Jurnal Sosial Humaniora Terapan

Volume 6
Issue 1 *January - June 2024*

Article 3

URGENSI PEMANFAATAN OPEN SOURCE INTELLIGENT (OSINT) DALAM UPAYA PENCEGAHAN AKSI TERORISME DI INDONESIA

Nia Lavinia
Universitas Indonesia, nia.lavinia@ui.ac.id

Puspitasari Puspitasari
Universitas Indonesia, puspitasari11@ui.ac.id

Recommended Citation

Lavinia, Nia and Puspitasari, Puspitasari (2023) "URGENSI PEMANFAATAN OPEN SOURCE INTELLIGENT (OSINT) DALAM UPAYA PENCEGAHAN AKSI TERORISME DI INDONESIA," *Jurnal Sosial Humaniora Terapan*: Vol. 6: Iss. 1, Article 3.
DOI: 10.7454/jsht.v6i1.1105
Available at: https://scholarhub.ui.ac.id/jsht/vol6/iss1/3

Jurnal Sosial Humaniora Terapan, 06 (01) (2024) 22-33
https://scholarhub.ui.ac.id/jsht/
P-ISSN: 2622-1764, E-ISSN: 2622-1152

URGENSI PEMANFAATAN *OPEN SOURCE INTELLIGENT* (OSINT) DALAM UPAYA PENCEGAHAN AKSI TERORISME DI INDONESIA

Nia Lavinia*, Puspitasari
Sekolah Kajian Stratejik dan Global, Universitas Indonesia, Indonesia

*Correspondence: nia.lavinia@ui.ac.id

Received: December 12, 2023 / **Approved:** January 09, 2024 / **Published:** January 14, 2024

Abstract

The invention of increasingly sophisticated technology and an increasingly connected world changed the nature of terror groups from "traditional terrorism" to "sophisticated terrorism". This complicates the task of the security forces because to be able to fight them, the apparatus is required to be sophisticated as well. Departing from the concept of information on the “ring of security,” it reveals that the successful collection of intelligence information will help prevent terrorist attacks. This research aims to illustrate the importance of using Open Source intelligence (OSINT) to increase the level of sophistication of the apparatus in gathering and analyzing intelligence information in the fight against terrorism. This is descriptive qualitative research with secondary data analysis collected through the literature study. The main argument of this research is that OSINT is still under-exploited as a source of intelligence information in Indonesia. This is due to intelligence agencies' collection of intelligence information from OSINT sources, which is still very close, so there is no room for collaboration between intelligence agencies and academics and OSINT practitioners. OSINT can be used as a solution to increase the effectiveness of counter-terror strategies by quickly identifying the roots of radicalism in online communities, which not only increases capabilities and opportunities to prevent terrorism attacks but also identifies planned attacks and early signs or signals of acts of terrorism in Indonesia.

Penemuan teknologi yang semakin canggih dan dunia yang semakin terhubung, mengubah nature kelompok teror dari “terorisme tradisional” menjadi “terorisme canggih”. Perubahan ini mempersulit tugas aparat keamanan karena untuk dapat melawan mereka, aparat dituntut untuk menjadi canggih pula. Berangkat dari konsep informasi “*ring of security*” yang mengungkap bahwa pengumpulan informasi intelijen yang berhasil akan membantu mencegah serangan terorisme. Riset ini bertujuan untuk menggambarkan pentingnya pemanfaatan *Open Source Intelligence* (OSINT) untuk menaikkan level kecanggihan aparat dalam pengumpulan informasi intelijen dalam melawan terorisme. Riset ini adalah riset kualitatif deskriptif dengan analisis data sekunder yang dikumpulkan melalui studi Pustaka. Argumen utama riset ini adalah: OSINT masih kurang dieksploitasi sebagai sebuah sumber informasi intelijen di Indonesia. Hal ini disebabkan oleh pengumpulan informasi intelijen dari sumber OSINT oleh badan intelijen yang masih sangat tertutup sehingga belum ada ruang kolaborasi antara badan intelijen baik dengan akademisi maupun praktisi OSINT. Padahal, ketika OSINT digunakan secara maksimal, OSINT dapat menjadi solusi untuk meningkatkan efektivitas strategi kontra-teror dengan mengidentifikasi secara cepat akar radikalisme dalam komunitas online yang bukan hanya meningkatkan kapabilitas dan kesempatan untuk mencegah serangan terorisme, tetapi juga dapat mengidentifikasi rencana serangan dan tanda atau sinyal awal aksi terorisme di Indonesia.

Keywords: *advance terrorism, OSINT, indonesia, intelligence information, terrorism prevention*

INTRODUCTION

Pasca serangan bom bunuh diri di Gereja Katedral Makassar dan aksi lone wolf yang terjadi di Mabes Polri, ancaman terorisme terus menunjukkan diri sebagai bahaya bagi masyarakat di Indonesia. Dua serangan yang terjadi dalam waktu berdekatan ini menjadi bukti bahwa diperlukan lebih banyak upaya untuk dapat mengidentifikasi dan mendeteksi rencana serangan teroris agar dapat mencegah kerusakan yang lebih jauh akibat aksi terorisme. Dua serangan tersebut dan banyak serangan lain di beberapa negara seperti Nigeria, Pakistan, Irak sampai Mozambik seperti menjadi penanda untuk negara khususnya aparat keamanan agar tidak terlalu terlena meskipun terjadi tren penurunan serangan teror dan kematian pasca ISIS berhasil dilumpuhkan.

Dari serangan yang terjadi baik di Makassar, Mabes Polri, dan beberapa negara lain tersebut dapat dilihat bagaimana ancaman ISIS semakin beragam dan menyebar secara geografis terutama setelah kehancuran kelompok mereka di Suriah dan Irak. Selain itu juga terjadi pergeseran modus operandi yang lebih menyasar pada serangan-serangan kecil dengan mengandalkan senjata api, pisau, dan kendaraan sebagai senjata pilihan yang lebih mudah diakses, selalu tersedia dan relatif lebih murah meskipun umumnya tidak membunuh banyak orang (Blackwell dan Alexander, n.d.). Pergeseran modus operandi ini meningkatkan ketakutan pada teroris karena serangan kecil yang mereka lakukan dapat terjadi di mana saja, kapan saja, dan oleh siapa saja tanpa membutuhkan banyak persiapan atau peringatan sebelumnya. Hal ini membuat masyarakat berada dalam keadaan ancaman yang konstan karena selalu berpotensi menjadi korban serangan teroris.

