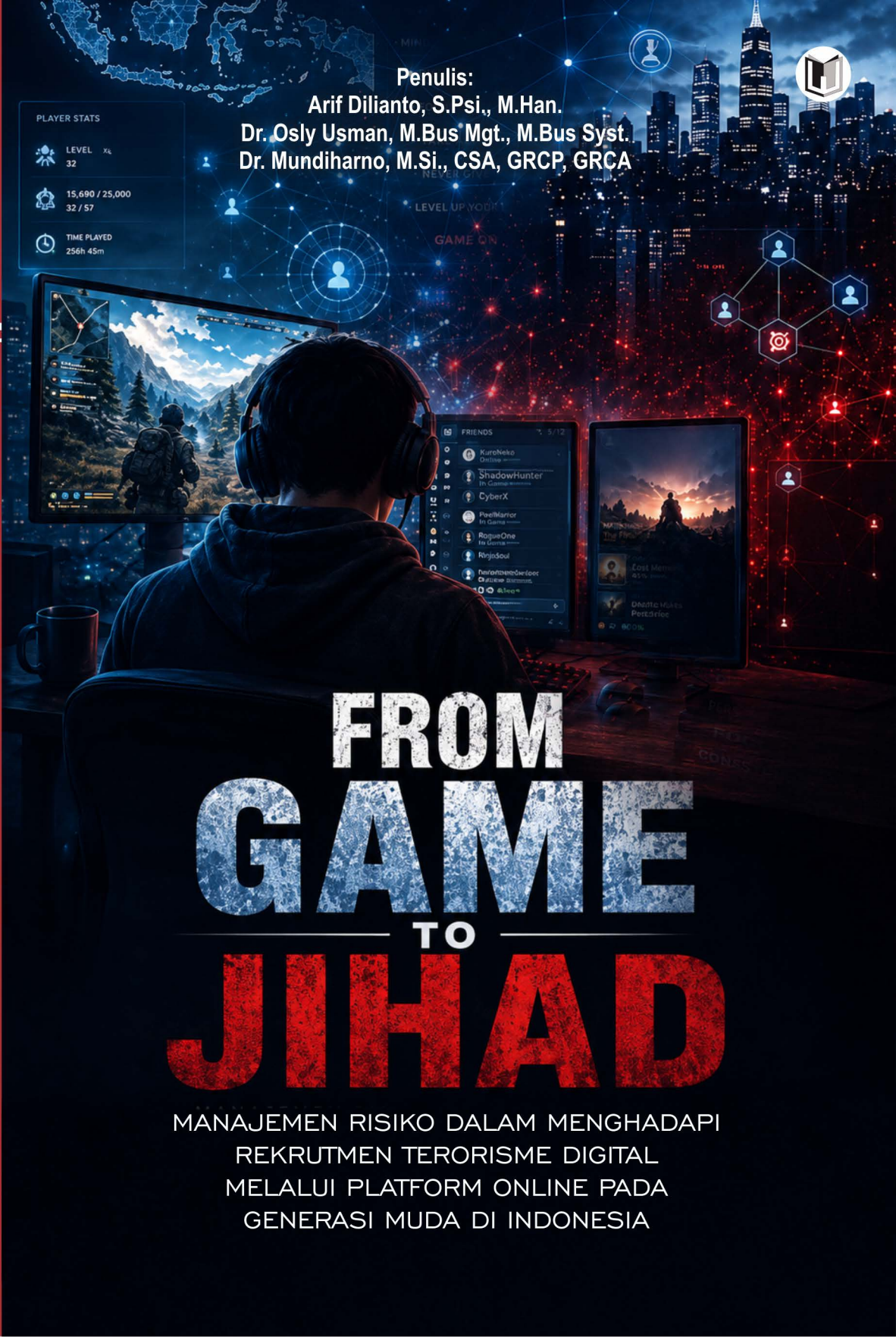




Penulis:

Arif Dilianto, S.Psi., M.Han.

Dr. Osly Usman, M.Bus Mgt., M.Bus Syst.

Dr. Mundiarno, M.Si., CSA, GRCP, GRCA

PLAYER STATS



LEVEL 32



15,690 / 25,000
32 / 57



TIME PLAYED
256h 45m

FROM

GAME

TO

JIHAD

MANAJEMEN RISIKO DALAM MENGHADAPI
REKRUTMEN TERORISME DIGITAL
MELALUI PLATFORM ONLINE PADA
GENERASI MUDA DI INDONESIA

FROM GAME TO JIHAD

MANAJEMEN RISIKO DALAM MENGHADAPI REKRUTMEN
TERORISME DIGITAL MELALUI PLATFORM ONLINE
PADA GENERASI MUDA DI INDONESIA

Penulis:

Arif Dilianto, S.Psi., M.Han.

Dr. Osly Usman, M.Bus Mgt., M.Bus Syst.

Dr. Mundiharno, M.Si., CSA, GRCP, GRCA

**FROM GAME TO JIHAD: MANAJEMEN RISIKO DALAM MENGHADAPI
REKRUTMEN TERORISME DIGITAL MELALUI PLATFORM ONLINE
PADA GENERASI MUDA DI INDONESIA**

Penulis:

**Arif Dilianto, S.Psi., M.Han.
Dr. Osly Usman, M.Bus Mgt., M.Bus Syst.
Dr. Mundiharno, M.Si., CSA, GRCP, GRCA**

Desain Cover:

Helmaria Ulfa

Sumber Ilustrasi:

www.freepik.com

Tata Letak:

Handarini Rohana

Editor:

Neneng Sri Wahyuni

ISBN:

978-634-317-204-8

Cetakan Pertama:

Agustus, 2026

Hak Cipta Dilindungi Oleh Undang-Undang

by Penerbit Widina Media Utama

Dilarang keras menerjemahkan, memfotokopi, atau memperbanyak sebagian atau seluruh isi buku ini tanpa izin tertulis dari Penerbit.

PENERBIT:

WIDINA MEDIA UTAMA

Komplek Puri Melia Asri Blok C3 No. 17 Desa Bojong Emas
Kec. Solokan Jeruk Kabupaten Bandung, Provinsi Jawa Barat

Anggota IKAPI No. 519/JBA/2025

Website: www.penerbitwidina.com

Instagram: [@penerbitwidina](https://www.instagram.com/penerbitwidina)

Telepon (022) 87355370

PRAKATA

Perkembangan teknologi digital telah membawa perubahan besar dalam kehidupan manusia modern. Internet, media sosial, kecerdasan buatan, dan berbagai platform digital telah mengubah cara manusia berkomunikasi, belajar, bekerja, hingga membangun identitas sosialnya. Dunia menjadi semakin terkoneksi tanpa batas, sementara arus informasi bergerak jauh lebih cepat dibandingkan sebelumnya.

Di balik berbagai kemudahan dan peluang yang ditawarkan, perkembangan tersebut juga menghadirkan tantangan baru yang semakin kompleks. Ancaman modern tidak lagi selalu hadir dalam bentuk kekerasan fisik atau konflik konvensional yang terlihat secara langsung, tetapi berkembang melalui ruang digital yang mempengaruhi cara manusia berpikir, merasakan, dan memahami realitas sosial di sekitarnya.

Salah satu tantangan paling serius adalah berkembangnya radikalisasi digital dan pola rekrutmen ekstremisme yang semakin memanfaatkan teknologi modern. Generasi muda menjadi kelompok yang paling rentan karena hidup di tengah budaya hiper-konektivitas, arus informasi tanpa batas, dan ekosistem digital yang sangat dipengaruhi algoritma media sosial.

Fenomena tersebut menunjukkan bahwa persoalan terorisme dan ekstremisme di era digital tidak lagi dapat dipahami hanya melalui pendekatan keamanan konvensional semata. Persoalan ini juga berkaitan erat dengan psikologi sosial, literasi digital, kesehatan emosional, perubahan pola interaksi manusia, hingga manajemen risiko sosial dalam masyarakat modern.

