ULIL ALBAB : Jurnal Ilmiah Multidisiplin
Vol.5, No.4, Maret 2026

Ruang Siber Dan Radikalisasi Online: Proses Komunikasi Dalam Terorisme Lone Wolf

Cahayani Yogaswari
Universitas Pembangunan Nasional "Veteran" Jakarta, Indonesia
E-mail: cahayaniy@upnvj.ac.id

Article History:
Received: 28 Januari 2026
Revised: 27 Februari 2026
Accepted: 04 Maret 2026

Keywords: *Terorisme lone wolf, radikalisasi online, komunikasi digital, ruang siber*

Abstract: *Perkembangan teknologi yang melahirkan ruang siber dan jaringan internet merupakan faktor yang memengaruhi peningkatan jumlah aksi teror yang dilakukan oleh oleh lone wolf dalam satu dekade terakhir. Hal ini terjadi karena karakteristik ruang siber yang memfasilitasi anonimitas, terdesentralisasi, memfasilitasi komunikasi tersembunyi, dapat diakses oleh siapa saja, mudah digunakan, tidak membutuhkan biaya besar, serta tidak diatur oleh regulasi ketat dapat memudahkan penyebaran propaganda dan ideologi ekstrimis. Proses radikalisasi untuk mengubah seorang individu menjadi lone wolf berlangsung melalui ruang siber dengan melalui empat tahapan yang dikemukakan oleh Spaaij, yaitu the funnel, social bonding, infection, dan activation. Ruang siber juga memfasilitasi para individu yang merasa terasing atau terpinggirkan di dunia nyata untuk berinteraksi dengan individu-individu lain dengan pemikiran dan semangat serupa melalui dark web. Interaksi berbasis ruang siber inilah yang memunculkan tantangan bagi upaya penanggulangan terorisme lone wolf.*

PENDAHULUAN

Selain membawa perubahan besar dalam proses komunikasi dengan meleburkan batas-batas geografis, kehadiran jaringan internet juga memungkinkan kelompok teroris untuk perlahan-lahan lepas dari ketergantungan mereka terhadap salah satu elemen vital aksi terorisme, yaitu publikasi Yar, 2006). Jika sebelumnya kelompok teroris mengandalkan liputan surat kabar, radio, televisi, dan media massa lainnya terhadap aksi teror yang dilakukannya, saat ini mereka memiliki kesempatan untuk berperan menjadi publisis bagi kelompok dan organisasinya sendiri di ruang siber. Dalam kaitannya dengan aktivitas terorisme, ruang siber dinilai sebagai wilayah yang tepat untuk melakukan komunikasi intra-organisasi, mengkoordinasikan aktivitas melalui penggunaan e-mail dan *bulletin board*, menyebarkan propaganda agar yang dapat dijangkau audiens dari seluruh penjuru dunia, menyerap informasi sensitif yang diunggah oleh pemerintah, lembaga publik, organisasi bisnis, maupun para pengguna internet di milyaran laman *online,* dan mengumpulkan donasi dari simpatisannya melalui situs web (Yar, 2006).

Pemanfaatan ruang siber oleh kelompok teroris juga meningkatkan fenomena terorisme *lone wolf,* yaitu serangan teror oleh individu yang tidak terafiliasi dengan organisasi teroris,

namun menganut ideologi radikal yang sama dengan jaringan maupun organisasi teroris terentu. Aksi peledakan bom pada kegiatan London Marathon di tahun 2013 merupakan salah satu peristiwa teror besar yang dilakukan oleh teroris yang 'lahir dari internet', yaitu Dzhokhar Tsarnaev dan Tamerlan Tsarnaev. Tsarnaev bersaudara mengaku bahwa dorongan untuk menjadi teroris muncul dalam diri mereka setelah membaca majalah *Inspire,* sebuah media *online* milik organisasi teroris Al-Qaeda. Mereka juga menyatakan terpesona oleh khotbah *online* yang disampaikan oleh Anwar-al Awlaki, salah satu propagandis Al-Qaeda merangkap editor majalah tersebut (Weimann, 2015). Aksi dengan pelaku yang memiliki alasan serupa juga beberapa kali terjadi di Indonesia, diantaranya ialah pengeboman Gereja Katolik Santo Yosep di Medan oleh Ivan, seorang remaja 17 tahun yang mengaku terinspirasi oleh ISIS dan memanfaatkan internet untuk mencari tahu teknik merakit bom (Faqih, 2016) dan percobaan bom bunuh diri di Polsek Kartasura oleh Rofik, pemuda berusia 23 tahun yang juga mempelajari cara merakit bom dan paham terorisme dari internet (CNN, 2019).

