Siberaman

EDISI 2026

KEAMANAN SIBER / POLITIK / MASYARAKAT

PERANG PROXY DI RUANG SIBER

Pelaku, kepentingan, dan dampaknya bagi masyarakat



Mochammad Rafi

Cyber Intelligence Analyst

Siberaman.id

SEBELUM MEMBACA

Di balik sebuah serangan

Ketika sebuah serangan siber dikaitkan dengan negara tertentu, perhatian biasanya langsung tertuju pada pelakunya. Padahal, nama pelaku baru menjawab sebagian persoalan. Kita juga perlu mengetahui apa yang dikerjakan, siapa yang memberi dukungan, dan apa akibatnya bagi orang yang menggunakan layanan tersebut.

Istilah perang proxy sering dipakai untuk merangkum semua persoalan itu. Dalam kajian cyber proxy, perhatian utamanya ada pada hubungan negara dengan pihak yang menjalankan operasi. Ada yang menerima tugas, memperoleh fasilitas, atau bergerak atas kemauan sendiri. Bentuk hubungan ini menentukan seberapa besar kendali sponsor dan bagaimana tanggung jawabnya dapat ditelusuri.

Pembahasan dalam buku ini bertumpu pada lima kasus: Star Blizzard, APT31, Doppelganger, KA-SAT, dan Volt Typhoon. Dari kasus-kasus itu, kita mengikuti pencurian informasi, operasi informasi, serta gangguan layanan. Bagian berikutnya membahas atribusi dan kesiapan menghadapi insiden: cara menilai temuan serta menyiapkan organisasi sebelum insiden terjadi.

Bagi pembaca di Indonesia, manfaatnya terletak pada kemampuan mengenali persoalan yang juga dapat muncul di lingkungan sendiri: akun kerja yang diambil alih, dokumen yang disebarkan tanpa konteks, pemasok yang menjadi sumber gangguan, dan layanan penting yang sulit dipulihkan. Memahami siapa yang menyerang tetap diperlukan. Mengetahui apa yang harus dilindungi sama mendesaknya.

Mochammad Rafi
Cyber Intelligence Analyst
Siberaman.id, November 2026

Daftar isi

Pendahuluan 2

1. Cyber proxy dan hubungan pelaku 4
2. Email sebagai pintu masuk 7
3. Operasi informasi 9
4. Gangguan layanan dan infrastruktur kritis 12
5. Atribusi: dari jejak ke pelaku 15
6. Mengukur dampak 18
7. Kesiapan menghadapi insiden 21
8. Ketahanan siber dan layanan publik 24

Glosarium 26

Daftar pustaka 27

BAB 01

Cyber proxy dan hubungan pelaku

Hubungan sponsor dan operator dapat berupa penugasan, dukungan, atau toleransi. Perbedaannya menentukan cara membaca sebuah operasi.



Sebuah kelompok peretas mengaku menyerang lawan politik sebuah negara. Sasarannya sesuai dengan kepentingan pemerintah negara itu, dan para anggotanya menggunakan bahasa serta simbol yang mendukung pemerintah tersebut. Keadaan ini menimbulkan dugaan adanya hubungan. Untuk mengetahui bentuk hubungannya, masih ada pekerjaan lain: mencari tahu apakah kelompok itu menerima tugas, memperoleh bantuan, atau hanya memilih sasaran yang sama.

Persoalan itulah yang dibahas ketika kita berbicara tentang proxy. Pusat perhatiannya adalah hubungan antara pihak yang berkepentingan dan pihak yang bertindak. Dalam perang proxy, hubungan tersebut berlangsung dalam permusuhan bersenjata. Dalam kegiatan siber, hubungan serupa juga dapat muncul di luar perang, misalnya dalam pengumpulan informasi atau persaingan politik. Karena itu, istilah proxy siber memiliki penggunaan yang lebih luas daripada perang proxy. [4]

Sponsor dan kepentingan pelaksana

Pihak yang memberi dukungan, atau sponsor, dapat memperoleh kemampuan yang belum dimilikinya sendiri. Ia juga dapat memanfaatkan pengetahuan, jaringan pertemanan, atau akses yang lebih mudah diperoleh pelaksana. Dari sisi pelaksana, hubungan itu dapat menyediakan uang, fasilitas, pekerjaan, perlindungan, atau kesempatan menjalankan kepentingannya sendiri. Maurer menempatkan keragaman hubungan negara dan aktor nonnegara sebagai persoalan utama dalam memahami proxy siber. [4]

Kepentingan kedua pihak dapat bertemu tanpa selalu sejalan. Sponsor mungkin menghendaki pengumpulan informasi secara diam-diam, sementara pelaksana ingin memamerkan hasilnya. Pelaksana mungkin pula memilih cara yang menimbulkan kerugian lebih besar daripada yang diharapkan sponsor. Hubungan melalui perantara dengan demikian membawa masalah pengawasan. Pemberi dukungan tidak selalu mengetahui seluruh tindakan pihak yang dibantunya.

Penugasan, koordinasi, dan toleransi

Ada tiga bentuk hubungan yang perlu dibedakan. Dalam delegation, pelaksana menerima tugas. Dalam orchestration, sponsor membantu atau mengoordinasikan kegiatan tanpa mengatur setiap langkahnya. Dalam pemberian keleluasaan atau sanctioning, pelaku diberi ruang bertindak karena kegiatannya ditoleransi. Tipologi dalam paper yang mendasari buku ini membedakan tingkat keterlibatan negara tersebut. [4]

Ketiganya mempunyai konsekuensi yang berbeda. Bukti penugasan dapat membantu menjelaskan siapa yang memilih sasaran. Bukti bantuan dapat menunjukkan sumber kemampuan pelaksana. Untuk menilai pembiaran, perlu diketahui apakah pihak yang dituduh memang mengetahui kegiatan tersebut dan memiliki kemampuan untuk bertindak. Kegagalan menghentikan serangan saja belum menjelaskan apakah ada persetujuan di belakangnya.



Sponsor, operator, dan target. Hubungan sponsor, pendukung, dan pelaksana dapat berbeda untuk setiap operasi. [4]

Spionase, pengaruh, dan sabotase

Spionase bertujuan memperoleh informasi. Operasi pengaruh berusaha mengubah pemahaman atau pilihan orang. Sabotase diarahkan pada gangguan atau kerusakan. Kejahatan siber dapat dilakukan untuk keuntungan finansial. Kegiatan-kegiatan tersebut bisa saling berhubungan, tetapi menyebut semuanya perang proxy akan menghilangkan perbedaan yang justru perlu dijelaskan.