Salah satu faktor kunci dalam difusi dan desentralisasi ancaman ISIS menurut banyak pengkaji terorisme adalah akibat dari meningkatnya penggunaan internet, serta media sosial dan berbagai platform digital lain untuk mendistribusikan propaganda atau hasutan, merekrut anggota baru, memberikan instruksi, dan mendorong operasi terorisme yang membuat ISIS tetap eksis meskipun tidak lagi memiliki wilayah yang dikuasai. Dengan bantuan sosial media dan platform digital tersebut, ISIS menampilkan wacana tentang peran agama dan kewajiban melakukan jihad, serta mengajarkan doktrin-doktrin lain yang membuat mereka dapat bertransformasi dari sekadar “pemberontak” yang menguasai sedikit wilayah menjadi sebuah kelompok yang berhasil mendirikan “kekhalifahan virtual” di seluruh dunia (Blackwell dan Alexander, n.d; Zoll, 2017).

Nada Bakos, mantan analis CIA yang menjadi senior fellow di Foreign Policy Research Institute bahkan menciptakan terma “Terror 2.0” untuk mendeskripsikan bagaimana ISIS benar-benar mengasah cara mereka menggunakan media sosial untuk menyebarkan propaganda (Zol, 2013). Bakos menyebut kelompok teror menggunakan Telegram, aplikasi pesan terenkripsi dan YouTube sebagai contoh bagaimana ISIS memanfaatkan teknologi modern untuk mempromosikan tujuan mereka. Meskipun beberapa platform media sosial berhasil menangkap tren ini dan melakukan penanggulangan dengan menghapus video propaganda dan konten- konten lain yang berhubungan dengan mereka, ISIS selalu menemukan jalan keluar dari pembatasan-pembatasan yang diberlakukan. Sebagai contoh, ketika Twitter membuat sebuah kebijakan menghapus ribuan akun terafiliasi ISIS, ISIS selalu dapat membuat akun-akun baru yang berpotensi lebih susah dideteksi karena dibuat secara anonim.

Selain media sosial yang digunakan untuk praktik manipulasi psikologi, moral, dan emosional seseorang, ISIS juga memanfaatkan dark web— jaringan halaman web yang

Doi: 10.7454/jsht.v6i1.1105

disembunyikan dari mesin pencari populer seperti Google. Selama ini dark web terkenal sebagai kendaraan populer untuk aktivitas kriminal termasuk perdagangan obat-obatan terlarang, pencurian identitas, perdagangan manusia, dan pornografi anak. Dalam konteks terorisme, berdasarkan laporan Newsweek, website yang dikontrol ISIS di dark web cukup populer karena memiliki sekitar 3000-5000 followers (Zol, 2013). Melalui dark web, ISIS melakukan taktik fisik dan taktik operasi dengan berfokus pada jual beli senjata dan amunisi, pembuatan dokumen palsu, penyebaran panduan pembuatan bahan peledak, hingga pendanaan cryptocurrency dan berbagai komunikasi anonim terenkripsi lainnya (Akhgar, 2016). Terakhir, kelompok teroris juga menggunakan internet untuk mengumpulkan informasi mengenai target sasaran mereka sebelum melakukan serangan, misalnya dengan menggunakan google maps untuk menyelidiki jalan menuju sasaran, menggunakan google satellite untuk melihat titik lemah sasaran, mencari dokumen-dokumen militer yang bocor, dll.

Dalam konteks terorisme, kemajuan teknologi, dan revolusi informasi pada akhirnya menjadi pisau bermata dua—karena bukan hanya memberikan akses dan kemudahan bagi masyarakat biasa, tetapi juga memberikan kemudahan bagi para kelompok teroris. Selain itu, penemuan teknologi, dan semakin terhubungnya dunia juga membuat kelompok teror ini semakin meningkat dan melibatkan dimensi lintas batas dan transnasional karena pesan-pesan yang mereka sampaikan dengan mudah teramplifikasi oleh internet, jaringan sosial di ruang online, dan alat komunikasi pintar—yang kemudian mengubah the very nature of terrorism dari teroris tradisional menjadi ‘teroris canggih’ (Staniforth, n.d.).

Ancaman nyata dari terorisme 2.0 atau teroris canggih ala ISIS—khususnya pasca runtuhnya kekuasaan mereka di Irak dan Suriah—adalah pergeseran propaganda yang awalnya banyak menyebut ajakan jihad ke Irak dan Suriah, menjadi lebih fokus pada instruksi untuk melakukan serangan di ‘dalam rumah’ yang ditujukan bukan hanya pada pengikut, tetapi juga pada simpatisan mereka. Itu artinya, serangan di dalam negeri masih akan terus terjadi sampai semua anggota dan simpatisan ISIS di ruang virtual dapat teridentifikasi untuk kemudian dilacak dan digagalkan rencananya.

Melihat bagaimana kelompok teroris semakin canggih dalam merencanakan aksi teror, peran aparat untuk menjaga hukum dan keteraturan serta melindungi warga negara dengan mencegah, mendeteksi, dan menginvestigasi kejahatan menjadi semakin penting. Aparat akhirnya dituntut untuk mengikuti jejak kelompok teror—dengan menjadi sama canggihnya untuk dapat mencegah, mengejar, melindungi dan mempersiapkan diri dalam menghadapi ancaman kelompok teror (Akhgar, 2016). Dan untuk dapat melakukan hal tersebut, dibutuhkan pendekatan holistik yang bukan hanya mengutamakan perlindungan fisik terhadap tempat- tempat strategis yang menjadi sasaran teror, tetapi juga dibutuhkan pendekatan terintegrasi dalam mengumpulkan informasi dan melakukan analisis intelijen terhadap organisasi teroris yang aktif di ruang online melalui propaganda, statement, atau pun rilis media yang mereka bagikan dalam kanal sosial media mereka.