Aksi teror yang melibatkan pelaku tunggal telah ditemukan dari abad ke-19 dan bukan merupakan merupakan fenomena baru (Pantucci; 2011, Spaaij, 2012), namun studi yang dilakukan oleh Institute for Safety, Security and Crisis Management on Terrorism (dalam Weimann, 2012) menunjukkan bahwa jumlah serangan *lone wolf* dalam dekade terakhir ditemukan meningkat dan menyatakan bahwa pelaku teror *lone wolf* berasal dari berbagai jenis kelompok ekstrimis, baik dalam konteks ideologi maupun agama. Meski demikian, kajian mengenai terorisme *lone wolf* belum banyak dilakukan (Spaaij, 2010; Pantucci, 2011). Menurut Spaaij (2010), terorisme lebih umum dipandang sebagai tindakan kolektif yang terorganisir yang identik dengan pengaruh dari tokoh pemimpin yang karismatik, proses perekrutan yang bersifat *top-down* atau *bottom-up*, memiliki tahapan *logical training* dan indoktrinasi, *moral disengagement*, solidaritas kelompok, konformitas dan kepatuhan, depersonalisasi, dan hal-hal yang berkaitan dengan organisasi. Hal ini menyebabkan riset mengenai terorisme lebih banyak berfokus pada serangan yang dilakukan oleh kelompok. Sementara itu, Pantucci (2011) berpendapat bahwa penyebab *lone wolf* masih jarang dijadikan topik kajian ialah adanya kesulitan untuk mengidentifikasi faktor-faktor dan kondisi yang mendorong seseorang untuk menjalankan aksi teror secara individual.

Melalui studi pustaka, tulisan ini berupaya mengelaborasi hasil penelitian terdahulu yang relevan dan menyajikan analisis untuk menjawab rumusan permasalahan mengenai keterkaitan ancaman terorisme *lone wolf* dengan ruang siber. Paparan konsep dan hasil analisis dalam tulisan ini akan disajikan dalam empat bagian. Pertama, tinjauan mengenai terorisme *lone wolf* yang meliputi definisi, karakteristik, tipologi, dan stereotip yang melekat pada teroris lone wolf. Kedua, tinjauan mengenai ruang siber sebagai alat terorisme, meliputi definisi dan karakteristik ruang siber, tujuan pemanfaatan ruang siber oleh kelompok teroris, serta pergeseran strategi organisasi teroris di ruang siber. Ketiga, tinjauan mengenai radikalisasi teroris *lone wolf* secara online, meliputi definisi radikalisasi, karakteristik radikalisasi *lone wolf*, serta komponen dan tahapan yang ada dalam proses radikalisasi seorang individu menjadi *lone wolf* secara online. Keempat, pemaparan mengenai tantangan untuk menghadapi terorisme *lone wolf* di ruang siber, meliputi bagaimana ruang siber memfasilitasi interaksi antar teroris serta faktor yang menyebabkan penanganan terhadap terorisme *lone wolf* sulit dilakukan.

METODE PENELITIAN

Artikel ini menggunakan pendekatan kualitatif dengan metode studi pustaka. Metode ini dipilih untuk menganalisis keterkaitan antara ruang siber, proses radikalisasi online, dan

terorisme *lone wolf* melalui penelusuran dan pembacaan kritis terhadap kajian-kajian terdahulu yang relevan. Sumber data meliputi buku akademik, artikel jurnal, dan laporan penelitian yang membahas karakteristik ruang siber, pemanfaatan internet oleh kelompok teroris, serta model dan tahapan radikalisasi *lone wolf*. Analisis dilakukan dengan mengelaborasi konsep dan temuan utama dari literatur tersebut guna memahami bagaimana proses komunikasi digital berperan dalam transformasi individu menuju aksi teror, serta tantangan penanggulangan yang muncul akibat karakter komunikasi di ruang siber.

HASIL DAN PEMBAHASAN

Terorisme *Lone Wolf*

Lone wolf merupakan istilah yang digunakan untuk menjelaskan perilaku individu yang bertindak berdasarkan keinginannya sendiri tanpa adanya arahan maupun hubungan dengan kelompok tertentu (Burton & Stewart, 2008). Dalam konteks terorisme, tindakan yang dilakukan oleh individu yang kadang disebut sebagai *homegrown terrorist* ini menerapkan taktik terorisme tradisional, termasuk menargetkan serangan terhadap masyarakat sipil, untuk mencapai tujuan politik maupun ideologi tertentu (Weimann, 2015). Teror yang dilakukan oleh *lone wolf* memiliki tiga ciri utama, yaitu pelaku yang menjalankan aksinya secara individu, tidak terikat dengan kelompok maupun jaringan teroris tertentu, dengan modus operandi yang ditetapkan sendiri tanpa adanya komando dari pihak luar (Spaaij, 2010).