Mencuri dokumen, misalnya, belum memberi tahu kita apa yang hendak dilakukan terhadap dokumen itu. Materi tersebut dapat disimpan untuk kepentingan intelijen, dijual, atau diterbitkan. Jika kemudian muncul di internet, hubungan antara pencurian dan penerbitannya masih perlu ditelusuri. Orang yang memperoleh data dan orang yang menyebarkannya bisa merupakan pihak yang berbeda.

Istilah yang tepat membantu kita memilih tindakan. Account takeover memerlukan penanganan akses. Informasi palsu memerlukan pemeriksaan asal dan isinya. Gangguan layanan memerlukan pemulihan fungsi. Dugaan keterlibatan negara dapat diteliti bersamaan dengan pekerjaan tersebut, tanpa membuat penanganan korban bergantung pada jawaban yang belum tersedia.

BAB 02

Email sebagai pintu masuk

Star Blizzard dan APT31 memperlihatkan bagaimana hubungan sehari-hari dapat membuka akses ke informasi sensitif.



Akun email menyimpan lebih dari pesan. Di dalamnya terdapat percakapan yang belum dipublikasikan, lampiran pekerjaan, daftar kontak, dan petunjuk tentang siapa mempercayai siapa. Bagi pelaku spionase, satu akun yang berhasil dikuasai dapat membuka jalan ke banyak orang lain. Inilah sebabnya keamanan sebuah organisasi tidak cukup dipahami sebagai perlindungan terhadap servernya saja.

Star Blizzard: membangun kepercayaan sebelum phishing

Laporan keamanan bersama yang diterbitkan pada 7 Desember 2023 menjelaskan cara Star Blizzard mendekati sasaran. Pelaku mempelajari minat dan hubungan profesional calon korban dari sumber terbuka. Mereka menyamar sebagai kenalan, membangun kedekatan, lalu mengirim tautan phishing setelah percakapan terasa wajar. Sasaran dapat diarahkan ke halaman login palsu. [15]

Laporan yang sama menyebut pencurian email dan lampiran, pembuatan aturan penerusan email, serta penggunaan daftar kontak untuk menyasar orang berikutnya. Alamat email pribadi juga sering dipilih. [15] Cara kerja ini menunjukkan bahwa serangan

dapat berkembang melalui hubungan sehari-hari, termasuk percakapan yang pada awalnya tidak meminta tindakan mencurigakan.

Pelaku menyediakan alasan yang masuk akal untuk membuka percakapan: nama yang dikenal, topik yang relevan, atau undangan pekerjaan. Perlindungan karena itu perlu mencakup pengamanan akun dan cara memverifikasi pesan, bukan hanya mengandalkan ketelitian pengguna.

Pada hari yang sama, pemerintah Inggris menyampaikan penilaian Pusat Keamanan Siber Nasional Inggris (NCSC) bahwa Star Blizzard hampir pasti berada di bawah Centre 18 pada badan keamanan Rusia, FSB. Inggris juga mengaitkannya dengan pembocoran selektif dan penyebaran informasi. [1] Sumber resmi tersebut menggambarkan hubungan organisasi yang lebih dekat daripada kelompok independen yang sekadar mendukung negara.

APT31 dan spionase siber

Pada 25 Maret 2024, Departemen Kehakiman Amerika Serikat (DOJ) mengumumkan dakwaan terhadap tujuh orang yang dikaitkan dengan APT31. Menurut uraian DOJ, kelompok itu melibatkan perwira intelijen Kementerian Keamanan Negara Tiongkok (MSS), peretas kontrak, dan personel pendukung. DOJ menggambarkannya sebagai bagian dari program spionase siber. Dakwaan tersebut berisi tuduhan yang harus dibuktikan, bukan putusan bersalah. [2]

DOJ juga menjelaskan pengiriman lebih dari 10.000 email berbahaya yang sering tampak seperti kiriman media atau jurnalis. Tautan pelacak dipakai untuk mengumpulkan informasi tentang penerima sebelum dilakukan penargetan lanjutan. [2] Membuka email dalam rangkaian yang dijelaskan itu tidak sama dengan otomatis menyerahkan seluruh isi komputer. Tahap pengenalan sasaran dan tahap pembobolan perlu dibaca sesuai peristiwa yang dilaporkan.

Nama kelompok merangkum banyak aktivitas dan peran. Pengelola infrastruktur, pengintai, dan penentu sasaran dapat merupakan orang yang berbeda. Untuk memahami hubungan kerja mereka, peneliti perlu memeriksa orang serta organisasi di balik aktivitas itu.

Perlindungan akun

Pesan dari akun yang dikenal dapat dipakai untuk melanjutkan penipuan. Pemeriksaan perlu mencari perubahan perilaku akun dan akses yang tidak semestinya, meskipun nama pengirim terlihat biasa.

BAB 03

Operasi informasi

Dokumen asli pun dapat menyesatkan ketika dipotong, diberi konteks baru, atau diterbitkan melalui sumber palsu.



Informasi yang diperoleh melalui peretasan dapat dipakai tanpa pernah diumumkan kepada publik. Namun, ketika materi itu diterbitkan, persoalannya berubah. Pembaca mulai menilai isi dokumen, orang yang disebut di dalamnya, dan penjelasan yang menyertai publikasi. Pada tahap ini, cara memilih serta menyajikan materi dapat sama berpengaruhnya dengan isi materi itu sendiri.

Keaslian dokumen dan konteksnya

Bayangkan sebuah notulensi rapat memuat usulan yang akhirnya ditolak. Jika hanya halaman berisi usulan yang disebarkan, pembaca dapat mengira organisasi telah menyetujuinya. Dokumennya mungkin asli. Kesimpulan yang muncul dari potongan itu tetap keliru karena keputusan akhirnya tidak ikut ditampilkan.

Contoh sederhana tersebut menjelaskan mengapa pemeriksaan dokumen perlu mencakup tanggal, kelengkapan, lampiran, dan kaitannya dengan dokumen lain. Keaslian menjawab asal materi. Konteks membantu menjelaskan maknanya. Keduanya diperlukan sebelum publikasi digunakan untuk menuduh seseorang atau menyimpulkan kebijakan sebuah organisasi.

