Journal of Innovative and Creativity
Journal Homepage: https://joecy.org/index.php/joecy
e-mail: journaljoecy@gmail.com

Faculty of Education
University of Pahlawan Tuanku Tambusai
ISSN 2775-771X (Online)
ISSN 2962-570X **(Printed)**
6 (2) 2026, Page: 28898-28904

Evaluasi Kesiapan Regulasi dan Keamanan Sistem Komunikasi Kementerian Luar Negeri Republik Indonesia dalam Menghadapi Tantangan Spionase Siber terhadap Arsip Diplomatik Digital

Nida Zaqiyya Meilinda Widianto[1)], Linggar Fajri Nur Tsaqif[2)], Dimas Naufal Danuartha[3)], Dhimas Anggana Syahreza Pratama[4)], Isnaini[5)], Helmi Saputra[6)], Rikza Safiq[7)], Munadzirotul Jannah[8)]

Universitas Tidar, Barito No. 2 Sidotopo, Magelang, Indonesia
nidazaqiyyq@gmail.com [1)], linggar193@gmail.com [2)], dimasnaufald@gmail.com [3)], dimasanggana803@gmail.com [4)], todayisisna@gmail.com [5)], hlmisptr@gmail.com [6)], fiqsafiq2006@gmail.com [7)], munazi911@gmail.com [8)]

Published: May , 2026

ABSTRAK

Kasus infiltrasi siber oleh kelompok ancaman persisten tingkat lanjut (APT) Mustang Panda pada tahun 2021, yang berhasil menembus jaringan internal sedikitnya sepuluh kementerian dan lembaga pemerintah Indonesia termasuk Badan Intelijen Negara (BIN), menyingkap kerentanan serius dalam arsitektur keamanan informasi diplomatik nasional. Bertujuan mengevaluasi kesiapan regulasi keamanan siber Indonesia khususnya yang relevan bagi sistem komunikasi Kementerian Luar Negeri (Kemlu) dalam menghadapi ancaman spionase siber terhadap arsip diplomatik digital. Dengan menggunakan pendekatan penulisan hukum normatif dan analisis kerangka kebijakan komparatif, penulisan ini mengkaji tiga instrumen regulasi utama yaitu Undang-Undang ITE No. 1 Tahun 2024, Peraturan Presiden No. 28 Tahun 2021 tentang BSSN, dan Peraturan BSSN No. 4 Tahun 2021 tentang Manajemen Keamanan Informasi SPBE. Hasil ini menunjukkan adanya tiga kesenjangan regulasi yang kritis yaitu tidak adanya regulasi khusus yang mengatur keamanan komunikasi diplomatik digital, absennya protokol respons insiden yang terintegrasi antara Kemlu dan BSSN, dan ketiadaan mandatori enkripsi end-to-end untuk transmisi arsip diplomatik berklasifikasi. Penulisan ini merekomendasikan pembentukan Peraturan Menteri Luar Negeri tentang Keamanan Siber Diplomatik sebagai instrumen hukum tersendiri, serta penguatan kapasitas Pusat Operasi Keamanan (SOC) khusus Kemlu. Temuan ini berkontribusi pada pengembangan kerangka hukum keamanan siber diplomatik di negara berkembang dengan ketergantungan tinggi pada arsitektur digital.

Kata Kunci: Spionase Siber, Mustang Panda, Arsip Diplomatik Digital, Regulasi Keamanan Siber, Kementerian Luar Negeri Indonesia

© The Author(s). 2021 Open Access This article is licensed under a Creative Commons Atibution 4.0 International License, which permits use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons licence, and indicate if changes were made. The images or other third party material in this article are included in the article's Creative Commons licence, unless indicated otherwise in a credit line to the material. To view a copy of this licence, visit http://creativecommons.org/licenses/by/4.0