Propaganda, statement, atau rilis tersebut dapat menjadi informasi penting yang dapat dianalisis oleh praktisi kontra-terorisme untuk menemukan petunjuk yang dapat membantu membangun strategi yang lebih efektif dalam melawan ancaman kelompok teroris tersebut (Amble, 2014). Harus diingat bahwa upaya untuk melawan teror online juga tidak kalah penting dari teror offline sehingga proses pengumpulan informasi intelijen di ruang online juga harus masuk ke dalam strategi utama keamanan negara. *Open Source*

Doi: 10.7454/jsht.v6i1.1105

Intelligent (OSINT) adalah tempat yang tepat untuk mengumpulkan informasi dan melakukan investigasi mengenai kelompok teror yang bermain di ruang online. Dengan bermodalkan perangkat komputer dengan koneksi internet yang stabil, aparat keamanan bisa mendapatkan informasi sebanyak-banyaknya tanpa membutuhkan skill spesifik karena semua alat investigasi online dan database sudah tersedia secara publik.

OSINT sejauh ini masih menjadi sumber intelijen yang belum teroptimalisasi padahal informasi yang ada di sana sangat esensial karena dapat membantu proses investigasi hingga membantu pengumpulan bukti untuk menguatkan tuntutan terhadap kelompok teror yang tertangkap. Memanfaatkan OSINT dapat membantu aparat keamanan untuk mengumpulkan data dan informasi secara cepat, memprosesnya dengan akurat, dan membuat rekomendasi kebijakan yang lebih efektif untuk mencegah, mengejar, melindungi dan mempersiapkan diri dalam menghadapi ancaman kelompok teror (Akhgar, 2016). Melihat skalanya yang besar, aksesibilitas yang mudah, dan hasil yang tinggi dengan hanya menggunakan sumber daya minimum, OSINT dapat melengkapi, menguatkan dan mengkonfirmasi pendekatan fungsi intelijen tradisional seperti human intelligence (HUMINT), maupun signals intelligent (SIGMINT).

Dengan menggunakan konsep informasi sebagai bagian dari *ring of security*, penelitian ini akan menjelaskan pentingnya penggunaan OSINT sebagai bagian dari proses intelijen yang setara dengan informasi yang dikumpulkan melalui metode pengumpulan informasi intelijen tradisional. Penulis juga akan memberikan contoh bagaimana OSINT telah digunakan oleh aparat keamanan di lingkup global serta contoh beberapa alat yang dapat digunakan untuk melakukan investigasi secara online dalam upaya pencegahan serangan terorisme di Indonesia.

Argumen utama riset ini adalah OSINT masih kurang dieksploitasi sebagai sebuah sumber informasi intelijen di Indonesia. Hal ini disebabkan oleh pengumpulan informasi intelijen dari sumber OSINT oleh badan intelijen yang masih sangat tertutup sehingga belum ada ruang kolaborasi antara badan intelijen baik dengan akademisi maupun praktisi OSINT. Padahal, ketika OSINT digunakan secara maksimal, OSINT dapat menjadi solusi untuk meningkatkan efektivitas strategi kontra-teror dengan mengidentifikasi secara cepat akar radikalisme dalam komunitas online yang bukan hanya meningkatkan kapabilitas dan kesempatan untuk mencegah serangan terorisme, tetapi juga dapat mengidentifikasi rencana serangan dan tanda atau sinyal awal aksi terorisme di Indonesia.

Definisi OSINT

Peran penting OSINT mungkin baru diperhatikan di awal abad 21 atas keberhasilan revolusi dan demokratisasi teknologi yang membuat data dan informasi dalam jumlah yang signifikan dapat ditransfer ke dalam bentuk digital (Klečková, 2021). Tetapi, penggunaan informasi dari sumber *open source* sebenarnya sudah dilakukan oleh pemerintah dan intelijen AS sejak lebih dari 200 tahun yang lalu. Para tentara di masa itu mengumpulkan sumber OSINT secara manual dengan cara mentranslasi, mempelajari artikel, buku, surat kabar, dll untuk dapat memperoleh pengetahuan mengenai tempat-tempat asing dan kemampuan militer negara lain. Di tahun 1939 percobaan untuk meng institusionalisasi pengumpulan analisis dan informasi eksklusif yang berasal dari open source baru berhasil saat dibentuknya BBC Monitoring yang kala itu ditugaskan untuk memonitor seluruh siaran radio yang terkait dengan kekuatan poros (Amble, 2014).

Doi: 10.7454/jsht.v6i1.1105

Sebelum membicarakan mengenai urgensi menggunakan OSINT, OSINT perlu didefinisikan terlebih dahulu. Untuk memahami apa itu OSINT, sebelumnya penting untuk memahami apa itu *open source data* (OSD), dan *open source information* (OSINF) yang menjadi bahan mentah untuk pembuatan OSINT. Klarifikasi atas perbedaan terma- terma ini akan berguna untuk mengilustrasikan bahwa OSINT bukan sekadar informasi sederhana yang dapat ditemukan siapa saja dalam domain publik.

Jika merujuk pada NATO dalam *Open Source Intelligence Handbook*, *open-source data* (OSD) adalah data yang belum diproses dan belum ada pengeditan oleh analis. Data ini dapat berupa cetakan mentah atau pembekalan lisan dari pejabat pemerintah, pustakawan atau jurnalis dengan keahlian di bidang tertentu; OSD juga dapat berupa surat pribadi atau bentuk informasi lainnya dari sumber utama. OSD juga dapat diperoleh dari sumber-sumber teknis seperti foto, rekaman pita atau citra satelit komersial. Karena OSD adalah data mentah, ia perlu menjalani beberapa elaborasi untuk mencapai level selanjutnya yaitu *open-source information* atau OSINF (Minas, 2010).

