Paradigma Jurnal Kajian Budaya Vol. 8 No. 2 (2018): 137–154

VIRUS WANNACRY DALAM TEKS BERITA: ANALISIS WACANA KRITIS ATAS LAMAN KEMKOMINFO, KOMPAS.COM, DAN JAWAPOS.COM

IZHATULLAILI
Fakultas Ilmu Pengetahuan Budaya, Universitas Indonesia; izhatullaili@gmail.com

DOI: 10.17510/paradigma.v8i2.273

ABSTRACT

Critical Discourse Analysis is a study that analyzes language usage in terms of linguistic features and a social practice. Each type of mass media shows a different tendency in conveying information through the language it uses. Likewise, there are some differences between government and non-government media as well. The data in this study were obtained by collecting texts related to WannaCry virus news taken from the Ministry of Communication and Information Technology, Kompas.com and JawaPos.com. Abductive inferences technique was used to draw conclusions by connecting one text to other texts. The different tendencies in media's linguistic features and ideologies were described using critical discourse analysis and Fairclough's three interrelated analysis processes (i.e. the dimension of text description, the dimension of discourse practice by textual interpretation, and the dimension of socio-cultural by text explanation). The results of this study showed that the three media had some differences in both of their linguistic features and ideology.

KEYWORDS

Critical Discourse Analysis; government media; nongovernment media

1. Pendahuluan

Analisis wacana kritis (CDA) merupakan sebuah studi yang tidak hanya menganalisis penggunaan bahasa dalam fitur linguistis tetapi juga pada bahasa sebagai praktik sosial. Pengaitan itu menyebabkan hubungan dialektis antara wacana dan situasi, institusi, serta struktur sosial yang membentuk wacana itu (Eriyanto 2001, 7). Dalam penelitian ini digunakan analisis berdasarkan ancangan yang ditawarkan oleh Fairclough: terdapat tiga proses analisis yang saling berhubungan, yaitu dimensi teks dengan deskripsi teks, dimensi praktik wacana melalui interpretasi teks, dan dimensi konteks sosial budaya melalui eksplanasi teks.

Oleh karena itu, dalam penelitian ini dilakukan analisis mulai dari pilihan kata, frekuensi, dan berbagai unsur teks lain sampai ke eksplanasi wacana yang menunjukkan suatu ideologi yang terungkap di setiap teks. Melalui analisis wacana kritis akan terlihat bagaimana pilihan kata membawa posisi dan makna ideologi tertentu. Dengan kata lain, ideologi diamati dengan melihat berbagai bukti teks yang digunakan dan analisis serta pembahasan yang dilakukan terpusat pada kajian SFL (*systemic functional linguistics*). Martin,

J.R dan David Rose (2003, 263) menyatakan bahwa SFL merupakan kajian yang tidak hanya berusaha mengidentifikasi struktur tetapi juga mencari tahu bagaimana sebuah struktur kata mengonstruksi makna, yang titik beratnya adalah pada pertanyaan "bagaimana sebuah makna teks diwujudkan". Jadi, dapat dinyatakan bahwa fokus SFL tidak hanya pada teks yang dibangun tetapi juga pada konteksnya (dalam hal ini dapat terkait dengan pihak yang memproduksi dan mengonsumsi teks).

1.1 Tujuan Penelitian

Berdasarkan analisis wacana kritis atas tiga teks dalam tiga laman yang berbeda, terdapat tiga sasaran penelitian ini, yaitu mendeskripsikan ideologi yang terkandung dalam ketiga teks pada laman Kemkominfo, Kompas.com, dan JawaPos.com, mendeskripsikan perbedaan teks berita dalam media pemerintah (laman Kemkominfo) dengan media Kompas.com dan JawaPos.com melalui analisis wacana kritis Fairclough, dan mendeskripsikan perbedaan teks berita dalam media Kompas.com dan JawaPos.com melalui analisis wacana kritis Fairclough.

1.2 Kerangka Teoretis

1.2.1 Tahapan Analisis CDA (*critical discourse analysis*) menurut Fairclough

Penelitian ini menggunakan ancangan Fairclough tentang prosedur analisis wacana kritis yang terdiri atas tiga proses, yaitu deskripsi, interpretasi, dan eksplanasi (1989, 26). Analisis teks pada tahap deskripsi mengacu pada tingkatan yang berhubungan dengan sifat formal teks, kajiannya meliputi aspek leksikal dan gramatikal yang tercakup dalam aspek makna eksperensial (ideasional), interpersonal, serta makna tekstual teks. Dapat pula dikatakan bahwa tahap deskripsi teks merupakan pengacuan pada fitur-fitur linguistis.

Selanjutnya, tahap interpretasi berkaitan dengan hubungan antara teks dan interaksi dalam teks, yaitu dengan melihat teks sebagai produk dari suatu proses, dan sebagai sumber dalam proses interpretasi. Tahap ini mengikutkan faktor-faktor sosial (interpretasi konteks) dari sebuah teks, misalnya perihal siapa yang terlibat, apa yang sedang terjadi, dalam hubungan apa, serta apa peran bahasa dalam teks itu. Selanjutnya, ditentukan interpretasi teksnya berdasarkan hubungannya dengan interpretasi konteks itu (Fairclough 1989, 146–148).

Fairclough (1989, 141) menyatakan bahwa interpretasi adalah penggeneralisasian melalui apa yang ada dalam teks dan apa yang ada dalam benak penafsir serta dalam kerangka pikirnya. Tahap selanjutnya adalah eksplanasi. Tahap ini berkaitan dengan hubungan antara konteks interaksi dan sosial. Tahapannya berhubunganan dengan penentuan proses sosial produksi dan interpretasi serta efek sosial sebuah teks. Pada tahap ini dilakukan analisis data yang terkait dengan terbentuknya wacana yang berhubungan dengan penentuan sosial yang meliputi level situasional, institusional, dan kemasyarakatan.

1.2.2 Teks Berita

Wacana merupakan contoh komunikasi aktual yang menggunakan bahasa sebagai media komunikasi (Johnstone 2002, 2). Sementara itu, menurut Eriyanto (2002, 91), berita pada dasarnya dibentuk dalam proses aktif dari pembuat berita. Peristiwa yang kompleks dan tidak beraturan disederhanakan dan dibuat bermakna oleh pembuat berita. Semua itu melibatkan proses lewat skema interpretasi dari pembuat berita. Fishman dalam Eriyanto (2002, 91) menyatakan pula bahwa peristiwa adalah sebuah fenomena atau

kejadian yang diinterpretasikan, sesuatu yang diorganisasikan dalam pikiran, ucapan, dan tindakan. Oleh karena itu, peristiwa yang kompleks itu diinterpretasikan dalam skema pembuat berita. Satu berita yang sama dapat disusun ke dalam struktur cerita yang berbeda-beda bergantung pada keinginan penulis berita.