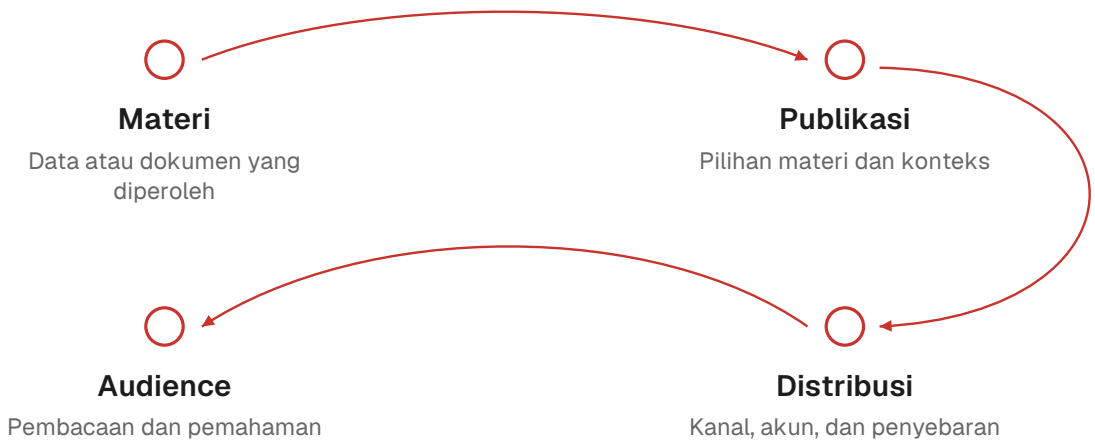
Dalam kebocoran data, pihak yang menerbitkan materi dapat memilih waktu, urutan, serta bagian yang hendak ditonjolkan. Pilihan itu dapat mengarahkan perhatian pembaca. Karena itu, mengetahui siapa memperoleh dokumen belum selalu cukup untuk menjelaskan siapa yang menyusun pesan publiknya. Rangkaian pencurian, penyerahan materi, dan penerbitan perlu ditelusuri melalui sumber yang tersedia. [6, 7]

Doppelganger dan penyamaran sebagai media

Operasi pengaruh juga dapat berjalan tanpa membocorkan dokumen. Pada 4 September 2024, DOJ mengumumkan penyitaan 32 domain yang dikaitkan dengan Doppelganger. Menurut dokumen pengadilan yang dijelaskan DOJ, perusahaan-perusahaan Rusia bekerja di bawah arahan Administrasi Kepresidenan Rusia untuk menyebarkan pesan yang menguntungkan kepentingan Rusia. [7]

Dalam uraian DOJ, domain yang menyerupai media sungguhan dipakai untuk membuat materi tampak berasal dari penerbit yang dipercaya. Akun media sosial, iklan, dan influencer kemudian mengarahkan pembaca ke situs-situs itu. Sebagian konten dibuat dengan bantuan AI. [7] Hubungan serta tindakan tersebut merupakan tuduhan dalam dokumen penegakan hukum.

Cara ini memanfaatkan kebiasaan membaca cepat. Sebuah judul ditemukan di media sosial, alamat situs tampak familier, dan materi dibaca dengan anggapan bahwa penerbitnya sudah dikenal. Kepercayaan kepada media asli seolah dipinjam oleh pihak lain. Pemeriksaan nama domain dan asal penerbit menjadi penting karena persoalannya sudah muncul sebelum pembaca menilai argumen di dalam artikel.



Alur informasi. Pengambilan informasi, penerbitan, dan penyebaran klaim dapat melibatkan pihak serta bukti yang berbeda. [6]

Menelusuri jaringan penyebaran

Dinas Luar Negeri Uni Eropa (EEAS) pada Maret 2025 melaporkan lebih dari 500 insiden manipulasi dan intervensi informasi asing yang dipantaunya sepanjang 2024. Aktivitas tersebut melibatkan sedikitnya 25 platform dan 38.000 akun, dengan sasaran di 90 negara. Laporan itu menyoroti hubungan antara kanal yang terlihat dan infrastruktur pendukung yang lebih tersembunyi. [6] Angka tersebut berlaku pada pemantauan EEAS, bukan seluruh aktivitas informasi di dunia.

Banyaknya akun belum menjelaskan siapa yang mengendalikannya. Orang dapat meneruskan pesan karena setuju, ingin membantah, atau sekadar tertarik. Penilaian tentang koordinasi perlu didukung perilaku dan hubungan yang lebih khusus, seperti asal materi serta keterkaitan antarkanal. Kesamaan pendapat saja tidak cukup.

Kritik dan ketidakpercayaan terhadap pemerintah dapat tumbuh dari pengalaman warga sendiri. Tuduhan campur tangan asing memerlukan bukti penyamaran atau manipulasi. Tanpa bukti itu, tuduhan tersebut justru dapat mengaburkan persoalan yang sedang dibicarakan masyarakat.

BAB 04

Gangguan layanan dan infrastruktur kritis

KA-SAT dan Volt Typhoon menunjukkan mengapa akses administrasi dapat berakibat jauh di luar ruang server.



Kebocoran informasi biasanya terlihat dari materi yang keluar. Gangguan layanan terasa melalui sesuatu yang hilang: koneksi tidak tersedia, perangkat tidak dapat terhubung, atau pekerjaan berhenti. Untuk memahami akibatnya, kita perlu mengikuti hubungan antara sistem yang dikelola penyedia dan kegiatan sehari-hari penggunanya.

KA-SAT: serangan melalui jaringan manajemen

Pada 24 Februari 2022, sebagian layanan broadband konsumen pada jaringan KA-SAT milik Viasat terganggu. Viasat melaporkan dampak terhadap beberapa ribu pelanggan di Ukraina dan puluhan ribu pelanggan lain di Eropa. Menurut laporan operator, penyusup memanfaatkan kesalahan konfigurasi perangkat remote access (VPN) untuk memasuki segmen manajemen, lalu menjalankan perintah yang menimpa data penting pada modem pelanggan. [8]

Dalam laporan itu, Viasat menyatakan tidak menemukan bukti bahwa satelit di orbitnya sendiri dikompromikan. Operator mengirim puluhan ribu modem pengganti sebagai

bagian dari pemulihan layanan. [8] Uni Eropa kemudian mengatribusikan serangan terhadap jaringan KA-SAT kepada Federasi Rusia dalam pernyataan 10 Mei 2022. [9] Penjelasan teknis operator dan atribusi pemerintah menjawab dua pertanyaan yang berbeda: bagaimana gangguan terjadi dan siapa yang dinilai bertanggung jawab.

Bagi pelanggan, kegagalan itu muncul sebagai hilangnya koneksi. Di belakangnya terdapat hubungan yang lebih panjang antara jaringan, perangkat pengelolaan, distributor, dan modem di lokasi pengguna. Hubungan tersebut menentukan siapa yang dapat mengubah sistem dalam jumlah besar dan siapa yang harus membantu ketika perangkat tidak dapat tersambung kembali.