OSD dapat menjadi OSINF ketika dianalisis, diedit, disaring, dan divalidasi pada tingkat tertentu— kemudian disebarluaskan di internet, surat kabar, siaran radio atau TV, jurnal akademik, laporan pemerintah, dll. Medium yang disebutkan tersebut menjadi sumber sekunder yang dapat didapatkan oleh publik. Namun, ada juga sumber OSINF yang tidak selalu mudah didapatkan seperti *grey literature*— mengacu pada materi yang tidak dapat diperoleh dengan mudah meskipun tidak disembunyikan seperti: prosiding konferensi, disertasi, atau buletin internal (Minas, 2010). Suatu sumber baru dapat dikatakan sebagai OSINT ketika OSINF atau informasi yang tersedia dianalisis, disaring, divalidasi, dan kemudian disebarluaskan sebagai produk intelijen (Minas, 2010:8). Jika disederhanakan, OSINT dapat dipahami sebagai eksploitasi informasi *open source* untuk tujuan intelijen sebagai bagian dari keseluruhan sumber dari proses intelijen (Hobbs, Moran and Salisbury, 2014 dalam Klečková, 2021).

Sumber OSINT

Sebelum muncul dan meluasnya Internet di pertengahan 1990-an, media (elektronik dan cetak) adalah sumber paling luas yang dapat digunakan oleh beberapa analis *open source* di masa tersebut untuk mengekstrak informasi yang berguna. Namun, meskipun sudah ada internet, media juga masih tetap menjadi salah satu kemampuan inti dari kegiatan OSINT karena pemantauan media cetak asing seperti surat kabar dan terbitan berkala serta media elektronik seperti siaran TV atau radio akan selalu penting. Baru setelah semakin berkembangnya ilmu pengetahuan dan teknologi, internet menjadi sumber informasi *open source* paling berharga karena selain sebagai penyedia sejumlah besar informasi yang tersedia bagi siapa saja, orang-orang menggunakan internet untuk berbagi informasi, berkomunikasi, bertukar ide, rencana, dan wawasan profesional yang membuat internet adalah sumber OSINT yang sangat kaya. Situs web banyak yang dapat diakses secara gratis maupun berlangganan, dan jika menginginkan informasi spesifik terkait suatu hal, pengguna dapat mencarinya dengan memasukkan karakteristik pencarian yang diinginkan seperti lokasi, organisasi, atau kata kunci lain yang dapat membuatnya lebih relevan dan berharga bagi analis OSINT (Minas, 2010).

Sosial media yang terdiri dari laman internet, aplikasi, blog, forum untuk memposting, membagikan, dan melihat konten menjadi sumber OSINT penting lainnya. Media sosial hari ini menjadi tempat yang mana pengguna dapat membuat dan membagi

Doi: 10.7454/jsht.v6i1.1105

informasi tentang diri mereka dan teman- teman, kesukaan, ketidaksukaan, gerakan, pemikiran, transaksi, dll, yang semua interaksinya meninggalkan jejak digital. Jejak digital ini lah yang menjadi sumber informasi terbesar yang pernah dimiliki mengenai seseorang dan masyarakat yang bahkan belum pernah ditemui. Analisis dari ruang sosial yang baru ini sudah tersebar melalui sektor privat untuk *marketing* dan manajemen brand, dalam politik untuk perencanaan pemilik dan sebagai topik minat akademisi yang berkembang (Omand dan Bartlett, 2014).

Sumber dengan nilai tertinggi untuk OSINT saat ini tampaknya adalah citra satelit komersial. Beberapa tahun yang lalu, negara-negara yang memiliki fasilitas satelit adalah negara-negara yang diistimewakan. Saat ini, setiap pemerintah atau aktor nasional atau internasional lainnya, yang bersedia membayar, memiliki kemampuan untuk mengakses citra satelit (Minas, 2010). Sumber OSINT berikutnya adalah penyedia informasi sektor swasta dan publik yang menawarkan jasa untuk melakukan pelacakan dan pemantauan siaran elektronik dan cetak seperti BBC Monitoring. Terakhir, sumber lain yang sangat penting untuk OSINT adalah jaringan para ahli. Jaringan para ahli menjadi penting ketika intelijen tidak dapat pergi ke suatu tempat untuk mencari informasi karena terkendala biaya atau jarak. Kontribusi yang diberikan oleh ahli mengenai pengetahuan lokal atau keilmuan yang dimilikinya dapat menambah nilai produk intelijen karena ahli dapat memberikan analisis yang sangat rinci. Jaringan para ahli ini dapat terdiri dari kelompok akademisi, jurnalis, pekerja organisasi internasional, atau bahkan masyarakat adat (Minas, 2010).

Bagaimana OSINT digunakan dalam upaya kontra-terorisme OSINT telah menjadi salah satu gudang senjata yang digunakan *Institute for Counter Terrorism* (ICT). OSINT menyediakan akses kepada kejadian dan database aktivis yang menjadi basis data untuk insiden terorisme di seluruh dunia. Sejak 1975, database yang berhasil direkam mencapai lebih dari 37.000 kejadian termasuk serangan yang berhasil, gagal, digagalkan, dan informasi mengenai operasi kontra teror di seluruh dunia dengan memuat latar belakang dan informasi lanjutan mengenai operasi tersebut. OSINT memungkinkan aparat keamanan untuk terlibat dan berbagi informasi dengan publik yang dapat membantu mencegah penyebaran rumor, hoax, atau disinformasi. OSINT juga mengizinkan masyarakat dan pihak keamanan untuk bekerja sama dalam investigasi yang sedang berlangsung melalui *volunteer based-crowd-sourced intelligence* (Bartlett, Miller dan Middleton, 2013 dalam Klečková, 2021).