1.3 Metodologi Penelitian

1.3.1 Data

Data penelitian ini adalah teks yang terkait dengan berita virus wannacry dari laman Kemkominfo, Kompas.com, dan JawaPos.com. Pemilihan teks pada laman Kemkominfo, Kompas.com, dan JawaPos.com didasarkan pada hipotesis: ketiga laman itu memiliki perbedaan ideologi yang disampaikan melalui teks yang diproduksi. Laman Kemenkominfo sebagai media instansi pemerintah berbeda dari Kompas.com dan JawaPos.com sebagai media nonpemerintah dalam menyampaikan berita.

1.3.2 Teknik Analisis Data

Dalam melakukan analisis, data berupa teks yang tersusun dari kalimat diuraikan menjadi klausa-klausa dan selanjutnya dianalisis dalam tiga tindakan, yaitu deskripsi teks, interpretasi, dan eksplanasi. Sementara itu, dalam penarikan simpulan digunakan teknik abduktif inferensi (*abductive inferences*) yaitu penarikan simpulan dengan cara menghubungkan satu teks dengan yang lain (Krippendorff 2004, 36). Cara itu untuk menunjukkan kesamaan dan perbedaan antara tiga teks yang dianalisis.

2. Analisis

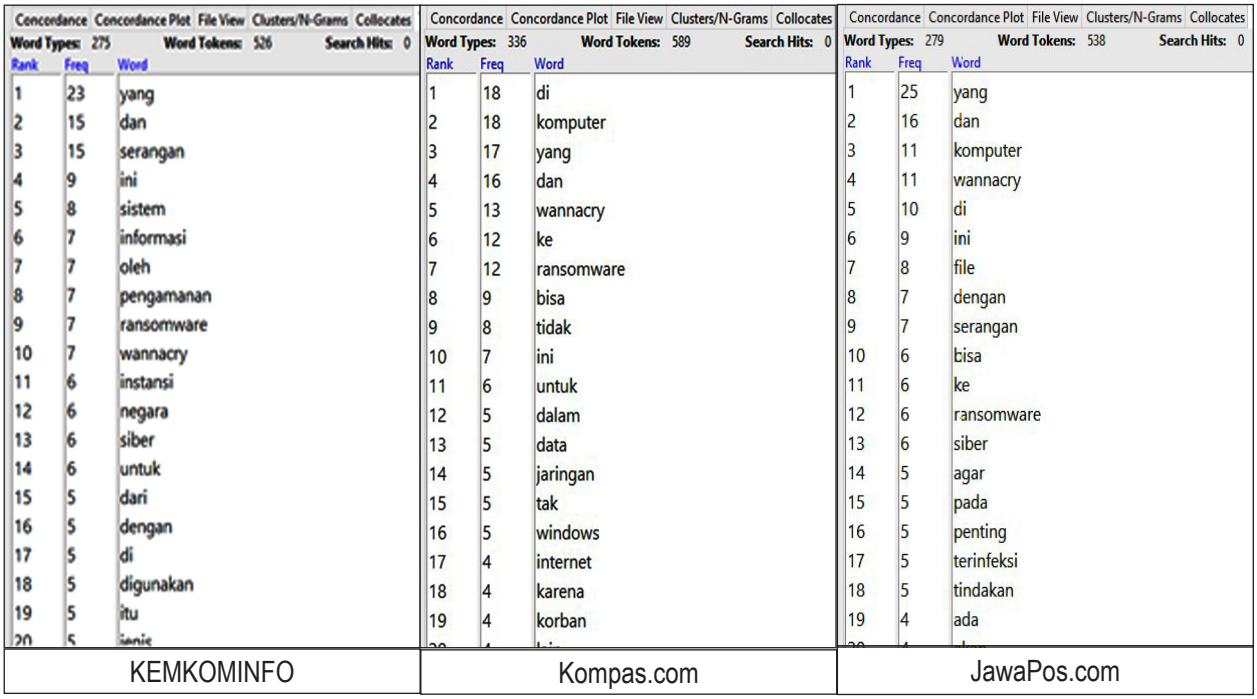
2.1 Deskripsi Teks

Dalam tahap deskripsi teks, dilakukan analisis dengan memilah kalimat yang terdapat dalam teks menjadi klausa-klausa. Dalam teks yang terdapat dalam laman Kemkominfo terdapat 71 klausa, sedangkan dalam Kompas.com terdapat 96 klausa dan dalam JawaPos.com terdapat 79 klausa.

Media	Jumlah		
	Kalimat	Klausa	Kata
Kemkominfo	37	71	529
Kompas.com	39	96	578
Jawa Pos.com	28	79	524

Tabel 1. Jumlah konstruksi kalimat, klausa, dan kata dalam laman Kemkominfo, Kompas.com dan JawaPos.com.

Selanjutnya, dari ketiga teks itu dianalisis kata yang paling sering digunakan dalam teks sebagai berikut.



Concordance | Concordance Plot | File View | Clusters/N-Grams | Collocates
Word Types: 275 Word Tokens: 526 Search Hits: 0

Rank	Freq	Word
1	23	yang
2	15	dan
3	15	serangan
4	9	ini
5	8	sistem
6	7	informasi
7	7	oleh
8	7	pengamanan
9	7	ransomware
10	7	wannacry
11	6	instansi
12	6	negara
13	6	siber
14	6	untuk
15	5	dari
16	5	dengan
17	5	di
18	5	digunakan
19	5	itu
20	5	jenis

KEMKOMINFO

Concordance | Concordance Plot | File View | Clusters/N-Grams | Collocates
Word Types: 336 Word Tokens: 589 Search Hits: 0

Rank	Freq	Word
1	18	di
2	18	komputer
3	17	yang
4	16	dan
5	13	wannacry
6	12	ke
7	12	ransomware
8	9	bisa
9	8	tidak
10	7	ini
11	6	untuk
12	5	dalam
13	5	data
14	5	jaringan
15	5	tak
16	5	windows
17	4	internet
18	4	karena
19	4	korban

Kompas.com

Concordance | Concordance Plot | File View | Clusters/N-Grams | Collocates
Word Types: 279 Word Tokens: 538 Search Hits: 0

Rank	Freq	Word
1	25	yang
2	16	dan
3	11	komputer
4	11	wannacry
5	10	di
6	9	ini
7	8	file
8	7	dengan
9	7	serangan
10	6	bisa
11	6	ke
12	6	ransomware
13	6	siber
14	5	agar
15	5	pada
16	5	penting
17	5	terinfeksi
18	5	tindakan
19	4	ada

JawaPos.com

Tabel 2. Kata dengan frekuensi tertinggi dalam laman Kemkominfo, Kompas.com dan JawaPos.com.

Dalam teks berita di laman Kementerian Kominfo mengenai virus ransomware, terdapat beberapa kata selain kata tugas dan pronomina dengan frekuensi tertinggi yaitu *serangan, sistem, informasi, pengamanan,* dan *ransomware.* Kata serangan muncul sebanyak 15 kali, *sistem* 8 kali, *informasi* 7 kali, *pengamanan* 7 kali, dan *ransomware* juga digunakan dalam teks sebanyak 7 kali.