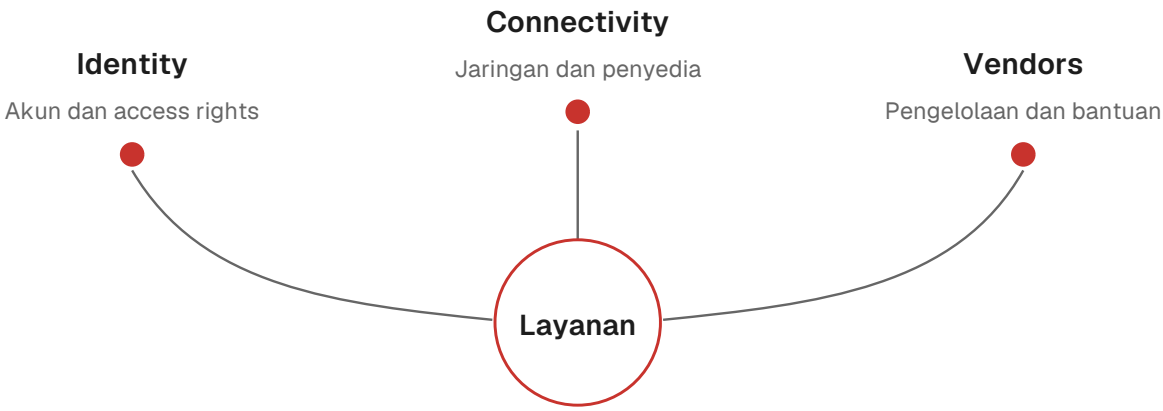
Pelajaran praktisnya adalah memahami akses administrasi. Organisasi dapat melindungi komputer pengguna dengan baik, tetapi tetap bergantung pada perangkat yang dikelola dari tempat lain. Bila jalur pengelolaan itu bermasalah, pemulihan mungkin membutuhkan bantuan pemasok atau penggantian perangkat. Daftar aset perlu memuat hubungan semacam ini, bukan hanya barang yang berada di kantor.

Volt Typhoon dan pre-positioning

Laporan keamanan bersama tanggal 7 Februari 2024 membahas akses Volt Typhoon ke jaringan infrastruktur kritis Amerika Serikat. Lembaga penerbit menilai dengan keyakinan tinggi bahwa aktivitas tersebut merupakan persiapan untuk memungkinkan gangguan terhadap sistem yang mengendalikan proses fisik ketika terjadi krisis atau konflik. Penggunaan akun yang sah dan alat yang sudah tersedia di lingkungan korban menjadi bagian dari aktivitas yang dijelaskan. [10]

Di sini, persoalannya belum tentu berupa layanan yang sudah berhenti. Akses yang bertahan dapat memberi pelaku kesempatan memahami lingkungan dan menyiapkan tindakan berikutnya. Organisasi dapat berada dalam keadaan berisiko meskipun pengguna belum merasakan gangguan. Karena itu, tidak adanya keluhan pelanggan belum menjawab apakah sistem aman.

Penanganan lingkungan yang terhubung dengan proses fisik juga memerlukan koordinasi. Memutus perangkat tanpa memahami fungsinya dapat mengganggu pekerjaan yang ingin dilindungi. Pengelola keamanan perlu bekerja dengan pemilik proses untuk menentukan cara memeriksa, membatasi akses, dan memulihkan sistem tanpa mengabaikan keselamatan.



Ketergantungan sistem menentukan dampak bagi pengguna.

Ketergantungan layanan. Contoh hubungan antara identitas, konektivitas, layanan organisasi, dan pengguna.

Perbandingan kasus

Kasus	Fokus laporan	Langkah perlindungan
Star Blizzard	Penargetan akun dan penggunaan informasi.	Lindungi akun serta hubungan korespondensi.
APT31	Dugaan spionase dengan pembagian peran pelaksana.	Periksa akses dan ruang lingkup data.
Doppelganger	Dugaan penyamaran penerbit dan distribusi pesan.	Periksa asal publikasi dan perilaku kanal.
KA-SAT	Gangguan pada sebagian layanan broadband.	Kenali jalur pengelolaan dan pilihan pemulihan.
Volt Typhoon	Akses yang dinilai menyiapkan gangguan.	Periksa akses yang bertahan dan batas antarsistem.

Perbedaan pokok antarkasus. Sumber kasus: [1, 2, 7, 8, 10, 15].

BAB 05

Atribusi: dari jejak ke pelaku

Alamat server adalah petunjuk. Menentukan siapa yang bertindak memerlukan hubungan antara banyak temuan.



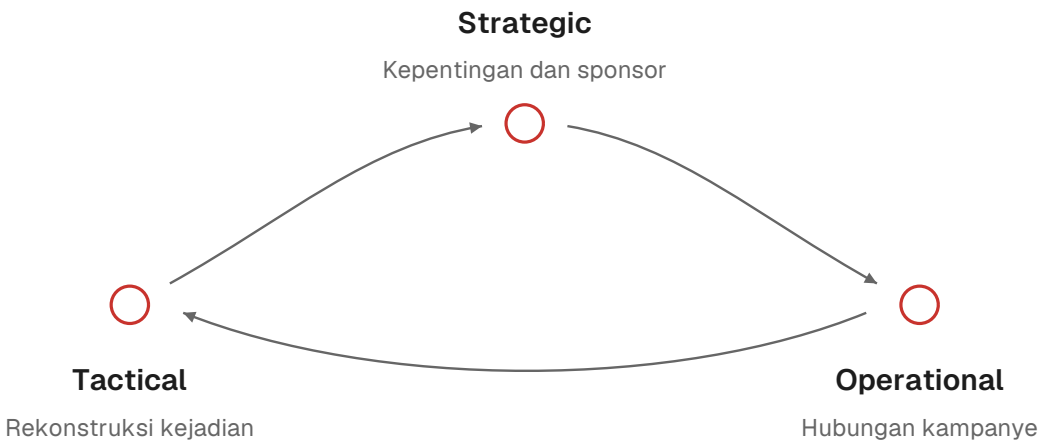
Dalam penyelidikan siber, jejak yang paling mudah ditemukan belum tentu menunjukkan pelaku sebenarnya. Alamat IP dapat mengarah ke server sewaan. Sebuah akun dapat digunakan oleh orang yang mengambil alihnya. Perangkat lunak yang sama dapat dipakai lebih dari satu kelompok. Jejak-jejak itu tetap berguna, tetapi maknanya bergantung pada hubungannya dengan temuan lain.