Berangkat dari kegelisahan tersebut, buku *From Game to Jihad: Manajemen Risiko dalam Menghadapi Rekrutmen Terorisme Digital pada Generasi Muda di Indonesia* disusun sebagai upaya untuk memahami transformasi ancaman modern melalui perspektif manajemen risiko dan ketahanan sosial. Buku ini mencoba melihat bahwa ruang digital bukan hanya arena pertukaran informasi, tetapi juga ruang pembentukan identitas, emosi, solidaritas kelompok, dan pengaruh ideologis yang bergerak sangat cepat melintasi batas negara.

Penulis menyadari bahwa perkembangan teknologi digital akan terus berubah dan ancaman masa depan akan semakin kompleks. Karena itu, pendekatan yang dibutuhkan tidak cukup hanya berupa penindakan atau pengawasan semata, tetapi juga pembangunan ketahanan sosial masyarakat, kemampuan berpikir kritis, literasi digital, serta penguatan

nilai-nilai kemanusiaan di tengah dunia yang semakin dipenuhi algoritma dan kecerdasan buatan.

Buku ini tentu masih memiliki berbagai keterbatasan. Namun penulis berharap tulisan ini dapat memberikan kontribusi pemikiran bagi pengembangan kajian keamanan digital, manajemen risiko, serta upaya membangun ketahanan masyarakat Indonesia dalam menghadapi tantangan era digital modern.

Akhir kata, penulis mengucapkan terima kasih kepada semua pihak yang secara langsung maupun tidak langsung memberikan dukungan, pengalaman, inspirasi, dan pemikiran dalam proses penyusunan buku ini. Semoga buku ini dapat memberikan manfaat bagi akademisi, praktisi, institusi, maupun masyarakat luas dalam memahami tantangan keamanan dan kemanusiaan di era digital.

Jakarta, 2026

Penulis

DAFTAR ISI

PRAKATA	iii
DAFTAR ISI	v
BAB 1 DI BALIK LAYAR: KETIKA RUANG DIGITAL	1
1. Dunia Berubah, Ancaman Ikut Berubah	2
2. Generasi Muda dan Kehidupan di Ruang Digital	2
3. Radikalisasi yang Tidak Terasa	3
4. Ketika Risiko Tidak Lagi Terlihat	5
5. Indonesia dan Tantangan Baru	6
6. Mengapa Buku Ini Ditulis	6
7. Penutup Bab	7
8. Daftar Pustaka	7
BAB 2 TERORISME TAK BERWAJAH	9
1. Dari Organisasi ke Ekosistem Digital	11
2. Ketika Hubungan Sosial Menjadi Jalur Pengaruh	11
3. Jaringan yang Fleksibel dan Sulit Dipetakan	12
4. Game Online dan Ruang Baru Radikalisasi	13
5. Radikalisasi yang Tidak Terasa	14
6. Terorisme yang Semakin Sulit Dikenali	14
7. Penutup Bab	15
8. Daftar Pustaka	15
BAB 3 DARI INTERAKSI KE IDEOLOGI: BAGAIMANA RADIKALISASI DIGITAL TERBENTUK	17
1. Dunia Digital dan Kebutuhan untuk Merasa Diterima	18
2. Ketika Interaksi Menjadi Keterikatan	20
3. Algoritma, Echo Chamber, dan Lingkungan Informasi	23
4. Dari Narasi ke Identitas	25
5. Kasus Aktual: Ketika Dunia Virtual Menjadi Ruang Radikalisasi	27
6. Penutup Bab	30
7. Daftar Pustaka	30
BAB 4 RISIKO: LEBIH DARI SEKADAR BAHAYA	33
1. Risiko sebagai Proses yang Berkembang	33
2. Ketidakpastian di Era Digital	36
3. Risiko yang Tumbuh di dalam Ekosistem	38
4. Dari Ancaman Individu ke Systemic Risk	41
5. Mengapa Risiko Digital Sulit Dideteksi	44
6. Membaca Radikalisasi sebagai Developing Risk	46

7. Penutup Bab	48
8. Daftar Pustaka	48
BAB 5 CASCADING RISK: KETIKA RISIKO DIGITAL	
MENYEBAR TANPA BATAS	51
1. Ketika Algoritma Memperbesar Ancaman	53
2. Dari Konten ke Mobilisasi	56
3. Risiko yang Menyebar ke Antarplatform	59
4. Ketika Risiko Menjadi Normal	61
5. Mengapa Cascading Risk Sulit Dihentikan?	64
6. Penutup Bab	66
7. Daftar Pustaka	67
BAB 6 MANAJEMEN RISIKO RADIKALISASI DIGITAL:	
MEMBACA, MEMETAKAN, DAN MENGELOLA ANCAMAN	69
1. Memahami Manajemen Risiko di Era Digital	70
2. ISO 31000 dan Relevansinya terhadap Radikalisasi Digital	72
3. Identifikasi Risiko: Membaca Tanda Awal Radikalisasi	75
4. Analisis Risiko: Memahami Interaksi Ancaman dalam Ekosistem Digital	78
5. Evaluasi Risiko: Menentukan Tingkat Ancaman dan Prioritas	80
6. Mitigasi Risiko: Dari Reaksi ke Pencegahan	83
7. Monitoring Risiko dan Early Detection di Era Digital	86
8. Risk Governance: Mengelola Risiko secara Sistemik	89
9. Digital Extremism Risk Register: Menerjemahkan Ancaman Menjadi Risiko yang Dapat Dikelola	92
10. Membangun Ketahanan Sosial Digital	97
11. Indonesia dan Tantangan Manajemen Risiko Digital	100
12. Penutup Bab	103
13. Daftar Pustaka	103
BAB 7 STRATEGI MITIGASI DAN PENCEGAHAN	
RISIKO RADIKALISASI DIGITAL	105
1. Literasi Digital sebagai Benteng	107
2. Ketahanan Emosional dan Psikologis Generasi Muda	110
3. Keluarga sebagai Sistem Deteksi dan Ketahanan	113
4. Pendidikan Sebagai Strategi Pencegahan	115
5. Counter Narrative dan Tantangan Komunikasi Digital	118
6. Membangun Positive Digital Ecosystem	120
7. Kolaborasi Multiaktor dalam Pencegahan Risiko	123
8. Indonesia dan Tantangan Pencegahan di Era Digital	126
9. Penutup Bab	128
10. Daftar Pustaka	129

BAB 8 RISK GOVERNANCE DAN STRATEGI NASIONAL DI ERA DIGITAL ...	131
1. Negara di Tengah Perubahan Ekosistem Digital.....	133
2. Platform Digital dan Kekuatan Algoritma.....	135
3. Regulasi Digital dan Dilema Kebebasan	138
4. Artificial Intelligence, Big Data, dan Monitoring Risiko	140
5. Strategi Nasional Indonesia dalam Pencegahan Ekstremisme Digital	143
6. Kolaborasi Negara, Platform, dan Masyarakat.....	145
7. Tantangan Implementasi Risk Governance di Indonesia	148
8. Menuju Adaptive Risk Governance	151
9. Penutup Bab	153
10. Daftar Pustaka	154
BAB 9 MASA DEPAN RISIKO DIGITAL.....	157
1. Deepfake, Synthetic Media, dan Krisis Kepercayaan	160
2. Metaverse, Virtual Community, dan Identitas Baru.....	162
3. Generasi Muda dan Masa Depan Kerentanan Digital	164
4. Ketahanan Sosial sebagai Fondasi Keamanan Masa Depan.....	167
5. Menuju Human-Centered Digital Governance.....	170
6. Refleksi: Menjaga Manusia di Tengah Dunia Digital	172
7. Penutup Bab	175
8. Daftar Pustaka	175
GLOSARIUM.....	177
TENTANG PENULIS	183

BAB 1

DI BALIK LAYAR: KETIKA RUANG DIGITAL MENJADI PINTU MASUK IDEOLOGI



Suatu malam, seorang remaja duduk di depan layar komputer. Ia tidak sedang membaca manifesto ideologi, tidak menghadiri pertemuan rahasia, dan tidak berada dalam lingkungan yang tampak berbahaya. Ia hanya bermain game online seperti jutaan anak muda lain di seluruh dunia.

