperti Undang-Undang Informasi dan Transaksi Elektronik (ITE), serta regulasi yang mengatur pertahanan dan keamanan nasional yang relevan dengan *Cyber espionage*. Analisis ini bertujuan untuk memahami sejauh mana regulasi dan kebijakan yang ada dapat mengakomodasi dan menangani ancaman siber, terutama yang terkait dengan espionase siber.
c. Wawancara dengan Narasumber Terkait. Penelitian ini juga melibatkan wawancara dengan para ahli dan praktisi di bidang keamanan siber guna memperoleh pandangan serta rekomendasi mengenai langkah-langkah yang dapat dilakukan TNI dalam meningkatkan kemampuan menghadapi ancaman *cyber espionage*. Wawancara tersebut dilakukan dengan personel TNI yang berperan dalam pengelolaan keamanan informasi dan pertahanan siber, serta dengan pihak-pihak terkait yang berkontribusi dalam pengembangan kebijakan siber di Indonesia.

d. Evaluasi dan Rekomendasi. Berdasarkan analisis yang dilakukan, evaluasi terhadap kapasitas dan kesiapan TNI dalam menghadapi ancaman siber akan dilakukan. Peneliti akan mengidentifikasi faktor-faktor yang dapat meningkatkan efektivitas pertahanan siber, termasuk pelatihan personel, peningkatan teknologi, serta penguatan kolaborasi dengan lembaga-lembaga terkait. Rekomendasi yang diberikan akan berfokus pada strategi peningkatan kemampuan dalam menghadapi ancaman *Cyber espionage* di lingkungan TNI.

4. Hasil dan Diskusi

a. Kemampuan dan Kompetensi *Cyber espionage* Prajurit TNI Serta Upaya Peningkatannya Dalam Menghadapi Ancaman Siber. Kemampuan dan keahlian spionase siber personel Tentara Nasional Indonesia (TNI) dalam menangkal ancaman siber memerlukan pelatihan komprehensif untuk mengantisipasi, mendeteksi, dan merespons ancaman yang ada. Spionase siber adalah pengumpulan informasi ilegal melalui serangan siber yang dapat mengancam stabilitas dan keamanan nasional. Oleh karena itu, TNI sebagai salah satu lembaga yang bertanggung jawab atas pertahanan negara, harus memiliki keahlian dan kapasitas untuk mengatasi ancaman siber, khususnya yang berkaitan dengan spionase siber. Berikut adalah beberapa kemampuan dan kompetensi *Cyber espionage* prajurit TNI:

1) Pengetahuan tentang keamanan siber. Prajurit TNI perlu memiliki pengetahuan dasar dan lanjutan mengenai aspek keamanan siber, termasuk pengenalan terhadap berbagai jenis serangan siber seperti *malware, phishing*, DDoS (*Distributed Denial of Service*), dan teknik *spionase* digital lainnya. Pengetahuan ini diperlukan untuk mengidentifikasi potensi ancaman dan cara-cara pencegahan yang tepat.

2) Kemampuan untuk mendeteksi serangan siber. Prajurit yang terlibat dalam pertahanan siber harus memiliki kemampuan untuk mendeteksi serangan

siber, baik yang dilakukan oleh individu maupun kelompok yang berusaha mengakses data sensitif secara ilegal. Kemampuan untuk menggunakan perangkat lunak deteksi ancaman dan sistem pemantauan jaringan akan menjadi bagian penting dari kompetensi mereka.

3) Keterampilan analisis forensik digital. Untuk menangani kasus *Cyber espionage*, prajurit TNI harus terampil dalam *digital forensics* untuk melacak, mengidentifikasi, dan mengumpulkan bukti dari serangan yang terjadi. Ini termasuk pemahaman tentang bagaimana serangan dilakukan, serta bagaimana mengamankan dan mengolah data yang didapatkan secara legal.

4) Kemampuan dalam mengelola infrastruktur keamanan siber. Prajurit TNI yang terlibat dalam pertahanan siber harus mampu mengelola dan melindungi infrastruktur teknologi informasi yang ada. Hal ini termasuk pengelolaan *firewall*, enkripsi data, pemantauan lalu lintas jaringan, serta pengamanan terhadap perangkat keras dan perangkat lunak yang digunakan dalam sistem militer.