Burton & Stewart (2008) menyatakan bahwa kemampuan untuk bergerak di bawah kontrolnya sendiri menjadi faktor yang membedakan *lone wolf* dengan *sleeper operation,* istilah yang mewakili individu anggota kelompok teroris yang berstatus dorman hingga mendapat arahan untuk melakukan 'aktivasi' dan menjalankan aksi teror. Sementara itu, Spaaij (2010) memaparkan bahwa meski sama-sama dilakukan oleh individu tunggal yang tidak dikontrol oleh pihak lain, aksi *lone wolf* berbeda dengan *lone assassin.* Faktor yang membedakan dua aksi tunggal ini ialah motif pelaku dalam melakukan teror, di mana aksi *lone wolf* didasari oleh tujuan politik, ideologi, atau agama, sedangkan aksi *lone assassin* cenderung didasari oleh tujuan personal. Berkaitan dengan tujuan melakukan teror, Sageman (dalam Pantucci, 2011) mengemukakan kategori serupa dengan istilah yang berbeda, yaitu *real lone wolf* dan *mass murderer. Real lone wolf* merupakan individu yang membawa ideologi terorisme dan biasanya terlibat dalam suatu komunitas virtual di internet, sedangkan *mass murderer* merupakan individu dengan ideologi dan 'kegilaannya' sendiri yang melakukan aksi teror untuk melampiaskan kemarahan personal.

Dalam studinya, Pantucci (2011) menawarkan tipologi yang mengelompokkan *lone wolf* ke dalam empat kategori berdasarkan hubungannya dengan kelompok teroris. Pertama, *loner,* yaitu individu terisolir yang merencanakan aksi teror dengan didasari ideologi ekstrim, tanpa terlibat hubungan langsung dengan para ekstrimis selain melalui konten yang dapat diakses di internet atau terbuka untuk publik. Kedua, *lone wolf,* yaitu individu yang melakukan aksi tunggal tanpa adanya dorongan dari pihak tertentu, namun teridentifikasi melakukan kontak dengan individu lain yang memiliki ideologi serupa maupun kelompok teroris tertentu. Ketiga, *lone wolf pack,* yaitu sekelompok individu yang melakukan swa-radikalisasi dengan berkiblat pada kelompok ekstrimis tertentu, namun belum melakukan kontak langsung dengan kelompok teroris. Keempat, *lone attackers,* yaitu individu yang melakukan aksi secara tunggal, namun melakukan kontak aktif dengan ekstrimis aktif dan teridentifikasi bahwa aksinya dilakukan atas arahan dan berafiliasi dengan kelompok teroris tertentu. Jika mengacu pada definisi yang menyatakan bahwa aksi *lone wolf* dilakukan oleh individu, maka kategori ketiga (*lone wolf* pack) dan keempat (*lone*

attackers) yang dikemukakan oleh Pantucci (2011) ini tidak dapat dikategorikan sebagai *lone wolf. Lone wolf pack* bukanlah individu yang bergerak secara tunggal, sedangkan *lone attacker* lebih cocok disebut sebagai *sleeper operation,* karena ia merupakan bagian dari kelompok teroris yang menunggu arahan untuk 'diaktivasi' sebelum melakukan aksi teror.

Sejumlah studi menunjukkan bahwa *lone wolf* kerap diidentikan dengan individu yang memiliki gangguan psikologis dan terasing secara sosial (Vasilenko, 2004; Burton & Stewart, 2008; Pantucci, 2011; Spaaij, 2012). Menurut Spaaij (2012), rasa kesulitan untuk berbaur inilah yang membuat sebagian *lone wolf* menunjukkan keinginan untuk keluar dari tatanan yang berlaku di kelompok masyarakat umum dan bertindak berdasarkan pertimbangannya sendiri. Meski memiliki ideologi radikal yang sejalan dengan kelompok teroris tertentu, aksi yang dilakukan oleh *lone wolf* tanpa arahan dari pihak luar (Weimann, 2012). Hal ini membuat aksi teror tunggal ini memiliki keunggulan dibanding teroris yang bergerak dalam kelompok atau jaringan, karena pelaku teror yang tidak mempublikasikan visi dan rencananya sulit untuk diidentifikasi dan dilacak keberadaannya, baik sebelum maupun setelah menjalankan aksi (Weimann, 2015).

