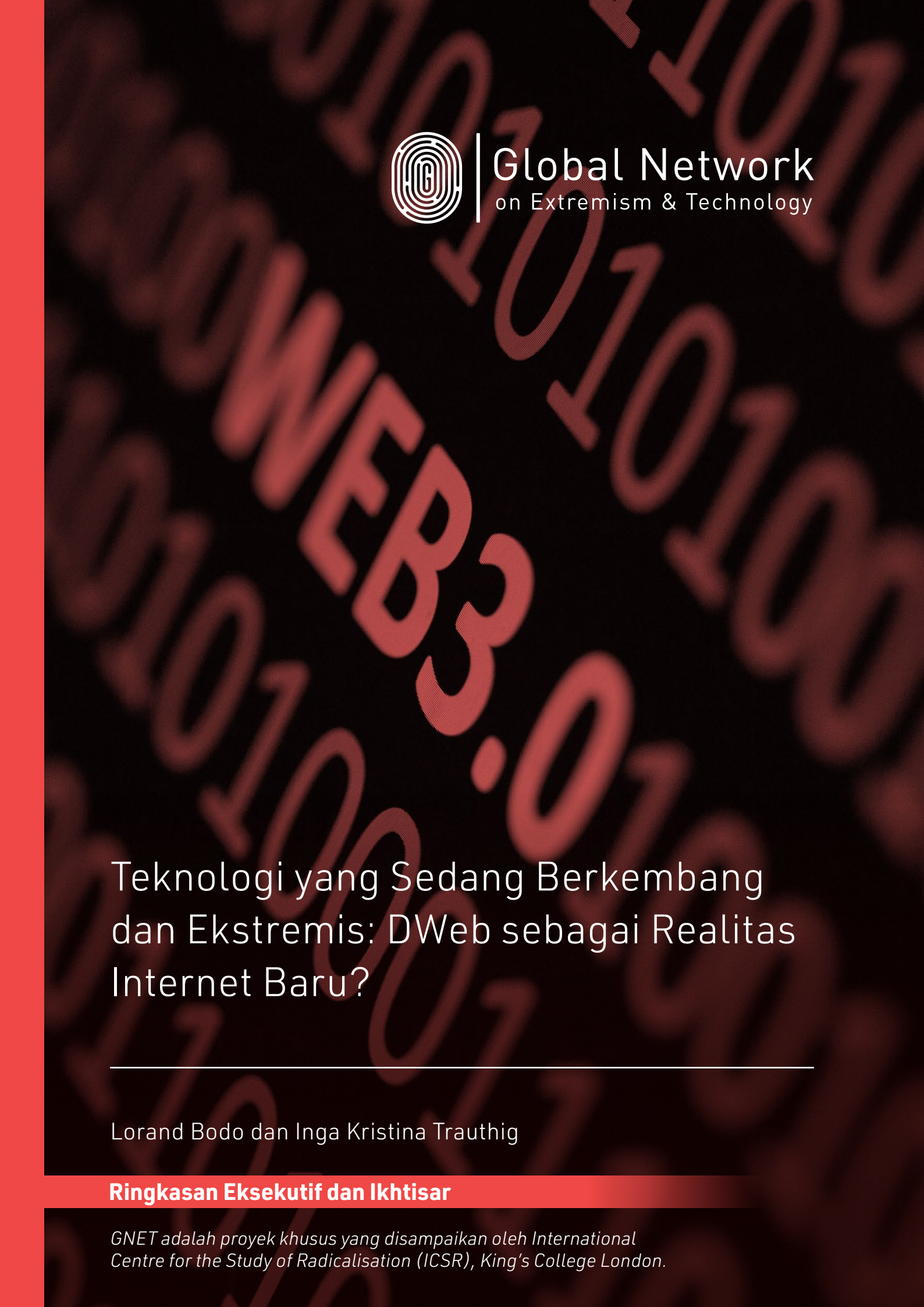

Teknologi yang Sedang Berkembang dan Ekstremis: DWeb sebagai Realitas Internet Baru?

Lorand Bodo dan Inga Kristina Trauthig

Ringkasan Eksekutif dan Ikhtisar

GNET adalah proyek khusus yang disampaikan oleh International Centre for the Study of Radicalisation (ICSR), King's College London.

Penulis laporan ini adalah Lorand Bodo dan Inga Kristina Trauthig

Global Network on Extremism and Technology (GNET) adalah inisiatif riset akademis yang didukung oleh Global Internet Forum to Counter Terrorism (GIFCT), yakni inisiatif independen, tetapi didanai industri, untuk memahami dengan lebih baik, serta melawan, penggunaan teknologi oleh teroris. GNET diadakan dan dipimpin oleh International Centre for the Study of Radicalisation (ICSR), sebuah pusat riset akademis yang berbasis di Department of War Studies (Departemen Penelitian Perang) di King's College London. Pandangan dan kesimpulan yang terdapat dalam dokumen ini adalah milik penulis dan tidak boleh ditafsirkan mewakili pandangan dan kesimpulan GIFCT, GNET, atau ICSR, baik tersurat maupun tersirat.

