INTEGRITAS: Jurnal Antikorupsi, 7 (1), 179-196
e-ISSN/p-ISSN: 2615-7977/2477-118X
DOI: 10.32697/integritas.v7i1.732

Menciptakan Ruang Siber yang Kondusif bagi Pegiat Anti-Korupsi

Wijayanto, Nur Hidayat Sardini, Gita N. Elsitra
Universitas Diponegoro

wijayanto@live.undip.ac.id, nhsardini@gmail.com, gita.n.elsitra@gmail.com

Abstract

This research aims to reflect cyber-terror cases undergone by the anti-corruption activists in Indonesia, also to formulate the alternative solutions for cyber safety in digital era. Using qualitative approach, focus group discussion with 16 front-liner activists, and digital ethnography, the research found that cyber-terror weakened the anti-corruption movement. For protecting its movement, this research formulated three alternative solutions, such as 1) Strengthening civil society organizations; 2) Supporting comprehensive cyber regulations; and 3) Implementing campus mitigation. Those solutions would help to fulfill and guarantee anti-corruption activists' digital rights, especially freedom of expression and protection in cyber-space, which is crucial for digital democracy in Indonesia.

Keywords*: Cyber-Terror, Cyber Protection, Anti-Corruption Movement, Anti-Corruption Activist*

Abstrak

Penelitian ini bertujuan untuk merefleksikan teror siber yang dialami oleh pegiat anti-korupsi di Indonesia, sekaligus merumuskan solusi alternatif untuk menjamin keselamatan para aktivis di era digital. Dengan menggunakan pendekatan kualitatif, menyelenggarakan focus group discussion terhadap 16 pegiat anti korupsi, serta melakukan etnografi digital, penelitian ini menemukan bahwa memang aktivis rentan mengalami teror siber dalam menyampaikan pendapat dan aspirasi mereka, teror tersebut juga melemahkan gerakan para pegiat anti korupsi. Untuk memproteksi para pegiat dari bahaya teror siber sekaligus memperkuat pergerakan anti-korupsi di era digital, penelitian ini memformulasikan tiga solusi alternatif, yang meliputi: 1) Memperkuat organisasi masyarakat sipil; 2) Mendukung perumusan regulasi siber yang komprehensif; 3) Menerapkan mitigasi kampus. Solusi alternatif tersebut dapat menjadi landasan dalam memenuhi dan menjamin hak-hak digital para pegiat anti-korupsi, utamanya dalam menyampaikan aspirasi dan mendapatkan proteksi di dunia siber, menjadi krusial bagi demokrasi digital di Indonesia.

Kata Kunci: Teror Siber, Proteksi Siber, Gerakan Anti-Korupsi, Pegiat Anti-Korupsi

Pendahuluan

Keselamatan aktivis anti-korupsi dalam menyampaikan aspirasi mereka di ruang publik menjadi hal yang krusial dalam rangka menjamin terpenuhinya hak digital di Indonesia. Tetapi, nyatanya, dibalik optimisme dan potensi internet dalam mempermudah tersalurkannya aspirasi publik (Jurriëns & Tapsell, 2017; Lim, 2013), ruang maya ini justru menempatkan para aktivis sebagai kalangan yang rentan mendapatkan represi (Frantz, Kendall-Taylor, & Wright, 2020). Banyak konsep telah diajukan para peneliti dalam ruang diskusi untuk menjelaskan permasalahan digital yang tengah dialami oleh banyak negara demokrasi. Konsep tersebut meliputi banyak hal, sedikit di antaranya merupakan *digital authoritarianism* (Xu, 2020), represi digital (Frantz et al., 2020), dan bahkan secara spesifik dapat diamati melalui kasus-kasus di mana teror siber justru dilakukan oleh negara dalam rangka mengontrol opini publik (Frantz et al., 2020; Gross, Canetti, & Vashdi, 2017).

Artikel ini akan berfokus pada kasus yang terakhir: teror siber yang dialami oleh para pegiat anti-korupsi demi menekan opini yang bertentangan dengan revisi UU KPK pada tahun 2019. Lebih lanjut, penelitian ini juga bertujuan untuk menemukan alternatif solusi agar dapat mengamankan ruang siber bagi pegiat anti-korupsi dengan terlebih dahulu melihat gambaran besar yang didapatkan setelah melakukan investigasi terhadap kasus teror siber dalam gerakan anti korupsi yang dilakukan oleh aliansi akademisi lintas perguruan tinggi di Indonesia yang mengeluarkan petisi untuk menolak revisi UU Komisi Pemberantasan Korupsi (KPK) pada September 2019 sebagai bagian dari kooptasi ruang publik digital.

Kasus teror siber yang dialami para aktivis akademis selama proses penolakan revisi UU KPK pada tahun 2019 tersebut menjadi salah satu contoh yang mempertegas seberapa parahnya konsolidasi publik di Indonesia di tengah tren kemunduran demokrasi. Dalam kaitan ini, Warburton dan Power (2020) mendefinisikan kemunduran demokrasi sebagai proses yang berlangsung lambat yang ditandai dengan situasi di mana aktor politik perlahan-lahan berpaling dari nilai-nilai dan institusi demokrasi. Ini tidak selalu mengarah pada otoritarianisme. Akan tetapi, kemunduran demokrasi perlahan-lahan melahirkan jenis rezim politik lain yang tidak sepenuhnya demokratis tetapi juga tidak sepenuhnya diktator, seperti demokrasi illiberal, sistem otoriter kompetitif, rezim campuran, dan sebagainya. Sementara itu, Mietzner (2018) mendefinisikannya sebagai proses di mana demokrasi secara bertahap kehilangan kualitasnya dari waktu ke waktu, dan yang mungkin mengarah pada pembalikan demokrasi penuh.

Penting untuk dicatat di sini adalah bahwa hampir semua studi menyepakati salah satu indikator terpenting kemunduran demokrasi di Indonesia adalah semakin menyempitnya ruang publik dan semakin tergerusnya kebebasan sipil. Temuan para ilmuwan di atas semakin diperkuat oleh laporan Economist Intelligence Units (EIU) pada akhir 2019 dan temuan IDEA di tahun yang sama yang juga menyebut tergerusnya kebebasan sipil sebagai salah satu masalah demokrasi di Indonesia. Dalam konteks ini, peristiwa teror siber terhadap para aktivis akademisi anti korupsi dan kooptasi ruang publik digital yang mengiringi penolakan terhadap revisi UU KPK tahun 2019 menjadi sesuatu yang

penting untuk diteliti dan dikaji secara lebih mendalam.

Berdasarkan berbagai latar belakang di atas, maka dapat dirumuskan pertanyaan penelitian ini sebagai berikut: 1) Bagaimana teror siber terhadap para aktivis yang tergabung dalam aliansi akademisi nasional dalam penolakan revisi UU KPK terjadi? 2) Bagaimana menciptakan ruang siber yang kondusif bagi pegiat anti korupsi?

Penelitian ini dilakukan untuk mengetahui bagaimana kooptasi ruang publik dilakukan baik melalui terror siber terhadap nomor WhatsApp para aktivis anti korupsi yang berisi para akademisi di Indonesia dalam menolak revisi UU KPK. Dari pengetahuan ini maka dapat dirumuskan bagaimana alternatif solusi untuk mengamankan ruang siber bagi para aktivis anti korupsi terhadap terror siber dan advokasi isu anti korupsi agar terlepas dari kooptasi kekuatan predatoris yang kontra terhadap gerakan pemberantasan korupsi di Indonesia.