Sementara itu, dalam teks berita Kompas.com, lima kata konsep dengan frekuensi penggunaan tertinggi adalah *komputer* (18 kali), *wannacry* (13 kali), *ransomware* (12 kali), *data* (5 kali) dan *jaringan* (5 kali). Dalam JawaPos.com, lima kata konsep yang paling sering digunakan dalam teks beritanya adalah *komputer* (11 kali), *wannacry* (11 kali), *file* (8 kali), *serangan* (7 kali) dan *ransomware* (6 kali).

Dari frekuensi kata-kata tersebut tampak kesamaan kata konsep tertentu di antara ketiga teks pada laman Kemenkominfo, Kompas.com dan JawaPos.com sebagai berikut.

	Kemkominfo	Kompas.com
Kemkominfo	-	Ransomware
Kompas.com	Ransomware	-
JawaPos.com	Serangan Ransomware	Ransomware Wannacry Komputer

Tabel 3. Kesamaan Kata Konsep Antamedia (Berdasarkan lima kata dengan frekuensi tertinggi).

Dalam tabel tersebut diketahui bahwa antara Media Kompas.com dan JawaPos.com terdapat tiga kata konsep sama yang termasuk dalam lima kata dengan frekuensi tertinggi, yaitu *ransomware*, *wannacry,* dan *komputer*. Itu menandakan bahwa yang diungkapkan dalam teks berita pada kedua media itu mengarah pada aspek pemberitaan virus penyerang komputer.

Wannacry dalam Kompas.com berkolokasi dengan beberapa bentuk, seperti *penyebaran*, *serangan*, *senjata*, dan *rahasianya*. Sementara itu, dalam JawaPos.com *wannacry* berkolokasi dengan *mengincar, berbasis*, *perusak*, dan beberapa bentuk lain yang menunjukkan subjek. Berdasarkan frekuensi kata yang sama dan kolokasi yang terdapat di dalamnya, dapat dinyatakan bahwa pada dua media itu, berita terkait virus ransomware lebih menitikberatkan pada penyampaian virus itu. Hal ini berbeda dengan temuan pada data teks terkait hal yang sama di laman Kemkominfo. Dalam laman itu teks yang disajikan cenderung mengungkapkan solusi dan suatu pernyataan tentang serangan virus *ransomware* yang dapat diatasi. Temuan ini diperoleh dari analisis lima kata konsep yang berfrekuensi tertinggi, satu di antaranya *pengamanan*. Selain itu, beberapa lainnya juga merupakan kata yang mengandungi makna netral (apabila dibandingkan kata yang terdapat pada Kompas.com dan JawaPos.com), seperti *sistem* dan *informasi* meskipun ada pula bentuk *serangan* dan *ransomware*.

Concordance | Concordance Plot | File View | Clusters/N-Grams | Collocates | Word List

Total No. of Collocate Types: 99 **Total No. of Collocate Tokens:** 130

Rank	Freq	Freq(L)	Freq(R)	Stat	Collocate
1	2	1	1	6.50168	kompas
2	2	1	1	6.50168	com
3	3	2	1	6.08665	penyebaran
4	1	1	0	5.50168	worm
5	1	0	1	5.50168	waktu
6	1	1	0	5.50168	terlanjur
7	1	0	1	5.50168	terbuka
8	1	1	0	5.50168	setidaknya
9	1	1	0	5.50168	serangan
10	1	0	1	5.50168	senjata
11	1	0	1	5.50168	selengkapnya
12	1	0	1	5.50168	security
13	1	0	1	5.50168	secara
14	1	0	1	5.50168	sebenarnya
15	1	1	0	5.50168	salahuddin
16	1	0	1	5.50168	response
17	1	1	0	5.50168	rahasianya
18	1	0	1	5.50168	pun
19	1	1	0	5.50168	potensi

Kolokasi wannacry dalam Kompas.com

Concordance | Concordance Plot | File View | Clusters/N-Grams | Collocates | Word List

Total No. of Collocate Types: 51 **Total No. of Collocate Tokens:** 70

Rank	Freq	Freq(L)	Freq(R)	Stat	Collocate
1	2	0	2	7.23156	pc
2	2	0	2	7.23156	mengincar
3	2	2	0	7.23156	disebut
4	2	0	2	7.23156	berbasis
5	1	1	0	6.23156	wanna
6	1	0	1	6.23156	sudah
7	1	0	1	6.23156	setelah
8	1	0	1	6.23156	semuel
9	1	1	0	6.23156	sebetulnya
10	1	1	0	6.23156	saat
11	1	1	0	6.23156	perusak
12	1	1	0	6.23156	paparnya
13	1	0	1	6.23156	merupakan
14	1	1	0	6.23156	kita
15	1	0	1	6.23156	jenderal
16	1	0	1	6.23156	hanya
17	1	0	1	6.23156	group
18	1	0	1	6.23156	direktur
19	1	0	1	6.23156	dipastikan
20	1	1	0	6.23156	diduga

Kolokasi wannacry dalam JawaPos.com

Concordance | Concordance Plot | File View | Clusters/N-Grams | Collocates | W

Total No. of Collocate Types: 77 Total No. of Collocate Tokens:

Rank	Freq	Freq(L)	Freq(R)	Stat	Collocate
1	2	0	2	6.61203	mengincar
2	2	2	0	6.61203	disebut
3	2	0	2	6.61203	berbasis
4	1	0	1	5.61203	wifi
5	1	0	1	5.61203	tetapi
6	1	0	1	5.61203	setiap
7	1	1	0	5.61203	setara
8	1	0	1	5.61203	sambungan
9	1	0	1	5.61203	rentan
10	1	1	0	5.61203	ransomare
11	1	0	1	5.61203	ransom
12	1	1	0	5.61203	potensi
13	2	2	0	5.61203	penyebaran
14	1	0	1	5.61203	pembayarannya
15	1	0	1	5.61203	menginfeksi
16	1	1	0	5.61203	menghentikan
17	1	0	1	5.61203	memutuskan
18	1	0	1	5.61203	meminta
19	1	1	0	5.61203	khususnya

Kolokasi wannacry dalam Kemkominfo

Concordance | Concordance Plot | File View | Clusters/N-Grams | Collocates

Total No. of Collocate Types: 36 Total No. of Collocate Tokens:

Rank	Freq	Freq(L)	Freq(R)	Stat	Collocate
1	2	0	2	7.48650	malicious
2	2	1	1	7.48650	disebut
3	2	1	1	7.48650	diperkirakan
4	2	2	0	7.48650	berjenis
5	3	1	2	7.07146	baru
6	1	1	0	6.48650	tahun
7	3	1	2	6.48650	sebuah
8	1	0	1	6.48650	muncul
9	1	0	1	6.48650	mengincar
10	1	1	0	6.48650	khususnya
11	1	1	0	6.48650	kembali
12	4	1	3	6.48650	jenis
13	1	0	1	6.48650	diberitakan
14	1	0	1	6.48650	berbasis
15	2	0	2	6.48650	adalah
16	2	2	0	5.90154	menyerang
17	2	2	0	5.90154	indonesia
18	1	1	0	5.48650	terhadap
19	1	0	1	5.48650	telah

Kolokasi wannacry dalam Kemkominfo

Concordance | Concordance Plot | File View | Clusters/N-Grams | Collocates | Word