PENDAHULUAN

Pada September 2021, laporan dari Recorded Future melalui divisi risetnya Insikt Group mengungkap fakta mengejutkan bahwa infrastruktur jaringan internal pemerintah Indonesia telah disusupi oleh kelompok ancaman siber yang dikaitkan dengan kepentingan negara asing.[1] Kelompok yang diidentifikasi sebagai Mustang Panda dikenal pula dengan nama Stately Taurus, BRONZE PRESIDENT, dan TA416 berhasil menanamkan malware PlugX pada Command and Control (C2) server yang berkomunikasi aktif dengan host di dalam jaringan kementerian dan lembaga pemerintah Indonesia, termasuk Badan Intelijen Negara (BIN).[2] Komunikasi mencurigakan tersebut dilacak setidaknya sejak Maret 2021.

Insiden ini bukan sekadar pelanggaran keamanan teknis. Bagi Kementerian Luar Negeri (Kemlu) sebagai instansi yang mengelola arsip diplomatik berklasifikasi mulai dari rekam jejak negosiasi bilateral, posisi Indonesia dalam forum multilateral, hingga komunikasi sandi antar perwakilan diplomatik infiltrasi semacam ini berpotensi merusak kepercayaan mitra negara, mengkompromikan posisi tawar dalam perundingan internasional, dan membahayakan sumber-sumber intelijen diplomatik. Namun, alih-alih respons hukum yang sistematis, pemerintah

Indonesia hampir tidak memberikan pernyataan resmi dan gagal merespons notifikasi awal yang dikirimkan oleh Insikt Group pada Juni dan Juli 2021.[3]

Situasi ini memunculkan pertanyaan akademis yang fundamental apakah kerangka regulasi keamanan siber Indonesia yang ada sudah cukup untuk melindungi arsip diplomatik digital dari ancaman spionase siber yang semakin canggih? Penelitian- penelitian sebelumnya cenderung membahas keamanan siber Indonesia secara umum (Yusuf et al., 2021; Ramli & Safiranita, 2022) atau berfokus pada dimensi teknis serangan APT (Dorais-Joncas & Munõz, 2021), tanpa secara eksplisit memetakan celah regulasi yang spesifik pada konteks komunikasi diplomatik dan perlindungan arsip kenegaraan. Di sinilah *research gap* penulisan ini berpijak.

Studi ini ditujukan untuk mengevaluasi kesiapan dan kelengkapan regulasi keamanan siber Indonesia dalam melindungi sistem komunikasi Kemlu dari ancaman. Sumber ini mengonfirmasi bahwa baik BIN maupun otoritas Indonesia lainnya tidak memberikan klarifikasi resmi. spionase siber, mengidentifikasi kesenjangan normatif antara regulasi yang ada dengan standar internasional perlindungan komunikasi diplomatk, dan merumuskan rekomendasi kebijakan hukum yang operasional guna menutup kesenjangan tersebut.

TINJAUAN PUSTAKA

Spionase Siber dalam Perspektif Hukum Internasional

Spionase siber (cyber espionage) merujuk pada penggunaan teknik peretasan komputer untuk memperoleh informasi rahasia dari pemerintah, organisasi, atau individu tanpa izin. Berbeda dari perang siber (*cyber warfare*), spionase siber secara historis beroperasi di area abu-abu hukum internasional tidak ada norma internasional yang secara eksplisit melarangnya meskipun melanggar kedaulatan digital negara target (Smith, 2015).[4] Konvensi Wina 1961 tentang Hubungan Diplomatik memberikan perlindungan bagi "dokumen dan arsip" misi diplomatik, namun tidak mengatur secara eksplisit arsip yang tersimpan secara digital (Schmitt, 2017).[5]

