Jurnal Ilmu Komunikasi, Administrasi Publik dan Kebijakan Negara
Volume. 2 Nomor. 2 April 2025
e-ISSN: 3063-7155 ; p-ISSN: 3063-7147, Hal. 143-159
DOI: https://doi.org/10.62383/komunikasi.v2i2.281
Available online at: https://ejournal.appisi.or.id/index.php/Komunikasi

Pencurian *Cryptocurrency* oleh Aktor Negara sebagai Strategi *Hybrid Warfare* (Studi Kasus Kelompok Lazarus)

Muhammad Asnul Husadi [1*], Nur Isdah Idris [2]
[1-2] Departemen Studi Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Hasanuddin, Indonesia

Alamat: Jl. Perintis Kemerdekaan KM.10,90245, Makassar, Indonesia
Korespondensi penulis: asnul05@gmail.com

Abstract. *This study analyzes state-sponsored cryptocurrency theft, focusing on the Lazarus Group affiliated with North Korea, within the framework of contemporary hybrid warfare strategy. Employing a qualitative case study approach, the article explains how systematic and large-scale crypto asset theft conducted by Lazarus Group serves not only financial motives but also functions as a strategic tool to evade international sanctions and fund North Korea's nuclear programs. The research finds that such cybercrimes reflect high-ambiguity, non-conventional tactics key features of hybrid warfare. This study expands the traditional concept of hybrid warfare by incorporating digital financial crimes as instruments of state geopolitical strategy. It further highlights the importance of international collaboration and strengthened cybersecurity policy to address increasingly complex digital-era threats.*

Keywords: *Lazarus Group, North Korea, cryptocurrency theft, hybrid warfare, cybercrime, digital geopolitics*

Abstrak. Penelitian ini menganalisis pencurian cryptocurrency oleh aktor negara, khususnya kelompok Lazarus yang berafiliasi dengan Korea Utara, dalam kerangka strategi *hybrid warfare* kontemporer. Dengan menggunakan pendekatan studi kasus kualitatif, artikel ini menjelaskan bagaimana pencurian aset kripto yang dilakukan secara sistematis dan berskala besar oleh Lazarus Group tidak hanya bermotif finansial, tetapi juga menjadi instrumen strategis untuk menghindari sanksi internasional dan mendanai program nuklir Korea Utara. Penelitian ini menunjukkan bahwa tindakan kejahatan siber tersebut mencerminkan taktik non-konvensional dengan ambiguitas tinggi, yang merupakan ciri utama dari *hybrid warfare*. Temuan ini memperluas konsep tradisional *hybrid warfare* dengan memasukkan kejahatan finansial digital sebagai instrumen geopolitik negara. Artikel ini juga menyoroti pentingnya kerja sama internasional dan penguatan kebijakan keamanan siber untuk menghadapi ancaman yang semakin kompleks di era digital.

Kata kunci: Lazarus Group, Korea Utara, pencurian cryptocurrency, hybrid warfare, kejahatan siber, geopolitik digital

1. LATAR BELAKANG

Dalam beberapa tahun terakhir, teknologi informasi telah berkembang dengan sangat pesat dan menjadi semakin kompleks. Perkembangan ini membawa berbagai kemudahan dalam kehidupan masyarakat, mulai dari akses informasi yang lebih cepat, kemudahan berbisnis secara daring, berkomunikasi jarak jauh, hingga melakukan transaksi pembelian barang dan jasa secara digital. Dalam berbagai transaksi elektronik tersebut, masyarakat kerap memanfaatkan uang digital, yang umumnya diperoleh melalui konversi dari uang fisik ke bentuk digital. Seiring dengan kemajuan teknologi, para ahli juga menciptakan bentuk baru dari sistem keuangan digital yang dikenal dengan istilah *cryptocurrency*. Istilah virtual dalam hal ini merujuk pada sesuatu yang sepenuhnya digunakan secara elektronik atau daring. *Cryptocurrency* merupakan uang digital yang dapat ditukar dengan uang asli dalam

Received: April 05, 2025; Revised: April 14, 2025; Accepted: April 27, 2025; Published: April 30, 2025

transaksi online, serta kian banyak dimanfaatkan dalam aktivitas perdagangan maupun investasi. Aset digital ini dapat diperoleh melalui pembelian di platform khusus maupun melalui proses *mining* secara digital, dan nilai tukarnya bahkan dapat mencapai puluhan juta rupiah (Azizah & Irfan, 2020).

Namun, di balik potensi inovatifnya, cryptocurrency juga menyimpan kerentanan serius. Sifatnya yang anonim, kurangnya regulasi global yang seragam, serta tingginya nilai aset membuatnya menjadi target empuk bagi berbagai bentuk kejahatan digital. Salah satu bentuk eksploitasi digital yang menonjol dalam konteks ini adalah pencurian aset kripto (*cryptocurrency theft*), yaitu tindakan ilegal yang menyasar aset digital, baik melalui peretasan sistem, pemalsuan identitas, manipulasi dompet digital, maupun eksploitasi celah keamanan lainnya. Dalam banyak kasus, aset kripto juga digunakan dalam tindak kejahatan seperti pencucian uang, pemerasan siber, phishing, penipuan investasi, hingga skema Ponzi (Reddy & Minnaar, 2018). Kompleksitas teknis dan sifat desentralisasi cryptocurrency membuat pelacakan dan penegakan hukum menjadi tantangan besar bagi otoritas keamanan siber global.

Fenomena ini menjadi semakin mengkhawatirkan ketika aktor-aktor negara mulai terlibat dalam pencurian aset kripto sebagai bagian dari strategi geopolitik. Laporan Chainalysis (2025) menyebutkan bahwa sepanjang tahun 2024, total aset kripto yang dicuri mencapai $2,2 miliar, dengan 61% di antaranya dikaitkan langsung dengan kelompok peretas Korea Utara. Salah satu kelompok yang paling menonjol adalah Lazarus Group, yang oleh FBI (2023) dikonfirmasi sebagai pelaku serangan terhadap platform Harmony's Horizon Bridge dan Ronin Bridge, dengan total kerugian lebih dari $700 juta. Panel Ahli PBB (2023) juga menyebut bahwa Lazarus Group bersama unit lain seperti Kimsuky dan Andariel, berafiliasi langsung dengan Reconnaissance General Bureau (RGB), badan intelijen Korea Utara, yang terlibat dalam penggalangan dana ilegal untuk mendukung program nuklir negara tersebut.