5) Kemampuan dalam menyusun strategi pertahanan siber. Selain kemampuan teknis, prajurit TNI harus memiliki kemampuan dalam merancang dan menerapkan strategi pertahanan siber yang efektif. Ini mencakup pengembangan prosedur untuk mencegah kebocoran data, merancang sistem pertahanan untuk mengatasi serangan, serta menyiapkan rencana tanggap darurat yang cepat dan efektif.

Sedangkan beberapa upaya peningkatan kemampuan *Cyber espionage* TNI yang dapat dilaksanakan adalah sebagai berikut:

1) Pelatihan dan pendidikan keamanan siber. Salah satu upaya utama dalam meningkatkan kemampuan prajurit TNI dalam menghadapi *Cyber espionage* adalah dengan memberikan pelatihan dan pendidikan yang intensif mengenai ancaman dan taktik siber yang sedang berkembang. Pelatihan ini tidak hanya

melibatkan teori, tetapi juga praktek langsung dalam mengidentifikasi dan merespons ancaman, serta cara-cara melindungi data penting.

2) Program pelatihan ini bisa mencakup kursus khusus mengenai analisis forensik, pengelolaan sistem keamanan informasi, serta teknik untuk mengatasi serangan dari musuh yang berusaha mencuri data strategis.

3) Pengembangan infrastruktur keamanan siber. TNI harus terus mengembangkan dan memperkuat infrastruktur siber yang ada, dengan investasi dalam perangkat keras dan perangkat lunak yang dapat mendeteksi dan mengatasi *Cyber espionage* secara *real-time*. Peningkatan ini mencakup sistem enkripsi yang kuat, penguatan sistem deteksi intrusi, dan peningkatan kemampuan *firewall* untuk mencegah akses ilegal ke data-data sensitif.

4) Kolaborasi dengan Lembaga Keamanan Siber Nasional. Untuk memperkuat kemampuan dalam menghadapi ancaman *Cyber espionage*, TNI perlu menjalin kerja sama dengan lembaga-lembaga nasional yang menangani keamanan siber, seperti Badan Siber dan Sandi Negara (BSSN) serta lembaga intelijen. Kolaborasi ini bertujuan untuk berbagi informasi mengenai potensi ancaman dan membangun sistem pertahanan yang terintegrasi.

5) Pengembangan keahlian melalui simulasi dan latihan bersama. Latihan simulasi serangan siber dan latihan bersama antara unit-unit TNI, pemerintah, serta sektor swasta yang terlibat dalam pertahanan siber dapat meningkatkan kesiapan dan respons prajurit TNI terhadap ancaman. Simulasi serangan siber yang realistis, termasuk serangan *Cyber espionage*, memungkinkan prajurit TNI untuk menghadapi skenario dunia nyata dan mengembangkan strategi efektif dalam merespons ancaman tersebut.

6) Pembentukan satuan khusus pertahanan siber. TNI bisa membentuk satuan khusus yang memiliki fokus utama dalam pertahanan siber, yang bertanggung jawab untuk memantau ancaman siber secara intensif, serta

bertindak sebagai garda terdepan dalam melawan dan mencegah *Cyber espionage*. Satuan ini juga dapat berfungsi sebagai pusat informasi dan koordinasi dalam setiap upaya mitigasi ancaman.

7) Penyusunan dan peningkatan kebijakan pertahanan siber. TNI perlu terus meninjau dan memperbarui kebijakan serta prosedur yang ada terkait dengan pertahanan siber, termasuk strategi pertahanan terhadap *Cyber espionage*. Kebijakan ini harus mencakup pencegahan, respons, dan pemulihan setelah serangan siber, serta peningkatan kesadaran di kalangan personel mengenai pentingnya menjaga kerahasiaan data.

8) Mengadaptasi teknologi baru. TNI harus beradaptasi dengan perkembangan teknologi terkini, seperti kecerdasan buatan (AI), *big data*, dan *blockchain*, untuk meningkatkan kemampuan deteksi ancaman dan memperkuat sistem pertahanan siber. Teknologi-teknologi ini dapat membantu prajurit TNI dalam memantau dan menganalisis ancaman secara lebih cepat dan akurat.

b. Ketersediaan Teknologi Pendukung *Cyber espionage* Serta Upaya Peningkatannya Dalam Menghadapi Ancaman Siber di Lingkungan TNI.