Total No. of Collocate Types: 44 Total No. of Collocate Tokens: 70

Rank	Freq	Freq(L)	Freq(R)	Stat	Collocate
1	2	0	2	7.23156	malicious
2	2	1	1	7.23156	disebut
3	2	1	1	7.23156	diperkirakan
4	2	2	0	7.23156	berjenis
5	1	0	1	6.23156	wanna
6	1	0	1	6.23156	telah
7	1	1	0	6.23156	tahun
8	1	0	1	6.23156	setelah
9	3	1	2	6.23156	sebuah
10	1	0	1	6.23156	pc
11	1	0	1	6.23156	muncul
12	1	1	0	6.23156	menyusul
13	1	0	1	6.23156	mengincar
14	1	1	0	6.23156	kita
15	1	1	0	6.23156	kembali
16	5	2	3	6.23156	jenis
17	2	2	0	6.23156	indonesia
18	1	1	0	6.23156	harapan
19	1	0	1	6.23156	dipastikan
20	1	0	1	6.23156	decryptor

Kolokasi ransomware dalam JawaPos.com

Concordance | Concordance Plot | File View | Clusters/N-Grams | Collocates | Word List

Total No. of Collocate Types: 87 Total No. of Collocate Tokens: 119

Rank	Freq	Freq(L)	Freq(R)	Stat	Collocate
1	2	1	1	6.61716	kompas
2	2	1	1	6.61716	com
3	2	1	1	6.61716	canggih
4	3	2	1	6.20212	penyebaran
5	1	1	0	5.61716	virus
6	1	1	0	5.61716	terlanjur
7	1	0	1	5.61716	terjadi
8	1	0	1	5.61716	terbuka
9	1	0	1	5.61716	tangan
10	1	1	0	5.61716	software
11	1	1	0	5.61716	si
12	1	0	1	5.61716	serupa
13	1	1	0	5.61716	serangan
14	1	0	1	5.61716	selengkapnya
15	1	0	1	5.61716	selalu
16	1	1	0	5.61716	sejak
17	1	0	1	5.61716	security
18	2	2	0	5.61716	sang
19	1	1	0	5.61716	salahuddin

Kolokasi ransomware dalam Kompas.com

Tabel 4. Kolokasi kata *ransomware* dan *wannacry.*

Selanjutnya, dilakukan analisis transitivitas klausa yang termuat dalam laman Kemkominfo, Kompas.com, dan JawaPos.com. Untuk keperluan deskripsi teks, setiap kalimat yang terdiri atas lebih dari satu klausa dipecah menjadi klausa-klausa. Perhitungan jumlah klausa berdasarkan jenis transitivitas klausa menunjukkan perbedaan pola kecenderungan identifikasi dan karakterisasi di antara ketiga media dalam menyampaikan berita yang terkait dengan serangan virus *wannacry*.

No.	Transitivitas	Jumlah Klausa					
		Kemkominfo	%	JawaPos.com	%	Kompas.com	%
1.	Material	51	71.83	30	37.97	74	77.08
2.	Relasional	8	11.27	31	39.24	13	13.54
3.	Mental	3	4.22	5	6.33	4	4.17
4.	Verbal	3	4.22	7	8.86	1	1.04
5.	Perilaku	4	5.63	2	2.53	1	1.04
6.	Eksistensial	2	2.82	4	5.06	3	3.12

Tabel 5. Jumlah Transitivitas Klausa dalam Situs Kementerian Komunikasi dan Informatika.

Dalam tabel tersebut, jenis klausa yang paling besar jumlahnya adalah klausa material, yaitu mencapai 51 (71.83%) dalam laman Kemkominfo dan 74 (77.08%) dalam Kompas.com. Sementara itu, dalam JawaPos.com, jumlah klausa material lebih kecil daripada jumlah klausa relasional meskipun hanya berselisih satu angka, yaitu klausa material berjunlah 30 (37.97%) dan klausa relasional 31 (39.24%). Itu menunjukkan perbedaan pada identifikasi dan karakterisasi JawaPos.com melalui jumlah klausa relasional dan material yang hampir sama.

Dari segi fungsi interpersonal, dilakukan analisis pola kecenderungan modus yang digunakan dalam ketiga teks. Klausa-klausa yang mengandungi kata *ransomware*, *wannacry* ataupun yang terkait dengan *serangan* dan *virus* kebanyakan ditemukan dalam modus deklaratif meskipun ada pula yang dalam modus interogatif terbuka (wh-interogatif).

Selanjutnya, dilakukan pula analisis struktur tematis pada klausa yang mengandungi kata *ransomware*, *wannacry* ataupun *serangan virus*. Dalam analisis ini ditemukan pola penggunaan kata-kata itu dalam teks. Temuan itu menunjukkan bahwa, apabila tidak digunakan pada posisi Tema, kata-kata itu digunakan pada posisi Rema. Berikut tabel yang menunjukkan penggunaan struktur itu.

Tema	Rema
Himbauan	Agar Segera Melakukan Tindakan Pencegahan Terhadap Ancaman Malware Khususnya Ransomware Jenis WannaCry
telah terjadi	fenomena serangan siber di beberapa negara
serangan siber ini	bersifat tersebar dan masif serta menyerang critical resource
serangan	ditujukan ke Rumah Sakit Harapan Kita dan Rumah Sakit Dharmais
Semmy menjelaskan	serangan siber yang menyerang Indonesia berjenis ransomware
Ransomware	adalah sebuah jenis malicious software
sebuah jenis ransomware baru	telah muncul
Ransomware baru ini	disebut Wannacry
Wannacry ransomware	mengincar PC berbasis windows
serangan Wannacry	sudah memakan banyak korban ke berbagai negara
Wannacry	menginfeksi sebuah computer
komputer yang berada pada jaringan yang sama	memiliki potensi terinfeksi terhadap ancaman Wannacry
Wannacry	meminta ransom atau dana tebusan
Wannacry	memberikan alamat bitcoin

Tema	Rema
belum ada	solusi yang paling cepat dan jitu untuk mengembalikan file-file yang sudah terinfeksi wannacry
memutuskan sambungan internet dari komputer yang terinfeksi	akan menghentikan penyebaran wannacry ke komputer lain yang rentan (*vulnerable*).

Tabel 6. Struktur Tematis Klausa dalam Laman Kemkominfo.

Tema	Rema
Penyebaran ransomware WannaCry	menimbulkan kekhawatiran besar
WannaCry	Pun tak pandang bulu dalam menyerang korban.
komputernya	dikunci oleh sang ransomware
16 rumah sakit	menjadi korban WannaCry.
sang ransomware	sudah menyebar ke 99 negara dan menginfeksi puluhan ribu, kalau bukan ratusan ribu, sistem komputer.
WannaCry	lebih canggih dan berbahaya
Ransomware ini	tak butuh campur tangan pengguna untuk bisa menginfeksi komputer
WannaCry	memanfaatkan tool senjata cyber milik dinas intel Amerika Serikat
Malware	hanya menampilkan pesan di layar komputer yang isinya meminta tebusan Rp 4 juta dalam bentuk mata uang virtual Bitcoin yang transaksinya tak bisa dilacak.
pembuat ransomware	benar-benar akan mengirimkan kunci enkripsi untuk membuka data di komputer korban.
Potensi penyebaran ransomware WannaCry	masih terbuka di Indonesia
WannaCry	bisa menyusup masuk ke komputer dan meluas di jaringan tanpa diketahui
celah keamanan yang dieksploitasi oleh WannaCry	sebenarnya sudah ditambal melalui patch sekuriti Windows oleh Microsoft pada Maret 2017 lalu
Pemerintah melalui Kementerian Komunikasi dan Informatika	telah merumuskan langkah-langkah pencegahan infeksi ransomware WannaCry
Apa yang bisa dilakukan	apabila terlanjur terinfeksi ransomware WannaCry?