Dalam konteks ini, konsep *hybrid warfare* menjadi penting untuk memahami dinamika baru dalam kejahatan siber yang melibatkan aktor negara. Mumford dan Carlucci (2023) menjelaskan bahwa esensi utama dari *hybrid warfare* terletak pada penggunaan ambiguitas secara strategis untuk membingungkan lawan mengenai niat politik, sasaran militer, maupun batas eskalasi konflik. Bentuk konflik ini tidak dimulai dengan deklarasi perang, melainkan dimanifestasikan melalui taktik non-konvensional dan tersembunyi seperti serangan siber, kampanye disinformasi, hingga tekanan ekonomi. Ketidakjelasan tersebut memaksa musuh menyebarkan sumber dayanya secara tidak efisien karena harus

bersiap menghadapi berbagai kemungkinan, mulai dari gangguan politik hingga aneksasi wilayah. Lebih lanjut, strategi ini memungkinkan aktor negara menggunakan beragam instrumen baik kekuatan militer terbuka maupun operasi terselubung secara kreatif untuk menciptakan kebuntuan kognitif di pihak lawan, tanpa harus melampaui ambang batas respons militer terbuka. Justru dalam ambiguitas inilah terletak kekuatan utama *hybrid warfare*, karena memungkinkan pelaku mempertahankan fleksibilitas politik, serta memulai atau mengakhiri konflik dengan cepat tanpa risiko eskalasi besar. Pencurian cryptocurrency oleh kelompok peretas yang didukung negara, seperti dalam kasus Korea Utara, menunjukkan karakteristik yang sejalan dengan pola *hybrid warfare* tersebut.

Dengan demikian, penelitian ini bertujuan untuk menganalisis keterkaitan antara pencurian cryptocurrency yang dilakukan oleh aktor negara dengan konsep *hybrid warfare* dalam kerangka konflik geopolitik modern. Penelitian ini juga bermaksud untuk menggali bagaimana strategi digital seperti serangan siber dan kejahatan finansial dapat digunakan sebagai instrumen non-konvensional dalam mencapai tujuan politik suatu negara, khususnya dalam konteks ambiguitas dan taktik non-linier yang menjadi ciri utama *hybrid warfare*.

Berdasarkan tujuan tersebut, penelitian ini merumuskan dua pertanyaan utama sebagai fokus kajian:

- Apakah pencurian cryptocurrency yang dilakukan oleh aktor negara dapat dikategorikan sebagai bentuk dari *hybrid warfare* dalam konteks konflik geopolitik modern?
- Bagaimana strategi digital seperti serangan siber dan kejahatan finansial digunakan sebagai instrumen non-konvensional untuk mencapai tujuan politik, khususnya melalui elemen ambiguitas dalam *hybrid warfare*?

Penelitian ini diharapkan dapat memberikan kontribusi baik secara teoretis maupun praktis. Secara teoretis, penelitian ini dapat memperkaya kajian mengenai konsep *hybrid warfare*, khususnya dalam konteks konflik digital yang melibatkan aktor negara dan instrumen kejahatan siber seperti pencurian *cryptocurrency*. Sementara itu, secara praktis, penelitian ini diharapkan dapat memberikan wawasan bagi para pembuat kebijakan, peneliti keamanan, serta aparat penegak hukum dalam memahami bentuk-bentuk ancaman non-konvensional di ruang digital, sehingga dapat mendorong perumusan kebijakan keamanan siber yang lebih adaptif dan strategis.

Berdasarkan hasil studi pendahuluan, sudah ada beberapa penelitian sebelumnya yang membahas tentang pencurian cryptocurrency, keterlibatan aktor negara dalam kejahatan siber, dan konsep hybrid warfare. Penelitian-penelitian ini menjadi dasar penting untuk memahami konteks kajian yang dilakukan dalam penelitian ini.

Dalam penelitian yang dilakukan oleh Perdana, Aminanto, dan Anggorojati (2024) berjudul *Hack, Heist, and Havoc: The Lazarus Group's Triple Threat to Global Cybersecurity* yang dipublikasikan dalam *Journal of Cyber Policy*, aktivitas siber yang dilakukan oleh kelompok Lazarus Group dianalisis secara terstruktur berdasarkan teknik dan taktik yang digunakan, seperti rekayasa sosial, injeksi malware, gangguan sistem, penghindaran deteksi, dan spionase. Studi ini mengungkap bahwa Lazarus Group tidak hanya memanfaatkan eksploitasi teknologi, tetapi juga memanfaatkan kerentanan perilaku manusia untuk melancarkan serangan mereka. Aktivitas kelompok ini dilihat sebagai bagian dari strategi perang asimetris Korea Utara, memungkinkan rezim tersebut untuk memproyeksikan kekuatan dan pengaruh secara tidak proporsional dibandingkan dengan kapasitas militer dan ekonominya yang terbatas. Selain itu, penelitian ini juga menunjukkan bahwa serangan Lazarus sering kali mengaburkan batas antara kejahatan siber terorganisasi dan operasi siber yang disponsori negara, memperlihatkan karakteristik campuran dari berbagai profil aktor ancaman, mulai dari kriminal terorganisir hingga entitas yang didukung negara. Temuan ini relevan dengan penelitian ini karena menunjukkan bahwa pencurian cryptocurrency yang dilakukan oleh aktor negara seperti Lazarus Group dapat dipahami sebagai bagian dari strategi *hybrid warfare*, yang memanfaatkan ambiguitas taktis dan instrumen non-konvensional untuk mencapai tujuan geopolitik.

