



INNOVATIVE: Journal Of Social Science Research

Volume 3 Nomor 5 Tahun 2023 Page 749-757

E-ISSN 2807-4238 and P-ISSN 2807-4246

Website: <https://j-innovative.org/index.php/Innovative>

Terorisme Siber Dilingkungan Generasi Millennial Saat Pandemi

Dutasena Mahardhika^{1✉}, Grace Cheryanti², Kelvin Salim³, Marleen Natania⁴

Program Studi Hukum, Falkuntas Hukum, Universitas Tarumanegara

Email: grace.205230078@stu.untar.ac.id^{1✉}

Abstrak

Di era digital saat ini, terorisme siber menjadi ancaman yang semakin nyata. Generasi milenial merupakan pengguna aktif teknologi dan media sosial sehingga menjadikan mereka sasaran empuk berbagai bentuk terorisme siber. Kekhawatiran terhadap terorisme siber semakin meningkat di kalangan generasi milenial karena mereka menghabiskan lebih banyak waktu online selama pandemi COVID-19. Studi ini membahas dampak cyber terrorism terhadap generasi milenial selama pandemi dan kemungkinan langkah mitigasinya. Kami menganalisis berbagai taktik dan strategi yang digunakan oleh kelompok teroris siber untuk mempengaruhi dan merekrut generasi milenial. Dalam konteks ini, kami juga membahas peran media sosial, penyebaran misinformasi, dan terorisme online. Temuan ini menunjukkan pentingnya pendidikan digital dan kesadaran digital sebagai kunci pertahanan generasi milenial serta bagaimana generasi milenial dapat berperan aktif dalam mengidentifikasi, melaporkan, dan merespons ancaman terorisme siber. Dengan pemahaman yang lebih mendalam mengenai risiko dan tindakan pencegahan ini, generasi Milenial dapat berkontribusi dalam perang melawan terorisme siber selama dan setelah pandemi. Pemerintah juga mencegah Terorisme siber meluas dengan cara membentuk Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) Namun terorisme siber semakin menyebar luas dan mengintai generasi milenial, mempengaruhi pandangan dunia dan keterlibatan politik mereka. Artikel ini membahas dampak dampak terorisme siber pada generasi milenial dalam konteks pandemi global. Generasi ini terpapar risiko radikalisasi online, penyebaran propaganda ekstremis, dan serangan siber yang mengancam dan merusak privasi dan keamanan mereka.

Kata Kunci: *Terorisme Siber; Generasi Millennial; Covid-19*

Abstract

In this digital era, cyber terrorism is becoming an increasingly real threat. The millennial generation is an active user of technology and social media, making them easy targets for various forms of cyber terrorism. Concerns about cyber terrorism are increasing among millennials as they spend more time online during the COVID-19 pandemic. This study discusses the impact of cyber terrorism on the millennial generation during the pandemic and possible mitigation steps. We analyze various tactics and strategies used by cyber terrorist groups to influence and recruit the Millennial generation. In this context, we also discuss the role of social media, the spread of misinformation and online terrorism. These findings show the importance of digital education and digital awareness as keys to the millennial generation's defense and how the Millennial generation can play an active role in identifying, reporting and responding to cyber terrorism threats. With a deeper understanding of these risks and precautions, Millennials can contribute to the fight against cyberterrorism during and after the pandemic. The government also prevents cyber terrorism from spreading by enacting Law Number 11 of 2008 concerning Information and Electronic Transactions (ITE). However, cyber terrorism is increasingly spreading and stalking the millennial generation, affecting their worldview and political involvement. This article discusses the impact of cyber terrorism on the millennial generation in the context of a global pandemic. This generation is exposed to the risks of online radicalization, the spread of extremist propaganda, and cyberattacks that threaten and undermine their privacy and security.

Keyword: *Cyber Terrorism, Millennial Generation, Covid-19*

PENDAHULUAN

Perkembangan teknologi menciptakan banyak perubahan pada kehidupan manusia ditambah lagi dengan Pandemi yang kemarin terjadi. Perubahan yang cukup signifikan terjadi pada kehidupan manusia dikarenakan adanya paksaan terhadap batasan mobilitas dan kontak fisik dengan sesama pada masa pandemi kemarin, memunculkan banyak sekali hal-hal yang berbau online, contohnya online shopping, E-learning, WFH (Work From Home) dan masih banyak lagi. Segala sesuatu pastinya memiliki dampak baik dan buruknya sama dengan perkembangan teknologi sekarang ini. Salah satu contoh yang menjadi dampak buruk yaitu pada bidang terorisme

Terorisme merupakan masalah yang sudah lama ada di dunia, terorisme ini sendiri telah terlibat dalam politik internasional sejak abad ke-19. Pada awalnya, terorisme masih kecil dan terlokalisasi di wilayah tertentu. Terorisme pada awalnya bersifat kecil dan lokal dengan sasaran terpilih tetapi terorisme semakin berkembang dan menjadi semakin merugikan negara, karena mereka sudah melakukan tindakan-tindakan merusak dan menghancurkan kehidupan manusia dalam bernegara. Terorisme bahkan sudah menjadi

masalah yang bersifat internasional dan membutuhkan tanggapan secara internasional.