Mustang Panda: Profil Ancaman dan Modus Operandi

Mustang Panda, aktif setidaknya sejak 2017, merupakan kelompok APT yang dikaitkan secara kuat dengan kepentingan negara Tiongkok.[6] Kelompok ini diidentifikasi secara konsisten menargetkan kementerian luar negeri, pertahanan, dan perdagangan di kawasan Asia Pasifik dan Eropa. Instrumen utamanya adalah PlugX trojan akses jarak jauh modular yang memungkinkan pencurian dokumen, eksekusi perintah tersembunyi, dan persistensi jangka panjang dalam jaringan korban. Penelitian Unit 42 Palo Alto Networks (2023) mendokumentasikan bahwa serangan Mustang Panda terhadap pemerintah Asia Tenggara berlangsung setidaknya dari Q2 2021 hingga Q3 2023 dengan tujuan utama eksfiltrasi dokumen sensitif terkait individu kepentingan strategis pemerintah.

Kerangka Regulasi Keamanan Siber Indonesia.

Indonesia membangun ekosistem regulasi keamanan siber nasional melalui beberapa lapisan instrumen hukum. UU ITE No. 11 Tahun 2008 (diubah dengan UU No. 1 Tahun 2024) menjadi landasan hukum utama yang mengatur akses ilegal terhadap sistem elektronik (Pasal 30) dan intersepsi ilegal (Pasal 31), dengan ancaman pidana delapan tahun penjara.[7] Di level kelembagaan, Perpres No. 28 Tahun 2021 tentang BSSN mengkonsolidasikan tugas keamanan siber nasional pada Badan Siber dan Sandi Negara. Peraturan BSSN No. 4 Tahun 2021 kemudian menetapkan pedoman manajemen keamanan informasi Sistem Pemerintahan Berbasis Elektronik (SPBE). Studi Syahrial & Makarim (2024) menegaskan bahwa setidaknya enam lembaga pemerintah memiliki tanggung jawab tumpang tindih dalam keamanan siber nasional, yang berimplikasi pada inefisiensi respons.[8]

Celah Penulisan

Dibandingkan penulisan sebelumnya, penulisan ini berbeda dalam tiga aspek yaitu pertama fokus spesifik pada konteks diplomatik yang selama ini terabaikan dalam literatur keamanan siber Indonesia, kedua menggunakan kasus Mustang Panda 2021 sebagai *critical case* yang memungkinkan evaluasi regulasi berdasarkan insiden nyata, ketiga mengintegrasikan perspektif hukum internasional (Konvensi Wina) dengan analisis regulasi domestik pendekatan yang belum dilakukan secara konsisten dalam literatur yang ada (Yusuf et al., 2021; Al- Bahst, 2024).

METODOLOGI PENELITIAN

Penulisan ini menggunakan pendekatan normatif (*normative legal research*), yang menggabungkan analisis dokumen hukum dengan studi kasus insiden keamanan siber nyata. Pendekatan ini dipilih karena mampu menjembatani *das sollen* (apa yang seharusnya diatur) dengan *das sein* (kondisi keamanan aktual yang terjadi di lapangan).

Dalam pelaksanaannya, penulisan ini mengadopsi pendekatan perundang- undangan (*statute approach*) dan pendekatan kasus (*case approach*) untuk menelaah berbagai peraturan perundang-undangan serta laporan insiden siber. Pengumpulan data didasarkan pada tiga tingkatan sumber, dimulai dari sumber data primer berupa regulasi keamanan siber Indonesia seperti UU ITE, Perpres BSSN, dan Peraturan BSSN yang dikaji melalui analisis isi normatif. Selain itu, digunakan pula sumber data sekunder yang berasal dari laporan intelijen ancaman siber global seperti Insikt Group/Recorded Future (2021), Unit 42, Cyble, dan CYFIRMA melalui analisis deskriptif, serta sumber data tersier berupa jurnal ilmiah hukum dan keamanan siber terbitan tahun 2018 hingga 2024 yang ditelaah dengan tinjauan literatur sistematis. Seluruh data yang terkumpul kemudian diolah menggunakan teknik analisis kesenjangan regulasi (*regulatory gap analysis*) dan perbandingan hukum komparatif yang dievaluasi menggunakan instrumen matriks evaluasi normatif.

