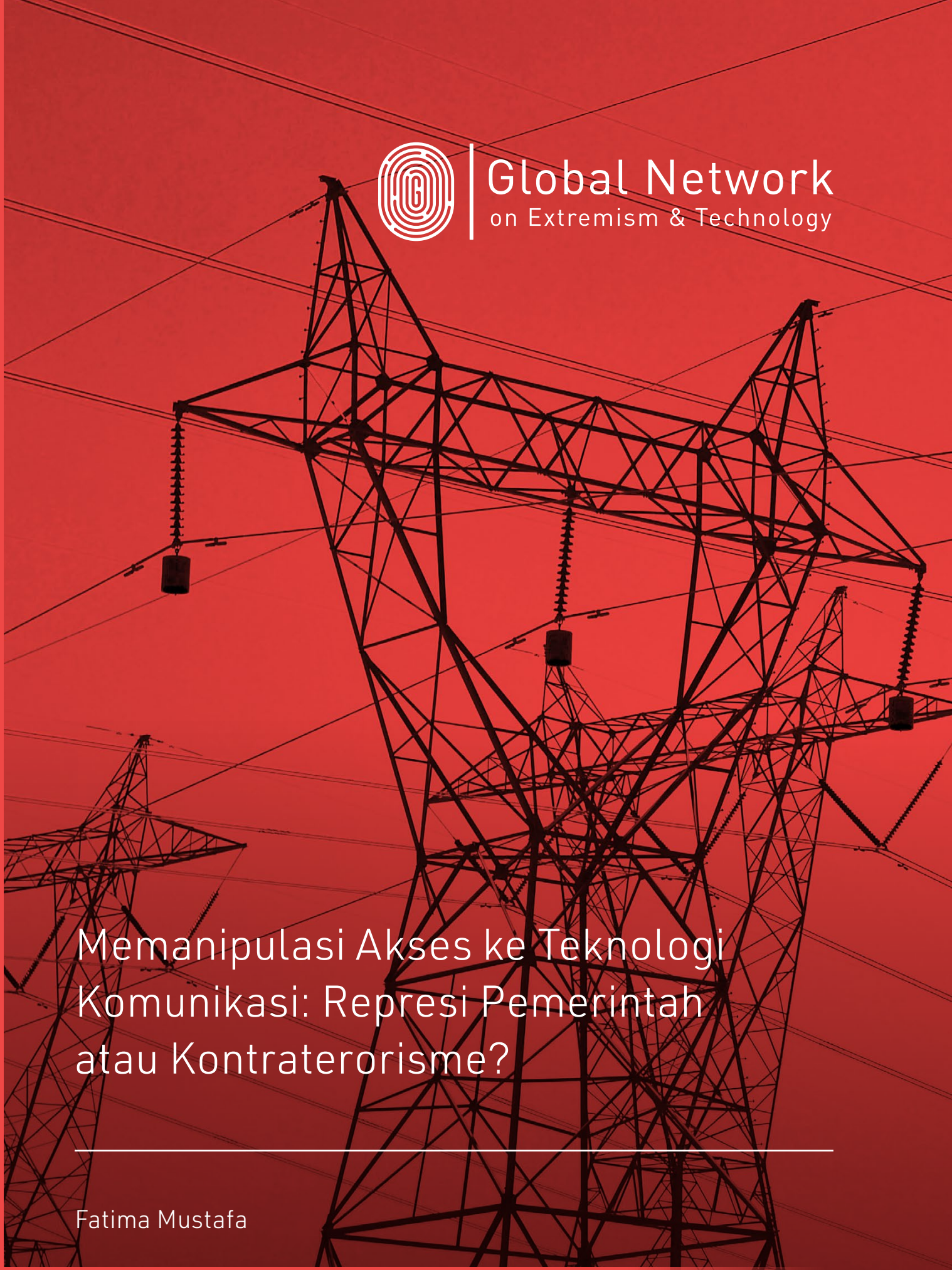

Global Network
on Extremism & Technology

Memanipulasi Akses ke Teknologi Komunikasi: Represi Pemerintah atau Kontraterorisme?