Dengan mengadopsi skema kontra-terorisme di Inggris (CONTEST) yang terdiri dari 4P yaitu *prevent*: untuk menghentikan orang menjadi teroris atau pendukung teroris; *pursue*: untuk menghentikan serangan teroris; *protect*: untuk memperkuat perlindungan melawan serangan terorisme; dan *prepare*: untuk memitigasi dampak dari serangan terorisme, berikut adalah contoh keberhasilan OSINT ketika digunakan dalam upaya kontra-terorisme dengan skema tersebut. Dalam strategi pencegahan atau *prevent*, OSINT digunakan untuk mengidentifikasi narasi, propaganda, dan pengaruh yang diberikan oleh kelompok teror dalam upaya mereka untuk menghasut dan merekrut anggota baru di internet. Di sini praktisi OSINT dapat mengidentifikasi propaganda, *disinformation*, dan narasi radikal untuk kemudian berkomunikasi dengan departemen keamanan agar terlibat dengan publik melalui media sosial untuk melawan propaganda dengan membuat kontra-narasi atau kontra-ideologi serta secara berkala membagikan informasi yang akurat kepada publik agar tercipta ketenangan di ruang online. OSINT juga dapat berkontribusi dalam pengumpulan informasi secara sistematis dan analisis media kelompok teroris yang dapat

Doi: 10.7454/jsht.v6i1.1105

mengidentifikasi aktor kunci dalam operasi teroris. Ini penting untuk memperkirakan sifat ancaman yang ditimbulkan oleh kelompok teror.

Sebuah aspek kontra-terorisme yang akan sulit dilakukan tanpa akses *open source* ke aktivitas online kelompok teror (Klečková, 2021). Keberhasilan pencegahan dengan menggunakan OSINT terjadi pada penangkapan Hosam Smadi, Antonio Martinez, dan Ali yang ditangkap setelah plot terornya digagalkan FBI yang memonitor *chat room* dan media sosial para jihadis dengan secara efektif serta melakukan penindakan lanjut. Monitoring yang efektif terhadap sumber tersebut membawa pada penilaian ancaman yang lebih akurat, sehingga media para jihadis selalu dianggap sebagai sumber intelijen yang penting dan gampang (Younas, 2014, dalam Klečková, 2021). Dalam upaya *global war on terror* (GWOT), pemeriksaan yang lebih dekat terhadap website jihadis dengan menggunakan OSINT juga berhasil memberikan petunjuk atas tanda-tanda awal perkembangan ideologis yang diprediksi akan mempengaruhi barat. Dalam strategi pengejaran atau *pursue*, OSINT dapat mengurangi ancaman teror dengan mengganggu operasi teroris yang sedang berjalan. Hal ini dapat dilakukan dengan mengumpulkan data intelijen melalui dark web. Pengumpulan informasi di sana dapat menjadi bukti untuk mengamankan tuntutan, memantau pergerakan kelompok teror, mendisrupsi jaringannya dengan memotong akses ke funding atau materi yang mereka butuhkan untuk melakukan serangan.

Sebagai contoh, situs web jihadis global pernah memposting isu-isu strategis seperti tujuan politik dan militer serta ideologi mereka. Postingan berisi ide dan strategi ini sengaja diterbitkan untuk menginspirasi dan membimbing pengikut Al Qaeda serta afiliasi globalnya. Dengan melakukan analisis terhadap postingan tersebut, pemerintah dapat memahami gambaran strategis para jihadis dan memperkirakan respon apa yang tepat untuk menjawab potensi ancaman yang dapat terjadi. Seperti yang terjadi ketika Maret 2005 yang mana *Center for Islamic Studies dan Research*, sebuah lembaga yang terafiliasi dengan Al-Qaeda menerbitkan dokumen berbahasa arab sebanyak 113 halaman yang berjudul "manajemen *barbarism*" (Idarat al-Tawahhush) di internet. Dokumen ini menjadi sejenis cetak biru atau blueprint untuk strategi militer yang harus dilakukan para jihadis untuk mengalahkan AS dan sekutunya. Dalam level strategis, dokumen itu memanggil untuk melakukan *"Disruption and Exhaustion*" sebuah fase berdasarkan premis bahwa penyerangan terhadap soft target akan memaksa AS dan sekutunya untuk menyebar sumber daya keamanan mereka yang terbatas.

Serangan terhadap soft target juga akan memberikan kerugian ekonomi dan finansial dalam prosesnya. Dokumen itu memanggil untuk menyerang destinasi wisata yang biasa didatangi oleh Barat, bank yang menawarkan bunga atau riba dan instalasi minyak seperti pipa, penyulingan, dan tempat pengiriman atau distribusi. "Musuh yang superior akan dikalahkan dengan gesekan ekonomi dan militer". Sehingga dalam dokumen disarankan untuk melakukan perang dengan cara memberikan gesekan yang berlarut-larut terhadap AS. Dokumen ini memberikan gambaran dan sejauh mana indikasi mental yang siap ditempuh oleh para jihadis global (Tow dan Yeo, 2005). Dengan analisis yang mendalam terhadap informasi tersebut, aparat keamanan dapat langsung mengetahui objek mana yang menjadi rentan terhadap serangan dan strategi apa yang harus dilakukan agar rencana teroris untuk mendisrupsi dan membuat lelah aparat yang hendak dilakukan oleh Al Qaeda dapat digagalkan.

OSINT dapat mengurangi kerentanan terhadap serangan teror dengan melakukan penilaian proaktif terhadap kerentanan dan area sosial berisiko, serta ancaman terhadap

Doi: 10.7454/jsht.v6i1.1105

perkumpulan massa. Ini juga membantu melindungi infrastruktur penting dengan meningkatkan keamanan. OSINT mendukung upaya kontra-teror melalui analisis kapabilitas secara real-time, memberikan kesadaran situasional yang lebih besar. Selain itu, OSINT memantau aktivitas media sosial jihadis, mengumpulkan data mengenai pertempuran, kondisi terkini, dan insiden, untuk melawan ISIS dan serangan lone wolf.