Ruang Siber sebagai Alat Terorisme

Ruang siber merupakan istilah yang digunakan untuk menjelaskan seperangkat jaringan komunikasi berbasis komputer (Bell, Loader, Pleace & Schuler, 2004; Goodman, Kirk & Kirk, 2007) yang memungkinkan terjadinya komunikasi termediasi komputer antara orang-orang dari berbagai penjuru dunia (Bell, Loader, Pleace & Schuler, 2004). Sebelum diulas secara lebih lanjut, perlu diperjelas bahwa ruang siber bukanlah sinonim dari internet. oleh Bell, Loader, Pleace & Schuler (2004) mendefinisikan internet sebagai "…*an international 'network of networks' that uses a common set of standards* (TCP/IP) *to permit the interconnection of millions of computers, enabling such services as electronic mail and remote access to information",* sedangkan Goodman, Kirk & Kirk (2007) menyatakan bahwa "*The internet is the largest single component of cyberspace, with a presence in over 200 countries and something approaching a billion user".* Berdasarkan dua definisi tersebut, dapat ditetapkan bahwa internet merupakan seperangkat jaringan yang menjadi komponen tunggal terbesar dalam ruang siber dan berperan sebagai penghubung bagi jutaan komputer serta memfasilitasi komunikasi antar penghuni ruang siber.

Lahir dari proyek yang dilakukan U.S. Defense Departement's Advanced Research Project Agency (ARPA) dan MIT pada beberapa dekade lalu untuk tujuan militer, kini ruang siber dengan jaringan internet yang hidup di dalamnya berubah menjadi medium komunikasi publik yang membuat penggunanya 'ketagihan' (Last & Kandel, 2005). Salah satu faktor yang mendorong ruang siber banyak diminati ialah karena komunikasi yang terjadi di ruang siber tidak menuntut komunikator dan komunikannya untuk hadir secara fisik (Bell, Loader, Pleace & Schuler, 2004) maupun *online* di saat yang bersamaan (Last & Kandel, 2005), melainkan lebih menekankan pada interkoneksi jutaan manusia yang saling terhubung dengan menggunakan surat elektronik, *news group, bulletin board,* dan ruang obrolan virtual (Bell, Loader, Pleace & Schulder, 2004).

Dengan tawaran teknologi yang memudahkan proses komunikasi, ditambah dengan semakin luasnya wilayah di berbagai belahan dunia yang terhubung oleh jaringan internet, membuat ruang siber semakin banyak dihuni oleh orang-orang dari berbagai kalangan dan kepentingan, termasuk di dalamnya ialah kelompok teroris. Studi terdahulu menunjukkan bahwa ruang siber merupakan wilayah yang ideal bagi aktivitas terorisme (Last & Kandel, 2005; Weimann, 2015). Anggapan ini dipengaruhi oleh beberapa karakteristik ruang siber, yaitu memfasilitasi anonimitas (Goodman, Kirk & Kirk, 2007; Michael, 2012; Weimann, 2015),

terdesentralisasi (Michael, 2012; Weimann, 2015), memungkinkan komunikasi tersembunyi (Goodman, Kirk & Kirk, 2007; Michael, 2012), dapat diakses oleh siapa saja (Last & Kandel, 2005; Goodman, Kirk & Kirk, 2007; Michael, 2012; Weimann, 2015), mudah digunakan (Goodman, Kirk & Kirk, 2007; Weimann, 2015), tidak membutuhkan biaya yang besar (Last & Kandel, 2005; Goodman, Kirk & Kirk, 2007; Michael, 2012; Weimann, 2015), serta tidak diatur oleh regulasi yang ketat (Michael, 2012; Weimann, 2015). Weimann (2015) menambahkan bahwa meningkatnya kepopuleran internet membuat lalu lintas pertukaran informasi antar penghuni ruang siber menjadi semakin padat dan membuat teroris mudah untuk melebur dengan pengguna internet lain. Interaktivitas yang ada di berbagai platform komunikasi *online* juga membantu teroris untuk menempatkan diri pada posisi proaktif, yaitu untuk melakukan aksi 'jemput bola' kepada para pengguna internet (Weimann, 2015).

Sejumlah studi mengenai terorisme di ruang siber telah mengkaji tujuan pemanfaatan ruang siber oleh kelompok teroris. Menurut Last & Kandel (2005), penggunaan ruang siber oleh teroris dapat dikelompokkan ke dalam empat tujuan besar. Pertama, tujuan komunikasi, khususnya komunikasi rahasia untuk memberi instruksi dan mengontrol infrastruktur. Kedua, tujuan untuk mengakses informasi, meliputi informasi mengenai target serangan dan instruksi teknis perakitan senjata. Ketiga, diseminasi propaganda dan perekrutan. Keempat, serangan siber yang dilakukan untuk merusak infrastruktur yang ada.

Studi yang dilakukan oleh Goodman, Kirk & Kirk (2007) mengidentifikasi bahwa kelompok teroris memanfaatkan ruang siber dengan tiga tujuan. Pertama, sebagai alat pendukung infrastruktur dan aktivitas teroris, namun tidak ditujukan untuk melakukan serangan siber. Kedua, untuk melakukan penyerangan terhadap komponen infrastruktur ruang siber. Ketiga, sebagai alat untuk melakukan penyerangan terhadap target lain.