Fatima Mustafa

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
Fatima Mustafa

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

Pemerintah di seluruh dunia, baik demokrasi maupun autokrasi, semakin sering mengandalkan disrupsi Internet dan telepon seluler untuk membatasi kekerasan, menangani protes, menghalangi oposisi, dan mengendalikan penyebaran informasi. Menurut data yang dikumpulkan Access Now, jumlah disrupsi jaringan terus meningkat antara tahun 2016 (75 disrupsi) dan 2019 (213 disrupsi), dengan berbagai negara, seperti Venezuela, India, Mesir, Sudan, dan lain-lain, membatasi akses ke teknologi komunikasi.[1] Meski pemerintah umumnya bersiteguh bahwa disrupsi jaringan merupakan alat yang penting dalam rangkaian alat mereka untuk menangani kekerasan, kritik pembela hak asasi manusia berpendapat bahwa tindakan pukul rata membatasi akses ke teknologi komunikasi seperti ini melanggar hak asasi manusia, termasuk hak kebebasan berpendapat, serta sangat mengganggu akses ke layanan kesehatan, pendidikan, dan pekerjaan. Tambahan pula, pemutusan jaringan mahal jika dilihat dari segi ekonomi, dengan satu estimasi memperkirakan, pada tahun 2019 saja, kerugian ekonomi global mencapai 8 milyar dolar akibat pemutusan semacam ini.[2] Terlepas dari biaya besar yang dikaitkan dengan disrupsi jaringan, hanya ada sedikit studi empiris yang mengkaji keefektifan disrupsi jaringan dalam mencapai hasil yang diklaim pemerintah sebagai tujuan mereka menggunakannya. Meski tanpa bukti tersebut, pemerintah sering kali menggunakan klaim menangani kekerasan, keamanan nasional, atau misinformasi sebagai kedok untuk disrupsi jaringan.

Secara khusus, laporan ini fokus pada satu justifikasi yang banyak diberikan terkait disrupsi jaringan tingkat nasional – untuk menangani terorisme – dan mengevaluasi keefektifan disrupsi jaringan dalam konteks ini. Menggunakan data harian pemutusan Internet dan telepon seluler tingkat nasional, pencekikan Internet, dan pelarangan media sosial antara tahun 2016 dan 2019 di negara-negara di seluruh dunia (disediakan oleh Access Now dan koalisi #KeepItOn),[3] laporan ini menyediakan analisis awal hubungan antara berbagai bentuk disrupsi jaringan dan kekerasan teroris. Data mengenai kematian dan cedera harian akibat serangan teroris di negara-negara di seluruh dunia berasal dari Global Terrorism Dataset.[4] Menggunakan sumber data ini, analisis regresi efek tetap dalam laporan ini menunjukkan bahwa disrupsi jaringan (yakni, pemutusan dan pencekikan) tidak memiliki korelasi dengan jumlah orang yang tewas atau cedera dalam serangan teroris. Selain itu, dalam analisis yang terpisah, laporan menunjukkan bahwa pelarangan platform media sosial, seperti Facebook, Twitter, dan WhatsApp, juga tidak memiliki korelasi dengan kematian dan cedera akibat kekerasan teroris. Mengingat keterbatasan analisis ini, yakni karena fakta bahwa disrupsi jaringan tidak terjadi secara

1 Access Now dan koalisi #KeepItOn, "Shutdown Tracker Optimization Project (STOP)" https://www.accessnow.org/keepiton/ (diakses 8 November 2021).
2 Chloe Taylor (2020) "Government-led internet shutdowns cost the global economy $8 billion in 2019, research says" CNBC, 8 Januari 2020, https://www.cnbc.com/2020/01/08/government-led-internet-shutdowns-cost-8-billion-in-2019-study-says.html (diakses 6 November 2021).
3 Access Now dan koalisi #KeepItOn, "Shutdown Tracker Optimization Project (STOP)".
4 National Consortium for the Study of Terrorism and Responses to Terrorism, Global Terrorism Dataset, https://www.start.umd.edu/gtd/ (diakses 6 Agustus 2021).

acak, pembuatan klaim sebab-akibat untuk hubungan antara disrupsi jaringan dan kekerasan teroris sulit dilakukan. Meski demikian, analisis ini memberikan gambaran awal dampak disrupsi jaringan pada terorisme sehingga membuka jalan untuk penelitian lebih lanjut. Bagian akhir laporan ini melihat melampaui justifikasi resmi pemerintah terkait disrupsi jaringan guna mengeksplorasi secara singkat kemungkinan alasan lain pemerintah menggunakan disrupsi jaringan, misalnya untuk menutupi represi dan mencegah pelaporan. Selain itu, ada diskusi singkat mengenai cara lain pemerintah menggunakan teknologi dan media sosial untuk menangani terorisme, misalnya meminta agar platform media sosial menghapus konten online ekstremis atau menyediakan data pengguna untuk penyelidikan lebih lanjut.