Di dalam permainan itu, ia berbicara dengan orang-orang yang belum pernah ditemuinya. Mereka bermain bersama, bercanda, saling membantu menyelesaikan misi, lalu perlahan mulai berbagi cerita di luar permainan. Percakapan berkembang dari strategi game menjadi kehidupan pribadi, dari kehidupan pribadi menjadi keresahan sosial, lalu perlahan menyentuh isu identitas, ketidakadilan, dan kemarahan terhadap dunia.

keamanan, sosiologi digital, analisis perilaku, dan manajemen risiko modern berbasis ISO 31000.

Fokus utamanya bukan hanya pada aksi teror, tetapi pada proses bagaimana pengaruh terbentuk, berkembang, dan menyebar di ruang digital.

Karena memahami ancaman hari ini berarti memahami dunia tempat ancaman itu tumbuh.

Penutup Bab

Di era digital, ancaman tidak selalu datang dalam bentuk yang mudah dikenali. Ia tidak selalu hadir sebagai organisasi besar atau propaganda yang terbuka. Kadang ia tumbuh melalui percakapan biasa, hubungan pertemanan, dan komunitas yang tampak normal.

Di sinilah tantangan terbesar kita hari ini.

Bagaimana mengenali sesuatu yang tidak terlihat sebagai ancaman? Bagaimana memahami proses yang berkembang secara perlahan di balik layar yang setiap hari kita gunakan?

Untuk menjawab pertanyaan tersebut, kita perlu memahami terlebih dahulu bagaimana terorisme itu sendiri telah berubah di era digital.

Bab berikutnya akan membahas transformasi bagaimana terorisme berkembang dari organisasi yang kaku menjadi jaringan yang lebih fleksibel, lebih tersembunyi, dan lebih sulit dipetakan.

DAFTAR PUSTAKA

- Aly, A., Macdonald, S., Jarvis, L., & Chen, T. M. (2017). *Violent extremism online: New perspectives on terrorism and the internet*. Routledge.
- Badan Nasional Penanggulangan Terorisme. (2024). *Counter terrorism and violent extremism outlook 2024*. BNPT.
- Badan Nasional Penanggulangan Terorisme. (2025). *Penyebaran paham radikal di ruang digital masif terjadi*. BNPT.
- Badan Nasional Penanggulangan Terorisme. (2026). *BNPT dukung penuh PP TUNAS sebagai benteng perlindungan anak dari radikalisme digital*. BNPT.
- Berger, J. M. (2018). *Extremism*. MIT Press.
- Cinelli, M., Morales, G. D. F., Galeazzi, A., Quattrociocchi, W., & Starnini, M. (2021). The echo chamber effect on social media. *Proceedings of the National Academy of Sciences*, 118(9), 1–8.
- Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research. *Studies in Conflict & Terrorism*, 40(1), 77–98.

- Europol. (2023). *European Union terrorism situation and trend report (TE-SAT) 2023*. Europol.
- Hopkin, P. (2018). *Fundamentals of risk management* (5th ed.). Kogan Page.
- International Organization for Standardization. (2018). *ISO 31000: Risk management—Guidelines*. ISO.
- Neumann, P. R. (2013). The trouble with radicalization. *International Affairs*, 89(4), 873–893.
- Renn, O. (2008). *Risk governance: Coping with uncertainty in a complex world*. Earthscan.
- The Soufan Center. (2025). *The online radicalization of youth remains a growing global threat*. The Soufan Center.
- United Nations Interregional Crime and Justice Research Institute. (2026). *The prevention of violent extremism and online gaming*. UNICRI.
- United Nations Office of Counter-Terrorism. (2024). *Countering terrorist narratives in digital environments*. UNOCT.
- United Nations Office on Drugs and Crime. (2023). *The use of the internet for terrorist purposes*. UNODC.
- Weimann, G. (2016). *Terrorism in cyberspace: The next generation*. Columbia University Press.
- Winter, C. (2020). *The digital caliphate: Terrorist propaganda and online radicalization in the digital age*. Routledge.

BAB 2

TERORISME TAK BERWAJAH



Ancaman hari ini tidak selalu datang dengan wajah yang mudah dikenali.

Jika pada masa lalu terorisme identik dengan organisasi bersenjata, kamp pelatihan tersembunyi, pertemuan rahasia, dan jaringan yang terstruktur rapi, maka perkembangan teknologi digital telah mengubah hampir seluruh pola tersebut. Ancaman tidak lagi selalu bergerak melalui struktur organisasi yang kaku, tetapi berkembang melalui ruang-ruang sosial digital yang justru terasa sangat akrab bagi masyarakat modern.

Perubahan ini terjadi seiring berubahnya cara manusia hidup dan berinteraksi. Internet yang awalnya hanya dipandang sebagai alat komunikasi kini telah berkembang menjadi ruang sosial baru. Di dalamnya, orang membangun relasi, mencari hiburan, membentuk identitas, hingga menemukan komunitas yang memberi rasa diterima. Media sosial, platform video, forum digital, dan game online tidak lagi sekadar teknologi, tetapi

Pertanyaan-pertanyaan ini menunjukkan bahwa memahami terorisme digital tidak cukup hanya dengan pendekatan keamanan konvensional. Diperlukan cara pandang yang mampu melihat ancaman sebagai proses sosial yang berkembang di dalam ekosistem digital modern.

Penutup Bab

Terorisme di era digital tidak lagi selalu memiliki wajah yang jelas.

Ia tidak selalu hadir dalam bentuk organisasi besar atau propaganda terbuka. Ia berkembang melalui hubungan sosial, komunitas digital, dan interaksi yang tampak biasa.

Di sinilah letak kompleksitas ancaman modern: ideologi bergerak di ruang yang justru terasa paling normal bagi generasi muda.

Ketika pengaruh dibangun melalui rasa diterima, rasa dimengerti, dan keterikatan sosial, maka proses radikalisasi menjadi jauh lebih sulit dikenali dibandingkan sebelumnya.

Untuk memahami bagaimana proses tersebut benar-benar bekerja, kita perlu melihat lebih dalam pada mekanisme yang terjadi di tingkat individu bagaimana interaksi digital perlahan membentuk keyakinan dan identitas.

Bab berikutnya akan membahas hal tersebut: bagaimana proses radikalisasi digital berkembang dari interaksi sederhana menjadi perubahan cara berpikir yang lebih dalam.

DAFTAR PUSTAKA

- Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism. *Studies in Conflict & Terrorism*, 40(1), 77–98.
- Neumann, P. R. (2013). The trouble with radicalization. *International Affairs*, 89(4), 873–893.
- The Guardian. (2025). *Far-right extremists using games platforms to radicalise teenagers, report warns*.
- Weimann, G. (2016). *Terrorism in cyberspace: The next generation*. Columbia University Press.

BAB 3

DARI INTERAKSI KE IDEOLOGI: BAGAIMANA RADIKALISASI DIGITAL TERBENTUK

Perubahan cara berpikir manusia hampir tidak pernah terjadi secara tiba-tiba.

Tidak ada garis yang benar-benar jelas antara seseorang yang “biasa” dan seseorang yang mulai bergerak menuju pola pikir ekstrem. Dalam banyak kasus, perubahan itu berlangsung perlahan-lahan hingga sering tidak disadari oleh orang yang mengalaminya sendiri.

Awalnya mungkin hanya rasa ingin tahu.

Seseorang melihat satu video, membaca satu komentar, atau bergabung dalam satu komunitas online karena merasa tertarik dengan topik tertentu. Tidak ada niat untuk menjadi radikal. Tidak ada keinginan melakukan kekerasan. Yang ada hanyalah interaksi kecil yang tampak tidak berarti.

Namun dunia digital bekerja dengan cara yang berbeda dibandingkan dunia nyata.