Sementara itu, Weimann (2015) mengelompokkan aktivitas teroris di internet ke dalam dua kategori, yaitu komunikatif dan instrumental. Tujuan komunikatif meliputi penyebaran propaganda, serangan psikologis, pengamanan komunikasi internal, dan radikalisasi anggota baru, sedangkan tujuan instrumental mencakup pelatihan teroris secara *online* dan pengadaan kamp pelatihan virtual.

Studi lain yang mengidentifikasi tujuan pemanfaatan ruang siber untuk aktivitas terorisme dilakukan oleh Yar (2006) yang menyatakan bahwa teroris memanfaatkan internet untuk melakukan komunikasi intra-organisasi, mengkoordinasikan aktivitas melalui penggunaan e-mail dan *bulletin board*, menyebarkan propaganda agar yang dapat dijangkau audiens dari seluruh penjuru dunia, menyerap informasi sensitif yang diunggah oleh pemerintah, lembaga publik, organisasi bisnis, maupun para pengguna internet di milyaran laman *online,* dan mengumpulkan donasi dari simpatisannya melalui situs web.

Stroobants (2018) dalam riset Global Terorrism Index 2018 menyatakan bahwa hibridisasi terorisme dan dunia siber dapat memudahkan penyebaran propaganda dan ideologi ekstrimis, memfasilitasi proses rekrutmen teroris dan radikalisasi, serta mendorong terjadinya lebih banyak aksi teror. Argumen tersebut didukung oleh fakta yang menunjukkan bahwa beberapa pelaku aksi teror yang terjadi beberapa tahun belakangan tidak hanya diradikalisasi secara *online,* melainkan juga mendapatkan 'panduan tugas' serta didalangi secara *live time* oleh organisasi teroris melalui internet dan platform komunikasi yang terenkripsi (Stroobants, 2018).

Hal ini merupakan wujud pergeseran strategi organisasi teroris yang sebelumnya terfokus pada upaya mendorong pengikutnya untuk melakukan jihad dengan cara pergi ke wilayah di mana organisasi teroris berada menjadi upaya untuk mendorong pengikutnya agar melakukan jihad dengan menjalankan aksi serangan di wilayahnya masing-masing (Hamm & Spaaij, 2017;

Stroobants, 2018). Stroobants (2018) menyatakan bahwa saat ini organisasi teroris melakukan mobilisasi sel terorisnya dan menggunakan pesan terenkripsi untuk menyusun perencanaan, melakukan perekrutan, dan menjalankan aksi dengan fokus pada *homegrown terrorist.* Hal ini sejalan dengan argumen Spaaij (2012) yang menyatakan bahwa internet merupakan inkubator atau akselerator bagi aksi terorisme yang dilakukan secara tunggal maupun dalam kelompok kecil.

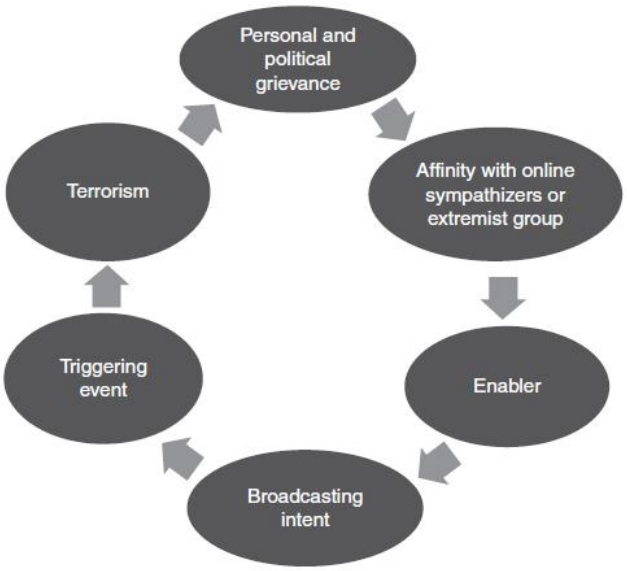
Radikalisasi *Lone Wolf* secara *Online*

Serupa dengan aksi teror yang dilakukan oleh anggota kelompok maupun jaringan tertentu, terorisme *lone wolf* juga berakar dari proses radikalisasi. Spaaij (2012) mendefinisikan proses ini sebagai upaya menerapkan sistem keyakinan ekstrim dengan tujuan untuk memfasilitasi tindakan kekerasan berbasis ideologi guna mencapai perubahan dalam sistem politik, agama, maupun sosial. Meningkatnya jumlah pengguna internet yang berbanding lurus dengan semakin luasnya akses terhadap segala jenis informasi, termasuk informasi bermuatan radikal di ruang siber merupakan faktor yang dianggap berperan besar pada meningkatnya jumlah *lone wolf* yang mendalami paham radikal secara otodidak (Pantucci, 2011; Thompson, 2011). Sebagaimana dinyatakan oleh Hamm & Spaaij (2017):

> The internet and social media make it possible for an individual to become radicalized in the solitude of his or her bedroom through linking and interacting with virtual "friends", electronically exchanging militant propaganda, and even acquiring technical know-how for commiting acts of terrorism through online manuals. (p. 38).