Tabel 7. Struktur Tematis Klausa dalam Kompas.com.

Tema	Rema
ancaman virus komputer jenis ransomware	bernama Wanna Decryptor atau WannaCry
Exploit itu	digunakan sebagai suatu metode untuk menyebarkan secara cepat software perusak yang bernama WannaCry ke seluruh dunia
dua RS yaitu RS Dharmais dan RS Harapan Kita	diserang virus Ransomware jenis WannaCry
hanya RS Dharmais	yang positif diserang virus tersebut
seperti apa	bahaya virus WannaCry?

Tema	Rema
serangan siber ini	bersifat tersebar
serangan ini	bisa dikategorikan sebagai teroris siber
serangan siber yang menyerang Indonesia	berjenis ransomware
Ransomware	adalah sebuah jenis malicious software atau malware
sebuah jenis ransomware baru	telah muncul
Ransomware baru ini	disebut WannaCry
WannaCry ransomware	mengincar PC berbasis windows
serangan WannaCry	sudah memakan banyak korban ke berbagai negara

Tabel 8. Struktur Tematis Klausa JawaPos.com.

2.2 Interpretasi: Produksi dan Konsumsi

Laman Kemkominfo merupakan media resmi yang dikelola oleh Kementerian Komunikasi dan Informatika. Tentu, terdapat beberapa ketentuan dalam setiap informasi yang disampaikan melalui laman itu. Bukanlah karakter lembaga publik dalam menyampaikan berita yang dapat menimbulkan kepanikan masyarakat. Begitu pula siaran teks yang terkait dengan virus *ransomware* dalam laman Kemkominfo. Sementara itu, Kompas.com dan JawaPos.com merupakan media nonpemerintah yang tentu sedikit banyak bertujuan komersial dalam persaingan di antara media daring lain. Bahkan, saat ini terdapat sekitar 43.300 media daring di Indonesia (Memahami *Media.sinarharapan.net*, 30 Januari 2017).

Ketiga media tersebut merupakan sarana komunikasi yang menjadi perantara masyarakat dan pemilik laman. Bagi Kemkominfo, laman juga berpengaruh pada pembentukan kepercayaan masyarakat pada pemerintah. Dengan kata lain, informasi yang disampaikan melalui laman itu menjadi cerminan pemerintah, dalam hal ini Kementerian Komunikasi dan Informatika, untuk menunjukkan segala citra yang positif. Itu berlaku juga pada Kompas.com dan JawaPos.com, artinya teks yang disampaikan menjadi sarana untuk menyampaikan karakter dan citra masing-masing.

Deskripsi frekuensi kata yang terdapat di awal menunjukkan bahwa ketiga teks tersebut menekankan pada *ransomware* dan *serangan virus*. Meskipun demikian, terdapat perbedaan dalam setiap teksnya sebagaimana interpretasi yang didapat dari hasil deskripsi teks sebagai berikut. Teks dalam laman Kemkominfo menekankan pada kewenangan, tanggung jawab, dan kekuasaan pemerintah dalam mengatasi serangan virus *wannacry*. Sementara itu, teks dalam Kompas.com dan JawaPos.com lebih menekankan pada status serangan *ransomware* sebagai virus yang berbahaya sehingga masyarakat harus mewaspadainya.

2.3 Eksplanasi Wacana

Kehadiran media publik pemerintah yang semakin memudahkan masyarakat untuk mengakses informasi menjadi hal yang penting. Begitu pula kehadiran laman resmi Kemkominfo. Dalam pelaksanaannya pun terdapat aturan dan ketentuan yang jelas sebagaimana tercantum dalam Undang-Undang Nomor 11/2008 tentang Informasi dan Transaksi Elektronik. Hasil revisi Undang-Undang itu merumuskan antara lain memperkuat peran pemerintah untuk mencegah penyebarluasan konten negatif di Internet. Selain memiliki kewenangan dalam mencegah penyebarluasan berita yang tidak seharusnya ada, penerbitan informasi di

laman resminya (pemerintah: Kemkominfo) juga merupakan tindakan yang dapat menstabilkan berita yang beredar mengenai serangan virus *ransomware*.

Bukan berita dengan konten negatif (seperti berita tentang anti NKRI dan pemberontakan) saja yang perlu mendapat perhatian pemerintah untuk melindungi masyarakat tetapi juga berita yang terkait dengan isu umum yang disampaikan secara berlebihan untuk menimbulkan kepanikan masyarakat. Oleh karena itu, perbedaan *ritme* informasi dalam teks yang terdapat di laman Kemkominfo dengan teks yang terdapat pada Kompas.com dan JawaPos.com merupakan hal yang beralasan. Kestabilan informasi dan efek yang ditimbulkan dari informasi pada laman pemerintah diperlukan untuk menjaga masyarakat dari kekhawatiran berlebihan dan meningkatkan kepercayaan masyarakat pada pemerintah.

Sebagaimana yang tercantum dalam Pedoman Umum Komunikasi Organisasi di Lingkungan Instansi Pemerintah (2011) berikut.

> Hubungan masyarakat di lingkungan instansi pemerintah, untuk selanjutnya disebut humas pemerintah, adalah lembaga humas dan/ atau praktisi humas pemerintah yang melakukan fungsi manajemen dalam bidang komunikasi dan informasi yang persuasif, efektif, dan efisien untuk menciptakan hubungan yang harmonis dengan publiknya melalui berbagai saran kehumasan dalam rangka menciptakan citra yang positif instansi pemerintah.

Jadi, sangat wajar bahwa teks di laman Kemkominfo tidak mengandungi penekanan pada serangan *ransomware* saja tetapi juga pada penyampaian tindakan pemerintah dan permintaan pemerintah pada masyarakat. Misalnya melalui klausa. “Dengan adanya serangan siber ini kami minta agar masyarakat tetap tenang dan meningkatkan kehati-hatian dalam berinteraksi di dunia siber”. Sementara itu, dalam Kompas.com dan Jawa Pos.com terdapat ritme berita yang berbeda dari yang termuat dalam laman Kemkominfo. Oleh karena itu, dapat dinyatakan bahwa selain kesamaan terdapat pula perbedaan di antara ketiganya.