Di ruang digital, manusia tidak hanya menerima informasi, tetapi terus-menerus hidup di dalam arus informasi. Apa yang dilihat hari ini akan mempengaruhi apa yang dilihat besok. Apa yang disukai akan menentukan lingkungan digital yang mengelilinginya. Sedikit demi sedikit, algoritma mulai membentuk pola konsumsi informasi seseorang.

Pada titik tertentu, individu tidak lagi sekadar mencari informasi, ia mulai hidup di dalam lingkungan informasi tertentu.

Di sinilah proses radikalisasi modern menjadi sangat kompleks.

Perubahan tidak terjadi melalui satu doktrin besar, tetapi melalui akumulasi pengalaman digital yang berlangsung terus-menerus. Percakapan kecil, video pendek, meme, forum diskusi, hingga komunitas online perlahan membentuk cara seseorang memahami dunia.

Ancaman tidak lagi bergerak terutama melalui struktur organisasi yang terlihat, tetapi melalui hubungan sosial virtual yang berkembang perlahan di dalam kehidupan sehari-hari generasi muda.

Dan ketika dunia virtual telah berubah menjadi ruang pembentukan identitas, maka pengaruh ideologis tidak lagi datang dari luar kehidupan manusia tetapi tumbuh dari ruang yang setiap hari mereka tinggali.

Penutup Bab

Radikalisasi digital tidak terjadi secara tiba-tiba. Ia tumbuh perlahan melalui interaksi sehari-hari, hubungan sosial virtual, dan lingkungan digital yang terus memperkuat cara berpikir tertentu.

Di era digital, pengaruh ideologis tidak selalu masuk melalui doktrin yang keras, tetapi melalui rasa diterima, keterikatan komunitas, dan kebutuhan manusia untuk merasa memiliki tempat. Ketika hubungan emosional mulai terbentuk di ruang digital, maka narasi perlahan dapat berubah menjadi identitas.

Inilah yang membuat ancaman modern menjadi jauh lebih kompleks. Terorisme tidak lagi hanya bergerak melalui organisasi formal, tetapi melalui komunitas online, algoritma, dan interaksi digital yang menjadi bagian dari kehidupan sehari-hari generasi muda.

Seseorang tidak merasa sedang direkrut. Ia justru merasa sedang menemukan lingkungan yang memahami dirinya.

Karena itu, memahami radikalisasi digital berarti memahami bagaimana manusia, teknologi, dan lingkungan informasi saling mempengaruhi dalam membentuk cara berpikir.

Bab berikutnya akan membahas fenomena tersebut melalui perspektif manajemen risiko, untuk melihat bagaimana radikalisasi digital berkembang sebagai risiko yang tumbuh secara bertahap di dalam ekosistem digital modern.

DAFTAR PUSTAKA

- Baumeister, R. F., & Leary, M. R. (1995). The need to belong: Desire for interpersonal attachments as a fundamental human motivation. *Psychological Bulletin*, 117(3), 497–529.
- Cinelli, M., Morales, G. D. F., Galeazzi, A., Quattrociocchi, W., & Starnini, M. (2021). The echo chamber effect on social media. *Proceedings of the National Academy of Sciences*, 118(9), 1–8.
- Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research. *Studies in Conflict & Terrorism*, 40(1), 77–98.

- Europol. (2023). European Union terrorism situation and trend report (TE-SAT) 2023. Europol.
- Kruglanski, A. W., Gelfand, M., Bélanger, J. J., Sheveland, A., Hetiarachchi, M., & Gunaratna, R. (2014). The psychology of radicalization and deradicalization: How significance quest impacts violent extremism. *Political Psychology*, 35(S1), 69–93.
- Neumann, P. R. (2013). The trouble with radicalization. *International Affairs*, 89(4), 873–893.
- Pariser, E. (2011). *The filter bubble: What the Internet is hiding from you*. Penguin Press.
- Reuters. (2026). White supremacist content grips teens plotting attacks in Southeast Asia. Reuters.
- The Soufan Center. (2025). The online radicalization of youth remains a growing global threat. The Soufan Center.
- Weimann, G. (2016). *Terrorism in cyberspace: The next generation*. Columbia University Press.

BAB 4

RISIKO: LEBIH DARI SEKADAR BAHAYA

Selama ini, banyak orang memahami risiko sebagai sesuatu yang identik dengan bahaya.

Ketika mendengar kata “risiko”, yang muncul di pikiran biasanya adalah ancaman, kerugian, bencana, atau sesuatu yang harus dihindari. Dalam konteks terorisme, risiko sering dipahami hanya sebagai kemungkinan terjadinya serangan atau aksi kekerasan.

Padahal risiko jauh lebih kompleks daripada sekadar peristiwa akhir.

Dalam dunia modern, risiko sebenarnya lebih tepat dipahami sebagai proses yang berkembang perlahan di bawah permukaan. Risiko tumbuh melalui hubungan sebab-akibat yang sering kali tidak terlihat secara langsung. Ia bergerak melalui akumulasi kondisi, kelemahan sistem, perubahan perilaku, dan lingkungan yang memungkinkan ancaman berkembang.

Karena itu, aksi teror sebenarnya bukan awal dari risiko.

Ia justru sering menjadi titik akhir dari risiko yang gagal dikenali sejak awal.

Risiko sebagai Proses yang Berkembang

Banyak orang membayangkan risiko sebagai sesuatu yang muncul secara tiba-tiba.

Ledakan bom dianggap sebagai risiko. Serangan teror dianggap sebagai risiko. Padahal dalam perspektif manajemen risiko modern, peristiwa seperti itu sebenarnya lebih tepat disebut sebagai hasil akhir dari proses risiko yang telah berkembang jauh sebelumnya.

Inilah perbedaan paling mendasar antara melihat risiko sebagai “kejadian” dan melihat risiko sebagai “proses”.

Dalam kehidupan sehari-hari, manusia cenderung baru menyadari risiko ketika dampaknya sudah terlihat. Ketika serangan terjadi, ketika korban mulai berjatuhan, atau ketika krisis mulai muncul ke permukaan. Namun

Pendekatan ini membuka kemungkinan intervensi yang jauh lebih awal. Bukan ketika kekerasan sudah terjadi, tetapi ketika:

lingkungan informasi mulai menyempit, keterikatan emosional mulai terbentuk, atau identitas mulai dibangun di atas narasi yang terus memperkuat polarisasi dan kebencian.

Di sinilah manajemen risiko memiliki peran yang sangat penting.

Karena inti dari manajemen risiko bukan sekadar menghentikan ancaman yang sudah terlihat, tetapi memahami bagaimana ancaman tumbuh sebelum mencapai titik yang sulit dikendalikan.

Dan dalam konteks radikalisasi digital, memahami proses perkembangan risiko sering kali jauh lebih penting dibandingkan hanya memahami tindakan akhirnya.

Penutup Bab

Radikalisasi digital tidak lahir sebagai ancaman yang langsung terlihat. Ia berkembang perlahan di dalam ekosistem digital melalui interaksi sosial, algoritma, komunitas online, dan perubahan cara berpikir yang sering tidak disadari.

Karena itu, memahami terorisme digital tidak cukup hanya melihat aksi kekerasannya. Yang jauh lebih penting adalah memahami bagaimana risiko tumbuh sebelum ancaman muncul di permukaan.

Di era digital, risiko berkembang secara dinamis, saling terhubung, dan sering tersembunyi di balik aktivitas yang tampak normal. Inilah yang membuat pendekatan manajemen risiko menjadi sangat penting—bukan hanya untuk merespons krisis, tetapi untuk membaca proses pembentukan ancaman sejak tahap awal.

Bab berikutnya akan membahas bagaimana risiko digital berkembang sebagai rantai yang saling terhubung dan mampu menciptakan efek berantai (cascading risk) dalam ekosistem digital modern.