Teknik analisis utama adalah *regulatory gap analysis* yang setiap aspek keamanan sistem komunikasi diplomatik diidentifikasi, kemudian dievaluasi apakah sudah tercakup dalam regulasi yang ada, cukup memadai, atau masih terdapat kesenjangan normatif. Analisis ini dilengkapi dengan perbandingan komparatif terhadap praktik regulasi keamanan diplomatik di Singapura (Cybersecurity Act 2018 dan Operational Technology Security Masterplan), Australia (Protective Security Policy Framework), dan Amerika Serikat (FISMA dan NSS Policy Framework), sebagai referensi praktik terbaik (*best practices*) internasional.

HASIL DAN PEMBAHASAN

Anatomi Serangan Mustang Panda 2021: Implikasi bagi Kemlu

Insikt Group mengidentifikasi pada April 2021 adanya C2 server PlugX yang beroperasi aktif dalam jaringan pemerintah Indonesia, dengan komunikasi yang dapat dilacak setidaknya sejak Maret 2021. Dari sepuluh kementerian dan lembaga yang teridentifikasi terkompromikan, Kemlu merupakan salah satu target paling sensitif mengingat volum dan karakteristik arsip yang dikelolanya. Metode infeksi utama yang digunakan Mustang Panda adalah *spear-phishing* dengan konten yang didesain menyerupai laporan resmi pemerintah atau berita aktual yang relevan teknik yang secara konsisten digunakan kelompok ini sejak 2017 dan memanfaatkan rendahnya kesadaran keamanan siber di kalangan aparatur sipil negara.[9]

Tren Insiden Siber Terhadap Lembaga Pemerintah Indonesia (2018–2023) lonjakan drastis insiden siber pada 2021 yang bertepatan dengan aktivitas Mustang Panda. Lonjakan ini tidak berdiri sendiri pada periode 2020–2021 ditandai oleh akselerasi transformasi digital dalam tata kelola pemerintahan akibat pandemi COVID-19, yang memperluas permukaan serangan (*attack surface*) tanpa diiringi penguatan keamanan yang proporsional. Kemlu, yang mengedepankan konektivitas digital dalam operasional perwakilan diplomatik selama pembatasan mobilitas internasional, menjadi salah satu entitas yang paling rentan.

Distribusi Vektor Serangan Mustang Panda (Kumulatif 2018–2023) memperlihatkan bahwa *spear-phishing* (42%) dan penggunaan malware PlugX melalui C2 server (28%) mendominasi vektor serangan Mustang Panda. Implikasi langsung bagi Kemlu merupakan kebutuhan mendesak atas dua lapisan perlindungan pertama, peningkatan kesadaran keamanan siber (*security awareness*) bagi seluruh aparatur yang mengelola komunikasi diplomatik. Kedua, penguatan deteksi dini berbasis *network traffic analysis* yang mampu mengidentifikasi pola komunikasi C2 yang mencurigakan.

Evaluasi Kesiapan Regulasi: Analisis Kesenjangan Normatif

Evaluasi regulasi dilakukan terhadap empat dimensi kesiapan cakupan normatif, kelembagaan dan koordinasi, mandat teknis, dan mekanisme penegakan. Pada tingkat kesenjangan kritis, terdapat tiga titik lemah utama yang membutuhkan intervensi regulasi segera. Pertama,

perlindungan arsip diplomatik digital saat ini masih bersandar pada aturan umum UU ITE, padahal standar internasional seperti Konvensi Wina 1961 dan Tallinn Manual 2.0 menuntut adanya norma perlindungan spesifik untuk arsip diplomatik di ruang siber. Kedua, ketiadaan Standar Operasional Prosedur (SOP) lintas kementerian yang terintegrasi untuk merespons insiden diplomatik membuat penanganan krisis kita tertinggal dari standar NIST maupun NCSC Inggris, karena saat ini hanya berpatokan pada aturan SPBE umum dari BSSN. Ketiga, komunikasi diplomatik Indonesia belum memiliki regulasi yang mewajibkan penerapan enkripsi *end-to-end*, dan masih bergantung pada prinsip keamanan umum yang tidak sejalan dengan kerangka kerja keamanan tingkat tinggi negara maju.