Tinjauan Pustaka

a. Aktivisme Digital

Teori-teori tentang peran aktivisme digital dalam politik dapat dikategorikan secara luas dalam empat argumen utama. Yang pertama berpendapat bahwa aktivisme digital bisa menjadi senjata yang kuat dari yang lemah atau bahkan orang-orang biasa untuk bertarung melawan partai-partai kuat dan benar-benar memenangkan pertempuran melawan mereka. Ini telah diperjelas dalam kasus gerakan anti korupsi di Indonesia untuk mendukung Komisi Pemberantasan Korupsi (KPK) agar tidak dilemahkan oleh polisi Indonesia. Lebih jauh, ini juga telah diperjelas dalam kasus Prita Mulya Sari, seorang wanita biasa yang anaknya menjadi korban praktik yang diduga dilakukan oleh rumah sakit swasta bernama Omni International. Dalam kedua kasus tersebut, internet telah menjadi sangat efektif sebagai alat bagi orang awam untuk mendapatkan dukungan dari masyarakat pada umumnya untuk melawan pemegang kekuasaan, baik itu pemegang kekuasaan politik yaitu polisi atau pemegang kekuasaan swasta yaitu rumah sakit swasta (Lim, 2013).

Yang kedua berpendapat bahwa aktivisme digital mungkin tidak berhasil membuat yang lemah menaklukkan pihak-pihak yang berkuasa, namun telah berhasil meningkatkan kesadaran warga tentang keberadaan penyalahgunaan kekuasaan oleh pemegang kekuasaan. Ini telah diperjelas dalam kasus aktivisme warga di media sosial untuk menginformasikan, mendiskusikan dan mengkritik masalah korupsi yang ada oleh para elit lokal di Banten (Fauzanafi, 2016). Kasus tersebut menunjukkan bahwa meskipun dinasti di Banten terlalu kuat untuk digulingkan dari kekuasaan, setidaknya para pejabat masih dapat mengungkapkan kesaksian, kekecewaan, dan permusuhan mereka terhadap praktik korupsi. Itu dilakukan melalui tindakan menyaksikan dan membakar yang penting sebagai bukti bahwa warga negara tidak menerima perilaku korup.

Teori ketiga dikemukakan oleh Tapsell (2017) yang mengemukakan bahwa internet dapat membuat baik orang biasa dan juga pemegang kekuasaan mendapatkan lebih banyak kekuatan. Internet memberi semakin banyak instrumen orang biasa untuk berpartisipasi dalam diskusi, membentuk konten media, dan melobi politisi agar suara mereka didengar dan membawa perubahan yang berarti. Namun, itu juga memungkinkan pemegang kekuasaan menjadi lebih kuat dengan modal yang sudah mereka miliki. Ini khususnya ditemukan dalam kasus oligarki politis-bisnis yang memiliki kekuatan politik dan ekonomi. Konglomerat media Indonesia

yang juga chaiperson atau elit di partai politik Indonesia adalah contoh sempurna dari ini. Bahkan sebelum internet tiba mereka sudah memiliki media arus utama di Indonesia mulai dari media cetak, radio dan televisi. Dengan kedatangan internet, mereka segera membuat bentuk internet atau membeli platform media yang ada untuk meningkatkan laba mereka serta pengaruhnya. Fakta bahwa memiliki media online membutuhkan sejumlah besar uang telah memungkinkan mereka mempertahankan kekuatan oligarki mereka.

Akhirnya, teori terakhir disarankan oleh Kurniawan dan Rye (Kurniawan & Rye, 2013) yang menyarankan bahwa alih-alih menjawab dampak internet terhadap "dunia luar", mereka menyarankan untuk melihat dampak internet terhadap struktur dan dinamika dalam masyarakat sipil, organisasi dan aktivisme mereka. Mereka berpendapat bahwa internet memang membawa dampak pada dinamika internal organisasi masyarakat sipil (CSO) ketika digunakan oleh organisasi mapan dengan jaringan internasional yang berkembang dengan baik untuk menjadi lebih profesional. Mereka memiliki dukungan keuangan untuk mengembangkan unit-unit internal terpisah yang ditunjuk untuk menangani alat komunikasi baru dan menyediakan infrastruktur yang stabil yang dapat diakses untuk komunikasi baik secara internal maupun eksternal. Sebaliknya, OMS yang kurang mapan dan lebih informal tidak dapat memanfaatkan internet secara maksimal untuk kemajuan pekerjaan mereka. Ini karena mereka juga masih berjuang untuk menemukan perangkat keras dan perangkat lunak yang paling bisa mereka gunakan.

Dari uraian di atas, berdasarkan Wijayanto, Hendra, & Esther (2020), dapat disimpulkan bahwa ada empat teori utama tentang aktivisme digital yaitu: (1). aktivisme digital oleh masyarakat sipil dapat menghasilkan perubahan politik dan mempengaruhi proses pembuatan kebijakan; (2). aktivisme digital oleh masyarakat sipil dapat menyebarkan kesadaran di kalangan masyarakat tentang adanya problem social politik tertentu; (3). aktivisme digital dapat memperkuat gerakan masyarakat sipil namun juga memperkuat oligarki pada saat yang sama; (4). medium digital dalam aktivisme berdampak positive sekurang-kurangnya dalam mendukung efektivitas koordinasi di internal gerakan masyarakat itu sendiri. Di sini, tampak terdapat semacam optimisme bahwa medium digital diposisikan sebagai satu ruang yang bebas yang dapat digunakan oleh siapa saja termasuk termasuk oleh masyarakat sipil dalam memperkuat aktivisme digital mereka. Pada bagian berikut akan dipaparkan satu studi terdahulu bahwa medium digital seringkali tidaklah sebebas yang dibayangkan karena ia ternyata dapat dikooptasi oleh kelompok anti demokrasi baik yang berasal dari negara ataupun di luar negara.

b. Teror Siber

Teror siber mulai dikenal sejak tahun 1995, saat para peneliti menggunakan '*electronic Pearl Habour'* sebagai peringatan pertama bagi Amerika Serikat (Lewis, 2003). Sejak saat itu, peneliti hingga pembuat kebijakan serta aparat militer menyoroti bagaimana teror dapat berevolusi bersama dengan berkembangnya teknologi. Puncaknya terjadi ketika peristiwa 9/11 menimpa World Trade Center pada 2001 dan sekelompok peretas yang disebut G-Force Pakistan mengakui kontribusi mereka dalam tragedi tersebut (Denning, 2011; Singh, 2011).

Banyak sekali akademikus yang mencoba meramu definisi dari teror siber, tetapi belum ada yang benar-benar

sepaham terkait pengertian dari istilah ini. Pollitt dalam artikelnya yang bertajuk "*Cyberterrorism — fact or fancy?*" meramu teror siber sebagai aktivitas terencana dengan motif politis untuk menyerang sistem teknologi dan informasi yang bertujuan untuk menyerang sekelompok target (Pollitt, 1998). Kemudian, Weimann dalam "*Cyberterrorism: The sum of all fears*?" menambahkan bahwa teror siber dapat terjadi karena adanya ketergantungan dari negara dan infrastruktur krusial terhadap teknologi digital (Weimann, 2005). Lalu, Eric Luiijf juga berkontribusi dalam mendefinisikan teror siber dengan mendetailkan dampak dari teror jenis baru ini, mulai dari kematian, dampak psikis, hingga kestabilan politik (Luiijf, 2014).

Pada awalnya, teror siber bisa dikatakan teror tradisional yang dilakukan untuk infrastruktur teknologi yang krusial dan mengancam fisik secara tidak langsung. Fokusnya, para akademikus memprediksi di akhir 1990-an, akan berkutat kepada dampak-dampak yang merugikan secara ekstrem, seperti memanipulasi manufaktur makanan dan obat-obatan, pusat kontrol lalu-lintas udara, bahkan mampu menghasilkan ledakan yang menyebabkan kematian (Beggs, 2007; Jones, 2005; Pollitt, 1998; ShockwaveWriter, 2000; Weimann, 2005).