DAFTAR PUSTAKA

- Conway, M. (2017). Determining the role of the internet in violent extremism and terrorism: Six suggestions for progressing research. *Studies in Conflict & Terrorism*, 40(1), 77–98.
- Europol. (2023). European Union terrorism situation and trend report (TE-SAT) 2023. Europol.
- Hopkin, P. (2018). *Fundamentals of risk management* (5th ed.). Kogan Page.
- International Organization for Standardization. (2018). *ISO 31000: Risk management—Guidelines*. ISO.

- Renn, O. (2008). Risk governance: Coping with uncertainty in a complex world. Earthscan.
- Weimann, G. (2016). Terrorism in cyberspace: The next generation. Columbia University Press.

BAB 5

CASCADING RISK: KETIKA RISIKO DIGITAL MENYEBAR TANPA BATAS

Di era digital, risiko tidak lagi bergerak secara perlahan dan terisolasi. Risiko menyebar dengan kecepatan yang belum pernah terjadi sebelumnya, melintasi batas geografis, sosial, bahkan psikologis manusia hanya dalam hitungan detik.

Satu unggahan dapat memicu gelombang kemarahan massal.

Satu video dapat membentuk opini jutaan orang.

Satu komunitas online dapat mempengaruhi perilaku generasi muda lintas negara tanpa pernah bertemu secara fisik.

Ini adalah wajah baru ancaman modern.

Dunia digital menciptakan lingkungan yang sangat terkoneksi. Ketika satu bagian sistem terganggu, dampaknya dapat menjalar dengan cepat ke bagian lain melalui jaringan sosial, algoritma platform, dan interaksi manusia yang terus berlangsung tanpa henti. Dalam konteks manajemen risiko, kondisi seperti ini dikenal sebagai cascading risk, risiko yang tidak berhenti pada satu titik, tetapi berkembang menjadi rangkaian dampak yang saling memperbesar.

Di sinilah ancaman digital berbeda dibandingkan ancaman konvensional.

Pada masa lalu, dampak sebuah peristiwa biasanya lebih terbatas oleh ruang dan waktu. Informasi bergerak lebih lambat, pengaruh lebih lokal, dan penyebaran ideologi membutuhkan struktur organisasi yang relatif jelas.

Namun internet mengubah seluruh pola tersebut.

Hari ini, dunia digital bekerja seperti sistem yang saling terhubung tanpa batas. Ketika satu narasi viral, algoritma mulai memperluas jangkauannya. Komunitas online memperkuat pesan tersebut melalui komentar, diskusi, dan distribusi ulang. Media sosial mempercepat

Hopkin (2018) menjelaskan bahwa risiko modern sering berkembang secara non-linear, di mana dampak kecil dapat menghasilkan konsekuensi besar melalui proses penguatan yang terus berulang. Dalam konteks digital, proses ini terjadi sangat cepat karena teknologi memungkinkan distribusi informasi berlangsung hampir tanpa hambatan.

Inilah yang membuat cascading risk memiliki karakter seperti efek domino yang tidak berhenti pada satu titik.

Satu narasi memicu polarisasi.

Polarisasi memperkuat identitas kelompok.

Identitas memperbesar keterikatan komunitas.

Komunitas memperluas distribusi narasi baru.

Dan siklus tersebut terus berulang di dalam ekosistem digital.

Yang paling mengkhawatirkan, banyak proses tersebut berjalan secara otomatis dan nyaris tidak terlihat. Masyarakat sering baru menyadari ancaman ketika dampaknya sudah muncul di dunia nyata:

aksi kekerasan, mobilisasi massa, atau meningkatnya fragmentasi sosial.

Padaahal proses pembentukan risikonya telah berlangsung lama sebelumnya.

Karena itu, tantangan utama di era digital bukan hanya menghentikan satu ancaman, tetapi memahami bagaimana sistem digital memungkinkan risiko terus bereproduksi dan menyebar secara berantai.

Di sinilah manajemen risiko modern menjadi sangat penting.

Pendekatan keamanan tidak lagi cukup hanya berfokus pada pelaku atau konten tertentu. Yang perlu dikelola adalah:

lingkungan digital, pola interaksi sosial, algoritma distribusi informasi, dan ketahanan sosial masyarakat terhadap polarisasi dan manipulasi digital.

Karena selama ekosistem digital masih terus memperkuat keterhubungan tanpa pengelolaan risiko yang memadai, maka cascading risk akan selalu memiliki kemampuan untuk tumbuh kembali dalam bentuk yang baru.

Penutup Bab

Ancaman berkembang melalui jaringan sosial, algoritma, komunitas online, dan platform digital yang saling terhubung satu sama lain.

Inilah yang membuat cascading risk menjadi sangat berbahaya. Satu narasi dapat memicu polarisasi, memperkuat identitas kelompok, lalu berkembang menjadi mobilisasi yang jauh lebih besar melalui efek domino digital.

Risiko modern tidak hanya menyebar lebih cepat, tetapi juga lebih adaptif dan sulit dihentikan. Ketika satu ruang ditutup, pengaruh berpindah ke ruang lain. Ketika satu akun dihapus, komunitas muncul kembali dalam bentuk baru.

Karena itu, menghadapi radikalisi digital tidak cukup hanya dengan pendekatan keamanan konvensional. Yang diperlukan adalah kemampuan memahami bagaimana risiko tumbuh, menyebar, dan diperkuat oleh ekosistem digital modern.

Bab berikutnya akan membahas bagaimana prinsip manajemen risiko dapat digunakan untuk membaca, memetakan, dan mengelola ancaman radikalisi digital secara lebih sistematis.

DAFTAR PUSTAKA

- Brookings Institution. (2023). *Digital emotional acceleration and online polarization*. Brookings Institution Press.
- Center for Countering Digital Hate. (2024). *Algorithms and the amplification of extremist content on social media*. CCDH.
- Europol. (2023). *European Union terrorism situation and trend report 2023*. Europol.
- Hopkin, P. (2018). *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management* (5th ed.). Kogan Page.
- Kruglanski, A. W., Gelfand, M., Bélanger, J. J., Sheveland, A., Hetiarachchi, M., & Gunaratna, R. (2014). The psychology of radicalization and deradicalization: How significance quest impacts violent extremism. *Political Psychology*, 35(S1), 69–93.
- Renn, O. (2008). *Risk governance: Coping with uncertainty in a complex world*. Earthscan.
- The Soufan Center. (2024). *Digital extremism and online radicalization trends 2024*. The Soufan Center.
- UNESCO. (2023). *Addressing hate speech and online extremism in the digital age*. UNESCO.
- United Nations Office of Counter-Terrorism. (2023). *Whole-of-society approaches to preventing violent extremism in the digital era*. UNOCT.
- United Nations Office on Drugs and Crime. (2022). *The use of the internet for terrorist purposes*. UNODC.

BAB 6

MANAJEMEN RISIKO RADIKALISASI DIGITAL: MEMBACA, MEMETAKAN, DAN MENGELOLA ANCAMAN

Ancaman modern tidak lagi selalu hadir dalam bentuk yang keras dan mudah dikenali. Ia justru sering tumbuh secara perlahan di ruang-ruang yang dianggap biasa oleh masyarakat. Melalui media sosial, komunitas online, forum permainan, hingga percakapan virtual sehari-hari, pengaruh dapat berkembang tanpa terasa sebagai ancaman. Yang bergerak bukan hanya ideologi, tetapi juga emosi, identitas, kebutuhan untuk diterima, dan rasa ingin memiliki tempat di tengah kehidupan yang semakin terkoneksi namun sering terasa asing secara sosial.

Inilah yang membuat terorisme digital menjadi jauh lebih kompleks dibandingkan pola ancaman konvensional. Proses radikalisasi tidak selalu dimulai dari doktrin keras atau pertemuan rahasia. Banyak individu awalnya hanya mencari hiburan, komunitas, atau ruang untuk mengekspresikan diri. Namun sedikit demi sedikit, lingkungan informasi yang terus berulang dapat membentuk cara pandang tertentu terhadap dunia. Ketika seseorang terus hidup di dalam narasi yang sama, menerima validasi dari komunitas yang sama, dan melihat realitas melalui sudut pandang yang semakin sempit, maka perubahan cara berpikir dapat berkembang tanpa disadari.