Bergerak pada tingkat kesenjangan serius, permasalahan utamanya berakar pada belum adanya pembaruan terhadap klasifikasi kerahasiaan arsip di era modern. Payung hukum yang digunakan pemerintah saat ini masih merujuk pada Peraturan Presiden Nomor 33 Tahun 1988 yang sudah sangat usang. Aturan warisan masa lalu tersebut belum menyentuh apalagi mengatur dimensi digital sama sekali. Jika dibandingkan dengan protokol internasional seperti Standar Keamanan Informasi NATO, kerangka hukum Indonesia tertinggal jauh dalam memberikan panduan klasifikasi yang jelas untuk melindungi lalu lintas dokumen diplomatik elektronik dari ancaman spionase atau kebocoran data.

Sementara itu, pada tingkat kesenjangan sedang, tantangan berpusat pada aspek sumber daya manusia dan mekanisme pengawasan. Berbeda dengan Kementerian Luar Negeri di Inggris yang mewajibkan pelatihan keamanan siber secara spesifik bagi diplomatnya, Indonesia belum memiliki program wajib khusus bagi aparatur Kemlu dan hanya merujuk pada Inpres SPBE yang bersifat umum. Di sisi pengawasan, standar internasional seperti ISO 27001 mewajibkan audit sistem secara disiplin, namun aturan audit keamanan komunikasi diplomatik di Indonesia (melalui Peraturan BSSN) belum menuntut pelaksanaan audit yang bersifat mandatori dan berkala, sehingga evaluasi kerentanan sistem tidak dapat berjalan optimal.

Perbandingan Skor Kesiapan Regulasi Eksisting vs. Standar Ideal (Skala 0– 100) seluruh dimensi regulasi keamanan komunikasi diplomatik digital Indonesia berada jauh di bawah standar ideal internasional, dengan kesenjangan terbesar pada aspek *audit kepatuhan* (skor 35 vs. standar ideal 90) dan *pengembangan SDM keamanan siber* (38 vs. 85). Ini bukan semata masalah teknis—melainkan kegagalan regulasi untuk mengantisipasi transformasi ancaman yang terjadi di lapangan.

Dari perspektif hukum, kesenjangan paling fundamental terletak pada *absennya norma khusus* yang mengatur perlindungan arsip diplomatik digital. UU ITE mengatur akses ilegal secara general, namun tidak memuat ketentuan yang mengakui kekhususan arsip diplomatik sebagai objek perlindungan hukum dengan tingkat sensitivitas lebih tinggi. Berbeda dengan Australia yang memiliki *Protective Security Policy Framework* (PSPF) dengan bab khusus tentang keamanan informasi dalam konteks hubungan luar negeri, atau Singapura yang mengintegrasikan keamanan siber ke dalam *Singapore Foreign Policy Architecture*-nya, Indonesia belum memiliki instrumen hukum setara.[10]

Radar Kesiapan Keamanan Siber Diplomatik Indonesia entuk yang tidak seimbang dan jauh dari lingkaran ideal, mengindikasikan profil kesiapan yang *asimetris*. Nilai terendah ada pada dimensi *SDM Siber* (40) dan *Teknis Enkripsi* (48)—dua komponen yang justru paling kritis dalam menghadapi serangan APT seperti Mustang Panda yang mengeksploitasi kelemahan teknis melalui rekayasa sosial terhadap pengguna sistem.

