**Presidensial: Jurnal Hukum, Administrasi Negara, dan Kebijakan Publik**
**Volume 2, Nomor 2, Juni 2025**
e-ISSN: 3063-1246; p-ISSN: 3063-1211, Hal. 316-327
DOI: https://doi.org/10.62383/presidensial.v2i2.850
*Available online at*: https://ejournal.appihi.or.id/index.php/Presidensial

# Ancaman Siber Internasional: Lazarus Group sebagai Instrumen Perang Asimetris Korea Utara

**Rika Sartika[1*], Nur Isdah Idris[2]**
[1-2]Universitas Hasanuddin, Indonesia

Alamat: JL. Perintis Kemerdekaan No. KM. 10
**Korespondensi penulis : rikakuliah2004@gmail.com*

***Abstract***. *The advancement of digital technology has made cyberspace a new arena for international conflict. The Lazarus Group, a hacking group allegedly affiliated with the North Korean government, has come to global attention for its involvement in numerous large-scale cyberattacks targeting financial institutions, global corporations, and public infrastructure. This study aims to analyze the group's operational patterns, strategic motives, and its implications for global cybersecurity. Using a qualitative approach and document analysis, the study investigates how Lazarus represents North Korea's strategy to counter international isolation and gain economic advantage. The results show that the international community's response to state actor threats in cyberspace is fragmented and ineffective. Therefore, a stronger and more coordinated multilateral framework is needed to respond to cyber threats from state actors.*

***Keywords:*** *Cybersecurity, Lazarus Group, North Korea, Transnational Threat, Yber Diplomacy.*

**Abstrak**. Kemajuan teknologi digital telah menjadikan ruang siber sebagai arena baru dalam konflik internasional. Lazarus Group, kelompok peretas yang diduga berafiliasi dengan pemerintah Korea Utara, menjadi perhatian global karena keterlibatannya dalam berbagai serangan siber berskala besar yang menargetkan institusi keuangan, perusahaan global, dan infrastruktur publik. Penelitian ini bertujuan untuk menganalisis pola operasional, motif strategis, dan implikasi aktivitas kelompok ini terhadap keamanan siber global. Menggunakan pendekatan kualitatif dan analisis dokumen, studi ini menemukan bahwa aktivitas Lazarus tidak hanya ditujukan untuk keuntungan ekonomi, tetapi juga sebagai bagian dari strategi diplomasi digital dan perang asimetris Korea Utara. Hasil penelitian menunjukkan bahwa respons komunitas internasional terhadap ancaman aktor negara dalam ruang siber masih terfragmentasi dan belum efektif. Maka untuk menanggapi ancaman siber dari aktor negara dibutuhkan kerangka kerja multilateral yang lebih kuat dan terkoordinasi.

**Kata Kunci**: Ancaman Transnasional, Diplomasi Siber, Keamanan Siber, Korea Utara, Lazarus Group.

## 1. LATAR BELAKANG

Di era digital saat ini, lanskap keamanan internasional telah mengalami perubahan mendasar. Teknologi informasi yang pada awalnya bertujuan mendukung pertumbuhan ekonomi dan konektivitas global, kini juga dimanfaatkan sebagai alat dalam konflik antarnegara. Ruang siber, yang dulunya dipandang sebagai domain teknis, kini menjadi arena kontestasi geopolitik baru. Negara-negara tidak hanya berinvestasi pada sistem pertahanan militer konvensional, tetapi juga mengembangkan kapabilitas siber ofensif yang mampu menjangkau target di seluruh dunia dengan tingkat risiko politik yang relatif rendah. Dalam konteks ini, ancaman siber menjadi salah satu tantangan utama bagi keamanan global karena sifatnya yang transnasional, sulit dilacak, dan memiliki potensi kerusakan besar terhadap sistem kritis suatu negara.