Terorisme siber atau cyber terrorism, merupakan suatu bentuk terorisme baru, yang muncul akibat perkembangan teknologi yang semakin pesat. Terorisme siber membuat pergerakan terorisme dapat terjadi secara global, dan ini bisa berbahaya karena bisa membuat terorisme semakin kuat dan semakin sulit untuk dibubarkan. Berdasarkan uraian di atas penulis ingin melakukan penelitian terhadap terorisme siber karena memiliki dampak yang cukup tinggi dan dapat mengganggu keseimbangan kehidupan manusia dalam bermasyarakat. Penelitian ini juga bertujuan agar Masyarakat bisa lebih menyadari tentang bahaya terorisme siber pada generasi millennial dan bagaimana cara penanggulangannya. Bagaimana bahaya terorisme bagi kalangan remaja dimasa pandemi dengan perkembangan teknologi sekarang?.

METODE PENELITIAN

Metode penelitian yang digunakan dalam artikel ini adalah metode penelitian yuridis normatif, termasuk penelitian hukum terhadap kepustakaan atau data sekunder. Pendekatan yang digunakan adalah pendekatan perundang-undangan atau "statutory pendekatan" guna memperoleh bahan hukum dan tulisan yang berkaitan dengan pelanggaran Pancasila sila pertama dan ke-dua, yang mana dianalisis seluruh ketentuan hukum yang relevant dengan permasalahan hukum yang dibicarakan. Hal ini dilakukan berdasarkan judul dan isu yang akan disebutkan dalam artikel agar dapat membuahkan hasil yang bermanfaat.

HASIL DAN PEMBAHASAN

Kata teror sendiri berasal dari kata latin *terrere* yang berarti menimbulkan gemetar atau gemetar. Pelaku terorisme sering disebut teroris. Terorisme merupakan permasalahan yang sangat serius di Indonesia karena aksi teroris sangat membahayakan masyarakat, misalnya saja sering melakukan serangan bom bunuh diri.

Menurut Pasal 1 Undang-Undang Nomor 5 Tahun 2018, terorisme diartikan sebagai perbuatan yang menggunakan kekerasan atau ancaman kekerasan yang menimbulkan suasana ketakutan atau teror yang meluas dan besar kemungkinannya menimbulkan korban jiwa dan/atau kerusakan atau kehancuran. . terhadap tujuan strategis penting, lingkungan hidup, ruang publik atau internasional dengan motif ideologis, politik atau yang merusak keamanan. Definisi terorisme didasarkan pada tiga faktor penting menurut Ganor (2002:126) meliputi:

1. Penggunaan ancaman atau kekerasan

kegiatan yang tidak melibatkan kekerasan atau ancaman kekerasan (termasuk

demonstrasi tanpa kekerasan, demonstrasi damai, pemberontakan pajak, dan lain-lain) tidak dianggap sebagai terorisme.

2. Tujuan aksi teroris selalu bersifat politis

Terorisme memiliki beberapa tujuan contohnya, untuk melindungi tujuan politik, untuk mengubah sistem, untuk mengubah orang yang berkuasa, untuk mengubah kebijakan sosial atau ekonomi. Tanpa tujuan politik, suatu tindakan tidak dapat dianggap terorisme. Suatu tindakan kekerasan terhadap warga sipil yang tidak mempunyai tujuan politik, kejahatan atau kegiatan kriminal tidak ada kaitannya dengan terorisme.

3. Sasaran terorisme adalah masyarakat sipil

Terorisme melakukan taktik dalam menyerang masyarakat mereka (Teroris) tidak sembarang memilih orang, mereka akan memilih orang yang menurut mereka kurang dalam pengetahuan mengenai terorisme karena biasanya mereka akan mudah diperdaya.