Laman Kemkominfo memiliki pola kecenderungan yang hampir sama dalam identifikasi dan karakterisasi dengan Kompas.com, yaitu mengedepankan penyampaian peristiwa melalui klausa material. Selanjutnya, sangat wajar bahwa hal ini dikaitkan dengan genre teks yang disampaikan yakni teks berita sebagaimana tujuan teks berita untuk menyampaikan atau melaporkan informasi berdasarkan peristiwa yang terjadi.

Sementara itu, identifikasi dan karakterisasi JawaPos.com agak berbeda, yakni memiliki jumlah klausa relasional dan material yang hampir sama. Keadaan itu menunjukkan bahwa di dalam teksnya, penyampaian informasi berdasarkan peristiwa yang terjadi diimbangi dengan pengidentifikasian topik berita. Jadi, dapat dinyatakan bahwa JawaPos.com tidak menitikberatkan pada penggunaan klausa material dalam penyampaian peristiwa, tetapi memberikan porsi yang hampir sama besar pada penggunaan klausa relasional yang cenderung mencirikan hal tertentu yang terjadi.

3. Kesimpulan

Berdasarkan temuan yang dijelaskan di atas, peneliti ini menarik simpulan sebagai berikut. Laman Kemkominfo memiliki pola kecenderungan yang hampir sama dalam identifikasi dan karakterisasi dengan Kompas.com, yaitu mengedepankan penyampaian peristiwa melalui klausa material. Artinya, sesuai dengan tujuan teks berita.

Identifikasi dan karakterisasi JawaPos.com agak berbeda yakni memiliki jumlah klausa relasional dan material yang hampir sama. Itu menunjukkan bahwa di dalam teksnya, penyampaian informasi berdasarkan peristiwa yang terjadi diimbangi dengan pengidentifikasian topik berita.

Teks yang terdapat pada laman Kemkominfo tidak mengandungi penekanan pada serangan *ransomware* saja tetapi juga pada penyampaian tindakan pemerintah dan tujuan menstabilkan informasi dan ketenangan masyarakat. Teks yang diproduksi juga mengandungi ideologi: terdapat kewenangan, tanggung jawab, dan kekuasaan pemerintah dalam penanganan serangan *ransomware*. Sementara itu, teks dalam Kompas.com dan JawaPos.com mengarah pada status *ransomware* yang berbahaya dan mengandungi ideologi menyadarkan masyarakat akan serangan yang berbahaya.

Perbedaan media pemerintah dan nonpemerintah juga diperlihatkan dalam ketiga teks, yaitu dalam menjaga kestabilan informasi yang menjadi konsumsi masyarakat. Perlu dicatat bahwa tulisan ini merupakan laporan sebuh penelitian awal yang perlu dilanjutkan dengan penelitian lain.

Daftar Referensi

Biro Humas, Kementerian Komunikasi dan Informatika. 2017. Siaran Pers Kementerian Komunikasi dan Informatika No. 55/HM/KOMINFO/05/2017. *Kementerian Komunikasi dan Informatika Republik Indonesia*, 13 Mei. https://www.kominfo.go.id/content/detail/9636/siaran-pers-no-55hmkominfo052017-tentang-himbauan-agar-segera-melakukan-tindakan-pencegahan-terhadap-ancaman-malware-khususnya-ransomware-jenis-wannacry/0/siaran_pers [diakses pada tanggal 26 Mei 2017].

Eriyanto. 2000. *Analisis Wacana.* Malang: LkiS.

Fairclough, N. 1989. *Language and Power.* London: Longman.

_____. 1995. *Critical discourse analysis: The critical study of language*. London: Longman.

Johnstone, Barbara. 2002. *Discourse Analysis*. UK: Blackwell Publishers Ltd.

Krippendorff, Klaus. 2004. *Content Analysis: An Introduction to its Methodology.* London: Sage Publications.

Martin, J.R and Rose, David. 2003. *Working With Discourse: Meaning Beyond the Clause.* London: Continuum.

Syadri, Muhammad. 2017. Ransomware bernama Wanna Cry! *JawaPos.com*, 14 Mei. https://www.jawapos.com/teknologi/14/05/2017/ayo-kenali-teroris-baru-dari-virus-ransomware-bernama-wanna-cry [diakses 26 Mei 2017].

Yusuf, Oik. 2017. Intel AS di Balik "Ransomware" yang Menyerang Rumah Sakit Indonesia. *Kompas.com,* 13 Mei. http://tekno.kompas.com/read/2017/05/13/15493697/.tool.nsa.di.balik.ransomware.yang.menyerang.rumah.sakit.indonesia [diakses pada tanggal 26 Mei 2017].

Lampiran 1

No	Klausa	Tipe Proses
1.	*diberitakan di beberapa media baik di dalam ataupun luar negeri,*	Material
2.	*telah terjadi fenomena serangan siber di beberapa negara*	Material
3.	*Direktur Jenderal Aplikasi Informatika, Semuel A. Pangerapan menyampaikan serangan siber*	Material
4.	*serangan siber ini bersifat tersebar*	Relasional
5.	*serangan siber ini bersifat masif*	Relasional
6.	*serangan siber menyerang critical resource*	Material
7.	*serangan ini bisa dikategorikan teroris siber*	Relasional
8.	*serangan ditujukan ke Rumah Sakit Harapan Kita*	Perilaku
9.	*serangan ditujukan ke Rumah Sakit Dharmais*	Material
10.	*kami minta agar masyarakat tetap tenang*	Material
11.	*masyarakat tetap tenang*	Material
12.	*masyarakat meningkatkan kehati-hatian*	Material
13.	*berinteraksi di dunia siber*	Material
14.	*Semmy menjelaskan serangan siber yang menyerang Indonesia berjenis ransomware*	Verbal
15.	*serangan siber (yang menyerang Indonesia) berjenis ransomware*	Relasional
16.	*Ransomware adalah sebuah jenis malicious software*	Relasional
17.	*Ransomware adalah sebuah jenis malware*	Relasional
18.	*... mengunci komputer korban*	Material
19.	... meng-encrypt semua file yang ada	Material
20.	... tidak bisa diakses kembali	Material
21.	sebuah jenis ransomware baru telah muncul	Material
22.	diperkirakan bisa memakan banyak korban	Mental
23.	*memakan banyak korban*	Material
24.	*Ransomware baru ini disebut Wannacry*	Relasional
25.	*Wannacry ransomware mengincar PC berbasis windows*	Material
26.	*Saat ini diduga seran gan Wannacry sudah memakan banyak korban ke berbagai negara.*	Material
27.	*Serangan Wannacry sudah memakan banyak korban ke berbagai negara.*	Material
28.	*... penting (untuk melakukan serangkaian tindakan pencegahan)*	Verbal
29.	*... melakukan serangkaian tindakan penanganan*	Material
30.	*terjadi insiden*	Material
31.	*Wannacry menginfeksi sebuah computer*	Material
32.	... meng-enkripsi seluruh file yang ada di komputer tersebut	Material
33.	*Bisa... (melakukan eksekusi perintah)*	Verbal
34.	*melakukan eksekusi perintah*	Material
35.	*menyebar ke computer windows lain*	Material
36.	*Semua komputer memiliki potensi terinfeksi terhadap ancaman Wannacry*	Perilaku
37.	*Setiap komputer windows (yang sudah terinfeksi) akan mendapatkan tampilan seperti gambar page di atas*	Perilaku