*Received Mei 16, 2025; Revised Mei 31, 2025; Accepted Juni 17, 2025; Published Juni 20, 2025*

Salah satu aktor yang paling sering disebut dalam diskursus keamanan siber global adalah Lazarus Group, sebuah kelompok peretas yang secara luas diyakini berafiliasi dengan pemerintah Korea Utara. Kelompok ini mulai dikenal publik sejak serangan terhadap Sony Pictures pada tahun 2014, yang diduga sebagai respons terhadap film satir "The Interview" yang mengolok-olok pemimpin Korea Utara. Sejak saat itu, Lazarus Group terus menjadi sorotan karena terlibat dalam serangkaian operasi siber berskala besar yang mencakup pencurian dana dari sistem SWIFT Bank Sentral Bangladesh pada 2016, penyebaran ransomware WannaCry pada 2017, serta berbagai serangan terhadap lembaga keuangan, perusahaan teknologi, dan bursa mata uang kripto di berbagai negara. Berbagai laporan dari FireEye, Kaspersky Lab, hingga Panel Ahli PBB menyebut bahwa kegiatan kelompok ini berfungsi sebagai instrumen negara untuk menggalang dana, melemahkan sistem keuangan negara lain, dan menantang tatanan keamanan global.

Fenomena Lazarus Group menunjukkan adanya perubahan strategi dari negara-negara yang mengalami isolasi atau sanksi internasional, seperti Korea Utara, dalam merespons tekanan global. Dengan keterbatasan ekonomi dan sumber daya, rezim di Pyongyang memanfaatkan dunia maya sebagai sarana untuk melakukan serangan siber dengan cakupan luas dan dampak nyata. Karakteristik serangan Lazarus menunjukkan keterkaitan erat antara dimensi militer, ekonomi, dan politik, yang membedakannya dari kelompok kriminal siber biasa. Serangan mereka seringkali menyasar sektor-sektor strategis, menggunakan teknik rekayasa sosial canggih, dan ditujukan untuk mengganggu tatanan global, bukan hanya untuk keuntungan pribadi. Dalam hal ini, Lazarus dapat dipahami sebagai representasi dari cara baru negara-negara tertentu menggunakan kekuatan non-konvensional untuk mempertahankan eksistensinya di tengah tekanan internasional.

Meskipun literatur terkait ancaman siber telah berkembang pesat, mayoritas penelitian yang ada hanya berfokus pada aspek teknis, seperti jenis malware, kerentanan sistem, atau metode enkripsi. Sedikit sekali studi yang menempatkan aktivitas Lazarus dalam kerangka besar studi hubungan internasional dan keamanan global. Padahal, aktivitas kelompok ini beroperasi di wilayah yang sangat politis. Mereka tidak hanya mencuri uang, tetapi juga merusak legitimasi negara, melemahkan stabilitas ekonomi global, dan menantang batas-batas norma hukum internasional yang ada. Ketiadaan kerangka hukum internasional yang mengikat dalam isu siber serta lemahnya kemampuan atribusi terhadap pelaku serangan memperparah situasi. Negara-negara yang menjadi korban sering kali kesulitan memberikan respons efektif, baik secara hukum, diplomatik, maupun strategis.

Kesenjangan ini menunjukkan pentingnya kajian yang lebih mendalam terhadap Lazarus Group, tidak hanya dari sisi teknis, tetapi sebagai representasi nyata dari bagaimana negara-negara tertentu mengembangkan dan menggunakan kapabilitas siber sebagai alat politik luar negeri. Selain itu, belum banyak penelitian yang membahas secara spesifik bagaimana komunitas internasional menanggapi serangan semacam ini, serta seberapa efektif mekanisme kerja sama multilateral dalam membendung eskalasi ancaman dari aktor negara di dunia maya. Dengan meningkatnya ketergantungan masyarakat global pada infrastruktur digital, kegagalan untuk mengelola ancaman seperti Lazarus berpotensi menciptakan instabilitas baru yang jauh lebih kompleks daripada perang konvensional.