Ikhtisar

Pemerintah menghadapi dilema seiring teknologi komunikasi, seperti Internet dan telepon seluler, menyebar cepat dan menjadi sentral dalam hidup kita, yang baru-baru ini ditunjukkan dengan ketergantungan kita pada teknologi ini selama pandemi koronavirus global. Jika pemerintah mengizinkan penggunaan teknologi komunikasi yang tidak terbatas, mereka berisiko harus menghadapi oposisi yang diorganisir melalui teknologi ini. Sebaliknya, jika pemerintah membatasi akses ke teknologi komunikasi, mereka mungkin harus menghadapi serangan balik. Fenomena ini, menurut Kedzie, adalah "dilema diktator".[5] Namun, pemerintah otoritarian bukan satu-satunya yang menghadapi dilema ini: Studi Agarwal, Howard, dan Hussain yang terkenal tentang pemadaman jaringan antara tahun 1995 dan 2011 menunjukkan bahwa 39% disrupsi jaringan ini terjadi di negara demokrasi.[6] Terkait "dilema diktator", mengapa beberapa pemerintah demokrasi dan non-demokrasi di dunia semakin sering membatasi akses ke jaringan komunikasi di waktu-waktu yang krusial?

Sementara pemerintah sering kali menyangkal penggunaan disrupsi jaringan dengan sengaja, di saat mereka mengakuinya, mereka menampilkan disrupsi jaringan sebagai alat untuk menangani kekerasan, membendung protes, menjamin keselamatan masyarakat, mencegah penyebaran misinformasi, dan mencegah kecurangan dalam ujian.[7] Data yang disediakan Access Now dan koalisi #KeepItOn tentang disrupsi jaringan di seluruh dunia antara tahun 2016 dan 2019 menunjukkan bahwa kontraterorisme merupakan justifikasi yang paling umum diberikan pemerintah untuk disrupsi jaringan tingkat nasional. Kadang-kadang, pemerintah mengeklaim bahwa disrupsi jaringan mencegah kelompok oposisi atau teroris saling berkoordinasi untuk merencanakan dan melaksanakan serangan, dan, secara umum, disrupsi tersebut membantu mengatasi masalah tindakan kolektif.[8] Kritik terhadap pemutusan jaringan berpendapat bahwa disrupsi semacam ini membahayakan hak asasi manusia, seperti hak kebebasan berpendapat, serta akses ke layanan kesehatan, pendidikan, dan pekerjaan. Tambahan pula, pemutusan jaringan mengganggu bisnis dan merugikan perekonomian. Sebagai contoh, India menghadapi biaya yang sangat besar tahun lalu, yakni 2,8 milyar dolar, karena pemutusan Internet.[9] Terlepas dari harga yang harus dibayar karena pemutusan jaringan, baik terkait pelanggaran hak asasi manusia maupun kerugian ekonomi, masih sedikit yang kita ketahui tentang keberhasilan disrupsi jaringan dalam hal yang diklaim pemerintah sebagai alasan mereka melakukannya.

5 Christopher Kedzie (1997) "Communication and Democracy: Coincident Revolutions and the Emergent Dictators", Santa Monica, CA: RAND Corporation, https://www.rand.org/pubs/rgs_dissertations/RGSD127.html (diakses 6 November 2021).

6 P. N. Howard, S. Agarwal & M. Hussain (2011) The Dictator's Digital Dilemma: When Do States Disconnect Their Digital Networks? *Issues in Technology Innovation* vol. 13: pp.1–11. Washington, D.C.: Center for Technology Innovation at Brookings.

7 Access Now dan koalisi #KeepItOn, "Shutdown Tracker Optimization Project (STOP)".

8 Fahad Desmukh (2012) "Ban on Cellphone Use in Pakistan," PRI, 31 Desember 2012, https://www.pri.org/stories/2012-12-31/ban-cell-phone-use-pakistan (diakses 13 September 2020).

9 Archana Chaudhary (2021) "World's Worst Internet Shutdowns Cost India $2.8 Billion in 2020", Bloomberg, 5 Januari 2021, https://www.bloomberg.com/news/articles/2021-01-05/world-s-worst-internet-shutdowns-cost-india-2-8-billion-in-2020 (diakses 6 November 2021).