Terorisme terus berkembang, salah satu contoh perkembangannya adalah munculnya Terorisme Siber atau *Cyber Terrorism*. Terorisme siber merupakan bentuk modern dari terorisme konvensional di mana teroris menggunakan informasi, jaringan, dan teknologi komputer (Internet) sebagai sarana untuk melakukan kejahatan. Bentuk terorisme siber dapat berupa, menyebarkan malware, peretasan (hacking, phishing), mengancam sistem komputer dan serangan berantai.

Terorisme siber dapat dikatakan sebagai bentuk kejahatan pada bidang komunikasi dan teknologi yang dilakukan oleh para teroris yang berfungsi untuk menciptakan kehancuran menggunakan Komputer. Terorisme siber bentuk kejahatan terorisme yang sulit untuk diidentifikasi karena sulit untuk mengetahui keinginan, identitas atau motivasi politik dari penyerang secara pasti dalam waktu yang cukup lama.

Dengan adanya terorisme siber membuat terorisme bisa melakukan beberapa kegiatan mereka secara daring sebagai contoh, adanya rekrutmen secara daring dan juga pelatihan bom. Seperti yang kita ketahui terorisme biasanya menargetkan remaja-remaja untuk dijadikan sebagai anggota mereka karena biasanya para remaja lebih mudah untuk dimanipulasi karena kurangnya pemahaman mengenai bahaya terorisme dan memiliki biasanya anak muda memiliki militansi yang kuat.

Terorisme siber memberikan dampak yang signifikan terlebih terhadap generasi milenial selama pandemi covid-19. Beberapa contoh dampak negatif dari terorisme siber atau *cyber terrorism* terhadap generasi milenial adalah sebagai berikut:

- Penyebaran propaganda ekstrimisme
propaganda ekstrem yang meluas melalui platform media sosial yang dapat

mempengaruhi pola pikir dan sikap generasi milenial.

- Radikalisasi dan rekrutmen
peningkatan radikalisasi yang terjadi dan dengan generasi milenial yang terisolasi menjadi lebih rentan terhadap proses radikalisasi online sehingga menciptakan banyak peluang bagi terorisme siber untuk mengundang masuk kedalam kehidupan generasi milenial secara perlahan.
- Keamanan data pribadi
terorisme siber juga dapat mengancam keamanan data pribadi generasi milenial dengan serangan dari terorisme siber yang dapat mencuri informasi pribadi dan dapat mengganggu aktivitas online para generasi milenial.
- Isolasi sosial
Pandemi telah meningkatkan isolasi sosial, yang membuat generasi milenial menjadi sangat rentan terhadap pengaruh pengaruh dari media sosial.
- Peran media sosial
Media sosial menjadi peran penting dalam mempengaruhi pengguna digital saat ini, bahkan media sosial dapat memfasilitasi penyebaran ideologi ekstremisme dan koordinasi terorisme siber di antara generasi milenial.

Dalam konteks ini penting dalam menjalankan Pendidikan siber dan meningkatkan kesadaran terhadap ancaman terorisme siber dikalangan generasi milenial untuk mengurai segala dampak negatifnya. Dengan generasi milenial yang mengandalkan internet sebagai sarana penyebaran informasi, generasi milenial dapat terjebak dalam jaringan informasi palsu yang dapat mempengaruhi pemikiran dan tindakan generasi milenial.

Hubungan langsung antara terorisme siber dan generasi milenial selama pandemi adalah kompleks dan mencakup beberapa aspek yang perlu dipahami. Generasi milenial cenderung lebih terkoneksi secara digital daripada generasi sebelumnya. Selama pandemi, banyak dari mereka menghabiskan lebih banyak waktu online untuk pekerjaan, pendidikan, dan hiburan. Hal ini membuat mereka lebih rentan terhadap eksposur terhadap konten teroris yang tersebar luas di internet.

Generasi millennial sering memiliki keahlian teknologi yang tinggi, yang dapat dimanfaatkan untuk menyebarkan propaganda atau bahkan terlibat dalam serangan siber teroris. Beberapa anggota generasi milenial mungkin kurang menyadari bahaya terorisme siber atau cara mengidentifikasinya. Ini membuat mereka lebih rentan terhadap serangan siber yang bisa merugikan masyarakat atau institusi.

Penting untuk diingat bahwa mayoritas generasi milenial adalah individu yang bertanggung jawab dan tidak terlibat dalam aktivitas teroris. Namun, perlu upaya dari

pemerintah, lembaga pendidikan, dan masyarakat untuk meningkatkan kesadaran tentang ancaman terorisme siber, memberikan pendidikan tentang literasi digital, dan mengembangkan strategi untuk mengatasi propaganda ekstremisme online demi melindungi generasi ini dari pengaruh negatif.