Tujuan penelitian ini adalah untuk menjawab kebutuhan akan pemahaman yang lebih komprehensif mengenai peran Lazarus Group sebagai ancaman keamanan siber global. Secara khusus, penelitian ini dilakukan untuk menganalisis pola dan strategi serangan Lazarus Group, mengkaji keterkaitannya dengan kepentingan negara Korea Utara, serta menilai efektivitas respons komunitas internasional terhadap ancaman tersebut. Lebih lanjut, penelitian ini diharapkan mampu memberikan kontribusi teoritis dalam pengembangan studi keamanan siber serta memberikan rekomendasi kebijakan yang relevan dalam menghadapi eskalasi ancaman siber yang bersifat lintas negara dan tersponsori oleh negara.

## 2. KAJIAN TEORITIS

### Teori Keamanan Siber (Cybersecurity Theory)

Teori ini membahas prinsip, kebijakan, dan praktik yang digunakan untuk melindungi sistem informasi, jaringan, dan data dari serangan, kerusakan, atau akses ilegal. Dalam kerangka ini, keamanan tidak hanya soal perangkat teknis, tetapi juga mencakup dimensi politik, ekonomi, dan sosial. Ancaman seperti yang dilakukan oleh Lazarus Group dipahami sebagai bagian dari lanskap ancaman digital yang kompleks, termasuk serangan terhadap infrastruktur penting dan pencurian data strategis.

### Teori Realisme dalam Hubungan Internasional

Teori ini memandang aktor utama dalam sistem internasional yang anarkis (tanpa otoritas tertinggi) adalah negara. Negara dianggap rasional dan akan selalu bertindak untuk memaksimalkan kepentingan nasional dan keamanannya. Dalam konteks ini, penggunaan Lazarus Group oleh Korea Utara bisa dipahami sebagai bentuk strategi bertahan hidup dan pembangkangan terhadap dominasi negara kuat, misalnya dalam merespons sanksi ekonomi atau isolasi politik.

**Teori Perang Asimetris (Asymmetric Warfare Theory)**

Perang asimetris merupakan konflik dimana kekuatan antara dua pihak tidak seimbang. Pihak yang lebih lemah menggunakan metode tidak konvensional seperti terorisme, perang gerilya, atau serangan siber untuk melemahkan lawan yang lebih kuat. Korea Utara melalui Lazarus Group dianggap menjalankan strategi asimetris dengan menggunakan teknologi siber sebagai alat untuk menciptakan dampak global dengan biaya rendah.

**Teori Aktor Non-Negara dan Keamanan Global**

Teori ini berangkat dari fakta bahwa aktor non-negara seperti organisasi teroris, kelompok kriminal, atau peretas dapat menjadi ancaman terhadap keamanan global. Dalam banyak kasus, kelompok seperti Lazarus Group beroperasi seperti aktor non-negara, namun sebenarnya memiliki dukungan negara. Hal ini menimbulkan ambigu dalam atribusi dan pertanggungjawaban, serta tantangan dalam kerja sama internasional.

**Teori Rezim Internasional (International Regime Theory)**

Teori ini menjelaskan bagaimana negara-negara dapat bekerja sama melalui norma, aturan, dan institusi internasional meskipun berada dalam sistem internasional yang anarkis. Dalam konteks keamanan siber, teori ini berguna untuk mengevaluasi efektivitas kesepakatan internasional seperti Konvensi Budapest tentang Kejahatan Siber atau kerja sama ASEAN dalam menangani kejahatan digital lintas negara.

**Teori Cyber Deterrence (Pencegahan Siber)**

Berangkat dari teori deterrence klasik, cyber deterrence bertujuan mencegah serangan siber dengan ancaman pembalasan, peningkatan pertahanan, atau respons hukum internasional. Namun, penerapan teori ini di dunia maya lebih rumit karena anonimitas serangan siber dan kesulitan melakukan atribusi terhadap pelaku. Studi Lazarus Group dapat digunakan untuk menilai seberapa efektif strategi deterrence ini dalam mencegah serangan lanjutan.

## 3. METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif dengan studi kasus yang bersifat eksploratif. Objek kajian adalah Lazarus Group sebagai representasi aktor negara dalam domain siber. Data dikumpulkan melalui studi literatur dan analisis dokumen sekunder dari laporan lembaga internasional, serta artikel ilmiah terkait ancaman siber dan keamanan global. Teknik analisis data yang diterapkan adalah analisis isi (content analysis) terhadap dokumen-

dokumen yang relevan. Validitas data dijaga dengan triangulasi sumber dan analisis lintas-referensi dari lembaga independen.