Respons Kelembagaan: Kegagalan Sistemik yang Terdokumentasi

Fakta bahwa Kemlu dan BIN tidak merespons notifikasi Insikt Group pada Juni dan Juli 2021 bukan sekadar kelalaian prosedural, ini adalah cermin dari kegagalan sistemik dalam tata kelola keamanan siber nasional. Paling tidak tiga faktor struktural dapat diidentifikasi pertama, tidak adanya saluran komunikasi formal yang mapan antara peneliti keamanan siber swasta internasional dengan lembaga pemerintah Indonesia, kedua tidak ada *mandatory breach notification* yang mewajibkan instansi pemerintah untuk mengonfirmasi atau menginvestigasi laporan insiden; *ketiga*, absennya SOC (*Security Operations Center*) yang berdedikasi di Kemlu dengan kapasitas deteksi dan respons 24/7.

Studi Syahrial & Makarim (2024) menemukan bahwa tanggung jawab keamanan siber

pemerintah terdistribusi pada setidaknya enam lembaga (Kemenkomdigi, BSSN, Polri, Kemenhan, BIN, Ombudsman) tanpa mekanisme koordinasi yang efektif—kondisi yang diistilahkan sebagai "*coordination without authority*." Mustang Panda berhasil mengeksploitasi celah koordinasi ini: mereka beroperasi dalam jaringan pemerintah Indonesia selama berbulan-bulan tanpa terdeteksi oleh mekanisme pengawasan internal manapun.

Perbandingan Komparatif: Praktik Terbaik Negara Lain

Berdasarkan perbandingan regulasi keamanan siber diplomatik, Indonesia masih tertinggal dalam ketersediaan payung hukum khusus jika disandingkan dengan Singapura, Australia, dan Amerika Serikat. Ketiga negara pembanding tersebut telah memiliki panduan perlindungan siber spesifik untuk kementerian luar negerinya, seperti *ICA + MFA Cyber Guidelines* di Singapura, *PSPF Chapter 5* di Australia, dan kerangka kerja *FISMA + FAM 5 FAH-11* di Amerika Serikat. Ketimpangan ini semakin nyata dalam penerapan kewajiban enkripsi *end-to-end* (E2E). Sementara Indonesia sama sekali belum mewajibkan pelindungan data tersebut, Singapura telah menerapkannya secara wajib untuk dokumen berklasifikasi *Top Secret* ke atas, Australia untuk level *PROTECTED* ke atas, dan Amerika Serikat mengaturnya secara ketat untuk informasi dengan tingkat kerahasiaan tertinggi (*TS/SCI*).

Dari sisi infrastruktur pemantauan dan respons krisis, Indonesia juga belum memiliki *Security Operations Center* (SOC) serta Standar Operasional Prosedur (SOP) penanganan insiden yang secara khusus didedikasikan untuk Kementerian Luar Negeri. Hal ini sangat kontras dengan kesiapan negara lain. Singapura telah mengintegrasikan SOC kementerian luar negerinya dengan *GovTech* dan memiliki SOP yang sejalan dengan *Cyber Security Agency* (CSA). Pendekatan serupa dilakukan oleh Australia yang menugaskan tim penghubung dengan badan siber nasionalnya (ACSC) berlandaskan MoU resmi, sedangkan Amerika Serikat bahkan mengoperasikan direktorat siber secara mandiri (*DS Cyber Directorate*) dengan prosedur respons krisis yang diatur langsung melalui arahan *NSC Directive.*