Dalam rangka melindungi generasi milenial dari dampak negatif terorisme siber, Pendidikan, kesadaran, dan upaya kolaboratif antara pemerintah, Perusahaan teknologi, dan Masyarakat umum sangat penting. Hal ini bertujuan untuk memastikan bahwa generasi ini dapat menggunakan teknologi secara aman dan bertanggung jawab dalam dunia yang semakin terhubung secara digital.

Adapun peran pemerintah dalam menangani kasus terorisme siber atau *cyber Terrorism* yang terjadi selama beberapa tahun belakangan ini terutama pada masa pandemic Covid-19 yaitu membuat peraturan yaitu Undang- Undang ITE (Informasi Teknologi Elektronik) seperti Undang-Undang NOMOR 19 TAHUN 2016 khusus nya pada pasal 27 sampai 30 mengenai perbuatan dilarang. Undang-undang ini juga mengatur tentang *hacking* yang berisi pelarangan-pelarangan secara Online di pasal 30 ayat (1), (2), dan (3) yaitu:

1. Mengakses sistem elektronik orang lain tanpa izin

Suatu perbuatan yang melibatkan seseorang dengan sengaja dan tanpa izin atau melanggar hukum dengan mengakses atau membobol komputer atau sistem elektronik orang lain.

2. Mengakses komputer orang lain untuk tujuan memperoleh informasi elektronik dan dokumen elektronik

Tindakan ini seperti tindakan mencuri atau memperoleh informasi elektronik atau dokumen elektronik yang dimiliki oleh orang lain tanpa izin atau melanggar hukum.

3. Mengakses komputer dan sistem elektronik dengan tujuan melanggar sistem pengaman

Tindakan ini sering kali dimaksudkan untuk menimbulkan kerugian, mencuri data penting, atau mengganggu operasi yang sah.

Hukuman terhadap tindakan-tindakan diatas berada pada pasal 30 UU ITE diatur dalam pasal 46 UU ITE yaitu:

1. Ayat (1): dipidana dengan pidana penjara paling lama 6 (enam) tahun dan/atau denda paling banyak Rp600.000.000,00 (enam ratus juta rupiah).
2. ayat (2) dipidana dengan pidana penjara paling lama 7 (tujuh) tahun dan/atau denda paling banyak Rp700.000.000,00 (tujuh ratus juta rupiah).
3. ayat (3) dipidana dengan pidana penjara paling lama 8 (delapan) tahun dan/atau denda

paling banyak Rp800.000.000,00 (delapan ratus juta rupiah).

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (ITE) di Indonesia tidak secara spesifik menyebutkan terorisme siber. UU ITE lebih menitikberatkan pada peraturan perundang-undangan pada berbagai aspek terkait penggunaan teknologi informasi dan transaksi elektronik, seperti perlindungan data pribadi, hak cipta, serta tindak pidana terkait penggunaan teknologi informasi. Namun dalam praktiknya, UU ITE bisa digunakan untuk menangani pelaku terorisme siber jika aktivitasnya melanggar ketentuan dalam UU.

Disamping itu kita juga bisa melihat pengaturan tentang Tindak Pidana Terorisme Cyber dilihat dalam ketentuan UU Nomor 15 Tahun 2003 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang (Perppu) Nomor 1 Tahun 2002. Hal ini dapat dilihat dalam Pasal 1 angka 1 Perppu yang menyatakan bahwa "segala perbuatan yang memenuhi unsur-unsur tindak pidana sesuai dengan ketentuan dalam Peraturan Pemerintah Pengganti Undang-Undang ini."

Dengan Undang-Undang yang ada maka generasi millennial bisa mengambil tindakan hukum, jika mereka merasa mendapatkan tindak kejahatan Terorisme Siber ini. Sekarang pemerintah sudah menerapkan pelaporan secara online mengenai kejahatan elektronik. Kalian bisa melaporkan kejahatan elektronik disitus layanan.komindo.go.id, berikut cara melaporkan secara online melalui kominfo:

1. Kalian harus menyiapkan bukti-bukti yang ada, seperti nomor telepon sang pelaku, jika kalian mendapatkan terror melalui telepon kalian bisa merekam percakapan kalian.
2. Bukalah situs layanan.kominfo.go.id dan meng-klik menu ADUAN BRTI.
3. Isi lah data diri dan pilihlah pengaduan pada kolom pengaduan atau informasi lalu isi.
4. Setelah itu klik MULAI CHAT
5. Kalian akan dilayani oleh Petugas Help Desk dan akan diminta melampirkan bukti.
6. Petugas Help Desk akan melakukan verifikasi dan analisis pada bukti.
7. Jika sudah sesuai maka Petugas Help Desk akan membuat tiket laporan pada sistem SMART PPI dan akan mengirimkan email kepada provider agar mereka dapat memanggil atau memblokir pemilik nomor tersebut.
8. Provider akan menindaklanjuti laporan dan akan melakukan pemblokiran atau pemanggilan pada pemilik nomor tersebut dalam waktu 1X24 jam.
9. Provider akan menghubungi BRTI mengenai kasus kejahatan ini.
10. Jika terbukti bahwa sang pemilik nomor tersebut buka pelaku kejahatan maka pemblokiran akan dibuka.

SIMPULAN

Terorisme siber merupakan suatu bentuk kejahatan yang cukup berbahaya dikalangan millennial, dikarenakan para millennial lebih mudah terpengaruh karena masih kurangnya kesadaran dan juga pengetahuan mereka dalam bidang terorisme, selain itu terorisme siber ini sendiri bergerak pada bidang teknologi yang sangat berhubungan erat pada kehidupan millennial yang sangat bergantung pada gadget. Luasnya internet juga bisa menjadi tombak berujung dua jika para generasi millennials tidak dengan bijak menggunakannya maka akan terjerumus kedalam terorisme siber ini apalagi terorisme siber ini mengadakan rekrutmen secara daring yang artinya terorisme memudahkan semua kalangan untuk bisa mendaftar dan mengikuti kejahatan terorisme ini. Penanggulangan yang bisa masyarakat lakukan jika sudah terjerat pada terorisme siber ini adalah dengan melakukan pengaduan pada pihak berwajib sesegera mungkin agar tidak terjerumus semakin dalam dan semakin sulit untuk keluar dari masalah terorisme siber ini.

DAFTAR PUSTAKA

- A. Monica, Danastri, *Cyber Terrorism Dalam Perspektif Undang-Undang Anti Terorisme Dan Undang-Undang Informasi Dan Transaksi Elektronik*, Jakarta, SMA Labschool Jakarta, 2011.
- Astuti, S. A. (2015). Penegakan Hukum terhadap Terorisme Dunia Maya di Indonesia. (157-165)
- Indonesia, R. (2019). *Sistem Nasional Ilmu Pengetahuan Dan Teknologi*
- Indonesia, C. (2023). BNPT: Lebih dari Separuh Pelaku Terorisme Berusia Muda. Retrieved 15 September 2023, <https://www.cnnindonesia.com/nasional/20210331203200-20-624631/bnpt-lebih-dari-separuh-pelaku-terorisme-berusia-muda> (diakses pada 10 September, 2023)
- Kitab Undang-Undang Hukum Pidana (KUHP)
- Kominfo, 18 September (2023). *Komunikasi dan informatika. Alur Penangan Pengaduan Pelanggan.*
<https://layanan.kominfo.go.id/microsite/aduanbrti#:~:text=Pelapor%20membuka%20laman%20layanan.kominfo,email%20dan%20nomor%20telepon%20seluler> (diakses pada 10 September, 2023)
- Mumtaaz, G. & Wardhana, T. & Diastutui, F. ANTI CYBER TERORISM SEBAGAI UPAYA STRATEGIS DALAM MENANGGULANGI VYBER TERORISM DI INDONESIA. 2(1), 48-57
- Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang
- Sarinastiti, E. & Vardhani, N. (2018). INTERNET DAN TERORISME: MENGUATNYA AKSI

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi

Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik

Undang-Undang Nomor 15 Tahun 2003 tentang Perppu Nomor 1 Tahun 2002 tentang Pemberantasan Tindak Pidana Terorisme Menjadi Undang-Undang sebagaimana telah diubah dengan Undang-Undang Nomor 5 Tahun 2018 tentang Perubahan atas Undang-Undang Nomor 15 Tahun 2003 tentang Penetapan Perppu Nomor 1 Tahun 2002 tentang

Waluyo, P. (2019). DINAMIKA KEPATUHAN (OBEDIENCE) TERHADAP NILAI-NILAI RADIKAL PADA MANTAN NARAPIDANA TERORIS (Doctoral dissertation, Universitas Muhammadiyah Surabaya). 1. 40-45

Yuniarto, T. (2022). Terorisme: Definisi, Inklusifitas, Skala, dan Evolusi. 15 September 2023, dalam <https://www.kompas.id/baca/paparan-topik/2022/04/20/terorisme-definisi-inklusifitas-skala-dan-evolusi> (diakses pada 10 September, 2023)