Dalam penelitian yang dilakukan oleh Kole Zellers (2024) berjudul *Hacked! North Korea's Billion-Dollar Crypto Heisting Scheme* yang dipublikasikan dalam *Penn State Journal of Law & International Affairs*, dianalisis bagaimana Korea Utara secara sistematis memanfaatkan kerentanan dalam platform keuangan terdesentralisasi (DeFi) untuk mencuri cryptocurrency dalam skala besar. Studi ini mencatat bahwa pada tahun 2022 saja, Korea Utara berhasil mencuri lebih dari satu miliar dolar AS dalam bentuk aset kripto dari protokol DeFi. Artikel ini juga menekankan bahwa pencurian ini digunakan untuk mendukung program nuklir negara tersebut, dengan mencatat bahwa hasil dari serangan Lazarus Group dan kelompok siber lainnya secara langsung berkontribusi terhadap pendanaan proyek senjata pemusnah massal Korea Utara. Selain itu, penelitian ini menguraikan strategi canggih yang digunakan Korea Utara untuk mencuci hasil curian, termasuk penggunaan mixer cryptocurrency seperti Tornado Cash untuk menyamarkan sumber dana. Temuan ini

memperkuat argumen penelitian ini bahwa pencurian cryptocurrency bukan sekadar tindakan kriminal biasa, melainkan merupakan bagian dari strategi geopolitik negara, selaras dengan konsep hybrid warfare yang menggabungkan kekuatan siber untuk mencapai tujuan politik tanpa keterlibatan militer langsung.

Dalam artikel *The Mouse Clicks of August: Hybrid Warfare, Nation-State Actors, and the Future of Cybersecurity*, Dougherty (2018) membahas bagaimana aktor negara seperti Rusia dan kelompok peretas yang mereka sponsori, seperti APT28, semakin memanfaatkan dunia maya sebagai arena utama dalam strategi *hybrid warfare*. Ia mencatat bahwa kelompok ini telah beralih dari sekadar pengumpulan informasi menjadi melakukan tindakan ofensif yang mencakup serangan *denial-of-service* (DoS), sabotase infrastruktur, dan penyebaran informasi yang memalukan untuk mencapai tujuan politik tanpa keterlibatan militer langsung. Dougherty menyoroti bahwa serangan siber terhadap Estonia pada 2007, Georgia pada 2008, dan Ukraina pada 2015, yang secara luas dikaitkan dengan Rusia, menunjukkan eskalasi penggunaan dunia maya dalam konflik geopolitik, termasuk pemadaman jaringan listrik dan gangguan terhadap situs pemerintah. Artikel ini menekankan bahwa sifat global dan anonim dari internet mempersulit atribusi serangan, memungkinkan negara-negara untuk melakukan tindakan agresif sambil menghindari tanggung jawab langsung. Dengan demikian, Dougherty memperkuat pemahaman bahwa dunia maya telah menjadi medan perang utama dalam strategi *hybrid warfare* modern.

Meskipun berbagai penelitian sebelumnya telah mengkaji fenomena pencurian cryptocurrency oleh aktor negara dan penggunaan dunia maya dalam konteks hybrid warfare, keterkaitan spesifik antara pencurian aset digital dan implementasi strategi hybrid warfare dalam konteks konflik geopolitik modern masih belum banyak dieksplorasi secara mendalam. Penelitian ini menawarkan kebaruan dengan menganalisis bagaimana tindakan pencurian cryptocurrency yang dilakukan oleh aktor negara, seperti Lazarus Group, dapat dipahami tidak hanya sebagai bentuk kejahatan siber, tetapi juga sebagai instrumen strategis dalam kerangka hybrid warfare yang memanfaatkan ambiguitas taktis untuk mencapai tujuan politik tanpa keterlibatan militer terbuka.

2. METODE PENELITIAN

Penelitian ini menggunakan metode kualitatif deskriptif dengan pendekatan studi kasus. Metode ini dipilih karena dapat menggambarkan secara mendalam fenomena pencurian cryptocurrency oleh aktor negara, khususnya oleh kelompok Lazarus Group, dalam kerangka strategi hybrid warfare. Menurut Baxter dan Jack (2008), metode studi

kasus memungkinkan eksplorasi secara komprehensif terhadap fenomena yang kompleks dan terikat pada konteks spesifik. Teknik pengumpulan data dilakukan melalui studi dokumentasi, yaitu dengan mengumpulkan data sekunder dari berbagai sumber terpercaya. Data dikumpulkan dari laporan resmi lembaga pemerintah dan internasional, seperti FBI dan PBB, artikel jurnal ilmiah yang relevan, laporan dari perusahaan keamanan siber seperti Chainalysis, serta berita investigatif dari media kredibel. Teknik ini dianggap efektif dalam memperoleh data kualitatif yang kaya dan mendalam, terutama ketika data primer sulit diperoleh (Marrelli, 2007). Dengan demikian, metode dan teknik pengumpulan data yang digunakan dalam penelitian ini bertujuan untuk mendapatkan pemahaman yang menyeluruh dan mendalam mengenai bagaimana pencurian cryptocurrency oleh aktor negara dapat dipahami sebagai bagian dari strategi hybrid warfare.

3. HASIL DAN PEMBAHASAN

Temuan Utama

- **Kasus Pencurian Cryptocurrency oleh Lazarus Group**

  Lazarus Group, kelompok peretas yang berafiliasi dengan pemerintah Korea Utara, telah menjadi aktor utama dalam serangkaian pencurian cryptocurrency berskala besar di seluruh dunia. Aktivitas kelompok ini tidak hanya menimbulkan kerugian finansial yang sangat besar tetapi juga menunjukkan adanya dimensi strategis dalam konteks geopolitik. Berdasarkan laporan Chainalysis (2023), pada tahun 2022, volume transaksi ilegal berbasis cryptocurrency mencapai $20,6 miliar, dengan 43% dari jumlah tersebut terkait langsung dengan entitas yang dikenai sanksi internasional. Di antara para pelaku utama, Lazarus Group tercatat sebagai pihak yang bertanggung jawab atas beberapa peretasan besar, termasuk Harmony’s Horizon Bridge pada 24 Juni 2022, yang mengakibatkan kerugian hingga $100 juta. Kasus ini dikonfirmasi oleh FBI pada awal 2023, yang menyatakan bahwa Lazarus Group menggunakan teknik peretasan canggih, termasuk rekayasa sosial dan injeksi malware. Setelah mencuri dana, kelompok ini menggunakan layanan mixer seperti Tornado Cash untuk menyamarkan asal-usul dana sebelum mengalirkannya ke berbagai dompet anonim (FBI, 2023). Pada tahun 2024, aktivitas Lazarus Group semakin masif dan sistematis. Berdasarkan laporan Crypto Crime Report 2025 dari Chainalysis, volume cryptocurrency ilegal pada tahun tersebut mencapai $40,9 miliar, meningkat signifikan dari tahun sebelumnya. Dari jumlah tersebut, $1,34 miliar atau sekitar 61% dari total cryptocurrency yang dicuri dapat ditelusuri kembali ke aktivitas Lazarus Group.