Karena itu, pendekatan keamanan semata tidak lagi memadai untuk membaca ancaman semacam ini. Menangkap pelaku atau menutup akun memang penting, tetapi langkah tersebut sering dilakukan ketika proses pengaruh sudah berkembang cukup jauh. Padahal ancaman sebenarnya tumbuh jauh sebelumnya di dalam pola interaksi, keterikatan emosional, dan lingkungan digital yang perlahan membentuk identitas seseorang.

Sebab pada akhirnya, ancaman digital bukan hanya tentang teknologi yang semakin canggih, tetapi tentang bagaimana manusia hidup, berpikir, dan membangun identitas di dalam dunia yang terus terkoneksi tanpa batas.

Dan di tengah perubahan sebesar itu, kemampuan Indonesia membangun ketahanan sosial digital akan menentukan apakah transformasi digital menjadi kekuatan nasional atau justru berkembang menjadi ruang kerentanan baru bagi masyarakatnya sendiri.

Penutup Bab

Radikalisasi digital menunjukkan bahwa ancaman modern tidak lagi berkembang secara sederhana. Risiko tumbuh melalui interaksi antara teknologi, algoritma, komunitas online, kondisi psikologis manusia, dan lingkungan sosial yang terus berubah. Karena itu, pendekatan keamanan semata tidak lagi cukup untuk menghadapi ancaman yang bergerak secara cair dan sistemik di dalam ruang digital.

Melalui perspektif manajemen risiko, ancaman dipahami bukan hanya sebagai tindakan akhir, tetapi sebagai proses yang berkembang secara perlahan melalui kerentanan, paparan informasi, dan keterikatan sosial digital. Pendekatan ini membantu membaca tanda awal, memahami interaksi ancaman, menentukan prioritas risiko, hingga membangun strategi mitigasi dan ketahanan sosial secara lebih menyeluruh.

Pada akhirnya, tantangan terbesar bukan hanya menghentikan ekstremisme, tetapi membangun masyarakat yang mampu bertahan terhadap manipulasi, polarisasi, dan tekanan informasi di tengah ekosistem digital yang semakin kompleks.

Karena di dunia yang semakin terkoneksi, keamanan masa depan tidak hanya ditentukan oleh kemampuan menghadapi ancaman, tetapi oleh kemampuan memahami bagaimana risiko tumbuh di dalam kehidupan digital manusia modern.

DAFTAR PUSTAKA

- APJII. (2024). *Survei penetrasi internet Indonesia 2024*. Asosiasi Penyelenggara Jasa Internet Indonesia.
- Europol. (2023). *European Union terrorism situation and trend report 2023*. Europol.
- Hopkin, P. (2018). *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management* (5th ed.). Kogan Page.
- ISO. (2018). *ISO 31000: Risk management—Guidelines*. International Organization for Standardization.

- Kruglanski, A. W., Gelfand, M., Bélanger, J. J., Sheveland, A., Hetiarachchi, M., & Gunaratna, R. (2014). The psychology of radicalization and deradicalization: How significance quest impacts violent extremism. *Political Psychology*, 35(S1), 69–93.
- Renn, O. (2008). *Risk governance: Coping with uncertainty in a complex world*. Earthscan.
- UNESCO. (2023). *Addressing hate speech and online extremism in the digital age*. UNESCO.

BAB 7

STRATEGI MITIGASI DAN PENCEGAHAN RISIKO RADIKALISASI DIGITAL

Perubahan pola ancaman digital memaksa negara dan masyarakat mengubah cara pandang terhadap keamanan. Ancaman tidak lagi selalu muncul dalam bentuk aksi yang mudah dikenali, melainkan tumbuh perlahan di dalam kehidupan digital sehari-hari. Pengaruh berkembang melalui media sosial, komunitas online, algoritma, dan hubungan virtual yang terus membentuk cara manusia berpikir tanpa disadari.

Dalam kondisi seperti itu, respons yang hanya berfokus pada penindakan sering datang terlambat.

Ketika aparat keamanan berhasil menemukan pelaku, membubarkan jaringan, atau memblokir propaganda tertentu, proses radikalisis biasanya telah berlangsung cukup lama sebelumnya. Perubahan cara pandang, keterikatan emosional terhadap komunitas digital, hingga pembentukan identitas kelompok sering berkembang jauh sebelum ancaman terlihat di permukaan.

Ini yang membuat pendekatan pencegahan menjadi semakin penting.

Penindakan memang mampu menghentikan dampak langsung dari ancaman. Namun pencegahan berusaha mengurangi kemungkinan ancaman itu tumbuh sejak awal. Fokusnya bukan hanya pada siapa yang melakukan tindakan ekstrem, tetapi pada bagaimana kerentanan berkembang di dalam masyarakat digital modern.

Pendekatan seperti ini mengubah cara memahami keamanan.

Ancaman tidak lagi dilihat semata sebagai persoalan pelaku dan aksi, tetapi sebagai hasil dari interaksi panjang antara teknologi, emosi manusia, lingkungan sosial, dan budaya digital. Seseorang bisa saja terlihat menjalani aktivitas normal bermain game, aktif di media sosial, bergabung dalam komunitas online tetapi perlahan hidup di dalam lingkungan informasi yang semakin tertutup dan emosional.

Iniilah yang membuat strategi pencegahan di Indonesia tidak dapat disamakan dengan negara lain secara sederhana.

Pendekatan keamanan saja tidak cukup.

Pendekatan teknologi saja juga tidak cukup.

Yang dibutuhkan adalah strategi pencegahan yang memahami karakter sosial masyarakat Indonesia:

budaya komunal yang kuat, pengaruh agama dan komunitas lokal, dominasi media sosial dalam kehidupan sehari-hari, serta pentingnya hubungan sosial dalam membentuk identitas generasi muda.

Karena itu, pencegahan harus bergerak secara multidimensional.

Pendidikan membangun kemampuan berpikir kritis.

Keluarga membangun ketahanan emosional.

Komunitas menciptakan ruang sosial yang sehat.

Media membangun kualitas informasi publik.

Dan negara menciptakan tata kelola digital yang adaptif terhadap perubahan zaman.

Seluruh elemen tersebut harus berjalan bersama.

Yang paling penting, Indonesia perlu membangun ketahanan sosial digital sebagai bagian dari ketahanan nasional modern.

Ancaman terbesar masa depan mungkin bukan hanya serangan fisik, tetapi fragmentasi sosial yang berkembang perlahan melalui ruang digital. Ketika masyarakat semakin mudah terpecah, saling curiga, dan kehilangan kemampuan berdialog secara sehat, maka ruang bagi ekstremisme akan menjadi semakin besar.

Karena itu, tantangan pencegahan di Indonesia pada akhirnya bukan sekadar menghentikan propaganda digital, tetapi menjaga agar transformasi teknologi tidak menghilangkan kohesi sosial, empati, dan kemampuan masyarakat untuk tetap hidup bersama di tengah perbedaan.

Sebab di era digital, keamanan nasional bukan hanya tentang melindungi wilayah negara, tetapi juga tentang menjaga stabilitas cara berpikir dan hubungan sosial masyarakat di dalam ruang digital yang terus bergerak tanpa batas.

Penutup Bab

Pencegahan radikalisasi digital tidak dapat dilakukan hanya melalui penindakan keamanan atau penghapusan konten ekstrem. Ancaman modern berkembang melalui proses sosial, emosional, dan digital yang jauh lebih kompleks. Karena itu, strategi mitigasi harus berfokus pada pengurangan kerentanan dan pembangunan ketahanan masyarakat sejak tahap awal.