No	Klausa	Tipe Proses
38.	*Wannacry meminta ransom*	Material
39.	*Wannacry meminta dana tebusan*	Material
40.	*File file (yang dibajak dengan enkripsi) bisa dikembalikan dalam keadaan normal lagi*	Material
41.	*Dana tebusan yang diminta adalah dengan pembayaran bitcoin yang setara dgn 300 dollar amerika.*	Relasional
42.	*Wannacry memberikan alamat bitcoin untuk pembayarannya*	Material
43.	*... memberikan deadline waktu terakhir pembayaran*	Material
44.	*denda tebusan bisa naik*	Perilaku
45.	*... belum dibayar juga*	Material
46.	*Lakukan beberapa langkah berikut*	Material
47.	*Cabut Kabel LAN/Wifi*	Material
48.	*Lakukan Backup Data*	Material
49.	*Update Anti-Virus*	Material
50.	*Update security pada windows*	Material
51.	*install Patch MS17-010 yang dikeluarkan oleh microsoft*	Material
52.	*Lihat : https://technet.microsoft.com/en-us/library/security/ms17-010.aspx*	Material
53.	*Jangan mengaktifkan fungsi macros*	Material
54.	*Non aktifkan fungsi SMB v1*	Material
55.	*Block 139/445 & 3389 Ports*	Material
56.	*Ulangi*	Material
57.	*selalu backup file file penting di komputer anda*	Material
58.	*disimpan backupnya ditempat lain*	Material
59.	*belum ada solusi yang paling cepat*	Eksisitensial
60.	*belum ada solusi yang paling jitu*	Eksistensial
61.	*... mengembalikan file file yang sudah terinfeksi wannacry*	Material
62.	memutuskan sambungan internet dari komputer yang terinfeksi	Material
63.	*.... menghentikan penyebaran wannacry ke komputer lain*	Material
64.	*ID-SIRTII menghimbau*	Mental
65.	*mohon diwaspadai ancaman ini*	Mental
66.	*melakukan hal-hal sebagai berikut*	Material
67.	*jangan terhubung ke LAN*	Material
68.	*jangan terhubung ke internet*	Material
69.	*lakukan backup data penting*	Material
70.	*Pastikan software anti virus sudah update*	Material
71.	*security patch (yang disarankan oleh microsoft) dilakukan terlebih dahulu*	Material

Tabel Transitivitas

Lampiran 2

No	Klausa	Tipe Proses
1.	*Kepala Badan Intelijen Negara (BIN) Budi Gunawan mengimbau seluruh instansi publik strategis*	Mental
2.	*... meningkatkan kemampuan sistem pengamanan informasi*	Material
3.	*... menyusul ancaman virus komputer jenis ransomware*	Material
4.	*... bernama Wanna Decryptor atau WannaCry*	Relasional
5.	*Serangan seperti itu merupakan bentuk ancaman baru berupa proxy war*	Relasional
6.	*Serangan seperti itu merupakan bentuk ancaman baru berupa cyber war*	Relasional
7.	*... melemahkan suatu negara*	Material
8.	*tegas pria yang kerap disapa BG*	Verbal
9.	*Senin (15/5)*	Relasional
10.	*dia meminta...*	Mental
11.	*negara dan seluruh instansi terkait pengamanan informasi, harus mulai merubah paradigma sistem pengamanan informasi*	Perilaku
12.	*pengamanan informasi konvensional seperti Firewall*	Relasional
13.	*pengamanan informasi konvensional seperti anti virus*	Relasional
14.	*pengamanan jenis ini memiliki kemampuan deteksi serangan secara dini*	Relasional
15.	*tak kalah penting katanya*	Verbal
16.	*koordinasi harus dilakukan*	Relasional
17.	*konsolidasi harus dilakukan*	Relasional
18.	*... mutlak dilakukan*	Relasional
19.	*Hal ini untuk mempercepat proses mitigasi*	Relasional
20.	*terjadi serangan secara masif*	Material
21.	*lanjut dia*	Verbal
22.	*terjadi serangan cyber*	Material
23.	*adanya konsolidasi*	Eksistensial
24.	*adanya koordinasi*	Eksistensial
25.	*adanya pertukaran cyber intelligence*	Eksistensial
26.	*... menentukan mitigasi*	Material
27.	*... menentukan tindakan preventif*	Material
28.	*terjadi serangan*	Material
29.	*BG menjelaskan*	Verbal
30.	*serangan terhadap sistem informasi intansi publik itu berawal*	Relasional
31.	*bocornya tool yang digunakan oleh National Security Agency (NSA)*	Material
32.	*Yaitu sebuah kode pemrograman*	Relaisonal
33.	*memanfaatkan kelemahan sistem dari Microsoft Windows.*	Material
34.	*Exploit itu digunakan*	Material
35.	*Group hacker yang menyebarkannya adalah Shadow Broker*	Relasional
36.	*Motif serangan berubah*	Perilaku
37.	*dulunya dilakukan oleh negara*	Material
38.	*serangan yang dilakukan merugikan masyarakat banyak*	Relasional
39.	*... dilihat dari exploit yang dibocorkan*	Material

No	Klausa	Tipe Proses
40.	*perlu kewaspadaan*	Mental
41.	*digunakan oleh state hacker*	Material
42.	*digunakan oleh non state hacker*	Material
43.	*melakukan penetrasi*	Material
44.	*memiliki kelemahan*	Relasional
45.	*tidak sempat diantisipasi oleh pembuat sistem*	Material
46.	*Sebelumnya disebutkan...*	Verbal
47.	*dua RS yaitu RS Dharmais dan RS Harapan Kita*	Relasional
48.	*diserang virus Ransomware*	Material
49.	*virus Ransomware jenis WannaCry*	Relasional
50.	*RS Dharmais yang positif diserang virus tersebut*	Relasional
51.	*seperti apa bahaya virus WannaCry?*	Relasional
52.	*Semuel A. Pangerapan Kementerian Komunikasi dan Informatika menyampaikan serangan siber...*	Verbal
53.	*serangan siber ini bersifat masif*	Relasional
54.	*serangan siber ini menyerang critical resource*	Material
55.	*serangan ini bisa dikategorikan sebagai teroris siber*	Relasional
56.	*kami minta*	Material
57.	*masyarakat tetap tenang*	Relasional
58.	*Masyarakat meningkatkan kehati-hatian*	Material
59.	*... disapa Semmy*	Material
60.	*Semmy menjelaskan serangan siber*	Verbal
61.	*serangan siber yang menyerang Indonesia berjenis ransomware*	Relasional
62.	*Ransomware adalah sebuah jenis malicious software*	Relasional
63.	*Ransomware adalah sebuah jenis malware*	Relasional
64.	*menyerang komputer korban*	Material
65.	*mengunci komputer korban*	Material
66.	*meng-encrypt semua file*	Material
67.	*tidak bisa diakses kembali*	Material
68.	*sebuah jenis ransomware baru telah muncul*	Eksistensial
69.	*sebuah jenis ransomware baru diperkirakan*	Mental
70.	*bisa memakan banyak korban*	Material
71.	*Ransomware baru ini disebut WannaCry*	Relasional
72.	*WannaCry ransomware mengincar PC*	Material
73.	*PC berbasis windows*	Relasional
74.	*... memiliki kelemahan*	Relasional
75.	*diduga serangan WannaCry*	Mental
76.	*serangan WannaCry sudah memakan banyak korban*	Material
77.	*penting untuk melakukan serangkaian tindakan pencegahan*	Relasional
78.	*penting untuk melakukan serangkaian tindakan penanganan*	Relasional
79.	*terjadi insiden*	Material