Beberapa kasus besar menunjukkan bagaimana aktor siber Korea Utara, terutama Lazarus Group, secara aktif melancarkan serangan terhadap berbagai platform cryptocurrency dunia. Salah satu insiden penting terjadi pada tanggal 4 September 2023, ketika platform perjudian kripto Stake.com mengalami peretasan besar yang menyebabkan kerugian sekitar $41 juta. Lazarus Group, yang secara jelas terafiliasi dengan pemerintah Korea Utara, melakukan serangan ini dengan menggunakan teknik rekayasa sosial (social engineering). Kelompok tersebut memperoleh akses ke dompet panas (hot wallets) yang berada pada jaringan Ethereum, Binance Smart Chain (BSC), dan Polygon. Insiden ini secara khusus menggarisbawahi tingginya tingkat kerentanan keamanan pada platform perjudian berbasis kripto, yang semakin sering menjadi sasaran utama kelompok peretas skala global (FBI, 2023).

Selanjutnya, pada Mei 2024, platform pertukaran kripto asal Jepang, DMM Bitcoin Exchange, mengalami peretasan besar-besaran yang mengakibatkan pencurian sebesar 4.502,9 BTC atau sekitar $308 juta. Serangan ini menjadi salah satu pencurian terbesar dalam sejarah cryptocurrency dan mendapatkan perhatian dari berbagai lembaga keamanan siber internasional, termasuk FBI, Department of Defense Cyber Crime Center (DC3), dan Kepolisian Nasional Jepang (NPA). Pelaku serangan, kelompok peretas yang disebut TraderTraitor, juga terafiliasi dengan pemerintah Korea Utara. Sama seperti serangan sebelumnya, teknik rekayasa sosial menjadi metode utama mereka untuk menembus sistem internal perusahaan secara sistematis (FBI, 2024).

Kasus lainnya terjadi pada bulan Juli 2024, ketika WazirX Exchange, platform pertukaran kripto terbesar di India, menjadi korban serangan yang mengakibatkan kerugian sekitar $235 juta. Lazarus Group kembali diidentifikasi sebagai pelaku utama, yang berhasil mengeksploitasi dompet multisignature melalui manipulasi kontrak pintar serta teknik rekayasa sosial yang kompleks. Dampak dari serangan ini begitu besar hingga memaksa WazirX menghentikan sebagian besar operasionalnya dan memicu investigasi internasional yang melibatkan Jepang, Korea Selatan, dan Amerika Serikat. Ketiga negara tersebut kemudian mengeluarkan pernyataan bersama yang secara resmi mengidentifikasi Lazarus Group sebagai pelaku, menegaskan bahwa serangan tersebut merupakan bagian integral dari kampanye peretasan yang dijalankan oleh aktor negara Korea Utara (Times of India, 2024).

Setelah berhasil mencuri dana, Lazarus Group menggunakan strategi pencucian uang digital yang sangat kompleks. Dana yang dicuri kemudian dipindahkan ke lebih

dari 40 alamat dompet kripto yang telah diidentifikasi oleh FBI. Proses pencucian tersebut dilakukan dengan memecah dana ke dalam beberapa transaksi kecil untuk menyulitkan upaya pelacakan oleh pihak berwenang. Menurut FBI dalam pernyataan resmi pada 6 September 2023, metode yang digunakan Lazarus Group mencerminkan karakteristik serangan yang sangat sistematis dan terstruktur, serta memanfaatkan infrastruktur digital global untuk memfasilitasi pencucian dana hasil kejahatan siber tersebut. FBI juga menegaskan bahwa aktivitas ini merupakan bagian integral dari strategi Korea Utara dalam mengumpulkan dana ilegal yang bertujuan untuk mendukung berbagai program strategis nasional, khususnya pengembangan senjata pemusnah massal (FBI, 2023).

Puncak dari aktivitas pencurian Lazarus Group terjadi pada Februari 2025, ketika kelompok ini melakukan peretasan terbesar dalam sejarah cryptocurrency dengan menyerang platform Bybit. Serangan tersebut mengakibatkan hilangnya sekitar $1,5 miliar dalam bentuk Ethereum. Berdasarkan laporan dari Cointelegraph (2025), teknik yang digunakan melibatkan rekayasa sosial melalui spear-phishing, yang memungkinkan para peretas memperoleh akses ke kredensial penting. Setelah mendapatkan akses, mereka melakukan pencurian aset digital melalui pertukaran terdesentralisasi dan menyembunyikan jejak transaksi dengan menggunakan dompet dorman. Strategi pencucian ini melibatkan pemecahan dana ke lebih dari 50 dompet berbeda, membuat proses pelacakan menjadi sangat sulit dilakukan.