Namun, seiring berjalannya waktu, beberapa akademikus mulai menyoroti bagaimana teror siber juga memberikan dampak secara psikologis kepada target mereka (Kaplan & Weimann, 2011; Lewis, 2003; Luiijf, 2012) dan bagaimana teroris justru menggunakan ruang siber sebagai tempat dan senjata untuk melakukan teror dan bukan lagi menjadi target utama mereka (Luiijf, 2014; Weimann, 2014). Terlebih, kebanyakan teroris di dunia siber, masih sama dengan pola tradisional yang mereka gunakan sebelumnya, menjadikan masyarakat sipil sebagai target. Hanya saja korban mereka bukanlah menjadi target, tetapi korban tersebut memiliki pengaruh kepada target yang sesungguhnya untuk menyebarkan ketakutan dan intimidasi (Hua & Bapna, 2012). Sehingga, perspektif terkait teror siber yang mengancam infrastruktur krusial terkait teknologi komunikasi secara ekstrim menjadi sedikit meluas.

Dari banyak literatur, teror siber dilakukan dengan motivasi yang meliputi: agenda politik dan/atau ideologi (Cavelty, 2007; Holt, 2012; Hua & Bapna, 2012; Luiijf, 2012, 2014; Pollitt, 1998; Veerasamy, 2020; Warren, 2007; Weimann, 2005); dan menyebar ketakutan juga mengintimidasi target (Beggs, 2007; Gross, Canetti, & Vashdi, 2016; Hua & Bapna, 2012; Kaplan & Weimann, 2011). Demikian juga diiyakan oleh Cavelty (2007) dengan menekankan dampak psikologis yang terjadi dari teror siber.

Seperti yang sudah disinggung pada paragraf sebelumnya, peranan media bagi para teroris siber ini sangatlah penting, terutama untuk menyebarkan ancaman kepada target (Debrix, 2001). Mereka menggunakan ICT (*Information and Communication Technology*) dalam berbagai tahapan dalam menjalankan rencana mereka (Pollitt, 1998) yang meliputi: publikasi manifesto dan propaganda, komunikasi, promosi aktifitas teror mereka (Cassim, 2012; Cohen, 2014; Lewis, 2003; Yunos & Hafidz, 2011). Dari sini lah, media sosial mengambil peranan dalam perkembangan terorisme siber.

Merambahnya teror siber ke ranah ruang publik digital ini bukan berarti tanpa dampak apapun, terutama dalam konteks kebebasan untuk berpendapat. Hal ini dapat terjadi ketika proteksi terhadap privasi dan kebebasan berpendapat memiliki celah yang dapat dimanfaatkan untuk peretasan dan

menjadi akses masuk para teroris siber (Krapp, 2005). Celah ini dapat diakses dengan lebih leluasa melalui keberadaan darknet yang sebenarnya pada awalnya bertujuan untuk memfasilitasi hak berpendapat masyarakat yang berada di bawah rezim pemerintahan yang represif. Ironisnya, kini darknet seolah menjadi jalan tikus yang digandrungi para teroris.

Jadi, penjabaran dari berbagai penelitian di atas menegaskan sekali lagi mengenai bagaimana teror siber terus berevolusi dan dampaknya semakin meluas hingga ke ranah kebebasan internet. Perluasan ini bukannya membuat teror di dunia maya menjadi semakin semu, melainkan mendekatkan para teroris dalam kehidupan sehari-hari tanpa kita sadari.

Argumen Penelitian

Berdasarkan wawancara mendalam maupun diskusi kelompok terarah dengan enam belas aktivis anti korupsi yang tergabung dalam gerakan akademisi nasional menolak revisi UU KPK, dan berdasarkan etnografi digital yang dilakukan oleh penulis pertama penelitian ini, juga dengan berdasarkan analisa atas ratusan ribu percakapan di media sosial dan ratusan artikel media daring, penelitian ini berargumen bahwa telah terjadi teror siber terhadap aktivis anti korupsi dan kooptasi secara terstruktur, sistematis dan massif terhadap ruang publik digital di Indonesia. Teror dan kooptasi ini telah secara signifikan melemahkan gerakan anti korupsi oleh masyarakat sipil di Indonesia, yang dalam hal ini adalah aliansi akademisi nasional yang menolak revisi UU KPK dan semakin memperburuk situasi demokrasi di Indonesia secara umum yang sesungguhnya telah mengalami trend kemunduran selama lima tahun terakhir. Berdasarkan temuan itu pula penelitian ini menemukan tiga rekomendasi upaya yang dapat dilakukan untuk mengamankan ruang siber bagi para aktivis agar hak-hak digital mereka dapat terpenuhi dan terjamin, utamanya dalam menyampaikan aspirasi dan memperoleh proteksi di dunia maya. Upaya tersebut terangkum dalam rekomendasi yang meliputi: memperkuat konsolidasi publik; mendukung perumusan regulasi siber yang komprehensif; serta penerapan mitigasi kampus.

Metode Penelitian

Untuk menjawab pertanyaan penelitian di atas, penelitian ini menggunakan metodologi campuran yang belum pernah digunakan di Indonesia. Proyek ini akan menguji dan mengembangkan integrasi teknik komputasi dan kerja lapangan kualitatif ini. Lebih khusus lagi, proyek ini akan mengadopsi strategi metode campuran interdisiplin, yang terdiri dari empat metode berikut ini:

a. Wawancara Mendalam

Metode pertama yang digunakan dalam penelitian ini adalah wawancara mendalam terhadap para akademisi yang ada dalam aliansi akademisi anti korupsi yang menolak revisi UU KPK. Wawancara ini dilakukan mengungkap bagaimana teror dilakukan kepada mereka dan bagaimana dampaknya bagi efektivitas komunikasi mereka dengan sesama aktivis yang tinggal di berbagai kota yang berjauhan di seluruh wilayah Indonesia, termasuk juga bagi motivasi dan semangat juang mereka untuk terus melanjutkan perjuangan anti korupsi. Dalam penelitian ini wawancara mendalam dilakukan secara terpisah maupun secara bersama-sama melalui suatu diskusi kelompok terarah (*focus group discussion*) terhadap 16 orang aktivis anti korupsi dari Agustus hingga September 2020.

b. Etnografi Digital

Penelitian ini juga menggunakan metode etnografi digital. Dengan metode antropologi ini, peneliti menyelidiki dan menafsirkan komunikasi online di media sosial secara kualitatif melalui lensa pembuatan makna dan kontestasi budaya.

Dalam penelitian ini, etnografi digital dimungkinkan karena peneliti utama dalam penelitian ini (Wijayanto) adalah juga anggota gerakan akademisi yang menolak revisi UU KPK yang juga tergabung dalam WhatsApp group aliansi akademisi nasional sekaligus juga mendapatkan terror telepon dari berbagai nomor tak dikenal di seluruh dunia. Etnografi digital ini dilakukan selama bulan September 2019 saat penulis utama terlibat dalam gerakan ini namun pemaknaan dan analisa tentangnya terus berlangsung hingga penulisan laporan ini.

Pembahasan

Teror siber yang dialami oleh para aktivis akademisi dalam gerakan menolak revisi UU KPK mencerminkan adanya represi digital yang menegaskan kondisi kemunduran demokrasi yang tengah dialami Indonesia. Di sisi lain, sebagai kalangan kritis, aktivis akademis yang rentan terhadap represi tersebut harus menjadi prioritas dalam pemenuhan hak-hak digital demi terselenggaranya demokrasi yang substantif di era revolusi digital. Sebagai entitas kelompok yang juga bagian dari peradaban digital, keselamatan aktivis dalam menyampaikan aspirasi mereka merupakan hak yang wajib dipenuhi negara.