DETAIL KONTAK

Untuk mengajukan pertanyaan, permintaan informasi, dan salinan tambahan laporan ini, silakan hubungi:

ICSR
King's College London
Strand
London WC2R 2LS
Inggris Raya

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter: **@GNET_research**

Ringkasan Eksekutif dan Ikhtisar ini tersedia dalam bahasa Arab, Inggris, Prancis, Jerman, Indonesia, dan Jepang. Seperti semua publikasi GNET lainnya, ringkasan ini dan laporan penuh dalam bahasa Inggris dapat diunduh secara gratis dari situs web GNET di www.gnet-research.org.

Ringkasan Eksekutif

World Wide Web, sejak pengembangannya oleh Tim Berners-Lee pada tahun 1989, terus berkembang menjadi ekosistem tempat milyaran pengguna bergantung pada relatif sedikit korporasi besar. Lewat mesin pencarian, postingan di media sosial, komunikasi dengan orang lain, atau penyimpanan data di cloud, misalnya, perusahaan-perusahaan ini telah memberi manfaat positif bagi milyaran pengguna. Namun, dengan semakin berkembangnya basis pengguna seiring waktu, kuasa perusahaan-perusahaan ini pun semakin besar. Peralihan kuasa dari sedikit korporasi besar ini ke tangan pengguna sangat penting untuk terlaksananya Web Terdesentralisasi (DWeb). “Re-desentralisasi” ini juga akan memberi pengguna kontrol yang lebih besar atas data mereka. Pelaku ekstremis mencoba menciptakan dan menemukan cara baru untuk menyebarkan propaganda mereka dan menjadi lebih kebal terhadap penghapusan akun dan konten; karena alasan ini, DWeb masuk ke dalam radar mereka. Laporan ini memberikan gambaran singkat mengenai kondisi DWeb saat ini serta mengaitkannya dengan eksploitasi DWeb yang ada sekarang dan mungkin di masa depan oleh ekstremis. Kami berfokus pada ekstremis sayap kanan (RWE) dan kelompok yang disebut sebagai Negara Islam (IS) karena keduanya merupakan dua rantai ekstremis dengan potensi ancaman tertinggi di banyak belahan dunia. Kami menganalisis sampel berupa tiga puluh saluran Telegram yang sesuai dengan fitur kategori kami sebagai tertaut dengan spektrum RWE. Dataset kedua, yang disediakan oleh Kemitraan Pemerintah Swasta-berdukungan-PBB Tech Against Terrorism (TAT), mengupas secara kritis eksploitasi DWeb oleh Negara Islam.

Berdasarkan tinjauan literatur, wawancara yang dilakukan, dan analisis data, kami menilai:

- Karena ekstremis mempertimbangkan untuk mengeksploitasi teknologi apa pun, DWeb juga masuk ke dalam radar mereka. Salah satu alasan yang membuat DWeb menarik adalah konten yang dihosting “di DWeb” tidak dapat dihapus karena tidak dikontrol oleh otoritas pusat sehingga tidak mudah dihapus.

- Namun, analisis menunjukkan bahwa teknologi lain yang sudah ada masih tetap lebih disukai oleh para pelaku ini.

- Secara keseluruhan, DWeb memiliki risiko sedang untuk eksploitasi oleh entitas RWE dan IS.

- Selanjutnya, DWeb belum tentu diperlukan untuk memungkinkan entitas ekstremis menghosting, mendistribusikan, dan mengontrol konten mereka, sebab layanan yang diperlukan untuk mencapai tujuan ini sudah ada.

- Terakhir, layanan DWeb dapat memitigasi risiko eksploitasi; maka dari itu, DWeb belum tentu merupakan tempat berlindung yang aman bagi ekstremis.

Ikhtisar

Istilah yang bermunculan sehubungan dengan web terdesentralisasi (DWeb), seperti Web3 atau bitcoin, telah menjadi istilah generik untuk segala sesuatu yang berhubungan dengan blockchain dan mata uang kripto. Secara keseluruhan, berbagai pertanyaan besar yang muncul terkait web terdesentralisasi berkisar di seputar dua tema utama: (1) Apakah web terdesentralisasi cukup hidup dan menarik bagi cukup banyak orang? dan (2) Bagaimanakah sifat "internet baru" ini; dengan kata lain, apakah web terdesentralisasi akan bisa menghindari kelemahan web yang ada saat ini? Pertanyaan kedua sering kali diterapkan untuk radikalisasi online atau untuk kemungkinan penguatan otoritarian. Sebaliknya, dapatkah DWeb memupuk aspek positif, seperti potensinya bagi aktivis untuk dapat menyelenggarakan aktivitas dengan menggunakan teknologi ini agar terlindung dari sensor rezim yang ada.