Strategi pencucian dana oleh Lazarus Group menunjukkan pola yang semakin terstruktur dan sulit dideteksi. Kelompok ini memanfaatkan berbagai metode pencucian uang digital, termasuk penggunaan mixer cryptocurrency seperti Tornado Cash dan Railgun, serta pertukaran terdesentralisasi seperti THORChain. Menurut laporan dari Elliptic, setelah pencurian dana dari *Harmony Horizon Bridge* pada Juni 2022, Lazarus Group mengalihkan lebih dari $555 juta melalui Tornado Cash. Setelah sanksi terhadap Tornado Cash diberlakukan pada Agustus 2022, mereka mulai menggunakan Railgun sebagai alternatif, dengan sekitar 70% dari dana yang dikirim melalui Railgun berasal dari peretasan Harmony. Dalam kasus peretasan Bybit pada Februari 2025, Lazarus Group menggunakan THORChain untuk menukar Ethereum yang dicuri menjadi Bitcoin dan aset kripto lainnya. Proses ini melibatkan pemecahan dana ke lebih dari 50 dompet berbeda, serta penyimpanan dana di dompet yang tidak aktif untuk jangka waktu lama sebelum dialirkan ke dompet lain, sehingga menyulitkan upaya pelacakan oleh lembaga keamanan siber. Motif utama dari aktivitas kriminal ini tidak hanya

berorientasi pada keuntungan finansial tetapi juga terkait dengan agenda geopolitik Korea Utara. Berdasarkan laporan Dewan Keamanan PBB (2023), hasil pencurian cryptocurrency ini digunakan untuk mendanai program nuklir negara tersebut. Hal ini mengindikasikan bahwa pencurian cryptocurrency oleh kelompok ini tidak hanya bersifat kriminal tetapi juga merupakan bagian dari strategi hybrid warfare, di mana kekuatan siber digunakan sebagai instrumen untuk mencapai tujuan politik tanpa keterlibatan militer langsung.

Secara keseluruhan, kasus pencurian cryptocurrency oleh Lazarus Group tidak hanya menimbulkan kerugian ekonomi global yang signifikan tetapi juga menunjukkan bagaimana aktivitas kriminal siber dapat dimanfaatkan sebagai alat geopolitik. Dengan memanfaatkan kerentanan dalam infrastruktur keuangan digital global, kelompok ini berhasil mengumpulkan dana dalam jumlah besar untuk mendukung agenda politik Korea Utara. Aksi mereka memperlihatkan bagaimana strategi hybrid warfare dapat beroperasi melalui serangan siber dengan cara yang sulit diidentifikasi dan ditanggulangi oleh komunitas internasional.

- **Motif dan Tujuan Strategis**

Motif utama di balik aktivitas pencurian cryptocurrency oleh Lazarus Group yang terafiliasi dengan Korea Utara mencerminkan berbagai dimensi strategis, yang meliputi aspek finansial, geopolitik, teknologi, serta implementasi konsep hybrid warfare.

Secara finansial, motif pencurian cryptocurrency oleh Lazarus Group secara nyata bertujuan mendanai program nuklir dan rudal balistik Korea Utara. Laporan Georgetown Journal of International Affairs (2024) menegaskan bahwa hasil curian aset digital digunakan secara sistematis untuk memperkuat kapabilitas militer negara tersebut, khususnya dalam pengembangan senjata nuklir dan balistik. Hal ini diperkuat oleh laporan FBI terkait peretasan platform Bybit, yang mengakibatkan kerugian sekitar $1,5 miliar. Dana hasil pencurian ini secara eksplisit disebut digunakan untuk membiayai program nuklir Korea Utara (The Guardian, 2025). Motif finansial ini menunjukkan bahwa pencurian cryptocurrency merupakan solusi strategis Korea Utara untuk memenuhi kebutuhan keuangan yang besar, tanpa terhambat oleh kontrol internasional.

Di sisi geopolitik, aktivitas pencurian cryptocurrency menjadi strategi efektif bagi Korea Utara untuk menghindari dampak buruk dari berbagai sanksi internasional. Dalam kondisi terisolasi secara ekonomi dan politik, Korea Utara memanfaatkan aset digital yang sulit dilacak sebagai instrumen untuk melewati regulasi keuangan global,

sekaligus menjaga kesinambungan pendanaan program-program strategis nasional. Strategi ini juga secara signifikan meningkatkan daya tawar Korea Utara dalam politik internasional, mengingat negara-negara lain sulit mengambil tindakan tegas tanpa risiko eskalasi konflik militer langsung. Dari perspektif teknologi, keberhasilan Lazarus Group menembus berbagai platform keuangan digital global menunjukkan kemampuan teknologis Korea Utara yang tinggi dalam domain siber. Keberhasilan ini bukan sekadar demonstrasi kapabilitas teknis, melainkan juga berfungsi sebagai bentuk deterrence strategis. Dengan memperlihatkan bahwa Korea Utara mampu melakukan serangan siber yang kompleks dan sulit dideteksi, rezim tersebut secara tidak langsung memperingatkan negara-negara lain mengenai potensi risiko konflik digital dengan Korea Utara. Serangan ini juga menciptakan ketidakpastian dalam ekosistem keuangan digital global, melemahkan kepercayaan publik terhadap stabilitas pasar cryptocurrency secara keseluruhan.

Secara strategis, aktivitas Lazarus Group sangat sejalan dengan implementasi konsep hybrid warfare. Dalam kerangka ini, Korea Utara memanfaatkan instrumen siber untuk menciptakan ambiguitas dan ketidakjelasan taktis dalam aksinya. Menurut Mumford dan Carlucci (2023), penggunaan serangan siber sebagai bagian dari hybrid warfare memungkinkan Korea Utara mencapai tujuan politiknya tanpa harus melintasi batas konfrontasi militer terbuka. Dengan demikian, Korea Utara berhasil menghindari respons militer langsung dari negara-negara lain, sekaligus mempertahankan fleksibilitas dalam menentukan intensitas konflik geopolitik. Namun demikian, perlu dicatat bahwa strategi ini tidak bebas dari risiko. Peningkatan perhatian global terhadap ancaman siber yang ditimbulkan oleh Lazarus Group dapat memicu respons internasional yang lebih agresif, baik berupa sanksi tambahan maupun peningkatan kapabilitas siber negara-negara lawan. Dengan kata lain, keberhasilan jangka pendek dalam pencurian cryptocurrency bisa saja menimbulkan konsekuensi jangka panjang berupa peningkatan isolasi diplomatik dan peningkatan kewaspadaan internasional terhadap ancaman Korea Utara.