Kelemahan sistemik di Indonesia juga berlanjut pada kesiapan kapasitas sumber daya manusia dan mekanisme akuntabilitas insiden. Pelatihan keamanan siber bagi aparatur diplomatik di Indonesia saat ini masih bersifat opsional, jauh berbeda dengan Singapura, Australia, dan Amerika Serikat yang mewajibkan aparatur diplomatiknya untuk mengikuti pelatihan siber secara berkala melalui instansi resmi masing-masing. Terkait transparansi kelembagaan, ketika terjadi insiden kebocoran atau serangan siber, Indonesia dan Singapura memang sama- sama tidak mewajibkan pelaporan kepada parlemen. Namun, Australia dan Amerika Serikat menerapkan standar akuntabilitas yang sangat ketat, di mana
pemerintah wajib memberikan notifikasi resmi kepada komite intelijen parlemen (PJCIS di Australia) atau para pimpinan kongres (yang dikenal sebagai *Gang of Eight* di Amerika Serikat) agar fungsi pengawasan negara tetap berjalan.

Mengungkap disparitas yang sangat signifikan antara Indonesia dan negara- negara yang memiliki arsitektur keamanan diplomatik digital yang matang. Singapura, dengan ukuran yang jauh lebih kecil, memiliki kerangka hukum yang jauh lebih komprehensif melalui integrasi Cybersecurity Agency (CSA) dengan Ministry of Foreign Affairs (MFA) dalam satu protokol respons insiden terintegrasi. Ketiadaan semua elemen ini di Indonesia bukan hanya melemahkan keamanan Kemlu secara teknis, tetapi juga menciptakan eksposur hukum: tidak ada standar yang jelas tentang apa yang harus dilakukan aparat Kemlu ketika terjadi insiden pelanggaran keamanan siber pada arsip diplomatik.

Rekomendasi: Arsitektur Regulasi Keamanan Siber Diplomatik Indonesia

Merekomendasikan tiga langkah regulasi yang terstruktur dan hierarkis. Pertama, dalam jangka pendek (0–12 bulan) yaitu Kemlu harus menerbitkan Peraturan Menteri Luar Negeri tentang Keamanan Siber Sistem Komunikasi Diplomatik, yang mengatur mengenai klasifikasi arsip diplomatik digital berdasarkan tingkat kerahasiaan, mandatori enkripsi *end-to-end* untuk seluruh transmisi arsip berklasifikasi, prosedur respons insiden siber yang terintegrasi dengan BSSN, dan program pelatihan keamanan siber wajib bagi seluruh aparatur Kemlu.

Kedua, dalam jangka menengah (1–3 tahun): perlu pembentukan Security Operations Center (SOC) Kemlu yang terintegrasi dengan National Cyber Operations Centre BSSN, dengan mandat

pemantauan 24/7 terhadap seluruh infrastruktur komunikasi diplomatik. SOC ini harus dilengkapi kapasitas deteksi berbasis *threat intelligence* yang mencakup pemantauan terhadap TTP (*Tactics, Techniques, and Procedures*) kelompok APT yang diketahui menargetkan diplomasi Indonesia. *Ketiga*, dalam jangka panjang (3–5 tahun): amendemen UU ITE atau penerbitan Undang-Undang Keamanan dan Ketahanan Siber yang komprehensif dengan pasal khusus tentang perlindungan arsip dan komunikasi kenegaraan digital.

KESIMPULAN

Kasus infiltrasi Mustang Panda 2021 telah menjadi batu uji yang menyingkap kelemahan fundamental regulasi keamanan siber Indonesia—khususnya dalam konteks perlindungan arsip dan komunikasi diplomatik digital Kementerian Luar Negeri. Penulisan ini menemukan bahwa Indonesia menghadapi setidaknya tiga kesenjangan regulasi yang kritis: ketiadaan norma khusus yang mengatur perlindungan arsip diplomatik digital, absennya protokol respons insiden terintegrasi antara Kemlu dan BSSN, serta tidak adanya mandatori enkripsi komunikasi diplomatik.