Literasi digital, ketahanan emosional generasi muda, peran keluarga, pendidikan, komunitas sosial, hingga kolaborasi lintas sektor menjadi bagian penting dalam membangun ruang digital yang lebih sehat dan resilien. Sebab pada akhirnya, ekstremisme tumbuh bukan hanya karena adanya propaganda, tetapi karena adanya ruang sosial dan psikologis yang memungkinkan propaganda tersebut diterima.

Di tengah dunia yang semakin terkoneksi, pencegahan terbaik bukan hanya membatasi ancaman, tetapi membangun manusia dan masyarakat yang tidak mudah kehilangan nalar, identitas, dan empati di tengah arus informasi yang terus bergerak tanpa batas.

DAFTAR PUSTAKA

- American Academy of Pediatrics. (2024). *Social media and youth mental health advisory*. AAP.
- American Psychological Association. (2023). *Health advisory on social media use in adolescence*. APA.
- APJII. (2024). *Survei penetrasi internet Indonesia 2024*. Asosiasi Penyelenggara Jasa Internet Indonesia.
- Benkler, Y., Faris, R., & Roberts, H. (2018). *Network propaganda: Manipulation, disinformation, and radicalization in American politics*. Oxford University Press.
- Borum, R. (2011). Radicalization into violent extremism I: A review of social science theories. *Journal of Strategic Security*, 4(4), 7–36.
- Braddock, K., & Horgan, J. (2016). Towards a guide for constructing and disseminating counter-narratives to reduce support for terrorism. *Studies in Conflict & Terrorism*, 39(5), 381–404.
- Center for Humane Technology. (2021). *The social dilemma and digital well-being report*. CHT.
- Europol. (2023). *European Union terrorism situation and trend report 2023*. Europol.
- Freire, P. (1970). *Pedagogy of the oppressed*. Continuum.
- Hopkin, P. (2018). *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management* (5th ed.). Kogan Page.
- Ingram, H. J. (2021). *Crafting effective counter narratives for preventing violent extremism*. International Centre for Counter-Terrorism.
- ISO. (2018). *ISO 31000: Risk management—Guidelines*. International Organization for Standardization.
- Kruglanski, A. W., Gelfand, M., Bélanger, J. J., Sheveland, A., Hetiarachchi, M., & Gunaratna, R. (2014). The psychology of radicalization and

- deradicalization: How significance quest impacts violent extremism. *Political Psychology*, 35(S1), 69–93.
- Livingstone, S., & Helsper, E. (2008). Parental mediation of children's internet use. *Journal of Broadcasting & Electronic Media*, 52(4), 581–599.
- Noddings, N. (2013). *Caring: A relational approach to ethics and moral education* (2nd ed.). University of California Press.
- OECD. (2021). *21st-century readers: Developing literacy skills in a digital world*. OECD Publishing.
- OECD. (2022). *Governance for youth, trust and intergenerational justice*. OECD Publishing.
- Papacharissi, Z. (2015). *Affective publics: Sentiment, technology, and politics*. Oxford University Press.
- Putnam, R. D. (2000). *Bowling alone: The collapse and revival of American community*. Simon & Schuster.
- Sieckelinck, S., & Gielen, A.-J. (2018). *Protecting children against radicalisation: The role of families*. Radicalisation Awareness Network.
- Twenge, J. M. (2017). *iGen: Why today's super-connected kids are growing up less rebellious, more tolerant, less happy—and completely unprepared for adulthood*. Atria Books.
- UNDP. (2023). *Digital resilience and preventing violent extremism among youth*. United Nations Development Programme.
- UNESCO. (2023). *Addressing hate speech and online extremism in the digital age*. UNESCO.
- UNESCO. (2024). *Education for peace, critical thinking, and digital citizenship*. UNESCO.
- United Nations Office of Counter-Terrorism. (2023). *Whole-of-society approaches to preventing violent extremism in the digital era*. UNOCT.
- We Are Social, & Meltwater. (2024). *Digital 2024: Indonesia*. We Are Social.

BAB 8

RISK GOVERNANCE DAN STRATEGI NASIONAL DI ERA DIGITAL

Perkembangan teknologi digital telah mengubah hampir seluruh cara manusia hidup dan berinteraksi. Informasi bergerak melintasi batas negara dalam hitungan detik, opini publik dapat berubah hanya karena satu konten viral, dan komunitas virtual dapat terbentuk tanpa harus memiliki hubungan fisik sama sekali. Dalam kondisi seperti itu, dunia bergerak jauh lebih cepat dibandingkan kemampuan banyak institusi untuk menyesuaikan diri. Sistem tata kelola yang sebelumnya dibangun untuk menghadapi ancaman konvensional kini berhadapan dengan realitas baru yang jauh lebih cair, kompleks, dan sulit diprediksi.

Masalah terbesar dari risiko digital bukan hanya pada kecepatan penyebaran informasi, tetapi pada perubahan struktur kekuasaan di ruang publik modern. Jika sebelumnya negara menjadi aktor utama dalam distribusi informasi dan pengendalian komunikasi publik, kini sebagian besar arus informasi bergerak melalui platform digital global yang bekerja berdasarkan algoritma dan ekonomi perhatian (*attention economy*). Akibatnya, negara tidak lagi sepenuhnya mengendalikan apa yang dilihat, dipercaya, dan dibicarakan masyarakat setiap hari.

Castells (2010) menjelaskan bahwa masyarakat modern telah berkembang menjadi *network society*, yaitu masyarakat yang hidup di dalam sistem jaringan informasi global yang sangat saling terhubung. Dalam sistem seperti ini, pengaruh dan kekuasaan tidak lagi hanya dimiliki negara, tetapi juga bergerak melalui jaringan digital, platform teknologi, komunitas online, dan aktor nonnegara yang mampu membentuk opini publik secara masif.

Perubahan tersebut menciptakan tantangan besar bagi tata kelola modern. Banyak institusi masih bekerja dengan pola birokrasi yang lambat dan formal, sementara ancaman digital berkembang secara real-time.

Dalam kondisi seperti itu, tata kelola tradisional sering mengalami keterbatasan karena perubahan teknologi bergerak jauh lebih cepat dibandingkan kemampuan sistem untuk beradaptasi.

Karena itu, pengelolaan risiko digital membutuhkan pendekatan *risk governance* yang lebih adaptif, kolaboratif, dan berbasis ketahanan sosial. Negara tidak dapat bekerja sendiri. Platform digital, masyarakat, lembaga pendidikan, komunitas, dan berbagai aktor sosial lainnya harus bergerak bersama dalam membangun ekosistem digital yang lebih sehat dan resilien.

Pada akhirnya, tantangan terbesar era digital bukan hanya mengendalikan teknologi, tetapi menjaga agar manusia dan institusi tetap mampu beradaptasi terhadap perubahan yang terus bergerak tanpa kehilangan kebebasan, kepercayaan sosial, dan stabilitas masyarakat.

Sebab di tengah dunia yang semakin dipengaruhi algoritma dan arus informasi global, keamanan masa depan tidak lagi hanya ditentukan oleh kekuatan negara, tetapi oleh kemampuan seluruh sistem sosial untuk belajar, beradaptasi, dan menjaga ketahanan di dalam ruang digital yang semakin kompleks.

DAFTAR PUSTAKA

- Aly, A., & Striegner, J.-L. (2012). Examining the role of religion in radicalization to violent Islamist extremism. *Studies in Conflict & Terrorism*, 35(12), 849–862.
- Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. *Journal of Public Administration Research and Theory*, 18(4), 543–571.
- Ansell, C., & Trondal, J. (2018). *Governance in turbulent times*. Oxford University Press.
- Balkin, J. M. (2018). Free speech in the algorithmic society: Big data, private governance, and new school speech regulation. *UC Davis Law Review*, 51(3), 1149–1210.
- Benkler, Y. (2006). *The wealth of networks: How social production transforms markets and freedom*. Yale University Press.
- Benkler, Y., Faris, R., & Roberts, H. (2018). *Network propaganda: Manipulation, disinformation, and radicalization in American politics*. Oxford University Press.
- Castells, M. (2010). *The rise of the network society* (2nd ed.). Wiley-Blackwell.
- Floridi, L. (2014). *The fourth revolution: How the infosphere is reshaping human reality*. Oxford University Press.