Ketersediaan teknologi pendukung dalam menghadapi ancaman *Cyber espionage* di lingkungan Tentara Nasional Indonesia (TNI) sangat penting untuk membangun sistem pertahanan siber yang tangguh. Teknologi ini bertujuan untuk mendeteksi, menganalisis, dan merespons ancaman dengan efektif, serta melindungi data dan sistem kritis dari akses tidak sah. Dalam menghadapi ancaman *Cyber espionage*, TNI memerlukan berbagai jenis teknologi, baik perangkat keras maupun perangkat lunak, yang dapat mendukung upaya pertahanan siber. Beberapa teknologi pendukung *Cyber espionage* di lingkungan TNI yang harus tersedia antara lain:

1) Sistem keamanan jaringan dan infrastruktur teknologi informasi. Untuk mendeteksi dan melawan serangan *Cyber espionage*, TNI membutuhkan sistem deteksi intrusi yang mampu mengidentifikasi serangan sejak dini. Sistem ini berfungsi untuk memantau lalu lintas jaringan secara *real-time* dan mendeteksi adanya aktivitas mencurigakan yang berpotensi menjadi serangan siber. Selain itu, *firewall* canggih dan sistem enkripsi data juga diperlukan untuk mengamankan data dari akses ilegal.

2) Perangkat lunak forensik digital. Teknologi pendukung lainnya adalah perangkat lunak forensik digital, yang digunakan untuk menganalisis bukti-bukti yang dikumpulkan dari serangan siber. Alat ini membantu dalam rekonstruksi kejadian serangan *Cyber espionage* dan mengidentifikasi teknik yang digunakan oleh pelaku. Teknologi ini juga penting dalam proses investigasi untuk menemukan jejak pelaku serangan dan mengumpulkan bukti yang sah untuk keperluan hukum.

3) Sistem pemantauan dan pengelolaan risiko. TNI juga membutuhkan sistem pemantauan keamanan siber yang dapat memberikan gambaran secara menyeluruh tentang ancaman siber yang sedang berkembang. Sistem ini harus mampu mengidentifikasi potensi kerentanannya dan memberikan rekomendasi mengenai langkah-langkah mitigasi yang perlu diambil. Selain itu, TNI perlu memiliki platform manajemen risiko siber untuk menganalisis dan mengelola potensi ancaman di berbagai level.

4) Perangkat keras keamanan siber. Selain perangkat lunak, perangkat keras yang mendukung pertahanan siber juga sangat penting, seperti server yang dilengkapi dengan proteksi tinggi, perangkat *virtual private network* (VPN), serta appliance keamanan lainnya untuk memantau, mengontrol, dan melindungi sistem jaringan dari serangan siber yang menargetkan infrastruktur fisik atau data.

5) Sistem deteksi *malware* dan analisis ancaman. Teknologi pendukung lainnya adalah sistem deteksi *malware*, yang berfungsi untuk mengidentifikasi dan memblokir perangkat lunak berbahaya yang digunakan dalam serangan *Cyber espionage*. Teknologi ini termasuk dalam antivirus canggih yang dapat mendeteksi file berbahaya, *keylogger*, atau alat lainnya yang digunakan oleh pelaku *spionase* untuk mencuri informasi.

6) Teknologi pengelolaan data dan keamanan *cloud*. Dalam era moderen ini, banyak data penting TNI yang disimpan di *cloud computing* atau infrastruktur berbasis *cloud*. Oleh karena itu, TNI membutuhkan teknologi pengelolaan data dan keamanan cloud yang handal, untuk memastikan bahwa data yang disimpan di *cloud* terlindungi dari ancaman *Cyber espionage*. Teknologi ini harus mencakup enkripsi data dan mekanisme *multi-factor authentication* untuk melindungi akses terhadap data sensitif.