## 4. HASIL DAN PEMBAHASAN

Dalam lanskap keamanan global yang semakin bergeser ke ranah digital, kelompok peretas Lazarus Group muncul sebagai salah satu ancaman siber paling signifikan di abad ke-21. Dikenal sebagai kelompok yang disponsori negara (state-sponsored group) oleh Korea Utara, Lazarus menampilkan karakteristik khas dari *advanced persistent threat* (APT), yaitu kemampuan untuk melakukan serangan siber secara berkelanjutan, terselubung, dan dengan target strategis yang kompleks. Tujuan utama kelompok ini tidak semata-mata ekonomi, tetapi juga politis dan militeristik yang pada akhirnya berusaha untuk mewujudkan kepentingan nasional Korea Utara melalui jalur non-konvensional.

Serangan yang dilancarkan oleh Lazarus mencerminkan kecanggihan teknik dan keberanian dalam memilih target. Salah satu taktik yang paling umum mereka gunakan adalah *phishing* dan *spear-phishing*, di mana email palsu yang tampak sah dikirimkan ke korban, sering kali berisi lampiran atau tautan berbahaya yang mengarahkan ke malware. Teknik ini secara efektif telah digunakan untuk menyusupi lembaga keuangan dan sektor pertahanan global (Kaspersky, 2021). Serangan semacam ini tidak hanya berhasil mencuri data, tetapi juga membuka akses bagi tahapan serangan lanjutan.

Selain itu, Lazarus dikenal melalui serangan malware dan ransomware berskala besar. Serangan WannaCry pada tahun 2017 menjadi tonggak penting, menandai kemampuan mereka dalam mengeksploitasi celah keamanan besar seperti EternalBlue dalam sistem Windows. Serangan ini menjangkiti lebih dari 200.000 komputer di 150 negara dan menunjukkan betapa luas dan dalam dampak kerusakan yang bisa mereka timbulkan (Europol, 2018). Lazarus juga diketahui menggunakan malware lain seperti Fallchill dan Volgmer untuk mengendalikan sistem korban secara diam-diam dan berkepanjangan (FireEye, 2020).

Lebih jauh lagi, kelompok ini telah mengadaptasi strategi pencurian digital yang lebih modern dengan menyasar aset mata uang kripto. Salah satu contohnya adalah serangan terhadap Ronin Network yang digunakan dalam permainan daring *Axie Infinity*. Dalam serangan tersebut, Lazarus berhasil mencuri lebih dari USD 600 juta, menjadikannya salah satu kasus pencurian kripto terbesar dalam sejarah (Chainalysis, 2023). Ini menunjukkan bahwa kelompok ini tidak hanya berevolusi secara teknis, tetapi juga secara strategis, mengikuti dinamika ekonomi digital global.

Aktivitas Lazarus Group dapat dianalisis melalui kerangka perang asimetris. Korea Utara, sebagai negara yang secara ekonomi dan militer tertinggal dibandingkan kekuatan besar seperti Amerika Serikat atau negara-negara G7, memilih untuk mengalihkan medan perangnya ke dunia maya. Dunia digital menawarkan keuntungan strategis yang besar: serangan dapat dilakukan dari jarak jauh, pelakunya sulit dilacak, dan biaya yang dikeluarkan jauh lebih rendah dibandingkan operasi militer konvensional (Jun & Krekel, 2014). Dalam hal ini, kapabilitas siber menjadi pengganti yang efektif atas keterbatasan kekuatan militer fisik.