Evaluasi komparatif memperlihatkan bahwa Indonesia masih jauh tertinggal dari negara-negara setara dalam membangun arsitektur hukum keamanan siber diplomatik. Respons kelembagaan yang lambat terhadap notifikasi Insikt Group dan ketiadaan SOC khusus Kemlu mencerminkan kegagalan sistemik dalam tata kelola yang melampaui sekadar masalah teknis keamanan siber. Rekomendasi penulisan ini dari Peraturan Menteri yang spesifik hingga pembentukan SOC terintegrasi merupakan peta jalan (*roadmap*) yang dapat menjadi acuan kebijakan konkret. Dalam konteks politik luar negeri Indonesia yang aktif dan semakin bergantung pada infrastruktur digital, penguatan keamanan siber diplomatik bukan lagi pilihan melainkan keharusan hukum dan strategis.

DAFTAR PUSTAKA

Dorais-Joncas, A., & Munõz, F. (2021). A wolf in sheep's clothing: Mustang Panda's PlugX dissected. ESET Research. https://www.eset.com/int/about/newsroom/research/mustang-panda- plugx/

Insikt Group. (2021). Chinese state-sponsored group Mustang Panda targets Indonesian government. Recorded Future. https://therecord.media/mustang-panda-china/

Makarim, E., & Syahrial, S. M. (2024). Pertanggungjawaban hukum pemerintah terhadap insiden siber. Technology and E-Law Journal, 5(1). https://scholarhub.ui.ac.id/telj/vol5/iss1/5/

Palo Alto Networks Unit 42. (2023). Cyberespionage attacks against Southeast Asian government linked to Stately Taurus. https://unit42.paloaltonetworks.com/stately-taurus-attacks-se-asian- government/

Ramli, A. M., & Safiranita, T. (2022). Hukum sebagai infrastruktur transformasi Indonesia: Regulasi dan kebijakan digital. Refika Aditama.

Schmitt, M. N. (Ed.). (2017). Tallinn Manual 2.0 on the international law applicable to cyber operations. Cambridge University Press.

Smith, M. (2015). Research handbook on international law and cyberspace. Elgar Publishing.

Yusuf, M., et al. (2021). Efektivitas sinergi lembaga keamanan siber Indonesia. Jurnal Politeia, 14(1), 1–18.

Al-Bahts. (2024). Regulasi keamanan siber di Indonesia: Analisis komparatif UU ITE dan regulasi internasional. Al-Bahst: Jurnal Ilmu Sosial, Politik, dan Hukum, 2(1). https://ejournal.unisi.ac.id/index.php/albahts/article/download/3044/1574

BSSN. (2021). Peraturan Badan Siber dan Sandi Negara Nomor 4 Tahun 2021 tentang Pedoman Manajemen Keamanan Informasi SPBE. Berita Negara RI No. 541.

Presiden Republik Indonesia. (2021). Peraturan Presiden Nomor 28 Tahun 2021 tentang Badan Siber dan Sandi Negara. Lembaran Negara RI Tahun 2021 No. 101.

Cyble Research. (2024). APT profile: Mustang Panda. https://cyble.com/threat-actor-profiles/mustang-panda/

CYFIRMA. (2024). APT profile — Mustang Panda. https://www.cyfirma.com/research/apt-profile-mustang-panda/

Infosecurity Magazine. (2021, September). Mustang Panda compromises Indonesian intelligence agency. https://www.infosecurity-magazine.com/news/mustang-panda-compromises/

Lumu Technologies. (2025). Who is Mustang Panda? https://lumu.io/resources/threat-glossary/mustang-panda/

Dexpose.io. (2025). Threat actor profile: Mustang Panda. https://www.dexpose.io/threat-actor-profile-mustang-panda/

DPR RI & Pemerintah Indonesia. (2024). Naskah akademik rancangan undang-undang tentang keamanan dan ketahanan siber. https://www.peraturan.go.id

Pemerintah Republik Indonesia. (2024). Undang-Undang Nomor 1 Tahun 2024 tentang Perubahan Kedua atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik. Lembaran Negara RI.