Kesimpulannya, motif dan tujuan strategis di balik pencurian cryptocurrency oleh Lazarus Group mencerminkan pendekatan baru dalam konflik geopolitik modern, di mana penggunaan instrumen digital menggantikan metode konvensional dalam mencapai tujuan politik dan militer. Fenomena ini tidak hanya mengubah dinamika konflik geopolitik, tetapi juga menghadirkan tantangan baru bagi keamanan global dalam menghadapi ancaman yang bersifat non-konvensional**.**

Analisis dalam Kerangka Hybrid Warfare

- **Ambiguitas dalam Strategi Hybrid Warfare**

Salah satu ciri utama strategi hybrid warfare adalah penggunaan ambiguitas secara strategis untuk menyamarkan niat, tujuan, serta asal-usul tindakan yang dilakukan. Ambiguitas ini bertujuan menciptakan kebingungan dan ketidakpastian di pihak lawan, sehingga membuat respons menjadi sulit dilakukan secara cepat dan efektif. Mumford dan Carlucci (2023) menjelaskan bahwa konsep hybrid warfare tidak ditandai dengan deklarasi perang terbuka, melainkan melalui tindakan yang sulit diklasifikasikan antara kriminalitas murni dan operasi militer formal. Dengan demikian, tindakan-tindakan dalam hybrid warfare sering kali berada dalam area abu-abu, sehingga tidak dapat dengan mudah dikategorikan sebagai agresi militer yang sah menurut hukum internasional.

Lazarus Group, sebagai bagian dari aktor negara Korea Utara, sering kali beroperasi dalam kerangka hybrid warfare dengan memanfaatkan teknik peretasan canggih yang secara formal tidak diklaim oleh pemerintah. Misalnya, dalam kasus Harmony's Horizon Bridge dan Ronin Bridge, teknik rekayasa sosial dan injeksi malware digunakan secara luas, namun tidak ada klaim langsung dari pemerintah Korea Utara. Hal ini sengaja dilakukan untuk menciptakan ambiguitas yang mempersulit proses atribusi langsung kepada negara asal. Dougherty (2018) juga mencatat bahwa negara-negara seperti Rusia melalui kelompok APT28 menggunakan taktik serupa, dengan menjaga ambiguitas agar tidak langsung dikaitkan dengan otoritas negara. Ambiguitas ini menciptakan kesulitan bagi komunitas internasional dalam memberikan respons yang tepat. Negara-negara korban sering kali kebingungan dalam menentukan jalur tindakan: apakah harus merespons dengan langkah diplomatik, ekonomi, atau bahkan tindakan militer. Situasi ini menciptakan ruang strategis bagi Korea Utara untuk menjalankan aksinya tanpa memicu eskalasi konflik yang lebih besar. Selain itu, ambiguitas juga memungkinkan Korea Utara untuk tetap mempertahankan fleksibilitas politik dan militer, karena tidak ada bukti eksplisit yang mengaitkan aksi siber tersebut dengan pemerintah secara langsung (Mumford & Carlucci, 2023).

Strategi ini sangat efektif dalam konteks geopolitik modern karena memungkinkan negara untuk mengeksploitasi celah dalam respons global terhadap ancaman non-konvensional. Dengan tidak adanya deklarasi perang atau klaim resmi, negara-negara korban cenderung menghindari eskalasi langsung, mengingat risiko

konflik militer yang lebih besar. Hal ini memberi Korea Utara keuntungan strategis untuk mencapai tujuannya tanpa melampaui batas konfrontasi militer terbuka.

- **Taktik Non-Konvensional dalam Kejahatan Siber**

  Taktik non-konvensional adalah bagian integral dari strategi hybrid warfare, terutama ketika negara menghadapi keterbatasan dalam kekuatan militer konvensional. Lazarus Group sebagai entitas yang didukung negara menunjukkan kemampuan tinggi dalam mengadopsi metode non-konvensional, seperti serangan siber dan pencurian cryptocurrency, untuk mendukung agenda geopolitik Korea Utara. Menurut Reddy dan Minnaar (2018), serangan siber adalah alat strategis yang sangat efektif dalam mencapai dampak ekonomi dan psikologis secara signifikan dengan risiko rendah bagi pelakunya.

  Salah satu contoh taktik non-konvensional yang digunakan oleh Lazarus Group adalah serangan terhadap Ronin Bridge pada Maret 2022, yang menyebabkan kerugian sekitar $625 juta. Teknik yang digunakan mencakup phishing canggih dan manipulasi dompet digital, yang tidak hanya menciptakan kerugian finansial besar tetapi juga merusak reputasi keamanan platform keuangan digital. Demikian pula, serangan terhadap Harmony's Horizon Bridge pada Juni 2022 berhasil mencuri sekitar $100 juta dengan menggunakan teknik serupa, yang mengakibatkan guncangan besar dalam komunitas kripto global (FBI, 2023). Selain itu, serangan terhadap Bybit pada Februari 2025 yang mengakibatkan kerugian sebesar $1,5 miliar juga menunjukkan penggunaan teknik spear-phishing dan pengelolaan dana curian melalui platform pertukaran terdesentralisasi seperti THORChain. Teknik ini memungkinkan pencucian uang digital secara efektif, dengan cara memecah dana ke dalam dompet kecil yang tersebar di banyak jaringan blockchain, sehingga mempersulit proses pelacakan oleh otoritas keamanan internasional. Menurut Zellers (2024), teknik ini memungkinkan Korea Utara tetap memperoleh keuntungan ekonomi tanpa menghadapi risiko tambahan dari tindakan pembalasan militer atau sanksi ekonomi langsung. Taktik non-konvensional dalam kejahatan siber ini secara efektif memanfaatkan kerentanan dalam infrastruktur digital global. Dengan tidak melibatkan kekuatan militer secara langsung, Korea Utara mampu menjaga kelangsungan program strategisnya tanpa menghadapi tekanan politik yang lebih besar. Serangan siber ini tidak hanya menciptakan dampak langsung dalam bentuk kerugian ekonomi, tetapi juga menghasilkan efek jera di kalangan pelaku bisnis digital yang mempertimbangkan risiko keamanan dalam menggunakan platform berbasis blockchain.