Bagian pembahasan ini, melalui analisis etnografi digital, akan mengelaborasi teror siber yang dialami oleh para aktivis akademisi dalam gerakan menolak revisi UU KPK pada tahun 2019. Kemudian, berdasarkan hasil wawancara mendalam yang dianalisis untuk meramu solusi alternatif, penelitian ini merekomendasikan tiga solusi alternatif sebagai respons atas urgensi dalam menjamin keselamatan para aktivis anti-korupsi di era demokrasi.

A. Rentannya Pegiat Anti-Korupsi di Dunia Siber: Kemunduran Demokrasi dalam Ranah Digital

Aktivis rentan terhadap represi. Realita itu sudah sangat dikenal dalam ruang lingkup pergerakan sosial. Secara *offline* maupun *online*, represi terhadap para pegiat acap kali menjadi fokus diskusi di ruang publik. Tentunya, tren kemunduran demokrasi yang tidak kunjung membaik justru memperparah represi terhadap para aktivis. Bagian ini akan berfokus dalam mengelaborasi kerentanan para aktivis dalam aktivisme digital, khususnya pada kasus penolakan revisi UU KPK di tahun 2019 ketika teror siber terjadi untuk memecah konsolidasi publik di ruang maya.

Tren kemunduran demokrasi yang terjadi di Indonesia sejak kurang dari satu dekade terakhir (Aspinall, Fossati, Muhtadi, & Warburton, 2020; Mietzner, 2018, 2020; Wijayanto, 2020) ternyata tidak hanya berdampak pada meningkatnya represi secara *offline*. Di dunia maya pun represi terus terjadi. Sebagai pembanding, di negara otoriter, pemanfaatan teknologi untuk stabilitas politik dilakukan dengan: 1) sensor dan represi terhadap kebebasan berpendapat (King, Pan, & Roberts, 2013), 2) pengumpulan preferensi dari masyarakat publik (Gunitsky, 2015), 3) *monitoring* berjalannya politik di ranah lokal (Qin, Strömberg, & Wu, 2017), 5) perbaikan persepsi masyarakat dengan bertindak seolah-olah demokrasi (Frantz et al., 2020), 6) melakukan kooptasi melalui manipulasi informasi dan opini publik (Frantz et al., 2020), dan 7) identifikasi demonstran dan musuh-musuh politik (Gunitsky, 2015). Pertanyaannya sekarang

adalah: apakah Indonesia sudah menerapkan ketujuh perilaku otoriter tersebut dalam praktik politik digital mereka? Setidaknya, penelitian ini menegaskan bahwa poin ketujuh sudah terbukti dalam kasus penolakan revisi UU KPK pada tahun 2019 silam. Tidak hanya mengidentifikasi lawan politik, seluruh narasumber dalam penelitian ini sepakat bahwa represi yang mereka alami pada kasus tersebut merupakan sebuah teror siber karena serangan tersebut menyebabkan perasaan takut dan paranoid.

Penelitian ini menemukan bahwa teror siber yang dialami oleh aktivis ternyata berbeda-beda, walaupun pada akhirnya tetap menimbulkan perasaan takut dan paranoid. Tidak hanya itu, salah satu dari narasumber mengalami peretasan WhatsApp yang kemudian digunakan untuk menyebarkan ajakan melakukan jihad, sebagaimana kutipan berikut:

Dia langsung kasih *capture* (pesan WhatsApp yang disebarkan saat diretas), isinya itu bukan sekedar mendukung KPK atau menolak. Tapi itu isinya ajakan, dia pakai bahasa spesifik teroris deh sebenarnya. Dia ajakan jihad untuk membunuh Kapolri waktu itu[1].

Semua aktivis akademisi yang terlibat dalam penolakan revisi UU KPK tersebut mendapatkan teror berupa rentetan telepon dari nomer luar negeri, peretasan akun media sosial, bahkan *doxing*. Bahkan salah satu narasumber mengaku sudah akun *Google*-nya sudah dicoba untuk diretas, ditandai dengan notifikasi pencobaan masuk ke dalam e-mail yang tidak seharusnya ada. Seperti yang dikatakan narasumber dalam pernyataan berikut:

Jadi *google account* itu HP ya, HP itu dicoba diambil alih itu akan ada notifikasi. Dan untuk upaya pengambil alihan akun google saya itu berlangsung dari bulan September, Oktober, November, Desember, Januari, terakhir kalau tidak salah Februari tahun 2020 itu masih berlangsung[2].

Serangan siber yang paling luas dan berpengaruh secara psikologis terhadap gerakan aktivis anti-korupsi selama proses penolakan revisi UU KPK dapat diamati melalui peretasan WhatsApp Group aktivis. Berdasarkan hasil temuan etnografi digital, Gambar 1 memperlihatkan tampilan layar grup WhatsApp (WAG) di saat teror telepon terjadi. Teror dalam bentuk ini biasanya diikuti dengan peretasan WhatsApp dan dilakukan menggunakan Pegasus Spyware buatan perusahaan swasta asal Israel: NSO Group. Siapa yang membeli dan menggunakan piranti tersebut, mengingat motif peretasan ditujukan pada kelompok aktivis, maka memiliki hubungan dengan pihak yang dirugikan oleh aspirasi penolakan revisi UU KPK.

***Gambar 1**. Screen capture ruang WAG ketika teror siber terjadi dalam ruang koordinasi aliansi akademisi penolakan revisi UU KPK*

Serangan ini tidak hanya mengancam keselamatan siber para pegiat, namun juga memiliki dampak psikologis tertentu.

[1] Wawancara Narasumber 4 pada 27 Agustus 2020 melalui Zoom.

[2] Wawancara Narasumber 3 pada 27 Agustus 2020 melalui Zoom.

Takut menjadi hal yang dirasakan oleh sebagian besar aktivis yang mengalami teror siber. Ketakutan ini bersumber dari keresahan mereka mengenai peretasan piranti digital (*smartphone/mobile phone)* dan akun-akun media sosial. Mengenai piranti digital, para aktivis merasa khawatir atas keamanan data pribadi mereka. Hal ini termaksud di antaranya akun transaksi perbankan dan pengambil alihan piranti dari jarak jauh. Hal tersebut senada dengan pernyataan salah satu narasumber:

> *Kita takut ya karena kita sudah diingatkan jangan diangkat karena kalau diangkat gadget bisa diambil alih, bisa di-remote dari satu arah, ngeri juga itu*[3]*.*

Selain itu, ketakutan yang dirasakan aktivis juga bersumber peretasan akun-akun sosial media. Hal ini dapat terjadi karena mereka semakin meragukan apakah teman sesama aktivis yang ada dalam satu grup benar-benar rekan mereka atau oknum peretas. Ketakutan ini kemudian menganggu komunikasi karena menyebabkan aktivis menjadi paranoid ketika berhubungan dengan aktor simpul gerakan penolakan revisi UU KPK. Hal tersebut dinyatakan sebagai berikut:

Nah yang agak paranoid adalah ketika salah satu koordinator gerakan tiba-tiba WhatsApp *blasting*-nya agak beda gitu. Dari situ ketahuan nge-*hack*, akhirnya kita juga pindah-pindah. Saling paranoid, tuh[4].