Sedangkan beberapa upaya peningkatan teknologi pendukung dalam menghadapi ancaman siber di Lingkungan TNI adalah sebagai berikut :

1) Investasi dalam pengembangan infrastruktur keamanan siber. Upaya pertama yang perlu dilakukan adalah investasi dalam pengembangan infrastruktur keamanan siber. Hal ini mencakup pembelian perangkat keras dan perangkat lunak terbaru yang mampu melindungi data dan sistem TNI dari ancaman siber, serta memperkuat sistem pemantauan dan deteksi intrusi yang lebih canggih. TNI perlu melakukan pembaruan secara berkala pada perangkat keras dan perangkat lunak untuk mengikuti perkembangan ancaman siber yang terus berubah.

2) Penguatan pelatihan dan pendidikan keamanan siber. Teknologi saja tidak cukup tanpa adanya kompetensi sumber daya manusia yang memadai. Oleh karena itu, TNI harus memperkuat program pelatihan dan pendidikan untuk personel yang terlibat dalam pertahanan siber. Pelatihan ini meliputi

penggunaan perangkat keamanan terbaru, analisis forensik digital, serta strategi mitigasi ancaman siber yang melibatkan teknologi terkini.

3) Kolaborasi dengan lembaga keamanan siber internasional. Untuk meningkatkan kapasitas teknologi dalam menghadapi *Cyber espionage*, TNI perlu memperluas kolaborasi dengan lembaga-lembaga keamanan siber internasional, seperti Badan Siber dan Sandi Negara (BSSN), serta organisasi internasional lainnya yang memiliki pengalaman dalam menangani ancaman siber. Kolaborasi ini bertujuan untuk berbagi pengetahuan, teknik, dan alat yang lebih baik dalam mendeteksi dan merespons serangan siber.

4) Pengembangan dan penerapan teknologi baru. TNI harus terus mengikuti perkembangan teknologi terbaru di bidang kecerdasan buatan (AI), *machine learning* (ML), *blockchain*, dan *big data* yang dapat digunakan untuk mendeteksi dan menganalisis ancaman siber dengan lebih efektif. AI dan ML, misalnya, dapat digunakan untuk mengidentifikasi pola serangan yang tidak biasa dan membantu dalam proses prediksi serangan siber di masa depan.

5) Penataan dan pembaruan kebijakan keamanan siber. Di samping pengembangan infrastruktur teknologi, TNI perlu melakukan pembaruan kebijakan keamanan siber yang lebih komprehensif dan responsif terhadap ancaman *Cyber espionage*. Kebijakan ini harus mengatur tentang pengelolaan data, prosedur tanggap darurat, serta tata kelola informasi yang aman. Pembaruan kebijakan juga harus mempertimbangkan perkembangan teknologi dan teknik serangan siber yang semakin canggih.

6) Simulasi dan latihan keamanan siber secara berkala. Melakukan simulasi dan latihan secara berkala di seluruh unit TNI yang terlibat dalam pertahanan siber. Latihan ini harus mencakup skenario serangan *Cyber espionage* yang realistis, sehingga prajurit dapat berlatih dalam menghadapi serangan yang

sebenarnya. Latihan ini dapat membantu meningkatkan kesiapan dan kecepatan respons terhadap serangan siber.

7) Peningkatan sistem perlindungan data dan komunikasi. Penguatan sistem perlindungan data yang digunakan oleh TNI sangat penting, terutama dalam komunikasi yang melibatkan informasi sensitif. TNI perlu memastikan bahwa semua data yang dipertukarkan di jaringan internal maupun eksternal terlindungi dengan enkripsi tingkat tinggi dan autentikasi ganda untuk mencegah akses ilegal.

c. Ketersediaan Peraturan dan Kebijakan Dalam Hal Pelaksanaan *Cyber espionage*.

Ketersediaan peraturan dan kebijakan yang mengatur pelaksanaan *Cyber espionage* di Indonesia, khususnya di lingkungan Tentara Nasional Indonesia (TNI), sangat penting dalam menghadapi dan menangani ancaman siber yang semakin berkembang. *Cyber espionage*, yang melibatkan upaya pengumpulan data atau informasi secara ilegal melalui serangan siber, menuntut adanya kebijakan yang dapat mengatur dan melindungi data dan informasi strategis negara, serta memberikan pedoman bagi institusi pertahanan seperti TNI dalam menghadapi serangan tersebut. Berikut adalah beberapa peraturan dan kebijakan yang terkait dengan pelaksanaan *Cyber espionage* di Indonesia, serta upaya untuk meningkatkan efektivitas pengaturan di masa depan.