Bukti teknis dan atribusi

Atribusi adalah proses menghubungkan tindakan dengan pihak yang melakukannya. Rid dan Buchanan membahasnya pada tiga tingkat: taktis, operasional, dan strategis. Setiap tingkat melibatkan keahlian serta pertanyaan berbeda, tetapi hasilnya saling memengaruhi. Penyelidikan dapat menghasilkan penilaian dengan tingkat keyakinan yang berbeda sesuai bukti yang tersedia. [5]

Pada tingkat taktis, penyelidik merekonstruksi kejadian: kapan akses dimulai, akun apa yang dipakai, dan tindakan apa yang tercatat. Pada tingkat operasional, temuan dibandingkan dengan aktivitas lain untuk mencari hubungan kampanye atau kelompok. Tingkat strategis mencakup kepentingan serta kemungkinan hubungan dengan sponsor.

Urutannya tidak selalu rapi. Sebuah informasi dari luar organisasi dapat mengarahkan pemeriksaan teknis. Sebaliknya, temuan di perangkat dapat melemahkan dugaan awal tentang kelompok yang terlibat. Yang perlu dijaga adalah alasan di balik setiap kesimpulan: temuan mana yang mendukungnya dan bagian mana yang belum diketahui.



Tiga tingkat atribusi. Temuan teknis, pola operasi, dan konteks strategis saling memberi masukan. [5]

Contoh kasus: delapan dokumen

Anggap sebuah organisasi menemukan delapan dokumen internal di sebuah situs. Pemeriksaan menunjukkan bahwa dokumen itu cocok dengan arsipnya. Log sistem kemudian memperlihatkan satu sesi tidak sah yang mengunduh delapan berkas tersebut. Sampai di sini, organisasi mempunyai dasar untuk menyatakan bahwa sebagian data telah diakses dan muncul di luar lingkungannya. Contoh ini adalah gambaran penyelidikan, bukan kejadian nyata.

Ada beberapa pertanyaan yang masih terpisah. Apakah pengunduh dan penerbit merupakan orang yang sama? Apakah data lain juga diambil? Dari mana pelaku memperoleh akses? Jika catatan hanya tersedia pada satu sistem, penyelidik belum dapat memastikan apa yang terjadi pada sistem lain. Batas catatan tersebut perlu memengaruhi penilaian ruang lingkup.

Misalnya, situs publikasi ternyata menggunakan penyedia hosting di negara tertentu. Informasi itu membantu menelusuri layanan yang dipakai. Ia belum menjelaskan kewarganegaraan operator atau siapa yang memberi perintah. Lokasi infrastruktur dan identitas manusia adalah dua hal yang harus dihubungkan melalui bukti tambahan.

Kemandirian sumber

Lima berita dapat memuat tuduhan yang sama karena semuanya mengutip satu pengumuman. Dalam keadaan ini, jumlah berita tidak sama dengan jumlah sumber bukti. Peneliti perlu mengetahui asal keterangannya dan membedakan temuan baru dari pengulangan. Tanpa pemeriksaan itu, kesimpulan dapat terlihat semakin kuat hanya karena semakin sering disebut.

Hal serupa berlaku bagi pengakuan pelaku. Pengakuan dapat memberi petunjuk tentang sasaran atau waktu kejadian, tetapi perlu dibandingkan dengan apa yang benar-benar ditemukan. Pelaku dapat membesar-besarkan hasil, mengklaim pekerjaan orang lain, atau menerbitkan materi lama. Catatan kejadian lebih berguna daripada besarnya klaim untuk menentukan cakupan insiden.

Tingkat keyakinan dan alasannya

Sebuah kesimpulan menjadi lebih berguna ketika pembaca memahami kekuatannya. Penilaian dapat dibatasi karena data hanya tersedia untuk periode tertentu, karena sebagian infrastruktur tidak dapat diperiksa, atau karena ada dua penjelasan yang masih sama-sama masuk akal. Menyebut alasan tersebut membantu pihak lain menentukan apakah informasi sudah cukup untuk keputusan yang hendak diambil.

Keputusan mengamankan akun biasanya tidak perlu menunggu identitas sponsor. Sebaliknya, tuduhan publik terhadap suatu pihak memerlukan dasar yang menjelaskan hubungan pihak itu dengan kejadian. Kebutuhan pembuktian mengikuti keputusan yang sedang dipertimbangkan. Tim dapat melindungi sistem sambil tetap melanjutkan penyelidikan terhadap pelakunya.

BAB 06

Mengukur dampak

Akses berhasil, data bocor, dan perubahan sikap publik merupakan hasil yang berbeda. Cara mengukurnya pun berbeda.

Kata berhasil dalam sebuah serangan dapat berarti pelaku masuk ke akun, mengambil data, atau membuat dokumen tersebar. Keberhasilan teknis semacam itu perlu dibedakan dari perubahan sikap publik dan tercapainya tujuan politik. Setiap hasil membutuhkan bukti sendiri; keberhasilan pada tahap awal tidak menjamin hasil berikutnya.

Keberhasilan teknis dan tujuan strategis

Pemerintah Inggris menyatakan pada Desember 2023 bahwa beberapa serangan Star Blizzard menghasilkan kebocoran dokumen, tetapi upaya mengganggu politik dan demokrasi Inggris tidak berhasil. [1] Pernyataan itu menunjukkan mengapa hasil teknis dan hasil politik perlu dibaca terpisah. Kebocoran tetap dapat merugikan korban meskipun tujuan yang lebih besar dinilai tidak tercapai.

Pada kasus APT31, DOJ secara khusus menjelaskan bahwa dakwaan yang diumumkannya tidak menuduhkan peretasan untuk memajukan operasi pengaruh pemerintah Tiongkok terhadap Amerika Serikat. [2] Penargetan orang atau organisasi politik dengan demikian tidak cukup untuk menyatakan bahwa data yang diperoleh telah digunakan untuk memengaruhi pemilih.

Perbedaan ini sering hilang ketika laporan hanya mencari satu ukuran keberhasilan. Bagi pemilik akun, hilangnya kerahasiaan sudah merupakan kerugian. Bagi pengelola layanan, waktu berhenti beroperasi dapat menjadi ukuran utama. Bagi peneliti politik, pertanyaannya bisa menyangkut perubahan perilaku masyarakat. Ukuran tersebut dapat sama-sama penting tanpa harus menghasilkan penilaian yang sama.