Karakter asimetris dari operasi Lazarus juga tercermin dalam pemilihan target. Mereka tidak hanya menyerang institusi keuangan, tetapi juga simbol-simbol budaya dan politik negara lain. Serangan terhadap Sony Pictures Entertainment pada tahun 2014, yang diduga sebagai balasan atas film *The Interview* yang memparodikan pemimpin Korea Utara, menunjukkan bagaimana serangan siber dapat digunakan sebagai alat represif terhadap kebebasan berekspresi dan budaya populer (FBI, 2014). Dengan modal relatif kecil, Lazarus mampu menciptakan efek disproporsional: menimbulkan kerugian finansial besar, mengacaukan infrastruktur digital, dan memperkeruh hubungan diplomatik.

Meskipun berkaitan erat dengan negara, secara formal Lazarus tetap berstatus sebagai aktor non-negara. Dalam konteks teori hubungan internasional, ini menjadikannya entitas yang unik, dimana mereka berada di antara batas-batas negara dan non-negara, memanfaatkan ruang siber sebagai wilayah abu-abu yang sukar dijangkau oleh hukum internasional. Lazarus sering kali menyamarkan operasinya melalui identitas digital palsu dan perusahaan fiktif, serta memanfaatkan infrastruktur server dari negara-negara dengan regulasi siber yang lemah (CrowdStrike, 2021). Keberadaan mereka yang lintas negara menciptakan tantangan yurisdiksi yang serius, di mana tidak ada otoritas tunggal yang bisa menuntut atau mengekstradisi pelaku secara efektif.

**Motif Strategis Korea Utara**

Dalam kerangka teori realisme, negara dipandang sebagai aktor utama dalam sistem internasional yang anarkis, di mana setiap negara berjuang untuk bertahan hidup dan memaksimalkan kekuatannya. Dalam konteks ini, tindakan Korea Utara yang memanfaatkan kelompok peretas Lazarus Group bukanlah hal yang irasional, melainkan strategi rasional dari

sebuah negara yang terkepung oleh sanksi ekonomi, isolasi diplomatik, dan tekanan politik global. Lazarus Group, dengan segala aktivitas sibernya yang kompleks, pada dasarnya

merupakan instrumen kebijakan luar negeri non-konvensional yang dimanfaatkan Korea Utara untuk menjaga eksistensinya di panggung global.

Salah satu motif utama di balik keterlibatan Korea Utara dalam operasi Lazarus adalah aspek *economic survival*. Dalam situasi ekonomi yang nyaris stagnan akibat berbagai sanksi internasional, Korea Utara membutuhkan sumber pembiayaan alternatif untuk mendukung program-program strategisnya, termasuk program nuklir dan militernya. Aktivitas Lazarus dalam mencuri aset kripto, meretas bank, dan melakukan pemerasan digital telah terbukti menghasilkan miliaran dolar, seperti yang dilaporkan oleh *United Nations Panel of Experts* (2022). Pendapatan dari operasi siber ini menjadi tulang punggung penting dalam menopang keberlangsungan rezim dan memperluas kapasitas pertahanan negara.

Di sisi lain, peran Lazarus juga dapat dipahami sebagai bagian dari strategi *proxy*. Mengingat keterbatasan kekuatan militer dan diplomatik, Korea Utara memilih untuk tidak tampil langsung dalam konflik terbuka, melainkan menggunakan kelompok seperti Lazarus sebagai *perpanjangan tangan* yang beroperasi di bawah prinsip *plausible deniability*. Dalam praktik realis, strategi ini umum digunakan oleh negara-negara untuk menghindari tanggung jawab langsung atas tindakan-tindakan agresif, sembari tetap memperoleh keuntungan strategis di arena internasional.

Pendekatan teori *perang asimetris* semakin menjelaskan relevansi taktik ini. Negara kecil dengan keterbatasan sumber daya seperti Korea Utara cenderung menghindari konfrontasi militer langsung dengan kekuatan besar, dan sebagai gantinya mengandalkan bentuk perlawanan non-tradisional yang efektif dan murah. Dalam hal ini, Lazarus Group berperan sebagai arsenal digital yang mampu menyerang infrastruktur musuh tanpa menimbulkan konfrontasi fisik. Serangan terhadap Sony Pictures pada tahun 2014 dan pencurian aset kripto bernilai ratusan juta dolar dari jaringan keuangan di Amerika dan Asia merupakan contoh konkret bagaimana Korea Utara melalui Lazarus mampu "membalas" tekanan eksternal tanpa mengerahkan pasukan di medan perang (Chainalysis, 2023).