Kesimpulannya, analisis ini mempertegas bahwa pencurian cryptocurrency oleh Lazarus Group bukanlah sekadar kejahatan finansial biasa, tetapi merupakan bagian dari strategi hybrid warfare yang sistematis. Ambiguitas dalam tindakan dan pemanfaatan taktik non-konvensional memungkinkan Korea Utara mempertahankan daya tawar politiknya tanpa melibatkan konflik militer langsung. Fenomena ini menunjukkan perubahan paradigma dalam strategi geopolitik modern, di mana kekuatan digital digunakan sebagai alat utama untuk mencapai tujuan politik tanpa memicu respons militer konvensional.

Diskusi: Kontribusi terhadap Pemahaman Hybrid Warfare

Penelitian ini memberikan kontribusi penting terhadap pengembangan literatur hybrid warfare, khususnya dengan memasukkan fenomena pencurian cryptocurrency oleh aktor negara sebagai bagian dari taktik perang non-konvensional. Sebelumnya, konsep hybrid warfare umumnya difokuskan pada perpaduan antara operasi militer terbuka, perang informasi, dan tindakan subversif, seperti yang diuraikan oleh Mumford dan Carlucci (2023). Namun, kajian ini memperluas cakupan tersebut dengan menekankan bahwa kejahatan finansial digital, khususnya pencurian aset kripto yang dilakukan secara terorganisir oleh kelompok seperti Lazarus Group, kini telah menjadi instrumen strategis dalam persaingan geopolitik antarnegara.

Dibandingkan dengan penelitian terdahulu yang cenderung hanya membahas cybercrime atau serangan siber sebagai ancaman tersendiri (Dougherty, 2018; Reddy & Minnaar, 2018), penelitian ini menyoroti keterkaitan langsung antara tindakan kriminal siber dengan strategi negara dalam konteks hybrid warfare. Temuan ini menunjukkan bahwa aktivitas Lazarus Group tidak dapat lagi dipahami semata-mata sebagai tindak kejahatan, melainkan sebagai bagian dari kebijakan luar negeri Korea Utara untuk membiayai program-program strategis nasionalnya, sekaligus menghindari sanksi internasional yang semakin ketat.

Dari sisi teoretis, penelitian ini mengusulkan bahwa konsep hybrid warfare perlu terus dikembangkan agar mampu mengakomodasi bentuk-bentuk baru ancaman non-konvensional di era digital. Penulis menegaskan bahwa pencurian cryptocurrency oleh aktor negara merupakan bentuk hybrid threat yang memadukan antara dimensi keuangan, teknologi, dan politik secara simultan. Hal ini menuntut pengembangan kerangka analisis baru yang tidak hanya mengandalkan deteksi dan penanggulangan serangan siber secara teknis, tetapi juga memahami motivasi strategis di balik tindakan tersebut. Secara praktis, hasil penelitian ini memberikan beberapa implikasi kebijakan yang krusial. Pertama,

diperlukan peningkatan koordinasi antarnegara, baik di level regional maupun global, untuk mengembangkan sistem deteksi, pelacakan, dan pencegahan kejahatan siber lintas batas yang berbasis aset digital. Kedua, penguatan regulasi dan pengawasan terhadap ekosistem cryptocurrency menjadi sangat penting guna menutup celah yang dapat dimanfaatkan oleh aktor negara maupun kelompok kriminal terorganisir. Ketiga, komunitas internasional perlu memperkuat diplomasi siber dan kerja sama pertahanan siber untuk merespons taktik hybrid warfare yang semakin kompleks.

Keterbatasan utama dalam studi ini terletak pada ketergantungan pada data sekunder dan keterbatasan akses terhadap data primer dari aktor negara terkait. Selain itu, fokus penelitian masih terpusat pada studi kasus Korea Utara melalui kelompok Lazarus Group, sehingga perlu dilakukan studi lanjutan dengan membandingkan pola serangan siber oleh aktor negara lain seperti Rusia, Iran, atau Tiongkok.

Secara keseluruhan, penelitian ini tidak hanya memberikan bukti empiris mengenai evolusi kejahatan siber sebagai instrumen strategi hybrid warfare, tetapi juga menawarkan perspektif baru bagi pengembangan teori keamanan internasional di era digital. Dengan memperluas pemahaman tentang ancaman hybrid warfare, penelitian ini diharapkan dapat mendorong perumusan kebijakan keamanan siber yang lebih adaptif dan komprehensif untuk menghadapi dinamika ancaman global ke depan.

4. KESIMPULAN DAN SARAN

Penelitian ini mengungkap bahwa pencurian cryptocurrency oleh Lazarus Group, yang berafiliasi dengan pemerintah Korea Utara, tidak hanya merupakan kejahatan siber transnasional semata, melainkan telah berevolusi menjadi instrumen strategis dalam kerangka hybrid warfare. Melalui analisis kasus-kasus besar, seperti peretasan terhadap Harmony’s Horizon Bridge, Ronin Bridge, DMM Bitcoin Exchange, WazirX, dan Bybit, ditemukan pola serangan yang sistematis, canggih, dan sulit dilacak. Serangkaian serangan ini tidak hanya menimbulkan kerugian finansial global yang sangat besar, tetapi juga secara signifikan memperkuat kapabilitas finansial dan daya tawar geopolitik Korea Utara di tengah tekanan sanksi internasional.

Studi ini menegaskan bahwa aktivitas Lazarus Group memperluas definisi hybrid warfare, di mana kejahatan siber berbasis aset digital digunakan sebagai taktik non-konvensional yang efektif dalam mendukung tujuan strategis negara. Konsep ambiguitas dan ruang abu-abu, sebagaimana diuraikan dalam teori hybrid warfare, tampak jelas dalam modus operandi Lazarus Group yang secara sengaja menyamarkan keterlibatan negara

untuk menghindari respons militer langsung dari komunitas internasional. Dengan demikian, kejahatan finansial digital telah menjadi bagian tak terpisahkan dari instrumen kebijakan luar negeri negara-negara yang menghadapi keterbatasan akses ekonomi dan tekanan global.