1) Undang-Undang Informasi dan Transaksi Elektronik (UU ITE). Undang-Undang No. 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE), yang direvisi dengan UU No. 19 Tahun 2016, menjadi dasar hukum utama yang mengatur aktivitas dunia maya di Indonesia. UU ITE ini mengatur tentang keamanan dan perlindungan informasi yang mencakup pemrosesan data elektronik, larangan terhadap penyalahgunaan informasi untuk tujuan tertentu, termasuk spionase digital yang mengarah pada *Cyber espionage*, dan

pelanggaran terhadap sistem elektronik, termasuk *hacking* dan pengambilan data tanpa izin, yang merupakan tindakan yang terkait dengan *Cyber espionage*. UU ITE juga memberikan dasar hukum bagi penegakan hukum terhadap pelaku yang melakukan perbuatan *Cyber espionage*, meskipun dalam prakteknya, penerapan UU ini belum cukup mencakup ancaman *Cyber espionage* yang spesifik.

2) Peraturan Pemerintah (PP) tentang Keamanan Siber. Selain UU ITE, ada beberapa Peraturan Pemerintah (PP) yang memberikan pedoman lebih lanjut tentang keamanan siber di Indonesia, antara lain PP No. 71 Tahun 2019 tentang Penyelenggaraan Sistem dan Transaksi Elektronik, yang mengatur penyelenggaraan infrastruktur dan sistem informasi di sektor publik dan swasta. PP ini memberikan pedoman bagi perlindungan data dan transaksi elektronik, yang sangat relevan untuk menangani ancaman *Cyber espionage* yang mengarah pada pencurian data strategis. PP No. 82 Tahun 2012 tentang Penyelenggaraan Sistem Transaksi Elektronik, yang mengatur aspek teknis dalam pengelolaan data dan sistem komunikasi di Indonesia, termasuk sistem yang digunakan oleh institusi pemerintah dan militer.

3) Peraturan Presiden (Perpres) dan Keputusan Presiden (Keppres). Beberapa Peraturan Presiden dan Keputusan Presiden (Keppres) yang mengatur kebijakan pertahanan siber juga mempengaruhi pelaksanaan upaya pencegahan dan penanganan *Cyber espionage*, antara lain Perpres No. 53 Tahun 2017 tentang Sistem Keamanan Nasional yang mengatur tentang ancaman dan kesiapsiagaan dalam menghadapi segala bentuk ancaman, termasuk yang berbasis teknologi informasi. Perpres No. 56 Tahun 2020 tentang Badan Siber dan Sandi Negara (BSSN), yang berfungsi untuk mengkoordinasikan dan mengawasi kebijakan keamanan siber di Indonesia, termasuk ancaman yang terkait dengan *Cyber espionage*. BSSN bertanggung jawab dalam memastikan bahwa kebijakan keamanan siber negara berjalan dengan baik, meliputi

pencegahan dan penanggulangan serangan siber yang dapat mengancam kedaulatan negara, termasuk tindakan *Cyber espionage*.

4) Undang-Undang Pertahanan Negara. UU No. 3 Tahun 2002 tentang Pertahanan Negara mengatur bahwa TNI memiliki peran penting dalam menjaga kedaulatan dan keutuhan negara, termasuk dalam menghadapi ancaman di dunia maya. Di dalam UU ini, *cyber warfare* dan serangan siber termasuk dalam bentuk ancaman yang perlu diwaspadai dan diatasi oleh TNI.

5) Doktrin Keamanan Siber di Lingkungan TNI. TNI telah mengembangkan berbagai kebijakan internal yang berkaitan dengan keamanan siber dan pelaksanaan *Cyber espionage* untuk menjaga kerahasiaan informasi dan data sensitif. Meskipun belum ada peraturan yang secara khusus menangani *Cyber espionage* dalam konteks militer secara terperinci, doktrin-doktrin yang ada sudah mencakup beberapa aspek penting, seperti perlindungan data sensitif dan intelijen yang harus diamankan dalam menghadapi ancaman siber, keamanan komunikasi dan infrastruktur TNI yang harus dilindungi dari potensi serangan *Cyber espionage*, serta strategi pertahanan siber yang mengharuskan TNI untuk mengembangkan kemampuan dalam mencegah, mendeteksi, dan merespons serangan siber yang berpotensi mencuri data atau merusak infrastruktur.

