POTENSI ANCAMAN HIBRIDA PERANG SIBER DAN PERUBAHAN IKLIM TERHADAP INFRASTRUKTUR VITAL DAN KETAHANAN NASIONAL

Aura Purify
Prodi Teknik Elektronika Pertahanan, Akademi Militer, Indonesia
aurapurify@nikelektronikahan.akmil.ac.id

Andri Purwoko
Prodi Teknik Elektronika Pertahanan, Akademi Militer, Indonesia
andripurwoko@nikelektronikahan.akmil.ac.id

Agustina Dwi M.P
Prodi Teknik Elektronika Pertahanan, Akademi Militer, Indonesia
atina.dmp@nikelektronikahan.akmil.ac.id

ABSTRAK

Perubahan iklim global telah meningkatkan frekuensi serta intensitas bencana alam seperti banjir, badai, dan kekeringan. Pada saat yang sama, perkembangan teknologi digital memperbesar peluang terjadinya serangan siber terhadap infrastruktur vital negara. Konvergensi dari dua jenis ancaman ini, berpotensi menciptakan efek ganda yang memperburuk dampak terhadap ketahanan nasional. Penelitian ini mengkaji potensi ancaman hibrida yang muncul dari konvergensi antara perang siber dan perubahan iklim, terhadap infrastruktur vital dan ketahanan nasional Indonesia. Melalui pendekatan analisis potensi berbasis deskriptif kualitatif, studi ini mengevaluasi tingkat kerentanan, kapasitas mitigasi, dan potensi dampak yang ditimbulkan dari serangan siber yang terjadi bersamaan dengan bencana iklim. Data dikumpulkan dari studi pustaka, studi kasus *blackout* Jakarta 2019, dan laporan lembaga yang relevan dalam lima tahun terakhir. Hasil analisis menunjukkan bahwa wilayah yang berpotensi tinggi terkena dampak ancaman hibrida yang krusial ialah di pesisir perkotaan, di mana infrastruktur digital rentan terhadap bencana lingkungan dan serangan siber secara simultan. Sementara itu, infrastruktur vital yang paling rentan ancaman hibrida ialah di sektor energi dan tanggap darurat. Penelitian ini merekomendasikan penguatan strategi ketahanan nasional berbasis intelijen geospasial dan peningkatan sinergi antar sektor sebagai respons terhadap kompleksitas ancaman yang terus berkembang.

Kata-kunci: *perang siber, perubahan iklim, infrastruktur kritikal, ketahanan nasional, ancaman hibrida.*

CYBERWARFARE AND CLIMATE CHANGE: POTENTIAL HYBRID THREATS TO CRITICAL INFRASTRUCTURE AND NATIONAL SECURITY

ABSTRACT

Global climate change has increased the frequency and intensity of natural disasters such as floods, storms and droughts. At the same time, the development of digital technology increases the chances of cyber attack on the country's vital infrastructure. The convergence of these two types of threats has the potential to create a double whammy that worsens the impact on critical infrastructure. This study examines the potential of hybrid threat arising from the convergence of cyberwarfare and climate change, particularly in relation to critical infrastructure and national resilience. Using a qualitative potential analysis method, the research evaluates Indonesia's vulnerability to coordinated cyber and climate-related threats. A case study based on the 2019

Jakarta blackout highlights the risks of cascading failures in interconnected systems. The findings reveal high strategic risks in urban coastal areas, where digital infrastructure is exposed to both environmental disasters and cyberattacks. While the critical infrstructure that most likely deeply impacted by the hybrid threats are energy and emergency response sector. The study recommends the integration of GeoINT-based early warning systems, the development of hybrid threat response protocols, and enhanced inter-agency coordination to strengthen national preparedness. These efforts are essential for building adaptive, future-ready national resilience.

***Keywords**: cyberwarfare, climate change, hybrid threats, critical infrastructure, national resilience*

PENDAHULUAN

Latar Belakang Masalah

Perubahan iklim global telah meningkatkan frekuensi serta intensitas bencana alam seperti banjir, badai, dan kekeringan. Pada saat yang sama, perkembangan teknologi digital memperbesar peluang terjadinya serangan siber terhadap infrastruktur vital negara.

World Economic Forum (2024) mencantumkan ancaman siber dan perubahan iklim sebagai dua dari lima risiko global tertinggi terhadap stabilitas sistemik. NATO STRATCOM (2021) menekankan pentingnya pendekatan integratif antara pertahanan siber dan adaptasi iklim dalam strategi keamanan nasional. Chertoff dan Simon (2022) menegaskan bahwa negara yang memiliki sistem informasi geospasial terintegrasi dan protokol respons adaptif cenderung lebih resilien terhadap serangan bersifat hibrida.