Terakhir, dalam strategi persiapan atau *prepare*, OSINT dapat membantu aparat untuk memastikan bahwa populasi siap dan memahami konsekuensi dari serangan teroris. Hal ini dapat dilakukan dengan resiliensi, dan persiapan untuk ancaman serangan *Chemical, Biological, Radiological, Nuclear and Explosive* (CBRNE) yang potensial, membuat deteksi dini untuk serangan akut (Akhgar, 2016).

METHODOLOGY

Penelitian ini adalah penelitian kualitatif deskriptif dengan analisis data sekunder yaitu artikel dan publikasi mengenai OSINT dan contoh penggunaan OSINT dalam konteks terorisme di Indonesia yang dikumpulkan melalui studi Pustaka. “Informasi” dalam konsep *ring of security* akan digunakan untuk mengelaborasi data untuk menunjukkan urgensi penggunaan OSINT dalam upaya pencegahan dan deteksi dini aksi teror di Indonesia.

Ring of security adalah sebuah konsep keamanan untuk mencegah serangan terorisme dengan memperhatikan tiga lapisan sistem pengamanan yaitu: keamanan fisik sebagai lapisan terdalam, keamanan teknis sebagai lapisan kedua, dan keamanan informasi sebagai lapisan terluar (Priyanto, 2021). Keamanan fisik terdiri dari sistem pengamanan yang meliputi desain bangunan, daerah- daerah yang mungkin tidak terkontrol, pintu gerbang bagi kendaraan atau pejalan kaki yang hendak masuk ke dalam bangunan, rintangan yang dibuat untuk menahan seseorang yang masuk tanpa izin ke dalam bangunan, jalan atau akses masuk yang digunakan oleh tamu (orang selain karyawan), dan akses layanan lain yang dibutuhkan oleh Gedung.

Sementara keamanan teknis terdiri dari personel keamanan yang bertanggung jawab atas keamanan di tempat ia ditugaskan, perangkat keamanan seperti CCTV, menara pengawas, alarm, *metal detector*, *drone*, dll; dan sistem pengamanan teknis dan prosedural lain seperti sistem pengawasan yang dilakukan petugas keamanan, waktu penjagaan, rotasi petugas jaga, serta standar operasional lain yang diatur untuk meminimalisir terjadinya kejahatan. Terakhir, keamanan informasi yang menjadi konsep utama yang digunakan untuk mengelaborasi temuan dalam penelitian ini, adalah sebuah sistem keamanan yang ada di luar gedung atau objek vital yang menjadi tempat berbagai aktivitas dan kejadian yang merupakan sumber informasi penting bagi keamanan gedung atau objek vital tersebut. Keamanan informasi juga mencakup peristiwa atau kejadian yang berlangsung di lingkungan sekitar baik itu sesuatu yang rutin atau bukan rutin, dan berita-berita yang berasal dari media massa (Priyanto, 2021:ibid).

FINDINGS AND DISCUSSION

Keamanan negara disimbolkan oleh keamanan objek-objek vital yang memiliki peran penting bagi kehidupan bangsa dan negara serta menyangkut hidup orang banyak

Doi: 10.7454/jsht.v6i1.1105

selalu berkaitan dengan kegiatan intelijen untuk menghindari adanya kemungkinan ancaman, gangguan, dan serangan terhadap keamanan objek vital tersebut. Keberhasilan proses intelijen untuk memberikan informasi yang mumpuni dapat menjadi *game changer* dalam melakukan deteksi dini dan mencegah potensial serangan terjadi.

Yang perlu menjadi perhatian, disiplin intelijen tradisional, khususnya *human intelligence* (HUMINT), bukan sebuah aktivitas yang dapat dilakukan dan diberhentikan dalam waktu singkat, ini membuat HUMINT sulit untuk digunakan sebagai sarana pengumpulan informasi atas kejadian yang bersifat *real time*. Sementara OSINT, dapat dilakukan kapan saja dengan memanfaatkan sumber data seperti citra satelit yang sekarang tersedia secara komersial, berita yang telah dikumpulkan, hasil pencarian di internet, jurnalisme warga, dan informasi dari para *blogger* yang membantu mengungkap misteri ketidakpastian yang terjadi dalam waktu yang cepat—atau bahkan real time. Ketika 'serangan kejutan' terjadi, seperti serangan teror, kerusuhan, penculikan, dan revolusi, analis dan pembuat kebijakan harus mengandalkan OSINT untuk mencari informasi pertama untuk dapat memahami kejadian tersebut (Gibson, 2014). Pemahaman dan pengalaman menggunakan OSINT akhirnya menjadi vital karena OSINT dapat membantu berkontribusi terhadap keamanan publik dengan menaikan informasi yang tersedia bagi pihak yang kesulitan membuat keputusan khususnya ketika dalam tekanan waktu yang akut melalui tiga level berbeda.

Level pertama dan paling penting adalah OSINT membantu otoritas membangun kesadaran situasional saat berbagai peristiwa terjadi. Dari analisis sosial media misalnya, fakta penting tentang dunia dapat diidentifikasi: kapan suatu peristiwa terjadi, bagaimana perkembangan peristiwa itu sekarang, dan terjadi di mana serta siapa saja yang terlibat dalam peristiwa tersebut. Level kedua yang lebih kompleks adalah untuk mengkonstruksi penjelasan paling memungkinkan yang menjadi penyebab kejadian tersebut dari apa yang telah diamati dari analisis sosial media. Dalam level ini, pertanyaan kenapa dan bagaimana dimunculkan. Level kedua analisis ini meminta tingkat pemahaman umum yang tinggi tentang fenomena yang jadi pertanyaan dan istilah-istilah yang biasa digunakan oleh pelaku untuk mengekspresikan dirinya.