6) Kebijakan Nasional tentang Keamanan Siber. Indonesia juga memiliki kebijakan yang lebih luas yang mencakup keamanan siber nasional melalui program-program strategis yang mendukung ketahanan siber. Salah satunya adalah Rencana Pembangunan Jangka Menengah Nasional (RPJMN) yang mencakup penguatan infrastruktur dan kapasitas keamanan siber nasional. Kebijakan ini mendukung pengembangan sistem pertahanan siber di semua sektor, termasuk pertahanan militer.

Sedangkan upaya peningkatan peraturan dan kebijakan dalam menghadapi *Cyber espionage*, antara lain sebagai berikut:

1) Penguatan Peraturan Khusus *Cyber espionage* TNI dan pemerintah Indonesia perlu menyusun peraturan khusus tentang *Cyber espionage* yang lebih spesifik untuk mengatasi ancaman siber yang menargetkan data dan informasi militer atau strategis. Peraturan ini harus mencakup pengaturan yang jelas mengenai definisi, tindakan hukum, serta prosedur mitigasi yang diperlukan untuk menangani serangan *Cyber espionage*.

2) Peningkatan Kerjasama Internasional dalam Keamanan Siber Upaya untuk menangani *Cyber espionage* juga memerlukan kerjasama internasional dengan negara-negara lain yang memiliki kemampuan pertahanan siber yang lebih maju. Hal ini bisa melibatkan perjanjian bilateral atau multilateral dalam hal berbagi intelijen, teknologi, serta praktik terbaik dalam menangani serangan siber.

3) Penyempurnaan Kebijakan di Sektor Pertahanan Kebijakan internal TNI mengenai keamanan siber perlu terus disempurnakan, terutama yang berkaitan dengan pengamanan informasi yang sangat sensitif. Hal ini termasuk pembaruan kebijakan dalam hal pengelolaan data intelijen, serta penanganan insiden keamanan siber yang melibatkan *Cyber espionage*.

4) Penyusunan Standar Keamanan Siber di Lingkungan Militer Pembuatan standar keamanan siber yang lebih ketat di lingkungan TNI juga sangat penting untuk memperkuat pertahanan terhadap ancaman *Cyber espionage*. Standar ini meliputi pengelolaan data, prosedur enkripsi, dan kontrol akses yang ketat terhadap informasi sensitif yang dikelola oleh TNI

5. Kesimpulan

Dari jurnal penelitian tentang peningkatan kemampuan *Cyber espionage* dalam menghadapi ancaman siber di lingkungan TNI, dapat disimpulkan antara lain sebagai berikut:

a. Peningkatan kemampuan TNI dalam *Cyber espionage* sangat penting untuk menjaga kerahasiaan negara. TNI perlu meningkatkan kemampuannya dalam menghadapi ancaman *Cyber espionage* untuk menjaga kerahasiaan informasi strategis dan operasional yang penting bagi negara. Serangan siber, terutama yang bertujuan untuk mencuri data intelijen militer, dapat membahayakan keutuhan dan kedaulatan negara. Oleh karena itu, penguatan sistem keamanan siber, pelatihan personel, serta penerapan teknologi terkini menjadi aspek yang sangat krusial dalam menjaga informasi yang sangat vital bagi keamanan negara.

b. Kolaborasi dengan lembaga keamanan siber dan pengembangan infrastruktur keamanan yang lebih baik. Untuk meningkatkan kemampuan pertahanan terhadap *Cyber espionage*, Tentara Nasional Indonesia (TNI) harus memperkuat kerja sama dengan badan keamanan siber nasional, seperti Badan Keamanan Siber dan Kripto Nasional (BSSN). Kolaborasi ini akan memungkinkan pertukaran informasi dan pengalaman dalam memerangi ancaman siber. Selain itu, pengembangan infrastruktur keamanan siber yang lebih kuat, termasuk sistem deteksi intrusi, *firewall* canggih, dan perangkat forensik digital, diperlukan untuk mendeteksi dan merespons ancaman secara lebih cepat dan efektif.