Meskipun keduanya memiliki karakteristik ancaman yang berbeda, konvergensi perang siber dan perubahan iklim berpotensi menciptakan efek ganda yang memperburuk dampak terhadap infrastruktur kritikal.

Infrastruktur seperti jaringan energi, air, transportasi, dan komunikasi sangat rentan mengalami gangguan ketika menghadapi dua ancaman tersebut secara simultan. Situasi ini secara langsung dapat mengancam ketahanan nasional (Busby et al., 2022; IPCC, 2023).

Berdasarkan paparan tersebut, maka penelitian ini merumuskan masalah: Bagaimana potensi ancaman hibrida dari perang siber dan perubahan iklim dapat mempengaruhi infrastruktur vital dan ketahanan nasional Indonesia?

Adapun tujuan dari penelitan ini ialah untuk:

1. Mengidentifikasi potensi ancaman hibrida dari konvergensi perang siber dan perubahan iklim.
2. Menilai kerentanan infrastruktur vital terhadap ancaman tersebut.
3. Menganalisis kapasitas mitigasi nasional dalam merespons ancaman konvergen.
4. Merumuskan rekomendasi strategis untuk memperkuat ketahanan nasional.

METODE PENELITIAN

Penelitian ini menggunakan pendekatan deskriptif kualitatif dengan teknik analisis potensi risiko. Data dikumpulkan melalui studi literatur dari jurnal ilmiah, laporan institusi (IPCC, WEF, NATO), serta dokumen kebijakan nasional dalam lima tahun terakhir..

Tahapan analisis meliputi:

1. Identifikasi potensi ancaman dari data sekunder.
2. Evaluasi kerentanan sektor infrastruktur melalui matriks risiko.

3. Analisis kapasitas mitigasi berdasarkan kesiapan teknologi, kebijakan, dan koordinasi institusi.

HASIL DAN PEMBAHASAN

Hasil identifikasi potensi ancaman hibrida didapatkan dari data-data laporan dan hasil publikasi, yaitu sebagai berikut : Menurut laporan dari IPCC (2023), Indonesia diperkirakan mengalami peningkatan kejadian iklim ekstrem sebesar 30% pada dekade mendatang. Sementara itu, laporan BSSN (2022) menyatakan bahwa serangan siber pada sektor energi meningkat sebesar 47% dari tahun sebelumnya. Studi oleh WEF (2024) menempatkan Indonesia dalam 10 besar negara dengan risiko tinggi terhadap ancaman konvergen akibat lemahnya integrasi sistem keamanan siber dan adaptasi iklim.

Sementara itu, data PLN (2023) menunjukkan bahwa lebih dari 40% jaringan listrik di Pulau Jawa masih bergantung pada satu jalur distribusi utama tanpa sistem redundansi. Peta risiko BNPB (2022) menunjukkan bahwa DKI Jakarta memiliki indeks risiko bencana tinggi, terutama terkait banjir dan pemadaman sistem transportasi akibat cuaca ekstrem.

Evaluasi Kerentanan Infrastruktur Kritikal di Indonesia

Kerentanan tertinggi ditemukan pada:

1. Wilayah pesisir seperti Jakarta dan Makassar yang padat penduduk dan rawan banjir.
2. Sistem energi yang belum memiliki redundansi digital memadai, terutama dalam merespons lonjakan beban atau cuaca ekstrem.
3. Sistem tanggap darurat yang belum sepenuhnya terintegrasi dengan sistem pemantauan dan peringatan dini berbasis digital.

Analisis terhadap infrastruktur kritikal di Indonesia menunjukkan bahwa sektor energi memiliki kelemahan struktural signifikan, khususnya karena tingginya ketergantungan pada jaringan distribusi utama tanpa sistem redundansi yang memadai. Kondisi ini memperbesar risiko apabila terjadi bencana iklim seperti banjir besar yang merusak jaringan fisik, terlebih jika disusul oleh serangan siber terhadap sistem SCADA (*Supervisory Control and Data Acquisition*) yang mengendalikan operasi kelistrikan. Kombinasi dua ancaman ini berpotensi menyebabkan pemadaman yang berlangsung lama dan sulit dipulihkan dalam waktu singkat (PLN, 2023; IPCC, 2023; BSSN, 2022).

Di sisi lain, sektor tanggap darurat juga menghadapi tantangan sistemik dalam hal koordinasi data antar lembaga kunci seperti Badan Nasional Penanggulangan Bencana (BNPB), Badan Meteorologi, Klimatologi, dan Geofisika (BMKG), serta Badan Siber dan Sandi Negara (BSSN). Kurangnya protokol terpadu dan interoperabilitas data menyebabkan respons terhadap ancaman hibrida menjadi tidak sinkron dan cenderung lambat, sehingga mengurangi efektivitas mitigasi di lapangan (BNPB, 2022; WEF, 2024).