Laporan ini menyediakan analisis awal keefektifan disrupsi jaringan dalam mencapai satu hasil spesifik: menangani kekerasan teroris. Laporan ini menganalisis hubungan antara disrupsi jaringan dan kematian serta cedera akibat serangan teroris guna menentukan ada tidaknya dukungan untuk argumen yang banyak dibuat bahwa disrupsi jaringan merupakan taktik kontraterorisme penting. Menggunakan set data panel insiden harian disrupsi jaringan tingkat nasional dan serangan teroris global antara tahun 2016 dan 2019, model regresi efek tetap menunjukkan bahwa disrupsi jaringan tingkat nasional tidak memiliki korelasi dengan jumlah orang yang tewas atau terluka dalam serangan teroris. Selain itu, tidak ada korelasi antara pelarangan platform media sosial – secara spesifik, Facebook, Twitter, dan WhatsApp – dan kematian serta cedera akibat kekerasan teroris. Analisis ini memiliki beberapa keterbatasan yang membuatnya sulit membuat klaim sebab-akibat, seperti penetapan perlakuan (yakni, disrupsi jaringan) yang nonacak dan tidak adanya variabel kontrol untuk menangkap peningkatan keamanan di seputar disrupsi jaringan. Secara umum, temuan ini menawarkan perspektif berbeda terhadap debat mengenai pemutusan jaringan, yang sering kali berpusat pada implikasi pemutusan bagi hak asasi manusia dan keterlibatan demokrasi, serta biasanya tidak menggali ke dalam bukti empiris terkait hal yang dapat atau tidak dapat dicapai dengan pemutusan jaringan.

Sedikit literatur akademis yang ada mengenai hubungan antara teknologi komunikasi dan organisasi serta pelaksanaan kekerasan memberikan temuan yang berbenturan. Sebagian ilmuwan berpendapat bahwa akses ke teknologi komunikasi seperti telepon seluler dan Internet memungkinkan anggota organisasi teroris untuk saling berkoordinasi dan merencanakan serangan,[10] sementara yang lain berpendapat bahwa teknologi komunikasi merupakan alat yang dapat dipakai warga sipil untuk melaporkan aktivitas teroris ke pemerintah dan, dengan demikian, menghalangi kekerasan.[11] Beberapa peneliti mengkaji bukti empiris terkait tingkat mobilisasi dan kekerasan selama pemutusan jaringan guna mendukung argumen bahwa disrupsi jaringan sebenarnya justru menyebabkan peningkatan kekerasan dan mobilisasi politik. Hassanpour menunjukkan bahwa inilah yang terjadi di Mesir,[12] sementara Rydzak menyajikan skenario yang hampir sama di India;[13] dalam dua kasus ini, pemutusan jaringan dikaitkan dengan peningkatan, dan bukan penurunan, mobilisasi politik. Dalam kasus Pakistan, Mustafa menunjukkan bahwa serangan teroris menurun saat pemerintah memberlakukan pemutusan jaringan, tetapi meningkat pada hari berikutnya.[14] Studi yang ada sekarang terkait keterkaitan antara jaringan komunikasi dan kekerasan didasarkan pada analisis yang spesifik untuk suatu negara. Laporan ini menganalisis dampak disrupsi jaringan terhadap kekerasan teroris di negara-negara di dunia dengan menggunakan set data panel lintas-negara sehingga memberikan temuan yang dapat digeneralisasi dan ditambahkan pada pengetahuan yang ada saat ini.

10 Jan H. Pierskalla dan Florian M. Hollenbach (2013) "Technology and Collective Action: The Effect of Cell Phone Coverage on Political Violence in Africa", *American Political Science Review* vol. 107, no. 2, pp: 207–24. https://doi.org/10.1017/S0003055413000075.

11 Jacob N. Shapiro dan Nils B. Weidmann (2015) "Is the Phone Mightier Than the Sword? Cellphones and Insurgent Violence in Iraq", *International Organization* vol. 69, no. 2, pp: 247–74. https://doi.org/10.1017/S0020818314000423.

12 Navid Hassanpour (2014) "Media Disruption and Revolutionary Unrest: Evidence from Mubarak's Quasi-Experiment", *Political Communication* vol. 31, no. 1, pp: 1–24. https://doi.org/10.1080/10584609.2012.737439.

13 Jan Rydzak (2019) "Of Blackouts and Bandhs: The Strategy and Structure of Disconnected Protest in India", https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3330413 (diakses 21 September 2021) .

14 Fatima Mustafa (2021) "Can Cellphone Shutdowns Stop Terrorist Violence? Evidence from Pakistan", *Terrorism and Political Violence*, https://doi.org/10.1080/09546553.2021.1908270.

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.