Dari akses ke outcome. Setiap tahap membutuhkan bukti sendiri. Akses menunjukkan pelaku berhasil masuk; data menunjukkan informasi yang diambil; penyebaran mengukur jangkauan materi. Perubahan persepsi dan perilaku perlu diamati secara terpisah. Outcome dinilai dari tercapainya tujuan sponsor. Keberhasilan tahap awal tidak menjamin hasil akhirnya. [1, 2, 8]

Jangkauan, persepsi, dan perilaku

Angka tayangan membantu menunjukkan seberapa sering materi muncul atau dibuka menurut cara platform menghitungnya. Angka itu belum menjelaskan apakah orang mempercayainya. Pembaca dapat membuka materi untuk memeriksa, membantah, atau sekadar mengetahui apa yang sedang diperdebatkan. Pembagian ulang juga dapat dilakukan untuk alasan-alasan tersebut.

Jika tujuan sebuah penelitian adalah menilai perubahan sikap, peneliti memerlukan informasi tentang sikap itu sendiri. Jika tujuannya menilai perubahan tindakan, ia perlu mengamati tindakan yang relevan. Kemudian masih ada pertanyaan sebab akibat: apakah perubahan berkaitan dengan materi yang diteliti atau juga dipengaruhi peristiwa lain? Tanpa pembanding yang memadai, angka yang besar dapat memberi kesan yang berlebihan.

Dampak terhadap layanan

Untuk gangguan operasional, ukuran dapat dibuat lebih dekat dengan pekerjaan nyata. Catat layanan apa yang tidak tersedia, siapa yang terdampak, berapa lama pekerjaan tertunda, dan apa yang diperlukan untuk memulihkannya. Pengelola kemudian dapat membedakan pemulihan koneksi dari pulihnya seluruh pekerjaan yang bergantung pada koneksi tersebut.

Sebuah halaman login yang kembali muncul belum berarti layanan pulih. Pengguna perlu memastikan data lengkap dan pekerjaan utama bisa dijalankan. Pada data breach, pemulihan akses juga tidak menghapus salinan yang sudah diambil. Informasi yang terpapar serta kebutuhan korban tetap perlu dinilai.

BAB 07

Kesiapan menghadapi insiden

Kenali layanan utama, lindungi akun dengan hak akses istimewa, siapkan logging, dan uji pemulihan sampai pekerjaan utama dapat berjalan.



Organisasi tidak harus mengetahui semua kemungkinan pelaku untuk mulai memperkuat pertahanannya. Pekerjaan awal justru berhubungan dengan hal yang seharusnya dikenali sendiri: layanan yang dijalankan, akun yang dapat mengendalikannya, informasi yang disimpan, dan pihak yang membantu mengoperasikannya. Persoalan menjadi lebih sulit ketika pengetahuan itu baru dicari setelah gangguan terjadi.

Layanan utama dan ketergantungannya

Mulailah dari pekerjaan yang paling dibutuhkan pengguna. Bagi sebuah organisasi, itu mungkin penerimaan pesanan. Bagi organisasi lain, itu bisa berupa pelayanan pasien, pembayaran, atau akses terhadap arsip. Pemilik proses perlu menjelaskan apa yang terjadi jika layanan berhenti dan pilihan apa yang masih tersedia untuk melanjutkan pekerjaan.

Pemetaan kemudian bergerak ke sistem pendukung. Aplikasi utama dapat bergantung pada penyedia identitas, koneksi, penyimpanan, dan akun administrator. Hubungan ini membantu memilih prioritas. Sistem yang tampak kecil dapat memiliki pengaruh besar jika banyak layanan bergantung kepadanya.

NIST CSF dalam pekerjaan sehari-hari

NIST Cybersecurity Framework 2.0 membagi pengelolaan risiko ke dalam enam fungsi: Govern, Identify, Protect, Detect, Respond, dan Recover. Kerangka ini menjelaskan hasil yang ingin dicapai, tanpa menetapkan satu cara teknis yang harus dipakai semua organisasi. [3]

Dalam penggunaan sehari-hari, keenam fungsi itu dapat diterjemahkan menjadi pertanyaan kerja. Siapa yang mengambil keputusan? Aset dan risiko apa yang perlu dipahami? Perlindungan apa yang tersedia? Bagaimana kejadian diketahui? Siapa yang menanganinya? Bagaimana layanan dikembalikan? Jawabannya perlu menunjuk pada orang, sistem, dan prosedur yang benar-benar ada.

NIST SP 800-61 Revision 3, yang diterbitkan pada April 2025, menghubungkan respons insiden dengan pengelolaan risiko tersebut dan menggantikan Revision 2. Panduan ini menempatkan perbaikan sebagai pekerjaan yang berlangsung di seluruh fungsi. Pelajaran yang sudah ditemukan dapat segera digunakan, tanpa harus menunggu seluruh pemulihan selesai. [11]



Kesiapan dan perbaikan berkelanjutan. Pengelolaan risiko mendukung deteksi, penanganan, dan pemulihan. Pelajaran dari insiden memperbaiki seluruh fungsi. [3, 11]

Hak akses istimewa dan pemulihan akun

Akun dengan hak akses istimewa perlu dikenali bersama pemilik dan tujuan penggunaannya. Periksa apakah hak itu masih diperlukan, bagaimana akses diberikan, serta apa yang terjadi ketika pemiliknya pindah tugas. Jika beberapa orang menggunakan akun bersama, organisasi juga perlu mempertimbangkan bagaimana tindakan masing-masing dapat ditelusuri.

Kualitas autentikasi perlu diperhatikan. CISA merekomendasikan phishing-resistant authentication, termasuk FIDO/WebAuthn dan pilihan berbasis sertifikat digital, serta penerapan bertahap dengan mendahulukan akun bernilai tinggi. Kode sekali pakai dan persetujuan login melalui notifikasi aplikasi tidak semuanya memiliki ketahanan yang sama terhadap phishing. [12]

Penerapannya perlu mencakup keadaan sehari-hari yang mudah terlewat: pengguna kehilangan perangkat, nomor telepon berubah, atau administrator utama tidak dapat dihubungi. Jalur pemulihan harus tetap dapat digunakan oleh pemilik sah dan mempunyai pengamanan yang sesuai. Organisasi perlu menguji seluruh proses, bukan hanya berhasil menyalakan metode autentikasi baru.

Logging untuk penyelidikan

Log sistem berguna jika dapat menjelaskan kejadian. Untuk layanan penting, periksa apakah tersedia riwayat masuk, perubahan hak akses, dan tindakan administrasi yang diperlukan dalam penyelidikan. Perhatikan pula periode penyimpanan serta siapa yang dapat mengambil catatan ketika terjadi masalah.