Weimann (2015) menyatakan bahwa terdapat dua karakteristik unik dari proses radikalisasi yang dalam buku 'Terrorism in Cyberspace: The Next Generation' (2015) ia istilahkan sebagai 'rekrutmen' terhadap individu yang ditargetkan menjadi *lone wolf.* Pertama, proses radikalisasi berlangsung secara *multistep* dengan melibatkan beberapa tahapan. Kedua, proses radikalisasi tersebut bergantung pada platform *online.* Meski kerap diasumsikan bahwa proses penanaman paham radikal kepada individu yang melakukan aksi teror *lone wolf* berbentuk "swa-radikalisasi" (Danzell & Maisonet Montañez, 2015), nyatanya proses tersebut dapat dilacak melalui beragam jejaring sosial (Hamm & Spaaij, 2017) serta dipengaruhi oleh kelompok radikal (Weimann, 2015).

Berdasarkan hasil riset studi kasus terhadap aksi terorisme *lone wolf* di Amerika Serikat, Hamm & Spaaij (2017) menawarkan model yang mencakup lima komponen yang berkaitan dengan proses radikalisasi individu hingga bertransformasi menjadi sosok teroris *lone wolf.*



Gambar 1. Model Radikalisasi Teroris *Lone Wolf* (Hamm & Spaaij, 2017)

Personal and political grievance merupakan komponen pertama dari proses radikalisasi *lone wolf.* Menurut Hamm & Spaaij (2017), komponen ini merupakan hal utama yang membedakan *lone wolves* dengan anggota organisasi teroris, di mana dalam organisasi teroris keluhan pribadi bukanlah fokus utama. Teroris *lone wolf* juga memiliki keunikan dari segi kepercayaan dan perilaku, karena mereka dapat menggabungkan beragam permasalahan politik dengan pembalasan dendam personal melalui cara-cara yang kompleks dan terindividualisasi.

Affinity with online symphatizers or extremist group merupakan komponen radikalisasi yang menunjukkan bahwa *lone wolf* memiliki rasa simpati terhadap kelompok ekstrim atau simpatisan teroris *online* tertentu dan mengacu pada keyakinan (ideologi) yang sama. Seiring perkembangan teknologi, terjadi pergeseran hubungan teroris *lone wolf* yang sebelumnya berlangsung dengan *extremist group* menuju *online symphatizers.* Hal ini merupakan transformasi penting dalam sejarah terorisme *lone wolf,* karena pergeseran tersebut menunjukkan bahwa dukungan terhadap *leaderless resistance,* yaitu sebuah konsep yang mendasari praktik terorisme *lone wolf* telah menjadi semakin kuat.

Enabler dapat dimaknai sebagai sebagai sosok yang 'memantik' semangat individu untuk bertransformasi menjadi *lone wolf,* mencakup sosok yang mencontohkan praktik serangan teror secara langsung, maupun sosok yang secara tidak langsung mendorong seseorang untuk melakukan aksi teror.

Broadcasting intent, kerap juga disebut sebagai "seepage" atau "signaling", merupakan istilah yang digunakan untuk menjelaskan 'pengumuman' bahwa sebuah aksi akan dilaksanakan. Proses ini merupakan komponen penting untuk memahami proses radikalisasi terhadap teroris *lone wolf* serta dapat digunakan sebagai upaya pencegahan aksi teror.

Triggering event merupakan komponen yang menjadi katalis utama bagi aksi terorisme *lone wolf.* Komponen ini dapat berwujud peristiwa personal, politis, maupun gabungan keduanya. Pemicu bagi aksi teror ini terkadang hadir secara tiba-tiba, sehingga bisa jadi seorang *lone wolf* melakukan serangan tanpa perencanaan.

Sebagai penjelas bagi gambar di atas, Hamm & Spaaij (2017) menyatakan bahwa panah '*terrorism'* yang mengarah ke '*personal and political grievences'* mewakili potensi adanya duplikasi dari aksi teror yang telah terjadi. Model tersebut menunjukkan bahwa radikalisasi

bukan merupakan proses yang bergantung pada sebuah faktor tunggal, melainkan merupakan kombinasi dari beberapa faktor yang berhubungan serta melakukan proses "*push and pull"* (Hamm & Spaaij, 2017). Hamm & Spaaij (2017) menambahkan bahwa model yang menunjukkan komponen-komponen radikalisasi tersebut tidak bersifat linear, sehingga proses transformasi seorang individu menjadi *lone wolf* tidak mesti melalui tahapan-tahapan tersebut secara urut.