Berdasarkan analisis SWOT, terdapat sejumlah temuan penting. Dari sisi kekuatan (*strengths*), Indonesia telah memiliki lembaga nasional khusus seperti BSSN dan BNPB yang memiliki mandat strategis dalam keamanan siber dan penanggulangan bencana. Namun, dari sisi kelemahan (*weaknesses)*, masih terletak pada lemahnya integrasi koordinasi antar lembaga dan

kurangnya protokol respons terpadu. Sementara itu, di sisi peluang (*opportunities*), kemajuan teknologi seperti pengembangan GeoINT (*Geospatial Intelligence*) dan sistem prediksi iklim berbasis AI memberikan potensi besar untuk meningkatkan kapasitas adaptasi dan respons terhadap ancaman. Di sisi lain, ancaman (*threats*) terbesar berasal dari kemungkinan serangan siber terkoordinasi yang dilakukan pada saat kondisi krisis sedang berlangsung, seperti saat terjadinya bencana alam, yang dapat melumpuhkan beberapa sektor vital secara simultan (Chertoff & Simon, 2022; NATO STRATCOM, 2021).

Studi Kasus: Blackout Jakarta 2019 dan Simulasi Serangan Siber

Salah satu studi kasus yang relevan dalam konteks potensi ancaman hibrida adalah peristiwa pemadaman listrik massal (*blackout*) yang terjadi di wilayah Jabodetabek dan sebagian Jawa Barat pada tanggal 4 Agustus 2019. Pemadaman ini berlangsung hingga lebih dari 12 jam di beberapa wilayah dan berdampak luas pada infrastruktur publik, termasuk layanan transportasi massal seperti MRT, jaringan komunikasi seluler, serta sistem distribusi air bersih (PLN, 2020). Penyebab utama *blackout* ini, dilaporkan sebagai gangguan pada transmisi Saluran Udara Tegangan Ekstra Tinggi (SUTET) 500 kV Ungaran–Pemalang, yang memicu pemutusan pasokan listrik secara berantai karena sistem interkoneksi yang belum memiliki cukup redundansi (Kementerian ESDM, 2020).

Kejadian ini mengindikasikan kelemahan sistemik dalam manajemen risiko sektor energi, terutama dalam konteks ketergantungan tinggi pada satu jalur distribusi utama dan ketiadaan sistem cadangan yang andal. Dalam skenario ancaman hibrida, pemadaman semacam ini dapat menjadi lebih parah apabila disertai dengan serangan siber yang menargetkan sistem SCADA (*Supervisory Control and Data Acquisition*) PLN, yang merupakan sistem kendali utama pada infrastruktur kelistrikan nasional. Laporan BSSN (2022) menyebutkan bahwa sistem SCADA merupakan salah satu target paling rentan dalam arsitektur infrastruktur kritikal nasional, karena konektivitasnya yang tinggi namun perlindungan keamanannya masih bervariasi di antara wilayah operasional.

Jika peristiwa *blackout* seperti 2019 terjadi bersamaan dengan bencana alam seperti banjir besar—yang semakin sering terjadi di Jakarta akibat intensitas hujan ekstrem (IPCC, 2023)—dan disusul serangan siber, maka skenario pemadaman bisa memakan waktu lebih lama untuk pemulihan. Hal ini akan berdampak domino terhadap sektor lain seperti transportasi, telekomunikasi, kesehatan, hingga keamanan publik. Studi simulasi oleh Pusat Studi Ketahanan Energi (2023) menunjukkan bahwa durasi *blackout* dapat meningkat hingga tiga kali lipat dalam skenario ancaman konvergen, dengan kerugian ekonomi diperkirakan mencapai lebih dari Rp1,5 triliun per hari pada kawasan metropolitan seperti Jabodetabek.

Kapasitas Mitigasi Nasional

Kapabilitas mitigasi nasional terhadap ancaman hibrida yang melibatkan perang siber dan bencana iklim masih menunjukkan karakter yang sektoral dan fragmentaris. Koordinasi antar lembaga seperti Badan Siber dan Sandi Negara (BSSN), Badan Nasional Penanggulangan Bencana (BNPB), Badan Meteorologi, Klimatologi, dan Geofisika (BMKG), serta Tentara Nasional Indonesia (TNI) belum

sepenuhnya terintegrasi dalam satu sistem komando yang responsif terhadap ancaman simultan. Hal ini menyebabkan respons terhadap krisis ganda, seperti banjir yang disertai serangan siber terhadap sistem energi atau komunikasi, menjadi lambat dan tidak sinkron. Menurut Laporan Evaluasi Sistem Penanggulangan Bencana Nasional oleh BNPB (2022), hanya 46% dari protokol tanggap darurat yang memiliki interoperabilitas digital antar lembaga.