Logging dapat diuji melalui perubahan yang sah dan telah disetujui. Setelah administrator menambah atau mencabut hak akses, tim memeriksa apakah tindakannya tercatat dengan jelas. Pemeriksaan ini dapat menunjukkan keterbatasan pemantauan sebelum tim harus menyelidiki insiden yang sebenarnya.

Backup dan pengujian pemulihan

Backup perlu diuji melalui pemulihan. Tentukan data yang akan dikembalikan, akses yang dibutuhkan, dan kondisi yang dipakai untuk menyatakan hasilnya benar. Pemilik layanan perlu ikut memeriksa apakah pengguna dapat menjalankan pekerjaan utama, termasuk ketika sistem bergantung pada penyedia di luar organisasi.

Hubungan dengan pemasok juga perlu memuat cara memperoleh bantuan saat insiden. Ketahui siapa yang benar-benar mengoperasikan layanan, siapa yang dapat menyediakan catatan, dan siapa yang berwenang melakukan tindakan darurat. Pengetahuan ini mengurangi waktu yang terbuang untuk mencari kontak ketika layanan sedang tidak tersedia.

Hasil latihan sebaiknya berujung pada pekerjaan yang jelas. Jika cadangan tidak dapat dipakai, ada pihak yang memperbaikinya. Jika catatan tidak cukup, pemilik sistem menindaklanjutinya. Jika kewenangan bertabrakan, pimpinan menyelesaikannya. Dengan cara itu, kesiapan dapat dinilai dari kemampuan yang telah diperiksa.

BAB 08

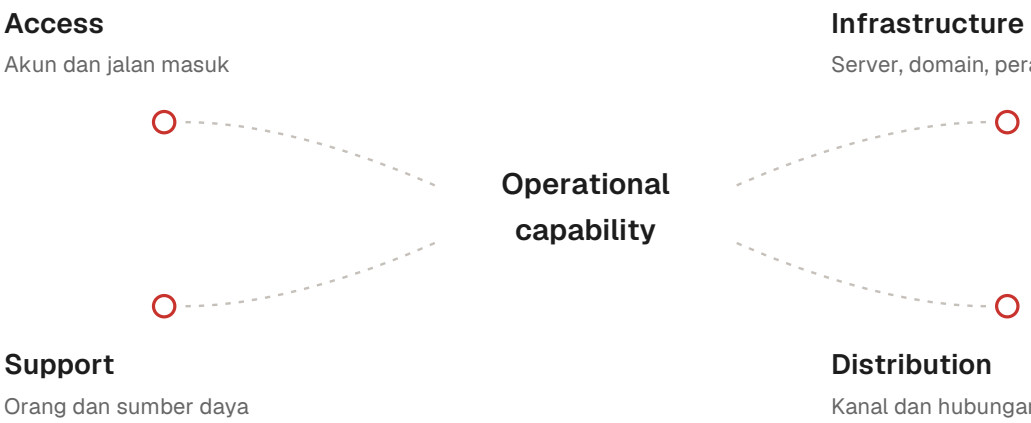
Ketahanan siber dan layanan publik

Ketahanan siber perlu dinilai dari kemampuan organisasi menjaga dan memulihkan layanan yang dibutuhkan orang.

Menutup satu server dapat menghentikan sebagian kegiatan pelaku. Namun, orang yang mengoperasikannya mungkin masih mempunyai akses lain, perangkat, pengetahuan, dan hubungan dengan penyedia layanan. Jika kemampuan itu tetap tersedia, kegiatan dapat berlanjut melalui sarana pengganti. Karena itu, penanganan ancaman tidak cukup dinilai dari jumlah akun atau domain yang ditutup.

Kemampuan yang tersisa setelah operasi diganggu

Laporan Chatham House pada Maret 2026 menelaah proxy siber dalam perang Rusia terhadap Ukraina. Penulisnya menyoroti keragaman hubungan pelaku dengan negara serta kemampuan kelompok untuk terbentuk kembali setelah gangguan. Mereka mengusulkan respons yang lebih terkoordinasi antara langkah operasional, penegakan hukum, ekonomi, dan kerja sama sektor swasta. [13]



Kemampuan yang menopang operasi. Akses, infrastruktur, dukungan, dan distribusi merupakan bagian yang perlu diperiksa saat menilai kemungkinan kegiatan berulang. [13]

Implikasi bagi organisasi di Indonesia

Kasus dari negara lain tidak membuktikan adanya hubungan proxy tertentu di Indonesia. Namun, persoalan pengelolaan yang diperlihatkannya relevan bagi organisasi di sini. Layanan dapat bergantung pada pemasok yang berlapis. Akun pribadi dan akun kerja dapat dipakai untuk urusan yang saling berkaitan. Dokumen internal dapat tersebar ke banyak mitra sehingga asal kebocoran tidak mudah ditentukan.

Organisasi dengan sumber daya terbatas dapat memulai dari satu layanan yang paling penting. Lengkapi daftar sistem dan akun yang menopangnya, pastikan ada orang yang bertanggung jawab, lalu uji satu proses pemulihan. Cakupan dapat diperluas setelah hasilnya dipahami. Prioritas seperti ini lebih membantu daripada mempunyai banyak rencana yang belum pernah dicoba.

Di media, perguruan tinggi, dan organisasi masyarakat sipil, informasi sensitif tidak selalu berupa data keuangan. Identitas narasumber, korespondensi riset, dan hubungan kerja juga dapat memerlukan perlindungan. Ketika anggota atau mitra berganti, akses terhadap ruang kerja dan dokumen perlu ditinjau agar tetap sesuai dengan kebutuhan.

Dampak terhadap masyarakat dan layanan publik

ICRC memperingatkan bahwa keterlibatan peretas sipil dalam konflik dapat membahayakan warga dan objek sipil. Penjelasannya menekankan perlindungan fasilitas medis, kegiatan kemanusiaan, serta infrastruktur yang dibutuhkan untuk kelangsungan hidup. ICRC juga mengingatkan risiko hukum dan perlindungan bagi warga yang berpartisipasi langsung dalam permusuhan. [14]

Bagi pengelola layanan, pertanyaan keselamatan perlu hadir sejak perencanaan. Bila sistem utama tidak tersedia, pekerjaan apa yang masih dapat dilakukan secara manual? Siapa yang harus segera diberi tahu? Apakah jalur komunikasi cadangan bergantung pada penyedia yang sama? Jawaban atas pertanyaan itu membantu mengurangi dampak saat gangguan teknis mencapai pelayanan sehari-hari.