Selain itu, teknik yang digunakan Lazarus mencerminkan bentuk perang yang *tak berwajah*. Operasi-operasi siber yang mereka lakukan sulit dilacak dan sering kali membingungkan aparat keamanan global. Keunggulan ini memberi Korea Utara kemampuan untuk memanipulasi situasi geopolitik secara tersembunyi, menciptakan ketidakstabilan tanpa menanggung risiko diplomatik atau militer secara langsung. Dunia siber menjadi ruang abu-abu yang ideal untuk menjalankan strategi semacam ini.

Lebih jauh, fenomena ini juga dapat dianalisis melalui kacamata *cyber deterrence*, yakni bagaimana kekuatan siber digunakan untuk mencegah agresi atau membalas tekanan, dengan pola yang mirip dengan *nuclear deterrence* pada era Perang Dingin. Dalam konteks

ini, Lazarus mewakili postur pertahanan digital Korea Utara yang dibangun untuk menciptakan efek jera terhadap musuh-musuhnya. Strategi ini bekerja dalam tiga lapis.

Pertama, *deterrence by punishment*, di mana Korea Utara menunjukkan bahwa ia mampu merusak ekonomi digital global, seperti dalam kasus serangan ransomware WannaCry. Serangan tersebut bukan hanya menghasilkan kerugian finansial besar, tetapi juga menimbulkan ketakutan dan kekhawatiran global atas kerentanan sistem siber yang ada. Kedua, *deterrence by denial*, di mana Korea Utara memperkuat kemampuan sibernya untuk mencegah infiltrasi sistem domestiknya oleh musuh luar, sekaligus menunjukkan kesiapan untuk melawan balik. Ketiga, *cyber coercion*, yaitu penggunaan serangan siber yang mengandung unsur pemaksaan. Dalam beberapa kasus, operasi Lazarus memuat ancaman kebocoran data atau kerusakan sistem sebagai cara untuk mempengaruhi keputusan negara lain atau perusahaan global.

Dari semua pendekatan ini, tampak jelas bahwa keberadaan Lazarus Group tidak bisa dipisahkan dari strategi bertahan hidup dan ekspansi kekuatan Korea Utara di era modern. Kelompok ini bukan semata-mata pelaku kriminal digital, melainkan instrumen geopolitik yang dirancang dengan cermat untuk menanggapi tekanan global, mengganggu sistem internasional yang tidak menguntungkan bagi Korea Utara, dan mempertahankan posisi negara tersebut dalam tatanan dunia yang penuh persaingan.

**Respons Komunitas Internasional terhadap Lazarus Group**

Di tengah meningkatnya ancaman siber global, komunitas internasional menghadapi dilema serius dalam merespons kelompok seperti Lazarus Group. Sebagai aktor non-negara yang diduga kuat disponsori oleh Korea Utara, Lazarus menempati posisi yang kompleks dalam tatanan hukum dan keamanan internasional. Pendekatan teori *rezim internasional* menyoroti bahwa meskipun terdapat norma dan aturan global yang berkembang, kapasitas kolektif untuk mengatur perilaku di ranah siber masih jauh dari memadai.

Upaya multilateralisme memang telah dilakukan melalui berbagai forum global, seperti *United Nations Group of Governmental Experts* (UN GGE) dan *Open-Ended Working Group* (OEWG), yang telah menghasilkan norma-norma dasar perilaku negara di ruang siber. Misalnya, disepakatinya larangan terhadap serangan siber yang menargetkan infrastruktur sipil. Namun, norma-norma ini bersifat *non-binding*, tidak mengikat secara hukum, sehingga daya dorongnya terhadap aktor seperti Korea Utara sangat terbatas. Tanpa sanksi konkret atas pelanggaran atau mekanisme penegakan yang jelas, aturan ini cenderung simbolik dan tidak mampu menghentikan agresi digital seperti yang dilakukan Lazarus Group.