Rasa takut ini dalam studi teror siber merupakan hal yang pasti diharapkan oleh para teroris siber. Lebih luas lebih baik, baik korban teror maupun targetnya. Dampak psikologis ini selanjutnya menjadi stimulus untuk mempengaruhi pengambilan kebijakan Luiijf (2014), dalam hal ini menekan gerakan penolakan terhadap revisi UU KPK agar regulasi tersebut dapat disahkan. Hal ini menunjukkan bahwa demokrasi di Indonesia tidak hanya dalam tahapan kemunduran yang sepele. Represi yang dilakukan dalam rentang waktu yang panjang terhadap para aktivis nyatanya juga dilakukan oleh negara-negara otoriter, seperti Rusia dan juga China (Xu, 2020).

Tidak berhenti di titik ini, teror yang terjadi pada aksi penolakan revisi UU KPK tersebut tidak hanya memberikan rasa takut dan paranoid, tetapi juga menyebabkan beberapa dampak lain. Salah satunya menyangkut konsolidasi masyarakat sipil yang terhambat. Gambar 2 di samping mengilustrasikan bagaimana para pegiat anti-korupsi langsung keluar dari grup saat dan setelah teror siber terjadi. Dampak yang paling nampak terlihat adalah kacau-nya koordinasi para aktivis pasca teror siber berlangsung. Awalnya, media sosial memang memberikan harapan untuk men-stimulus partisipasi publik (Jurriëns & Tapsell, 2017; Lim, 2013). Oleh karena itu, para aktivis akademisi pun menggunakan WhatsApp sebagai sarana untuk berkumpul juga melakukan koordinasi dalam tingkat nasional. Tetapi, teror berupa telepon WhatsApp yang terjadi secara beruntun membuat para aktivis pun satu per satu keluar dari grup WhatsApp tersebut. Para aktivis kunci pun berinisiatif mengganti platform sosial media, tetapi konsolidasi para aktivis tidak sekuat sebelumnya.

[3] Wawancara Narasumber 16 pada 2 September 2020 melalui Zoom.

[4] Wawancara Narasumber 11 pada 1 September 2020 melalui Zoom.

***Gambar 2**. Screen capture ketika WAG aliansi akademisi nasional mulai mengalami kepanikan karena adanya teror siber*

Kacau-nya koordinasi tersebut semakin diperparah dengan perasaan paranoid yang dialami oleh aktivis simpatisan yang notabene-nya berjumlah lebih banyak daripada aktivis kunci yang berada di garis depan gerakan penolakan revisi UU KPK. Lebih lagi, represi digital yang dilakukan melalui teror siber semakin akut ketika ditambah dengan adanya ko-optasi sosial media dan manipulasi opini publik. Strategi melumpuhkan konsolidasi publik tersebut nyata-nya sukses memutar balikkan opini publik dari yang awalnya menolak revisi UU KPK menjadi mendukung perubahan regulasi tersebut. Temuan ini mempertegas kembali literasi terkait praktik-praktik otoriter yang dilakukan negara demokrasi demi kestabilan kekuasaan yang tengah terjadi di regional Asia Tenggara dan Indonesia, utamanya di dunia maya demi mengontrol oposisi (Sinpeng, 2020; Bünte, 2021).

Teror siber yang terjadi pada kasus penolakan revisi UU KPK bukan lah terakhir, tetapi pola yang serupa (walaupun tidak sama persis) juga terjadi pada pengesahan Omnibus Law. Dengan kata lain, konsolidasi masyarakat sipil menjadi kunci yang selalu dilemahkan oleh kelompok oligarki demi pemenuhan kepentingan politik mereka.

Sehingga, berdasarkan hasil wawancara dan etnografi digital tersebut, penelitian ini pun memformulasikan beberapa solusi alternatif untuk memastikan proteksi atas gerakan aktivis anti-korupsi di era digital.

B. Tiga Solusi Alternatif Untuk Menciptakan Ruang Siber yang Kondusif Bagi Pegiat Anti-Korupsi

1. Konsolidasi Publik yang Menjadi Urgensi: Mempererat Jejaring dan Memperluas Advokasi Masyarakat Sipil

Jika pelemahan konsolidasi publik menjadi salah satu strategi oligarki untuk melanggengkan kekuasaannya, maka tentunya penguatan masyarakat sipil menjadi salah satu solusi yang krusial bagi Indonesia. Tentunya hal tersebut bukan hal yang mudah, tetapi setidaknya penelitian ini memformulasikan dua pendekatan yang dapat digunakan untuk memperkuat konsolidasi masyarakat sipil.

Pertama, memperkuat jejaring organisasi masyarakat sipil. Upaya memperkuat network atau jejaring ini merupakan salah satu hal yang dapat dilakukan oleh gerakan kerakyatan dengan memperkuat antisipasi terhadap teror-teror yang serupa. Misalnya, mengajak ahli IT sebagai partner. Hal ini sebagaimana yang dialami oleh sebagian aktivis akademisi yang merasa resah karena ditelepon oleh orang yang tidak dikenal dengan nomer dari luar negeri. Mereka tidak tahu harus melakukan apa ketika pertama kali menjadi korban teror siber, sehingga perasaan panik dan takut menjadi hal yang tidak dapat dihindari. Belum lagi mengingat ketidaktahuan sebagian besar pegiat terkait hal pertama yang harus mereka lakukan ketika mengalami serangan siber dalam bentuk apa pun.

Selain itu, penguatan jejaring juga dibutuhkan untuk memperkuat dukungan moril kepada para pegiat anti-korupsi. Sehingga dengan banyaknya dukungan dari pihak lain maka akan semakin berhati-hari dalam langkah gerakan.

Kedua, memperluas advokasi masyarakat sipil. Dengan kata lain, menginisiasi dan memperbanyak organisasi masyarakat sipil yang memberikan advokasi serta perlindungan pada kejahatan di internet seperti SafeNet. Hal ini menjadi krusial karena dapat memberikan pertolongan pertama ketika masyarakat sipil mengalami hal serupa teror siber yang dialami oleh para aktivis itu. Organisasi semacam ini menjadi penting karena tampaknya pemerintah dan negara sejauh ini belum menunjukkan iktikad baik dan kerja nyata dalam melindungi para aktivis anti korupsi dari kejahatan di internet sehingga, seperti tampak dalam temuan penelitian ini, hampir semua aktivis menolak lapor kepada apparat yang berwenang dan justru khawatir masalah akan menjadi semakin runyam jika mereka melapor.

Namun, upaya untuk memperluas advokasi dan jejaring dalam rangka proteksi bagi masyarakat sipil oleh organisasi masyarakat sipil tersebut akan mengalami batasan di negara yang melakukan represi terhadap organisasi yang kontra-pemerintah (Fransen, Dupuy, Hinfelaar, Mazumder, & Sharp, 2020). Salah satu batasan tersebut berupa terbatasnya donor dan dukungan pemerintah, terlebih jika organisasi tersebut memiliki agenda atau bersifat politik (Toepler, Zimmer, Fröhlich, & Obuch, 2020). Bahkan SafeNet yang notabene-nya merupakan salah satu LSM yang memperjuangkan keselamatan siber pun, sampai tulisan ini disusun, belum memiliki donor lembaga untuk menyokong kegiatan mereka.

Upaya memperkuat konsolidasi publik ini patut menjadi prioritas karena memang belum ada kebijakan perlindungan terhadap keselamatan digital yang komprehensif di Indonesia. Terutama di aspek perlindungan data pribadi dan privasi. Ketidakadaan perundangan inilah yang memberikan celah untuk serangan atau bahkan teror siber, baik dengan motif politik maupun tidak.