Laporan ini memberi kontribusi dengan mempertanyakan bagaimana ekstremis mengeksploitasi DWeb dalam eksploitasi yang telah berlangsung dan bagaimana mereka dapat mengeksploitasinya di masa depan. Mengapa web terdesentralisasi itu "baik" atau "buruk"? Mengapa orang menggunakannya? Apakah sedikit persentase yang menyalahgunakannya telah membuat versi internet ini menjadi berbahaya? Apa yang harus dipertimbangkan pengembang jika melihat bukti yang sudah ada? Apa yang perlu diingat pembuat kebijakan saat menggodok legislasi di bidang teknologi? Berkenaan dengan DWeb, ada banyak dan beragam sudut potensial yang telah dieksplorasi periset dan wartawan, mulai dari pertanyaan yang melibatkan masalah ekonomi politis hingga ramifikasi normatif dasar etika di kalangan pengembang Web3 yang tidak dapat dipercaya oleh "Big Tech". Untuk laporan ini, fokus kami adalah implikasi bagi pelaku ekstremis dengan implikasi keamanan yang terkait bagi masyarakat secara keseluruhan.

Strategi bercabang tiga memandu pendekatan riset kami. Pertama, kami melakukan tinjauan literatur sistematis terhadap bahan yang ada mengenai DWeb, yang terutama berfokus pada moderasi konten serta ekstremisme. Kedua, kami mengumpulkan dan menyusun bukti bahwa entitas ekstremis sayap kanan dan Negara Islam bereksperimen dengan DWeb. Terakhir, kami melakukan wawancara semi terstruktur dengan pendukung, pengkritik, dan pengembang DWeb untuk memberitahukan pemahaman kami terkait topik yang sedang berkembang ini. Hal yang sangat mendasar dalam laporan ini adalah sifatnya yang mengeksplorasi, yang berkaitan langsung dengan fakta bahwa saat ini DWeb masih lebih berupa gagasan daripada kenyataan bagi banyak orang di seluruh dunia.

Risiko besar dalam konteks terorisme dan ekstremisme kekerasan online adalah bahwa teknologi DWeb dapat dieksploitasi untuk tujuan penyimpanan dan pengambilan data. Dalam hal itu, "[…] metode penyimpanan data yang terdesentralisasi dapat menyulitkan, jika bukan memustahilkan, satu entitas untuk menyensor konten".[1] Akibatnya, konten ekstremis tidak dapat dihapus dengan mudah dan akan dapat diakses siapa saja yang mengetahui tempat untuk mengaksesnya.

Tinjauan literatur kami menyimpulkan bahwa teknologi DWeb telah masuk ke dalam radar entitas ekstremis cukup lama, tetapi fitur yang membatasi serta terbatasnya jangkauan audiens yang terkait telah menahan eksploitasinya oleh kelompok tersebut. Meski demikian, hal yang semakin dikhawatirkan adalah bahwa pengembangan DWeb secara umum dapat beriringan dengan peningkatan eksploitasinya oleh pelaku ekstremis.

Empat temuan utama untuk data RWE kami adalah:

(1) Layanan DWeb tidak direpresentasikan secara signifikan.

(2) Mayoritas tautan yang beredar mengarahkan ke dua platform media sosial utama.

(3) Sampel ekstremis sayap kanan lebih banyak membagikan tautan ke berita dan blog yang tidak dapat diandalkan daripada sumber berita yang andal.

(4) Layanan Pengarsipan sama banyaknya digunakan dengan layanan DWeb.

Tiga temuan utama untuk data IS kami adalah:

(1) Layanan terdesentralisasi dieksploitasi, tetapi tidak sampai ke tingkat yang sama dengan layanan yang tersentralisasi.

(2) Layanan hosting dan berbagi file merupakan target utama.

(3) Ada lebih banyak konten teroris terverifikasi di layanan hosting dan berbagi, pengarsipan, serta penempelan file dibandingkan di media sosial.

1 Barabas, Chelsea, Neha Narula, dan Ethan Zuckerman. 'Defending Internet Freedom through Decentralization: Back to the Future?' The Center for Civic Media & The Digital Currency Initiative MIT Media Lab, Agustus 2017. https://static1.squarespace.com/static/59aae5e9a803bb10bedeb03e/t/59ae908a46c3c480db42326f/1504612494894/decentralized_web.pdf.

Global Network
on Extremism & Technology

DETAIL KONTAK

Untuk mengajukan pertanyaan, permintaan informasi, dan salinan tambahan laporan ini, silakan hubungi:

ICSR
King's College London
Strand
London WC2R 2LS
Inggris Raya

T. **+44 20 7848 2098**
E. **mail@gnet-research.org**

Twitter: **@GNET_research**

Seperti semua publikasi GNET lainnya, laporan ini dapat diunduh secara gratis dari situs web GNET di www.gnet-research.org.