Memahami proxy siber membantu kita melihat hubungan yang sering tersembunyi di balik sebuah insiden. Pengetahuan itu berguna ketika menghasilkan perlindungan yang lebih baik, penyelidikan yang lebih teliti, dan pemulihan yang lebih cepat. Organisasi yang mengenali ketergantungan layanannya, menjaga akses, dan menguji pemulihan akan lebih siap menjalankan tanggung jawabnya terhadap orang yang dilayani.

ISTILAH

Glosarium

Account takeover. Penguasaan akun oleh pihak yang tidak berhak.

Atribusi. Proses menghubungkan aktivitas dengan pelaku, kampanye, atau sponsor berdasarkan bukti yang tersedia.

Eksfiltrasi. Pemindahan data keluar dari sistem atau lingkungan yang semestinya menguasainya.

FIMI. Foreign Information Manipulation and Interference; istilah EEAS untuk manipulasi dan intervensi informasi asing.

Hak akses. Kewenangan yang diberikan kepada akun untuk membaca, mengubah, atau mengelola sesuatu di dalam sistem.

Intrusi. Akses atau kegiatan tanpa izin pada sistem digital.

Kesiapan menghadapi insiden. Kesiapan orang, sistem, dan prosedur untuk mendeteksi, menangani, serta memulihkan insiden.

Operasi pengaruh. Kegiatan untuk memengaruhi pemahaman, pilihan, atau perilaku orang.

Phishing. Penipuan yang menyamar sebagai pihak tepercaya untuk memperoleh informasi atau mendorong tindakan tertentu.

Pre-positioning. Penempatan akses atau kemampuan untuk memungkinkan tindakan pada kemudian hari.

Proxy siber. Aktor yang menjalankan kegiatan siber dengan dukungan, arahan, atau toleransi pihak lain. Bentuk hubungan dan tingkat kendalinya dapat berbeda.

Spear-phishing. Phishing yang disiapkan untuk orang atau kelompok tertentu dengan memanfaatkan informasi tentang sasarannya.

Sponsor. Pihak yang menyediakan dukungan atau pengarahan kepada pelaksana.

Teknologi operasional. Sistem yang digunakan untuk memantau atau mengendalikan perangkat serta proses fisik.

SUMBER

Daftar pustaka

[1] UK Government. UK exposes attempted Russian cyber interference in politics and democratic processes. 7 Desember 2023.
https://www.gov.uk/government/news/uk-exposes-attempted-russian-cyber-interference-in-politics-and-democratic-processes

[2] U.S. Department of Justice. Seven Hackers Associated with Chinese Government Charged with Computer Intrusions Targeting Perceived Critics of China and U.S. Businesses and Politicians. 25 Maret 2024; halaman diperbarui 6 Februari 2025.
https://www.justice.gov/archives/opa/pr/seven-hackers-associated-chinese-government-charged-computer-intrusions-targeting-perceived

[3] C. Pascoe, S. Quinn, dan K. Scarfone. The NIST Cybersecurity Framework (CSF) 2.0. NIST CSWP 29, 26 Februari 2024. doi: 10.6028/NIST.CSWP.29.
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

[4] Tim Maurer. "Proxies" and Cyberspace. Journal of Conflict & Security Law, vol. 21, no. 3, hlm. 383 sampai 403, 2016. doi: 10.1093/jcsl/krw015.
https://carnegieendowment.org/files/JConflictSecurityLaw-2016-Maurer-383-403.pdf

[5] Thomas Rid dan Ben Buchanan. Attributing Cyber Attacks. Journal of Strategic Studies, vol. 38, no. 1 sampai 2, hlm. 4 sampai 37, 2015. doi: 10.1080/01402390.2014.977382.
https://www.sipa.columbia.edu/sites/default/files/2022-11/Cyber_Workshop_Attributing%20cyber%20attacks.pdf

[6] European External Action Service. Inside the infrastructure of Foreign Information Manipulation and Interference (FIMI) operations. 19 Maret 2025; penjelasan pendamping 3rd EEAS Threat Report.
https://www.eeas.europa.eu/eeas/inside-infrastructure-foreign-information-manipulation-and-interference-fimi-operations_en

[7] U.S. Department of Justice. Justice Department Disrupts Covert Russian Government-Sponsored Foreign Malign Influence Operation Targeting Audiences in the United States and Elsewhere. 4 September 2024.
https://www.justice.gov/archives/opa/pr/justice-department-disrupts-covert-russian-government-sponsored-foreign-malign-influence

[8] Viasat. KA-SAT Network cyber attack overview. 30 Maret 2022.
https://www.viasat.com/perspectives/corporate/2022/ka-sat-network-cyber-attack-overview/

[9] Council of the European Union. Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union. 10 Mei 2022.
https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/

[10] CISA dan lembaga mitra. PRC State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure. Joint Cybersecurity Advisory AA24-038A, 7 Februari 2024.
https://www.cisa.gov/sites/default/files/2024-02/aa24-038a-jcsa-prc-state-sponsored-actors-compromise-us-critical-infrastructure_1.pdf

[11] A. Nelson, S. Rekhi, M. Souppaya, dan K. Scarfone. Incident Response Recommendations and Considerations for Cybersecurity Risk Management: A CSF 2.0 Community Profile. NIST SP 800-61r3, April 2025. doi: 10.6028/NIST.SP.800-61r3.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r3.pdf

[12] CISA. Implementing Phishing-Resistant MFA. Lembar panduan implementasi.
https://www.cisa.gov/sites/default/files/2023-01/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf

[13] Joyce Hakmeh, Harriet Moynihan, dan Nayana Prakash. Holding state-sponsored hackers and other cyber proxies to account: Lessons from tackling proxies in Russia's war on Ukraine. Chatham House, 25 Maret 2026; ringkasan dan pengantar penelitian. doi: 10.55317/9781784136772.
https://www.chathamhouse.org/2026/03/holding-state-sponsored-hackers-and-other-cyber-proxies-account/summary

[14] International Committee of the Red Cross. Eight rules for "civilian hackers" during war, and four obligations for states to restrain them. 2 Agustus 2024.
https://www.icrc.org/en/article/8-rules-civilian-hackers-during-war-and-4-obligations-states-restrain-them

[15] NCSC dan lembaga mitra. Russian FSB cyber actor Star Blizzard continues worldwide spear-phishing campaigns. Advisory bersama, 7 Desember 2023.
https://media.defense.gov/2023/Dec/07/2003353251/-1/-1/0/ADVISORY-RUSSIAN-FSB-CYBER-ACTOR-STAR-BLIZZARD-CONTINUES-WORLDWIDE-SPEAR-SPHISHING-CAMPAIGNS.PDF