Implikasi praktis dari penelitian ini menyoroti pentingnya penguatan kolaborasi internasional dalam menghadapi ancaman hybrid warfare berbasis digital. Penguatan regulasi, pengawasan pada ekosistem cryptocurrency, serta peningkatan kapasitas pertahanan siber menjadi sangat krusial guna mengurangi risiko penyalahgunaan aset digital oleh aktor negara. Selain itu, diperlukan pendekatan lintas sektor antara pemerintah, otoritas keuangan, lembaga keamanan, dan sektor swasta untuk membangun sistem deteksi dan mitigasi yang lebih adaptif terhadap serangan siber lintas negara.

Namun, penelitian ini memiliki keterbatasan pada akses data primer dan fokus yang masih terpusat pada kasus Korea Utara. Untuk itu, diperlukan studi lanjutan yang membandingkan pola dan dampak serangan siber serupa oleh aktor negara lain, serta riset lapangan yang mendalam tentang efektivitas respons kebijakan di berbagai yurisdiksi. Secara keseluruhan, penelitian ini memberikan kontribusi empiris dan teoretis yang signifikan terhadap kajian keamanan internasional dan pengembangan teori hybrid warfare di era digital. Diharapkan, temuan dan rekomendasi dalam penelitian ini dapat menjadi referensi penting bagi pembuat kebijakan, akademisi, serta praktisi keamanan siber dalam merumuskan strategi penanggulangan ancaman keamanan siber yang semakin kompleks dan dinamis di masa depan.

DAFTAR REFERENSI

Azizah, A. S. N., & Irfan. (2020). Fenomena cryptocurrency dalam perspektif hukum Islam. *Shautuna: Jurnal Ilmiah Mahasiswa Perbandingan Mazhab*, *1*(1), 63.

Baxter, P., & Jack, S. (2008). Qualitative case study methodology: Study design and implementation for novice researchers. The Qualitative Report, 13(4), 544–559.

Borger, J. (2025, February 27). *North Korea behind Bybit crypto exchange hack, FBI says*. *The Guardian*. https://www.theguardian.com/world/2025/feb/27/north-korea-bybit-crypto-exchange-hack-fbi

Chainalysis. (2025). *The 2025 crypto crime report* [Report]. https://www.chainalysis.com

Cointelegraph. (2025). *How the Bybit hack happened*. https://cointelegraph.com/learn/articles/how-the-bybit-hack-happened

Dougherty, J. (2018, January 26). The mouse clicks of August: Hybrid warfare, nation-state actors, and the future of cybersecurity. *Small Wars Journal*. https://archive.smallwarsjournal.com/index.php/jrnl/art/mouse-clicks-august-hybrid-warfare-nation-state-actors-and-future-cybersecurity

Elliptic. (2022, June 30). *FBI confirms North Korea's Lazarus Group as hackers behind $100 million Harmony Horizon Bridge theft*. https://www.elliptic.co/blog/analysis/fbi-confirms-north-korea-s-lazarus-group-as-hackers-behind-100-million-harmony-horizon-bridge-theft

Federal Bureau of Investigation. (2022, April 14). *FBI statement on attribution of malicious cyber activity posed by the Democratic People's Republic of Korea* [Press release]. https://www.fbi.gov/news/press-releases/fbi-statement-on-attribution-of-malicious-cyber-activity-posed-by-the-democratic-peoples-republic-of-korea

Federal Bureau of Investigation. (2023, January 23). *FBI confirms Lazarus Group cyber actors responsible for Harmony's Horizon Bridge currency theft* [Press release]. https://www.fbi.gov/news/press-releases/fbi-confirms-lazarus-group-cyber-actors-responsible-for-harmonys-horizon-bridge-currency-theft

Federal Bureau of Investigation. (2023, May 31). *FBI, DC3, and NPA identification of North Korean cyber actors tracked as TraderTraitor responsible for theft of $308 million from bitcoin.dmm.com* [Press release]. https://www.fbi.gov/news/press-releases/fbi-dc3-and-npa-identification-of-north-korean-cyber-actors-tracked-as-tradertraitor-responsible-for-theft-of-308-million-from-bitcoindmmcom

Federal Bureau of Investigation. (2023, September 7). *FBI identifies Lazarus Group cyber actors as responsible for theft of $41 million from Stake.com* [Press release]. https://www.fbi.gov/news/press-releases/fbi-identifies-lazarus-group-cyber-actors-as-responsible-for-theft-of-41-million-from-stakecom

Hybrid CoE. (2021). *Cyber conflict in a hybrid threat environment: Death by a thousand cuts* (Hybrid CoE Paper 10). https://www.hybridcoe.fi/wp-content/uploads/2021/11/Hybrid_CoE_Paper_10_Cyber_conflict_in_a_hybrid_threat_environment_WEB.pdf

Marrelli, A. F. (2007). The performance technologist's toolbox: Case studies. Performance Improvement, 46(7), 39–44.

Mumford, A., & Carlucci, P. (2023). Hybrid warfare: The continuation of ambiguity by other means. *European Journal of International Security*, *8*, 192–206.

Perdana, A., Aminanto, M. E., & Anggorojati, B. (2024). Hack, heist, and havoc: The Lazarus Group's triple threat to global cybersecurity. *Journal of Information Technology Teaching Cases*, *14*(1), 1–10.

Reddy, E., & Minnaar, A. (2018). Cryptocurrency: A tool and target for cybercrime. *Acta Criminologica: Southern African Journal of Criminology*, *31*(3), 71–87.

Times of India. (2024, July 6). *Japan, US, and South Korea issue joint statement on $235 million hacking of India's Bitcoin exchange WazirX*. https://timesofindia.indiatimes.com/technology/tech-news/japan-us-and-south-korea-

issue-joint-statement-on-235-million-hacking-of-india-ka-bitcoin-exchange-wazirx/articleshow/117270475.cms

United Nations Security Council. (2023). *Final report of the Panel of Experts submitted pursuant to resolution 2627 (2022)* (S/2023/171, para. 137, p. 69). https://undocs.org/S/2023/171

Zellers, K. (2024). Hacked! North Korea's billion-dollar crypto heisting scheme. *Penn State Journal of Law & International Affairs*, *12*(2), 261–302.