- Folke, C., Hahn, T., Olsson, P., & Norberg, J. (2005). Adaptive governance of social-ecological systems. *Annual Review of Environment and Resources*, 30, 441–473.
- Gillespie, T. (2018). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.
- Heifetz, R., Grashow, A., & Linsky, M. (2009). *The practice of adaptive leadership*. Harvard Business Press.
- Kettl, D. F. (2022). *The future of governance in a digital world*. Brookings Institution Press.
- Kitchin, R. (2017). Thinking critically about and researching algorithms. *Information, Communication & Society*, 20(1), 14–29.
- Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.
- O’Neil, C. (2016). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown Publishing Group.
- OECD. (2021). *Government at a glance 2021*. OECD Publishing.
- Pariser, E. (2011). *The filter bubble: What the internet is hiding from you*. Penguin Press.
- Renn, O. (2008). *Risk governance: Coping with uncertainty in a complex world*. Earthscan.
- Sunstein, C. R. (2018). *#Republic: Divided democracy in the age of social media*. Princeton University Press.
- Tufekci, Z. (2015). Algorithmic harms beyond Facebook and Google: Emergent challenges of computational agency. *Colorado Technology Law Journal*, 13(203), 203–218.
- UNESCO. (2023). *Addressing hate speech and online extremism in the digital age*. UNESCO.
- United Nations Office of Counter-Terrorism. (2023). *Whole-of-society approaches to preventing violent extremism in the digital era*. UNOCT.
- Van Dijck, J., Poell, T., & De Waal, M. (2018). *The platform society: Public values in a connective world*. Oxford University Press.
- Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

BAB 9

MASA DEPAN RISIKO DIGITAL DAN KETAHANAN SOSIAL



Perkembangan teknologi digital telah membawa manusia memasuki dunia yang semakin terkoneksi tanpa batas. Internet tidak lagi sekadar alat komunikasi, tetapi telah menjadi ruang utama tempat manusia bekerja, belajar, berinteraksi, membangun identitas, hingga memahami realitas sosial di sekitarnya. Aktivitas yang sebelumnya berlangsung secara fisik kini semakin banyak berpindah ke ruang digital yang terus aktif selama dua puluh empat jam tanpa henti.

Kondisi ini menciptakan perubahan besar dalam kehidupan manusia modern.

TENTANG PENULIS

Arif Dilianto, S.Psi., M.Han.



Arif Dilianto, atau yang akrab dipanggil John, adalah praktisi, peneliti isu strategis dan keamanan. Ia menyelesaikan pendidikan Sarjana Psikologi, Magister Asymmetric Warfare, dan saat ini sedang menempuh pendidikan doktoral di bidang Manajemen Bisnis. Perspektifnya dibentuk oleh perpaduan pengalaman profesional dan kajian akademik yang berfokus pada dinamika keamanan, pengambilan keputusan strategis, manajemen risiko, serta pengembangan organisasi yang adaptif dan berkelanjutan. Wawasannya semakin diperkaya melalui berbagai program pengembangan profesional, antara lain di National Security College Australia, European Bodyguard & Security Services Academy (EBSSA), dan Jakarta Centre for Law Enforcement Cooperation (JCLEC). Melalui buku *From Game to Jihad: Manajemen Risiko dalam Menghadapi Rekrutmen Terorisme Digital melalui Platform Online pada Generasi Muda di Indonesia*, Penulis mengangkat perubahan karakter ancaman di era digital dan bagaimana ruang digital dapat menjadi lingkungan berkembangnya risiko radikalisasi. Buku ini memadukan perspektif keamanan, psikologi, manajemen risiko, dan tata kelola untuk memahami proses yang bergerak dari interaksi digital, keterikatan sosial, pembentukan identitas, hingga berkembangnya risiko ekstremisme.

Dr. Osly Usman, M.Bus Mgt., M.Bus Syst.



Beliau adalah seorang akademisi dan peneliti senior di Fakultas Ekonomi, Universitas Negeri Jakarta (UNJ). Dengan latar belakang pendidikan spesifik yang menghasilkan gelar ganda di bidang Manajemen Bisnis (*Master of Business Management*) dan Sistem Bisnis (*Master of Business Systems*), kepakaran beliau berfokus pada irisan antara manajemen strategis, sistem informasi manajemen, pemasaran, dan perilaku organisasi. Sebagai pendidik di tingkat sarjana hingga pascasarjana, Dr. Osly sangat aktif menghasilkan berbagai

publikasi riset terapan di jurnal nasional maupun internasional, menjadikannya figur akademik yang solid dalam mengawal metodologi dan strategi bisnis berkelanjutan.

Dr. Mundiharno, M.Si., CSA, GRCP, GRCA



Beliau merupakan representasi ideal dari perpaduan antara akademisi dan praktisi strategis di sektor publik dan keuangan. Selain perannya di dunia pendidikan tinggi, Dr. Mundiharno memiliki rekam jejak kepemimpinan eksekutif yang sangat kuat, salah satunya pernah mengemban amanah sebagai Direktur Keuangan dan Investasi di BPJS Kesehatan. Kepakarannya dalam hal tata kelola organisasi dan mitigasi ketidakpastian terlegitimasi secara ketat melalui sertifikasi

profesional yang disandanginya, yakni *Certified Securities Analyst (CSA)*, *Governance, Risk, and Compliance Professional (GRCP)*, serta *Governance, Risk, and Compliance Auditor (GRCA)*. Latar belakang ini menjadikan beliau otoritas yang sangat mumpuni dalam disiplin ilmu Manajemen Risiko, khususnya dalam konteks arsitektur kelembagaan dan instrumen pengendalian publik.

FROM GAME TO JIHAD

MANAJEMEN RISIKO DALAM MENGHADAPI REKRUTMEN TERORISME DIGITAL MELALUI PLATFORM ONLINE PADA GENERASI MUDA DI INDONESIA

Buku ini mengulas perubahan pola terorisme di era digital, ketika proses radikalisasi tidak lagi berlangsung melalui pertemuan fisik atau organisasi formal, melainkan melalui media sosial, komunitas daring, dan platform permainan digital. Dengan pendekatan yang memadukan kajian keamanan, psikologi sosial, serta manajemen risiko, buku ini menjelaskan bagaimana interaksi yang tampak biasa di ruang digital dapat berkembang menjadi proses pembentukan identitas, keterikatan emosional, hingga penyebaran ideologi ekstrem pada generasi muda. Lebih dari sekadar membahas ancaman terorisme, buku ini menawarkan perspektif manajemen risiko berbasis ISO 31000 untuk mengidentifikasi, menganalisis, mengevaluasi, dan memitigasi risiko radikalisasi digital secara sistematis. Pembaca diajak memahami mekanisme kerja algoritma, fenomena echo chamber, cascading risk, hingga pentingnya risk governance dalam menghadapi ancaman yang terus berkembang seiring pesatnya transformasi teknologi informasi. Berbagai contoh kasus dan dinamika aktual turut memperkaya pembahasan sehingga konsep yang disajikan menjadi lebih kontekstual dan mudah dipahami. Sebagai referensi bagi akademisi, praktisi keamanan, pembuat kebijakan, pendidik, maupun masyarakat umum, buku ini menegaskan bahwa pencegahan ekstremisme digital tidak cukup dilakukan melalui pendekatan represif semata. Diperlukan kolaborasi multipihak untuk membangun literasi digital, ketahanan psikologis, kesadaran kritis, dan ekosistem digital yang sehat sebagai fondasi dalam melindungi generasi muda Indonesia dari ancaman radikalisasi di era digital.

 www.penerbitwidina.com
 @penerbitwidina
 penerbit widina
 penerbitwidina@gmail.com
 widina store
 widina bookstore

Layanan Pembaca & Penerbitan Buku
0815-7000-699



SCANME

Manajemen

ISBN 978-634-317-204-8



9 786343 172048