2. Regulasi Siber Yang Komprehensif: Sebuah Urgensi di Era Digital

Kemudian, untuk melengkapi alternatif solusi sebelumnya, diperlukan pengesahan undang-undang yang menjamin keamanan berselancar di internet, seperti undang-undang perlindungan data pribadi, undang-undang peretasan, dan undang-undang siber yang lebih komprehensif dalam melindungi hak-hak digital masyarakat. Regulasi yang dimaksud sebagai komprehensif ini meliputi kebijakan yang mampu mencegah serangan siber dan memproteksi masyarakat secara inklusif, tentunya dengan monitor dan evaluasi yang dilakukan secara rutin dan menyeluruh. Setidaknya, ada tujuh tema krusial yang harus termaksud dalam regulasi siber, meliputi: keamanan data, tata kelola penyedia network dan internet, penggunaan piranti oleh perusahaan, keamanan fisik (infrastruktur digital), penanganan dan pelaporan kasus-kasus pelanggaran atau serangan siber, monitoring dan evaluasi, serta isu-isu administratif (Lubua & Pretorius, 2019).

Hal tersebut sudah seperlunya menjadi sorotan para pembuat kebijakan, terutama terkait dengan proteksi data pribadi (*personal data protection*). Tidak hanya bahaya terkait teror siber, tetapi regulasi tersebut juga penting untuk melindungi masyarakat dari ancaman digital lain. Teror siber yang diarahkan

kepada para aktivis seharusnya menjadi stimulus untuk disahkannya perundangan terkait proteksi data pribadi, mengingat draf regulasi tersebut sesungguhnya sudah diajukan pada awal 2020.

Terkait dengan perundangan data pribadi, sebenarnya hal tersebut adalah sebuah kewajiban negara dalam menjamin hak-hak digital warga negaranya. Padahal, melalui riwayat data pribadi mereka, oknum yang tidak bertanggungjawab dapat mengambil keuntungan dari kecenderungan pilihan dan perilaku digital pengguna terkait (Wachter & Mittelstadt, 2019).

Terkait penyalahgunaan data pribadi, dalam aspek politik, *online political micro-targeting* merupakan salah satu kegiatan yang menyimpan risiko tersendiri. Apalagi, berdasarkan riset, perusahaan penyedia jasa voting politik berhasil meraup secara ilegal data pribadi dari 50 juta pengguna internet tanpa ijin melalui online political micro-targeting (Dobber, Fathaigh, & Zuiderveen Borgesius, 2019). Penyalahgunaan data pribadi oleh oligarki melalui online political micro-targeting juga dilakukan demi mengintai dan mengontrol opini publik, utamanya dilakukan di negara yang otoriter (Frantz et al., 2020). Teror siber yang ditargetkan kepada para aktivis, merupakan salah satu contoh di mana data pribadi diretas dan pengintaian sosial media para aktivis kunci dilakukan oleh 'oknum yang memiliki kapabilitas dan kapital' untuk melakukan teror.

Namun, di sisi lain, pengawasan digital juga menjadi dilema tersendiri bagi kedaulatan digital. Pasalnya, di negara yang cenderung represif, pengawasan digital justru digunakan untuk mengintai lawan politik dan mencederai hak-hak digital yang seharusnya dilindungi (Wilson, 2020), suatu pelanggaran hak digital yang terjadi dalam kasus penolakan revisi UU KPK pada 2019. Dengan menyusun regulasi siber yang tidak komprehensif, maka akan dimungkinkan muncul celah-celah yang justru dimanfaatkan oligarki demi kepentingan mereka. UU ITE tentunya menjadi cerminan untuk hal tersebut, di mana regulasi yang mengatur penggunaan teknologi digital tersebut justru digunakan pejabat publik dan politisi untuk melemahkan masyarakat kritis dengan dalih penghinaan, provokasi dan penyebaran kebencian (Safenet, 2020).

Terkait dengan teror siber, regulasi yang memproteksi hak-hak digital ini menjadi krusial. Terutama ketika para oknum teroris, terlepas keberpihakan nya dengan kelompok oligarki, secara aktif menggunakan teknologi digital dalam kegiatannya (Cassim, 2012; Cohen, 2014; Lewis, 2003; Pollitt, 1998; Yunos & Hafidz, 2011). Bahkan tidak hanya kelompok teroris, kalangan peretas pun justru memiliki aturan norma informal yang jauh lebih efektif daripada regulasi yang disusun oleh pemerintah (Wilson, 2020). Ditambah lagi dengan realita bahwa regulasi tidak mampu menjangkau sisi gelap dunia siber (*deep web*, *dark web* dan *darknet*), membuat sisi itu luput dari proteksi yang seharusnya dijamin oleh negara.

Meskipun begitu, regulasi yang mengatur dan melindungi hak-hak digital masyarakat sipil untuk merasa aman dalam aktivitas mereka di dunia siber perlu diperjuangkan. Terutama keselamatan para aktivis anti-korupsi yang menjadi salah satu kalangan yang rentan memperoleh represi digital. Selain regulasi siber yang komprehensif, perlu juga adanya mitigasi kampus yang pro-aktivis muda milenial.

3. Memproteksi Aktivis Milenial: Mitigasi Kampus yang Pro-Aktivis di Era Digital

Mitigasi kampus yang pro-aktivis di era digital ini dimaksudkan untuk

menjawab pertanyaan bagaimana jika terjadi ketidakberesan kampus terutama pada isu perubahan undang-undang KPK. Kondisi tersebut pun tidak muncul secara tiba-tiba. Sistem keamanan data yang diterapkan oleh sebagian besar perguruan tinggi ternyata masih dirasa mudah untuk diretas. Selain cenderung lemahnya keamanan digital di tataran perguruan tinggi, sikap kampus dalam menanggapi isu-isu politik pun juga masih terkesan tidak menyatu.

Lebih dalam misalnya, bagaimana akademisi yang menjadi aktivis tolak revisi undang-undang KPK terlindungi? Bagaimana jika terjadi konflik antara akademisi? Bagaimana jika terjadi teror siber dan peringatan dari pejabat kampus? dan pertanyaan lain yang kemungkinan menyelimuti dunia aktivis akademisi. Pertanyaan semacam ini perlu diberi rambu dengan mitigasi kampus.

Di sisi lain, kampus menjadi ladang kaderisasi aktivis-aktivis muda anti-korupsi, sehingga sebenarnya memiliki peran krusial dalam regenerasi pergerakan anti-korupsi di masa depan yang tentunya tidak terlepas dari teknologi digital. Sehingga kurikulum anti-korupsi yang diajarkan di dalam kampus tidak hanya seputar masalah legal-formal, tetapi juga meliputi proteksi dan keselamatan siber untuk aktivis (Cho, 2020).

Selain itu, sebagai sarana pendidikan, perguruan tinggi juga dapat menjadi wadah untuk melakukan edukasi politik yang berdasarkan pada integritas dan moralitas. Terlebih, integritas moral masyarakat berhubungan erat ketika politik. Teror siber ini mau tidak mau mencerminkan adanya salah satu kelompok masyarakat yang menyabotase kebebasan berpendapat dan keamanan data para aktivis untuk kepentingan politis. Sehingga, lagi-lagi mengingat dalangnya kemungkinan besar adalah elit bangsa, etika politik menjadi satu hal yang patut nya dipertanyakan. Karena itu, upaya memperkuat integritas moral masyarakat juga seharusnya menjadi perhatian.

Terutamanya, terkait edukasi mengenai hak politik digital. Masyarakat sipil, dan termaksud di antaranya para pegiat anti-korupsi, masih asing dengan hak politik mereka di tengah demokrasi digital. Seperti misalnya, hak untuk proteksi data dan privasi, hak untuk berpendapat (secara digital), dan sebagainya.