c. Penyusunan kebijakan keamanan siber yang lebih komprehensif. TNI perlu menyusun kebijakan dan prosedur yang lebih komprehensif untuk menghadapi *Cyber espionage*, termasuk peraturan yang lebih spesifik mengenai ancaman siber di sektor militer. Kebijakan ini harus mencakup pengelolaan data sensitif, perlindungan terhadap infrastruktur teknologi, serta langkah-langkah mitigasi yang tepat. Peningkatan standar keamanan siber internal TNI dan pembaruan kebijakan yang responsif terhadap ancaman yang terus berkembang akan

memperkuat kesiapsiagaan TNI dalam menghadapi serangan siber yang semakin canggih.

Daftar Pustaka

1. Buku

Kementerian Pertahanan Republik Indonesia. (2014). Pedoman Pertahanan Siber.

2. Jurnal

Setiawan, K. E. (2022). Perlunya Tentara Nasional Indonesia Memiliki Angkatan Siber Guna Menghadapi Era Cyber Warfare. Journal of Education, Humaniora and Social Sciences (JEHSS), 5(1), 264–274. https://doi.org/10.34007/jehss.v5i1.1192

Sa'diyah, N. K., & Vinata, R. T. (2016). Rekonstruksi Pembentukan National Cyber Defense sebagai Upaya Mempertahankan Kedaulatan Negara. Perspektif, 21(3), 168–187. https://doi.org/10.30742/perspektif.v21i3.587

Mustameer, H. (2022). Penegakan Hukum Nasional dan Hukum Internasional Terhadap Kejahatan Cyber Espionage Pada Era Society 5.0. Jurnal Yustika, 25(1), 40–53. https://doi.org/10.24123/yustika.v25i01.5090

Kurniawan, A., Gultom, R. A. G., & Mantoro, T. (2024). Strategi Peningkatan Kapabilitas Satuan Siber Dispamsanau melalui Pemanfaatan Artificial Intelligence pada Keamanan Siber Berdasarkan National Institute of Standards and Technology Cybersecurity Framework Version 1.1. Jurnal Review Pendidikan dan Pengajaran, 7(1), 968–975. https://doi.org/10.21070/jrpp.v7i1.24878

Sulaiman, A. (2024). Profesionalisme TNI di Era Keamanan dan Pertahanan Siber Indonesia. DAS Sollen: Jurnal Kajian Kontemporer Hukum Dan Masyarakat, 7(1), 1–10. https://doi.org/10.28932/das.v7i1.188

Setiawan, K. E. (2022). Perlunya Tentara Nasional Indonesia Memiliki Angkatan Siber Guna Menghadapi Era Cyber Warfare. Journal of Education, Humaniora and Social Sciences (JEHSS), 5(1), 264–274. https://doi.org/10.34007/jehss.v5i1.1192

Chotimah, H. C. (2019). Tata Kelola Keamanan Siber dan Diplomasi Siber Indonesia di Bawah Kelembagaan Badan Siber dan Sandi Negara. Jurnal Politica Dinamika Masalah Politik Dalam Negeri dan Hubungan Internasional, 10(2), 113–128. https://doi.org/10.31289/politica.v10i2.1447

Ridwan, M. (2021). Cyber Warfare dan Ancaman Terhadap Keamanan Nasional. Jurnal Ilmu Sosial dan Ilmu Politik, 25(3), 215–225. https://doi.org/10.22146/jsp.65994

Suryanto, E. (2023). Peran TNI dalam Meningkatkan Kesadaran Bela Negara terhadap Ancaman Cyber Espionage. Jurnal Ilmu Sosial dan Ilmu Politik, 27(1), 45–60. https://doi.org/10.22146/jsp.121760

Setiyawan, K. (2018). Perlunya Tentara Nasional Indonesia Memiliki Angkatan Siber Guna Menghadapi Era Cyber Warfare. Journal of Education, Humaniora and Social Sciences (JEHSS), 5(1), 264–274. https://doi.org/10.34007/jehss.v5i1.1192

3. Sumber Dokumen

Badan Siber dan Sandi Negara. (2020). Rekap Serangan Siber (Januari – April 2020)