Level ketiga, ketika sudah mendapatkan penjelasan memadai mengenai kejadian dan motivasi dari pelaku, maka menjadi masuk akal untuk mencari sebuah prediksi mengenai bagaimana kejadian itu akan terungkap. Level analisis ketiga ini melibatkan penggunaan intelijen yang paling kompleks termasuk apa yang berasal dari media sosial, untuk menjawab pertanyaan tak terhindarkan dari otoritas politik dan operasional tentang apa selanjutnya dan di mana selanjutnya (Omand, Miller dan Bartlett, 2014)

Dalam konteks indonesia, proses intelijen masih menjadi sebuah aktivitas yang sangat rahasia karena pendekatan tradisional yang menggunakan HUMINT masih menjadi pendekatan utama ketika berbicara mengenai aktivitas intelijen (Mapparessa, 2021). Hal ini membuat publik tidak mengetahui bagaimana operasi intelijen dilakukan dan upaya-upaya apa yang selama ini telah dilaksanakan dalam mengumpulkan dan menganalisis sebuah informasi untuk dijadikan rekomendasi kebijakan. Artinya, publik—khususnya akademisi yang berada di luar lingkaran intelijen juga tidak mengetahui sejauh mana OSINT telah digunakan oleh aparat keamanan. Hal ini dibuktikan dengan sangat minimnya penelitian dan publikasi terkait topik ini. Satu-satunya informasi mengenai keberhasilan OSINT dalam pencegahan terorisme di Indonesia yang dapat diakses oleh publik adalah operasi yang dilakukan pada Mei 2013 yang berhasil mendeteksi dan menggagalkan sebuah

Doi: 10.7454/jsht.v6i1.1105

rencana serangan bom terhadap kedutaan besar Myanmar di Indonesia. Rencana ini berhasil digagalkan karena salah satu pelaku mengungkapkan rencana untuk melakukan serangan melalui status facebooknya (Younas, 2014 dalam Klečková, 2021).

Sebuah kasus di mana teroris membagikan rencananya secara sengaja atau pun tidak sengaja di media sosial adalah kasus yang langka, namun, hal ini dapat menjadi permulaan yang baik dalam memanfaatkan OSINT mengingat salah satu keunggulan OSINT adalah mencari sebanyak- banyaknya potongan informasi yang dapat menjadi petunjuk dalam sebuah proses investigasi. Meskipun tidak terbatas pada media sosial, tetapi analisis media sosial untuk kasus terorisme dapat memperlihatkan bagaimana potensial pelaku dapat terlihat dari kebiasaan-kebiasaannya ketika menggunakan platform tersebut. Apalagi, menurut hasil wawancara dengan pelaku teror, beberapa serangan yang terjadi di Indonesia berhasil dieksekusi karena mereka juga mendapatkan banyak informasi dari media sosial dan internet (Mapparessa, 2021:ibid).

Melihat kecanggihan kelompok teror, pengumpulan informasi dan analisis untuk kepentingan intelijen juga harus "naik level" dengan lebih banyak memanfaatkan sumber-sumber *open source* yang jumlahnya sangat melimpah. OSINT dikatakan dapat menyediakan 80% data dan informasi yang dibutuhkan oleh negara (Gibson, 2014). CIA unit Bin Laden bahkan menyebutkan bahwa 90% informasi dan data yang ingin seseorang ketahui dapat didapatkan dari OSINT. Lebih jauh, EUROPOL menyebut kontribusi OSINT bisa sampai 95% untuk isu kontra terorisme. Yang perlu dilakukan oleh aparat keamanan dan badan intelijen negara (BIN) adalah mengelaborasi dan maksimalisasi penggunaannya. Dan akan lebih optimal jika aparat melakukan investigasi dengan melibatkan atau berkolaborasi dengan praktisi OSINT lain seperti jurnalis, periset independen, dan organisasi masyarakat sipil untuk mengumpulkan data dan mencari sebanyak mungkin petunjuk agar dapat melengkapi mozaik dari kelompok teror— sebuah hal yang telah lama dilakukan oleh komunitas OSINT di seluruh dunia yang terbukti berhasil mengungkap kasus-kasus besar yang selama ini menjadi teka-teki.

Bellingcat— kolektif peneliti, investigator, dan jurnalis independen yang menggunakan OSINT, misalnya, berhasil mengungkap cerita di balik sebuah video mengerikan yang menarik perhatian dunia pada tahun 2018 mengenai eksekusi perempuan dan anak yang dibunuh secara kejam oleh sekelompok laki- laki bersenjata. Awalnya tidak diketahui bagian dari kelompok mana para lelaki bersenjata tersebut. Juga tidak jelas di mana insiden terjadi dan siapa perempuan yang menjadi korban tersebut. Namun tim investigator dan *volunter* dalam skala internasional sangat ber determinasi untuk membongkar kenyataan di balik video tersebut. Mereka berhasil melakukannya dengan cara menjahit potongan-potongan informasi yang didapatkan dari berbagai pihak seperti logat atau aksen bahasa yang digunakan pelaku untuk mengidentifikasi di wilayah mana kejadian itu terjadi; menggunakan analisis *geospasial* untuk mengetahui titik pasti kejadian yang dapat dilacak dengan mencocokan kondisi alam dan cuaca serta kontur wilayah dalam video dengan gambar dari pemantauan satelit; hingga mengidentifikasi corak seragam para tentara dan senjata yang mereka gunakan (Bellingcat, 2020). Investigasi menggunakan OSINT juga pernah dilakukan oleh jurnalis media *Tirto.id* ketika menelusuri keberadaan senjata Pindad—yang biasa digunakan oleh TNI dan Polri—ternyata digunakan kombatan ISIS di Marawi. Investigasi ini dilakukan dengan mencocokkan gambar senjata yang didapatkan dari sebuah foto di Campo Ranao ketika operasi militer di Marawi dengan banyak footage dan gambar lain yang tersedia di internet (Hanifan, 2017).

Doi: 10.7454/jsht.v6i1.1105

Selain yang telah disebutkan sebelumnya (analisis geolokasi, *google earth*, pemantauan CCTV, satelit google, image recognition), masih banyak *tools* lain yang dapat digunakan untuk mengumpulkan dan menganalisis informasi dengan menggunakan OSINT. Sebuah website bernama OSINT Framework (https://osintframework.com/) bahkan sengaja didedikasikan untuk mengumpulkan OSINT resource dan tools yang dapat digunakan secara gratis untuk mencari dan menganalisis data dari sumber open source.