Penutup

Studi penelitian ini telah secara jernih menunjukkan bahwa telah terjadi kooptasi ruang publik digital di Indonesia yang telah secara signifikan melemahkan gerakan anti korupsi oleh masyarakat sipil di Indonesia, yang dalam hal ini adalah aliansi akademisi nasional yang menolak revisi UU KPK itu dan semakin memperburuk situasi demokrasi di Indonesia secara umum yang sesungguhnya telah mengalami tren kemunduran selama lima tahun terakhir.

Wawancara mendalam dan diskusi kelompok terarah dengan para akademisi anti korupsi yang tergabung dalam aliansi akademisi nasional penolak revisi UU KPK juga etnografi digital penulis telah menunjukkan dengan jelas bahwa telah terjadi teror siber terhadap para akademisi yang dilakukan secara sengaja oleh kekuatan predatoris yang menentang aspirasi kelompok kritis tersebut terkait dengan revisi UU KPK. Teror ini telah secara nyata berdampak baik secara psikologis terhadap masing-masing aktivis sebagai individu maupun gerakan anti korupsi yang mereka perjuangkan sebagai kolektifitas karena teror ini telah menganggu koordinasi, memutus komunikasi dan menghambat eskalasi gerakan yang saat itu tengah terus

membesar seiring dengan banyaknya akademisi yang terus bergabung dan mengeluarkan petisi penolakan revisi RUU KPK.

Dalam konteks literatur tentang aktivisme digital di Indonesia, situasi ini membantah temuan para sarjana yang optimis pada efektivitas ruang publik digital untuk memperkuat aktivisme masyarakat sipil (Jurriëns & Tapsell, 2017; Lim, 2013). Namun di sisi lain, temuan ini memperkuat potret buram situasi demokrasi di Indoensia yang terus mengalami kemunduran seiring dengan semakin menyempitnya kebebasan sipil dan semakin terbatasnya ruang gerak para aktivis pro demokrasi, utamanya melalui aktivitas mereka di dunia maya (Sinpeng, 2020; Bünte, 2021). Tragsinya, saat masrakat sipil semakin mengalami pelemahan, kekuatan oligarki justru semakin mengalami penguatan dan berhasil mendesakkan agenda predatorisnya yang dalam hal ini: merevisi UU KPK.

Gambaran situasi ruang siber yang tidak aman bagi para aktivis anti-korupsi tersebut pada akhirnya menjadi landasan untuk merumuskan beberapa solusi alternatif yang dapat digunakan sebagai upaya mengamankan ruang siber. *Pertama,* memperkuat konsolidasi masyarakat sipil. Upaya memperkuat network atau jejaring ini merupakan upaya yang dapat dilakukan oleh gerakan kerakyatan yang dapat memperkuat antisipasi terhadap teror-teror yang serupa. Selain sistem jejaring, upaya kedua menyangkut upaya menginisiasi dan memperbanyak organisasi masyarakat sipil yang memberikan advokasi dan memberikan perlindungan pada kejahatan di internet.

Kedua, merumuskan regulasi siber yang komprehensif dan inklusif. Dengan kata lain, negara seharusnya mampu menjamin keselamatan siber warganya di era digital, bukannya malah membiarkan teror siber terjadi pada kalangan aktivis kritis. Bukan hanya memproteksi pegiat anti-korupsi dalam aktivitas maya mereka mengaspirasikan nilai-nilai anti-rasuah, tetapi regulasi ini juga diperlukan demi melindungi masyarakat dari ancaman digital lain.

Ketiga, menerapkan mitigasi kampus. Alternatif solusi ini diperlukan untuk menjamin proteksi atas aktivis akademisi dalam melakukan konsolidasi publik sebagai respons mereka terhadap kebijakan pemerintah. Tidak hanya itu, kampus yang menjadi ladang kaderisasi aktivis muda juga dituntut untuk mampu memberikan lingkungan yang kondusif bagi regenerasi aktivis di era digital.

Ketiga solusi alternatif tersebut diharapkan mampu membantu mewujudkan ruang siber yang kondusif bagi pegiat anti-korupsi di era digital. Terutama, mengingat represi digital terhadap kelompok aktivis semakin nampak dalam ruang maya. Sehingga, optimisme yang muncul pada awal berkembangnya teknologi digital terkait dampak positif untuk menstimulus partisipasi dan mempercepat konsolidasi publik dapat menjadi realita di tengah pertarungan narasi politik di peradaban digital.

Referensi

Aspinall, E., Fossati, D., Muhtadi, B., & Warburton, E. (2020). Elites, masses, and democratic decline in Indonesia. *Democratization 27*(4): 505–526. *https://doi.org/10.1080/13510347.2019.1680971*

Aspinall, E., & Mietzner, M. (2019). Southeast Asia's Troubling Elections: Nondemocratic Pluralism in Indonesia. *Journal of*

Democracy 30(4): 104–118. *https://doi.org/10.1353/jod.2019.0055*

Beggs, C. (2007). Cyber-Terrorism in Australia. In M. Quigley (Ed.), *Encyclopedia of information ethics and security*. IGI Global.

Bünte, M . (2021). Democratic Backsliding and authoritarian resilience in southeast asia: the role of social media. Dalam Sinpeng, A., & Tapsell, R. (Eds.). *From Grassroots Activism to Disinformation : Social Media in Southeast Asia*. Singapore 119614: ISEAS Publishing.

Cassim, F. (2012). *Addressing The Spectre of Cyber Terrorism: A Comparative Perspective 15*(2).

Cavelty, M. D. (2007). Looming Threat or Phantom Menace ? The Framing of the US Cyber-Threat Debate. *Journal of Information Technology 4*(1): 19–37. *https://doi.org/10.1300/J516v04n01*

Cho, K. S. (2020). *Responding to Campus Racism: Analyzing Student Activism and Institutional Responses*. University of California.

Cohen, D. (2014). Cyber terrorism: Case studies. In *Cyber Crime and Cyber Terrorism Investigator's Handbook*. Elsevier Inc. *https://doi.org/10.1016/B978-0-12-800743-3.00013-X*

Debrix, F. (2001). Cyberterror and Media-Induced Fears: The Production of Emergency Culture. *Strategies: Journal of Theory, Culture & Politics 14*(1): 149–168. h*ttps://doi.org/10.1080/10402130120042415*

Denning, D. E. (2011). 10 Years after September 11 Whither Cyber Terror ? *A Social Science Research Council Essay Forum* 11–13.

Dobber, T., Fathaigh, R., & Zuiderveen Borgesius, F. J. (2019). The regulation of online political micro-targeting in Europe. *Internet Policy Review 8*(4): 1–20. *https://doi.org/10.14763/2019.4.1440*

Fauzanafi, M. Z. (2016). Searching for digital citizenship: Fighting corruption in Banten, Indonesia. *Austrian Journal of South-East Asian Studies 9*(2): 289–294. *https://doi.org/10.14764/10.ASEAS-2016.2-7*

Fransen, L., Dupuy, K., Hinfelaar, M., Mazumder, S. M. Z., & Sharp, W. (2020). *Adjust, Resist or Disband? The effect of political repression on civil society organizations in Bangladesh and Zambia*. Leiden.