Secara regional, institusi seperti ASEAN telah menyusun strategi kolaboratif seperti *ASEAN Cybersecurity Cooperation Strategy*. Namun, strategi ini masih bersifat deklaratif dan belum dilengkapi dengan sistem pertahanan kolektif atau mekanisme respons cepat terhadap insiden siber. Negara-negara Asia Tenggara, termasuk Indonesia, masih mengandalkan

kebijakan nasional masing-masing, yang menciptakan celah besar dalam koordinasi lintas batas saat menghadapi serangan siber yang sifatnya transnasional dan kompleks.

Ketiadaan rezim siber formal menjadikan dunia maya sebagai "grey zone" hukum, yaitu wilayah yang tidak secara jelas diatur oleh hukum internasional. Di ruang inilah Lazarus beroperasi, memanfaatkan kerentanan sistem hukum global untuk menjalankan misinya dengan minim risiko akuntabilitas.

Pendekatan *cyber deterrence* yang secara teori bertujuan mencegah agresi digital juga menemui tantangan besar dalam kasus Lazarus. Salah satu hambatan utamanya adalah *attribution problem*, yaitu kesulitan dalam mengidentifikasi secara pasti siapa pelaku serangan. Dengan teknik penyamaran yang canggih, penggunaan infrastruktur global, serta eksploitasi kerentanan digital, Lazarus mampu menghindari pelacakan langsung. Hal ini membuat negara-negara sulit memberikan respons yang tegas karena keterbatasan bukti hukum yang kuat. Tanpa atribusi yang jelas, tindakan pembalasan dapat diperdebatkan secara etis maupun legal.

Selain itu, *deterrence by denial*, kemampuan negara untuk memperkuat pertahanan sibernya agar serangan gagal masih belum optimal. Banyak negara, termasuk negara maju, belum memiliki sistem pertahanan digital yang cukup kuat untuk menangkal serangan seperti yang dilancarkan oleh Lazarus. Sementara itu, *deterrence by punishment* telah diupayakan melalui sanksi ekonomi dari Amerika Serikat, Uni Eropa, dan resolusi Dewan Keamanan PBB. Namun, efektivitasnya masih dipertanyakan. Karakter terdesentralisasi dan fleksibel dari operasi Lazarus membuat mereka tetap dapat menjalankan aksinya, bahkan di tengah tekanan sanksi.

Lebih jauh lagi, keberadaan Lazarus sebagai *state-sponsored non-state actor* menimbulkan kebingungan hukum internasional. Mereka bukan bagian resmi dari militer Korea Utara, tetapi berbagai laporan dan bukti teknis menunjukkan keterkaitan erat dengan strategi negara. Ini menciptakan ambiguitas hukum, apakah mereka harus diperlakukan sebagai entitas kriminal, kelompok teroris, atau sebagai bagian dari kebijakan negara yang memerlukan respons diplomatik dan militer. Hukum internasional saat ini belum sepenuhnya mengantisipasi keberadaan entitas semacam ini yang beroperasi di antara celah negara dan non-negara.

Di sisi lain, kerja sama internasional dalam menanggulangi kejahatan siber juga terganjal oleh masalah yurisdiksi, disparitas hukum nasional, dan kapasitas lembaga internasional seperti INTERPOL atau UNODC yang belum cukup siap menghadapi bentuk *cyber warfare*. Hambatan ini membuat penegakan hukum atas pelaku serangan seperti Lazarus menjadi sangat sulit, terutama ketika negara asal mereka menolak kerja sama atau justru menjadi pelindung mereka.

Akhirnya, muncul pula persoalan *legitimasi balasan*. Jika suatu negara diserang oleh Lazarus dan memutuskan untuk merespons dengan serangan balik digital, maka timbul pertanyaanterkait sah atau tidaknya tindakan itu secara hukum. Mengingat Lazarus tidak secara resmi mewakili negara, membalas dengan kekuatan negara dapat menimbulkan eskalasi yang tak terkendali dan melanggar prinsip proporsionalitas dalam hukum internasional.