Sementara itu, Weimann (2015) menawarkan perspektif lain berdasarkan model yang ditetapkan oleh RAND Corporation untuk mengidentifikasi empat tahapan proses radikalisasi *lone wolf* oleh kelompok radikal. Pertama, *the net.* Sejumlah pengguna internet yang dijadikan sasaran akan disuguhi beragam konten media bermuatan radikal. Meski tidak seluruh pengguna internet yang terpapar konten tersebut akan bereaksi positif, secara umum seluruh populasi dipandang sebagai audiens potensial yang homogen dan dapat dijangkau dengan satu pendekatan yang sama. Pada tahapan ini, kelompok radikal menggunakan segala platform yang tersedia *online,* mulai dari laman Facebook hinggal surel pribadi, video Youtube, atau situs web resmi.

Kedua, *the funnel.* Kelompok radikal akan menggunakan pendekatan secara bertahap setelah berhasil mengidentifikasi bahwa terdapat audiens yang berpotensi menjadi *lone wolf.* Tahapan ini menekankan pada teknik psikologi kognitif, sosial, dan klinis, serta melibatkan paparan materi bermuatan agama, politik, atau ideologi tertentu. Keberhasilan tahapan ini bergantung pada *social bonding* secara virtual yang dipengaruhi oleh rasa keterasingan, kesulitan untuk berinteraksi secara sosial, kesendirian, dan pesimisme yang dimiliki oleh target.

Ketiga, *infection.* Target yang memiliki ketidakpuasan terhadap status sosial maupun sistem politik atau agama yang mereka anut akan diarahkan pada proses *self-radicalization* yang berlangsung secara *online* dan bergantung pada tingkatan komitmen dan ekstrimisme target. Tahapan ini melibatkan paparan terus-menerus terhadap konten bermuatan radikal serta panduan virtual secara *online.*

Keempat, *activation.* Tahap akhir dari proses radikalisasi ini meliputi paparan materi berupa instruksi praktis, diantaranya ialah panduan *online* mengenai penggunaan bahan peledak, senjata, racun, maupun bahan kimia; arahan mengenai pemilihan target serangan, lokasi, dan waktu pelaksanaan serangan; hingga target tersebut dinilai siap menjadi *lone wolf.*

Kunci untuk untuk memahami bagaimana seorang individu yang telah teradikalisasi berubah menjadi *lone wolf* ialah sejauh mana mereka melihat dirinya sendiri sebagai sosok yang merasa bertanggungjawab untuk melakukan aksi kekerasan (Spaaij, 2012; Danzell & Maisonet Montañez, 2015)

Tantangan Menghadapi *Lone Wolf* di Ruang Siber

Dengan mengacu pada argumen di beberapa studi terdahulu yang menyatakan bahwa para pelaku aksi teror *lone wolf* merupakan individu yang cenderung terasing dari kehidupan sosial (Vasilenko, 2004; Burton & Stewart, 2008; Pantucci, 2011; Michael, 2012; Spaaij, 2012; Hamm & Spaaij, 2012), maka kehadiran ruang siber dapat dinyatakan sebagai substitusi dari interaksi sosial yang sulit didapatkan di dunia nyata (Pantucci, 2011). Substitusi tersebut dapat terjadi karena internet menyediakan akses bagi para penggunanya untuk dapat terhubung dengan individu-individu lain dengan pemikiran serupa yang berasal dari berbagai belahan dunia (Pantucci, 2011; Michael, 2012).

Dalam praktiknya, seorang *lone wolf* juga tidak benar-benar bergerak sendiri (Burton & Stewart, 2008; AIVD, 2012; Hamm & Spaaij, 2012; Weimann, 2015). Menurut Weimann (2015), individu-individu yang melakukan aksi *lone wolf* saling terhubung, berkomunikasi, berbagi informasi, serta bertukar pengetahuan di ruang siber melalui *dark web.* Sementara itu, Burton & Stewart (2008) menekankan bahwa salah satu masalah terbesar yang dihadapi oleh *lone wolf*

untuk melakukan aksi yang dikategorikan berhasil ialah penguasaan keterampilan, sehingga hampir mustahil seorang *lone wolf* dapat mempersiapkan aksinya tanpa campur tangan dari orang lain. Argumen ini sejalan dengan pernyataan Badan Intelijen dan Keamanan Umum Belanda (AIVD, 2012):

In the aftermath of such events, it is often discovered that lone wolves hardly had any contacts with like-minded individuals in real life, but did maintain active contact with people on the internet. In retrospect, it is then concluded that these contacts, as well as the consumption of jihadist propaganda and the online discourse, have contributed to their radicalization and (may also) have inspired them to commit such a violent act. (p. 21).