Meskipun demikian, terdapat inisiatif yang menjanjikan dalam penguatan kapasitas mitigasi melalui pengembangan sistem Intelijen Geospasial (GeoINT). TNI AD bersama Badan Riset dan Inovasi Nasional (BRIN) tengah mengembangkan platform GeoINT untuk mendukung sistem peringatan dini dan pengambilan keputusan dalam situasi darurat berbasis spasial (BRIN, 2023). GeoINT dapat memainkan peran strategis dalam mengintegrasikan data cuaca ekstrem dari BMKG, lokasi aset kritikal dari kementerian teknis, serta informasi kerentanan siber dari BSSN, sehingga memungkinkan pembuatan skenario respons adaptif dan prediktif.

Namun demikian , hingga kini belum terdapat payung hukum atau regulasi nasional yang secara khusus mengatur manajemen risiko hibrida antara bencana alam dan perang siber. Hal ini menjadi tantangan tersendiri dalam membangun sistem mitigasi yang responsif, sinergis, dan adaptif. Oleh karena itu, diperlukan perumusan kerangka kebijakan terpadu yang menjembatani aspek keamanan digital dan perubahan iklim secara simultan dalam kerangka ketahanan nasional.

SIMPULAN

1. Potensi ancaman hibrida tertinggi berada pada
2. Infrastruktur vital yang paling rentan terhadap ancaman hibrida tersebut adalah pada sektor energi dan tanggap darurat.
3. Kapasitas mitigasi nasional masih belum optimal dan memerlukan perbaikan lintas sektor.

Rekomendasi Strategis:

1. Memperkuat sistem intelijen geospasial (GeoINT) untuk deteksi dan respons dini terhadap risiko konvergen.
2. Menyusun protokol nasional yang bersifat adaptif untuk menghadapi ancaman hibrida.
3. Meningkatkan kapasitas sumber daya manusia dan membangun koordinasi antarlembaga melalui pelatihan terpadu dan integrasi kebijakan digital dan ketahanan iklim.

DAFTAR PUSTAKA

Badan Meteorologi, Klimatologi, dan Geofisika. (2023). *Riset cuaca ekstrem dan peringatan dini nasional*. BMKG.

Badan Nasional Penanggulangan Bencana. (2022a). *Indeks risiko bencana Indonesia*. BNPB.

Badan Nasional Penanggulangan Bencana. (2022b). *Laporan evaluasi sistem penanggulangan bencana nasional*. BNPB.

Badan Riset dan Inovasi Nasional. (2023). *Laporan inisiatif GeoINT untuk ketahanan nasional*. BRIN.

Badan Siber dan Sandi Negara. (2022). *Laporan tahunan keamanan siber nasional 2022*. BSSN.

Busby, J. W., Smith, T., White, K., & Peterson, J. (2022). Climate and security risks. *Journal of Strategic Studies, 45*(2), 123–145. https://doi.org/10.1080/01402390.2022.2011657

Chertoff, M., & Simon, T. (2022). *Cybersecurity and climate resilience: Bridging the gap*. Council on Foreign Relations. https://www.cfr.org/report/cybersecurity-and-climate-resilience

Intergovernmental Panel on Climate Change. (2023). *Sixth assessment report*. https://www.ipcc.ch/ar6

Kompas. (2019, August 4). Pemadaman listrik massal Jakarta dan Jawa Barat, ini kronologinya. *Kompas.com*. https://nasional.kompas.com/read/2019/08/04/21194711

Liputan6. (2019, August 6). Blackout Jakarta: PLN klaim sistem kelistrikan rawan jika tak ada redundansi. *Liputan6.com*. https://www.liputan6.com/bisnis/read/4035411

NATO Strategic Communications Centre of Excellence. (2021). *Cyber and climate security: Converging risks*. NATO STRATCOM.

PT PLN (Persero). (2023). *Sistem kelistrikan Jawa-Bali: Evaluasi dan penguatan keandalan*. PLN.

Pusat Studi Ketahanan Energi. (2023). *Simulasi skenario ancaman ganda terhadap sistem energi nasional*. Universitas Pertahanan Indonesia.

The Jakarta Post. (2019, August 5). Jakarta's massive blackout: What went wrong and what's next? *The Jakarta Post*. https://www.thejakartapost.com/news/2019/08/05/jakartas-massive-blackout

World Economic Forum. (2024). *Global risks report 2024*. https://www.weforum.org/reports/global-risks-report-2024