Frantz, E., Kendall-Taylor, A., & Wright, J. (2020). *Digital Repression in Autocracies* (March): 1–54. *www.v-dem.net.*

Gross, M. L., Canetti, D., & Vashdi, D. R. (2016). The psychological effects of cyber terrorism. *Bulletin of the Atomic Scientists 72*(5): 284–291. *https://doi.org/10.1080/00963402.2016.1216502*

Gross, M. L., Canetti, D., & Vashdi, D. R. (2017). Cyberterrorism: Its effects on psychological well-being, public confidence and political attitudes. *Journal of Cybersecurity 3*(1): 49–58.

https://doi.org/10.1093/cybsec/tyw018

Gunitsky, S. (2015). Corrupting the cyber-commons: Social media as a tool of autocratic stability. *Perspectives on Politics 13*(1): 42–54. *https://doi.org/10.1017/S1537592714003120*

Holt, T. J. (2012). Exploring the intersections of technology, crime, and terror. *Terrorism and Political Violence 24*(2): 337–354. *https://doi.org/10.1080/09546553.2011.648350*

Hua, J., & Bapna, S. (2012). How Can We Deter Cyber Terrorism? *Information Security Journal 21*(2): 102–114. *https://doi.org/10.1080/19393555.2011.647250*

Jones, A. (2005). Cyber terrorism: Fact or fiction. *Computer Fraud and Security 2005*(6): 4–7. *https://doi.org/10.1016/S1361-3723(05)70220-7*

Jurriëns, E., & Tapsell, R. (2017). Challenges and opportunities of the digital 'revolution' in Indonesia. *Digital Indonesia: Connectivity and Divergence* 2020: 275–288. *https://doi.org/10.1355/9789814786003-007*

Kaplan, A., & Weimann, G. (2011). Freedom and terror: Reason and unreason in politics. In *Freedom and Terror: Reason and Unreason in Politics*. *https://doi.org/10.4324/9780203831205*

King, G., Pan, J., & Roberts, M. E. (2013). How censorship in China allows government criticism but silences collective expression. *American Political Science Review* 107(2): 326–343. *https://doi.org/10.1017/S0003055413000014*

Krapp, P. (2005). Terror and play, or what was hacktivism? *Grey Room* (21): 71–93. *https://doi.org/10.1162/1526381057745397770*

Kurniawan, N. I., & Rye, S. A. (2013). Online environmental activism and Internet use in the Indonesian environmental movement. *Information Development*. *https://doi.org/10.1177/0266666913485260*

Lewis, J. (2003). Cyber terror: Missing in action. *Knowledge, Technology, & Policy* 16(2): 145–153. *https://doi.org/10.4324/9781315130712-9*

Lim, M. (2013). Many Clicks but Little Sticks: Social Media Activism in Indonesia. *Journal of Contemporary Asia* 43(4): 636–657. *https://doi.org/10.1080/00472336.2013.769386*

Lubua, E. W., & Pretorius, P. D. (2019). Cyber-security policy framework and procedural compliance in public organisations. *Proceedings of the International Conference on Industrial Engineering and Operations Management* July: 1847–1856.

Luiijf, E. (2012). Understanding cyber threats and vulnerabilities. *Lecture Notes in Computer Science (Including Subseries Lecture Notes*

in Artificial Intelligence and Lecture Notes in Bioinformatics) 7130: 52–67. *https://doi.org/10.1007/978-3-642-28920-0_4*

Luiijf, E. (2014). Definitions of Cyber Terrorism. *In Cyber Crime and Cyber Terrorism Investigator's Handbook*. Elsevier Inc. *https://doi.org/10.1016/B978-0-12-800743-3.00002-5*

Mietzner, M. (2018). Fighting Illiberalism with Illiberalism: Islamist Populism and Democratic Deconsolidation in Indonesia. *Pacific Affairs 91*(June): 261–282. *https://doi.org/10.1080/00324728.2012.754486*

Mietzner, M. (2020). Populist Anti-Scientism, Religious Polarisation, and Institutionalised Corruption: How Indonesia's Democratic Decline Shaped Its COVID-19 Response. *Journal of Current Southeast Asian Affairs 39*(2): 227–249. *https://doi.org/10.1177/1868103420935561*

Pollitt, M. M. (1998). Cyberterrorism — fact or fancy? *Computer Fraud & Security 1998*(2): 8–10. *https://doi.org/10.1016/s1361-3723(00)87009-8*

Power, T., & Warburton, E. (2020). The decline of Indonesian democracy. In T. Power & E. Warburton (Eds.), *Democracy in Indonesia: From Stagnation to Regression?* (pp. 1–20). Singapore: ISEAS – Yusof Ishak Institute. *https://doi.org/10.1355/9789814881524-006*

Qin, B., Strömberg, D., & Wu, Y. (2017). Why does China allow freer social media? Protests versus surveillance and propaganda. *Journal of Economic Perspectives* 31(1): 117–140. *https://doi.org/10.1257/jep.31.1.117*

Safenet. (2020). *Bangkitnya Otoritarian Digital*. Denpasar.

ShockwaveWriter. (2000). Is it Cyber-Terrorism, Techno-Terrorism, or None of the Above? *Computer Fraud & Security 2000*(7): 18–20. *https://doi.org/10.1016/s1361-3723(00)89015-6*

Singh, B. (2011). Why Successful Counter-Terrorism Can Beget More Terrorism? Indonesia Since The 2002 Bali Bombings. In E. Noor (Ed.), *Proceeding of Southeast Asia Regional Center for Counter Terrorism's (SEARCCT) Selection of Articles* 2(2). *https://doi.org/10.1017/S002246341400006X*

Sinpeng, A. (2020). Digital media, political authoritarianism, and Internet controls in Southeast Asia. *Media, Culture & Society 42*(1): 25–39. *https://doi.org/10.1177/0163443719884052*

Toepler, S., Zimmer, A., Fröhlich, C., & Obuch, K. (2020). The Changing Space for NGOs: Civil Society in Authoritarian and Hybrid Regimes. *Voluntas 31*(4): 649–662. *https://doi.org/10.1007/s11266-020-00240-7*

Veerasamy, N. (2020). Cyberterrorism – the spectre that is the convergence of the physical and virtual worlds. *In Emerging Cyber Threats and*

Cognitive Vulnerabilities. Elsevier Inc. *https://doi.org/10.1016/b978-0-12-816203-3.00002-2*

Wachter, S., & Mittelstadt, B. (2019). A right to reasonable inferences: Re-thinking data protection law in the age of Big Data and AI. *Columbia Business Law Review 2*(2): 443–493. *https://doi.org/10.31228/osf.io/mu2kf*

Warren, M. J. (2007). Hackers and Cyber Terrorists. In M. Quigley (Ed.), *Encyclopedia of information ethics and security*. IGI Global. Singapore.

Weimann, G. (2005). Cyberterrorism: The sum of all fears? *Studies in Conflict and Terrorism 28*(2): 129–149. *https://doi.org/10.1080/10576100590905110*

Weimann, G. (2014). New Terrorism and New Media. *Communicating Unreality*, *2*. *http://www.wilsoncenter.org/staff/gabriel-weimann.*

Wilson, M. P. (2020). *The Politics of Privacy Protection: an Analysis of Resistance to Metadata Retention and Encryption Access Laws*. Queensland University of Technology.

Wijayanto. (2020). Democratic Regression and Authoritarian Practices in Indonesia. *Indonesian Journal of Political Research 1*(December).

Wijayanto, W., Ardianto, H., & Astuti, E. S. (2020). Campaigning Online and Offline: The use of YouTube Movie in the Movement Against Environmental Destruction in the Movie "Samin vs Semen." *ICIPSE 2019*. *https://doi.org/10.4108/eai.21-10-2019.2294459*

Xu, X. (2020). To Repress or to Co-opt? Authoritarian Control in the Age of Digital Surveillance. *American Journal of Political Science*. *https://doi.org/10.1111/ajps.12514*

Yunos, Z., & Hafidz, S. (2011). Cyber Terrorism And Terrorist Use of ICT and Cyberspace. In E. Noor (Ed.), *The Problem with Cyber Terrorism*. Southeast Asia Regional Centre for Counter-Terrorism (SEARCCT). Kuala Lumpur.