Spaaij (2012) memaparkan lima faktor utama yang menyebabkan pencegahan aksi terorisme *lone wolf,* sekalipun dengan melibatkan intelijen, menjadi sulit untuk dilakukan. Pertama, teroris *lone wolf* tidak menunjukkan bahwa ada orang lain yang terlibat dalam aksinya serta cenderung merahasiakan rencana aksi tersebut. Kedua, keterasingan sosial dan kecenderungan *lone wolf* untuk menghindar dari kontak dengan orang lain berdampak pada minimnya tanda yang menunjukkan bahwa ia akan menjalankan aksi teror. Ketiga, *lone wolf* mewakili beragam latar belakang dengan spektrum ideologi dan motivasi yang luas, sehingga sulit untuk mengidentifikasi dari kalangan mana ia berasal. Keempat, identifikasi antara individu ekstrimis yang memiliki tujuan untuk melakukan aksi teror dan individu yang hanya ingin menunjukkan bahwa ia penganut paham radikal cenderung sulit untuk dilakukan. Kelima, mayoritas *lone wolf* hanya melakukan satu kali serangan.

KESIMPULAN

Kemajuan teknologi berwujud ruang siber dan jaringan internet membantu kelompok teroris untuk melakukan penyebaran propaganda dan ideologi ekstrimis, serta mendorong terjadinya lebih banyak aksi teror. Hal ini disebabkan karena proses radikalisasi untuk menanamkan ideologi ekstrimis ke dalam diri seseorang dapat dilakukan secara online, sehingga seorang individu yang memiliki ketertarikan terhadap ideologi tersebut dapat melakukan proses radikalisasi secara mandiri sebelum melakukan aksi teror sebagai *lone wolf.* Ruang siber juga memfasilitasi para individu yang merasa terasing atau terpinggirkan di dunia nyata untuk berinteraksi dengan individu-individu lain dengan pemikiran dan semangat serupa melalui *dark web*. Interaksi berbasis ruang siber inilah yang memunculkan tantangan bagi upaya penanggulangan terorisme *lone wolf.*

DAFTAR REFERENSI

AIVD (General Intelligence and Security Service). (2012). *Jihadism on the Web: A Breeding Ground for Jihad in the Modern Age.* Amsterdam: Ministry of the Interior and Kingdom Relations of the Netherlands.

Bell, D. J., Loader, B. D., Pleace, N., & Schuler, D. (2004). *Cyberculture: The key concepts.* London & New York: Routledge.

Burton, F., & Stewart, S. (2008). The ‘lone wolf’ disconnect. *Terrorism Intelligence Report-STRATFOR*.

Danzell, O. E., & Maisonet Montañez, L. M. (2016). Understanding the lone wolf terror phenomena: Assessing current profiles. *Behavioral Sciences of Terrorism and Political Aggression*, *8*(2), 135-159.

Goodman, S. E., Kirk, J. C., & Kirk, M. H. (2007). Cyberspace as a medium for

terrorists. *Technological Forecasting and Social Change*, *74*(2), 193-210.

Hamm, M. S., Spaaij, R. F. (2017). *The age of lone wolf terrorism.* New York: Columbia University Press.

Institute for Economics & Peace. (2018). Global Terrorism Index 2018: Measuring the impact of terrorism. Retrieved from from: http://visionofhumanity.org/reports.

Last, M., & Kandel, A. (Eds.). (2005). *Fighting terror in cyberspace*. Singapore: World Scientific Publishing.

Michael, G. (2012). *Lone wolf terror and the rise of leaderless resistance*. Nashville: Vanderbilt University Press.

Pantucci, R. (2011). A typology of lone wolves: Preliminary analysis of lone Islamist terrorists. London: International Centre for he Study of Radicalization and Political Violence.

Spaaij, R. (2010). The enigma of lone wolf terrorism: An assessment. *Studies in Conflict & Terrorism*, *33*(9), 854-870.

Spaaij, R. (2012). Understanding lone wolf terrorism: Global patterns, motivations and prevention. London & New York: Springer.

Thompson, R. (2011). Radicalization and the use of social media. *Journal of strategic security*, *4*(4), 167-190.

Vasilenko, V. I. (2004). The concept and typology of terrorism. *Statutes and Decisions*, *40*(5), 46- 56.

Weimann, G. (2012). Lone wolves in cyberspace. *Journal of Terrorism Research*, 3(2), 75-90.

Weimann, G. (2015). Terrorism in Cyberspace The Next Generation. New York: Columbia University Press.

Yar, M. (2006). Cybercrime and Society. London, Thousand Oaks & New Delhi : SAGE Publications.