Tabel JawaPos

Lampiran 3

No	Klausa	Tipe Proses
1.	*Penyebaran ransomware WannaCry menimbulkan kekhawatiran besar*	Material
2.	*program jahat ini bisa masuk diam-diam*	Material
3.	*... tanpa diketahui*	Material
4.	*... mengenkripsi data di dalamnya*	Material
5.	*komputer terkunci*	Material
6.	*komputer tidak bisa dipakai*	Material
7.	*WannaCry pun tak pandang bulu*	Perilaku
8.	*... menyerang korban*	Material
9.	*Sejumlah rumah sakit di Indonesia dibuat kesulitan*	Material
10.	*... memberikan layanan medis*	Material
11.	*komputernya dikunci oleh sang ransomware*	Material
12.	*Kejadian serupa terjadi pula di Inggris*	Material
13.	*16 rumah sakit menjadi korban WannaCry*	Relasional
14.	*sang ransomware sudah menyebar ke 99 negara*	Material
15.	*... menginfeksi puluhan ribu sistem komputer*	Material
16.	*... menginfeksi ratusan ribu sistem komputer*	Material
17.	*... Dibanding ransomware lain*	Relasional
18.	*WannaCry lebih canggih*	Relasional
19.	*WannaCry lebih berbahaya*	Relasional
20.	*Ransomware ini tak butuh campur tangan pengguna*	Relasional
21.	*Bisa menginfeksi komputer*	Material
22.	*... diperlukan untuk menyebar*	Mental
23.	*Apa rahasianya?*	Relasional
24.	*WannaCry memanfaatkan tool senjata cyber*	Material
25.	*tool senjata cyber milik dinas intel Amerika Serikat pada April lalu dicuri*	Material
26.	*tool senjata cyber milik dinas intel Amerika Serikat pada April lalu dibocorkan*	Material
27.	*kelompok hacker bernama Shadow Broker*	Relasional
28.	*Tool bernama "EnternalBlue"*	Relasional
29.	*... memanfaatkan celah keamanan*	Material
30.	*... berhasil masuk ke satu komputer*	Material
31.	*worm dalam WannaCry secara otomatis akan mencari sendiri komputer lain*	Material
32.	*Akibatnya fatal*	Relasional
33.	*komputer-komputer yang diserang akan terkunci*	Material
34.	*Data didalamnya dienkripsi*	Material
35.	*... tidak bisa diakses.*	Material
36.	*Malware hanya menampilkan pesan di layar komputer*	Material
37.	*isinya meminta tebusan Rp 4 juta dalam bentuk mata uang virtual Bitcoin*	Relasional
38.	*transaksinya tak bisa dilacak*	Material
39.	*tebusan dibayar ke dompet digital*	Material
40.	*tak ada jaminan*	Eksistensial
41.	*si pembuat ransomware benar-benar akan mengirimkan kunci enkripsi*	Material

No	Klausa	Tipe Proses
42.	*... membuka data di komputer korban*	Material
43.	*M. Salahuddin mengungkapkan potensi penyebaran ransomware WannaCry*	Verbal
44.	*penyebaran ransomware WannaCry masih terbuka*	Relasional
45.	*kejadian awalnya berlangsung di akhir pekan*	Material
46.	*sebagian kantor sedang libur*	Material
47.	*... mematikan komputer*	Material
48.	*komputer kembali dinyalakan*	Material
49.	*WannaCry bisa menyusup masuk ke komputer*	Material
50.	*... meluas di jaringan*	Material
51.	*ini long weekend*	Relasional
52.	*... sudah terinfeksi*	Material
53.	*Senin pada aktif*	Material
54.	*... jadi bencana yang meluas*	Relasional
55.	*kerap disapa Didin*	Material
56.	*Bagaimana cara mencegah*	Material
57.	*jangan sampai menjadi korban*	Material
58.	*Didin menyarankan...*	Material
59.	*pengguna tidak langsung menyalakan komputer*	Material
60.	*pengguna tidak langsung menyambungkan komputer*	Material
61.	*pengguna diimbau*	Mental
62.	*terlebih dahulu mem-backup data penting*	Material
63.	*Terlebih dahulu melakukan update Windows*	Material
64.	*celah keamanan yang dieksploitasi oleh WannaCry sebenarnya sudah ditambal melalui patch sekuriti Windows oleh Microsoft pada Maret 2017 lalu*	Material
65.	*belum semua komputer memasang update tersebut*	Material
66.	*semua komputer memasang update tersebut*	Material
67.	*Pemerintah melalui Kementerian Komunikasi dan Informatika telah merumuskan langkah-langkah pencegahan infeksi ransomware WannaCry*	Material
68.	*Selengkapnya bisa dilihat di bawah*	Material
69.	*Cabut sambungan LAN*	Material
70.	*matikan Wi-Fi komputer*	Material
71.	*Update sekuriti Windows*	Material
72.	*memasang patch MS17-010*	Material
73.	*dapat diperoleh di tautan berikut*	Material
74.	*Pengguna Windows XP disarankan*	Mental
75.	*... mengganti sistem operasi ke versi yang lebih baru*	Material
76.	*OS lawas ini sudah tidak mendapat dukungan patch sekuriti dari Microsoft*	Material
77.	*Jangan mengaktifkan fungsi macros*	Material
78.	*Non aktifkan fungsi SMB v1.*	Material
79.	*Blokir port 139/445 dan 3389*	Material
80.	*Perbarui software anti-virus dan anti-ransomware*	Material
81.	*Selalu backup file penting di komputer*	Material

No	Klausa	Tipe Proses
82.	*simpan di tempat lain*	Material
83.	*... memungkinkan di storage*	Material
84.	*tidak terhubung ke jaringan*	Material
85.	*Tidak terhubung ke internet*	Material
86.	*... dirasa (tidak dapat dilakukan sendiri)*	Mental
87.	*Anda bisa meminta bantuan rekan*	Material
88.	*Anda bisa ke tim TI kantor*	Material
89.	*Apa yang bisa dilakukan*	Material
90.	*terlanjur terinfeksi ransomware WannaCry*	Material
91.	*belum ada solusi yang cepat*	Eksistensial
92.	*Belum ada solusi yang jitu*	Eksistensial
93.	*mengembalikan data yang disandera*	Material
94.	*putuskan sambungan ke internet*	Material
95.	*putuskan sambungan ke jaringan*	Material
96.	*infeksi tak menyebar ke komputer lain*	Material

Tabel Kompas.com