Dengan mempertimbangkan berbagai faktor ini, jelas bahwa respons komunitas internasional terhadap Lazarus Group masih terbatas. Ketidakefisienan norma global, lemahnya mekanisme pencegahan, dan ambiguitas hukum menjadikan Lazarus sebagai contoh nyata dari kegagalan kolektif dalam menyesuaikan aturan internasional terhadap dinamika ancaman siber. Untuk itu, diperlukan pembaruan menyeluruh dalam kerangka hukum dan kebijakan internasional, penguatan koordinasi multilateral, serta peningkatan kapasitas nasional guna menghadapi tantangan digital yang terus berkembang.

## 5. KESIMPULAN DAN SARAN

Lazarus Group merupakan cerminan dari pergeseran strategi keamanan negara yang memanfaatkan ruang siber sebagai instrumen politik dan ekonomi. Sebagai aktor negara yang beroperasi di wilayah hukum yang belum teregulasi dengan baik, Lazarus menjadi simbol tantangan baru dalam keamanan global yang sulit diatasi dengan pendekatan tradisional. Penelitian ini menyimpulkan bahwa dibutuhkan penguatan kerja sama internasional, pembentukan norma hukum internasional yang lebih konkret, serta peningkatan kapasitas negara-negara berkembang dalam mendeteksi dan merespons ancaman siber. Ke depan, studi lanjutan dapat mengkaji lebih dalam respons regional seperti ASEAN dalam membentuk pertahanan siber kolektif terhadap aktor negara seperti Korea Utara.

## DAFTAR REFERENSI


Arreguín-Toft, I. (2001). How the weak win wars: A theory of asymmetric conflict. *International Security, 26*(1), 93–128. https://doi.org/10.1162/016228801753212868

CrowdStrike. (2021). *CrowdStrike global threat report*. https://www.crowdstrike.com/resources/reports/global-threat-report/

Deibert, R. (2019). Authoritarianism goes global: Cyberspace edition. *Journal of Democracy, 30*(2), 64–78. https://doi.org/10.1353/jod.2019.0024

Europol. (2018). *Internet organised crime threat assessment (IOCTA)*. https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2018

FBI. (2014). *Update on Sony investigation*. Federal Bureau of Investigation. https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation

Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review, 100*(4), 817–885. https://doi.org/10.15779/Z38QC7N

Krasner, S. D. (Ed.). (1983). *International regimes*. Cornell University Press.

Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. RAND Corporation. https://www.rand.org/pubs/monographs/MG877.html

Lin, H. (2012). Cyber conflict and national security strategy. In K. Geers (Ed.), *Cyber security: Understanding cyber crimes, computer forensics and legal perspectives* (pp. 153–170). NATO CCDCOE Publications.

Mandiant. (2020). *APT38: Details on North Korea's financially motivated cyber operations*. https://www.mandiant.com/resources/apt38-north-korea-cyber-operation

Nye, J. S. (2017). Deterrence and dissuasion in cyberspace. *International Security, 41*(3), 44–71. https://doi.org/10.1162/ISEC_a_00266

Slaughter, A.-M. (2001). The real new world order. *Foreign Affairs, 80*(1), 183–197. https://doi.org/10.2307/20050020

Tikk, E., & Kerttunen, M. (2020). *International cyber norms: Legal, policy & industry perspectives*. Geneva Centre for Security Policy. https://cybernorms.dialoguesecurity.org

U.S. Department of the Treasury. (2018–2023). *Sanctions on North Korean cyber actors*. https://home.treasury.gov/news/press-releases

UN Group of Governmental Experts. (2015, 2021). *Reports on developments in the field of information and telecommunications in the context of international security*. United Nations Office for Disarmament Affairs. https://www.un.org/disarmament/ict-security/

United Nations Panel of Experts. (2022). *Final report of the Panel of Experts submitted pursuant to resolution 2569 (2021)*. United Nations Security Council. https://undocs.org/S/2022/132

Waltz, K. N. (1979). *Theory of international politics*. McGraw-Hill.