Bellingcat sebagai kolektif jaringan para praktisi OSINT independen juga menyediakan panduan menggunakan OSINT untuk melakukan investigasi secara online berikut *tools* yang dapat digunakan untuk mencari atau menganalisis informasi spesifik. Tugas dari badan intelijen adalah mengelaborasi dan memaksimalkan penggunaan *tools* tersebut agar dapat mengumpulkan dan menganalisis informasi dengan lebih efektif, murah, dan menghasilkan informasi intelijen yang akurat agar dapat mencegah aksi terorisme dengan menggagalkan rencana dan persiapan para kelompok teror.

CONCLUSION

OSINT adalah alat yang relatif baru dalam kontra- terorisme, selain membawa banyak peluang, juga membawa banyak tantangan. Kemunculan atau eksistensi teknologi jelas tidak secara langsung memiliki konsekuensi "positif" atau "negatif". Penilaian apakah teknologi bernilai positif atau negatif menjadi sangat subjektif karena *outcome* teknologi (baik atau buruk) tergantung dari persepsi terhadap teknologi dan untuk tujuan apa itu digunakan. Dalam konteks OSINT, OSINT sangat potensial untuk dibangun sebagai disiplin intelijen baru yang dapat menjawab tantangan intelijen modern. Namun, bukan berarti bahwa OSINT dapat sepenuhnya menggantikan peran intelijen tradisional karena tidak ada yang namanya panasea. OSINT tidak akan secara tiba-tiba dapat mendominasi, namun perlu ada rekognisi mengenai pentingnya memanfaatkan OSINT dengan menjadikannya sebagai bagian dari proses intelijen yang vital untuk menghasilkan produk intelijen yang dapat menjawab tantangan global.

OSINT bukanlah sumber informasi yang sempurna. Meskipun menawarkan banyak data, tantangan utama adalah waktu yang diperlukan untuk memilah informasi yang berguna dari yang tidak. Kualitas data OSINT tidak seragam, yang membuat pemilihan informasi menjadi krusial. Selain itu, karena mudah diakses, siapa pun bisa terlibat, dan jika tidak dianalisis oleh ahli, informasi bisa dangkal. Kelompok teroris pun memanfaatkan OSINT untuk menghindari deteksi.

Analis harus memastikan data yang dikumpulkan tepat waktu, akurat, relevan, dan dapat diverifikasi, namun verifikasi sering kali sulit dilakukan. Untuk mengatasi kekurangan ini, perlu ada pengembangan metodologi canggih dalam pengumpulan dan analisis data. Aparat juga harus hati-hati dalam mempublikasikan data agar tidak memberikan informasi yang dapat disalahgunakan oleh kelompok teroris. Kolaborasi dengan sektor privat dan akademisi sangat penting untuk menciptakan solusi yang efektif dan efisien.

REFERENCES

Akhgar, B. (2016). OSINT as an Integral Part of the National Security Apparatus. In B. Akhgar, P. Bayerl, F. Sampson (Eds.), *Open Source Intelligence: From Strategy to Implementation* (pp. 3-10). New York: Springer International Publishing.

Doi: 10.7454/jsht.v6i1.1105

Amble, J. C. (2014). Jihad Online: What Militant Groups Say About Themselves and What it Means for Counterterrorism Strategy. In C. Hobbs, M. Moran, D. Salisbury (Eds.), *Open Source Intelligence in the Twenty-First Century: New Approaches and Opportunities* (pp. 168-184). London: Palgrave Macmillan.

Bellingcat. (2020). *The Bellingcat Podcast Season 2 - The Executions*. Bellingcat.

Blackwell, S., Alexander, K. (n.d.). *Global Terrorism Trends Suggest Extremist Will Adapt and Evolve*. Trends Research and Advisory.

Gibson, S. D. (2014). Exploring the Role and Value of Open Source Intelligence. In C. Hobbs, M. Moran, D. Salisbury (Eds.), *Open Source Intelligence in the Twenty-First Century: New Approaches and Opportunities* (pp. 9-23). London: Palgrave Macmillan.

Hanifan, A. F. (2017, August 25). *Senjata Pindad Dipakai Kombatan ISIS Marawi.* Tirto.id.

Homeland Security Market Research. (2019). *How to Stop Lone Wolf Attacks: OSINT*. Homeland Security Market Research.

Institute for Economics and Peace. (2020). *Global Terrorism Index 2020: Measuring the Impact of Terrorism*. Sydney: Institute for Economics & Peace.

Klečková, A. (2021). *Open-Source Intelligence and Terrorism*. Prague: Prague Security Studies Institute.

Mapparessa (2021). *Presentasi Intelijen dan Interogasi dalam Terorisme*. Mapparessa Report.

Minas, H. (2010). *Can the Open-Source Intelligence Emerge as an Indispensable Discipline for the Intelligence Community in the 21st Century?* Athens: Research Institute for European and American Studies.

Omand, D., Miller, C., Bartlett, J. (2014). Towards the Discipline of Social Media Intelligence. In C. Hobbs, M. Moran, D. Salisbury (Eds.), *Open Source Intelligence in the Twenty-First Century* (pp. 24-43). London: Palgrave Macmillan.

Priyanto, S. (2021). *Ring of Security: How to Prevent Terrorist Attack*.

Secretary of State for the Home Department. (2018). *CONTEST: The United Kingdom's Strategy for Countering Terrorism*. United Kingdom Government.

Staniforth, A. (2016). Open Source Intelligence and the Protection of National Security. In B. Akhgar, P. Bayerl, F. Sampson (Eds.), *Open Source Intelligence: From Strategy to Implementation* (pp. 11-20). New York: Springer International Publishing.

Tow, J., Yeo, W. (2005). *The Role of Open Source Intelligence in The Global War on Terror*. S. Rajaratnam School of International Studies.

Zoll, A. (2017). *Open-Source Intelligence: When Terror Meets Technology*. Hillard Heintze, A Jensen Hughes Company.

Doi: 10.7454/jsht.v6i1.1105