BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Ekstremisme berbasis kekerasan yang mengarah pada terorisme sudah menjadi isu berkepanjangan di Indonesia. Dengan perkembangan peradaban yang menjadi serba digital, ancaman yang ada pun juga berevolusi. Indonesia sebagai negara berkembang tentunya harus terus bersiap dalam menghadapi ancaman-ancaman yang terus berkembang. Media sosial membuat semua orang dapat terekspos dengan seluruh bentuk informasi yang ada di Internet, baik itu bermanfaat ataupun mengancam. Pandemi Covid-19 pun membuat media sosial menjadi salah satu sumber infomasi utama bagi masyarakat.

Melalui pertimbangan-pertimbangan diatas, Indonesia sebagai sebuah negara berupaya melakukan tindakan sekuritisasi untuk melindungi masyarakat yang terancam eksposur ekstremisme berbasis kekerasan di ruang digital. Perihal radikalisme di media sosial, banyak aspek yang melingkupi ancaman ini. Dari batas-batas ruang siber yang belum jelas, entitas-entitas yang bisa berbuat tanpa adanya konsekuensi, teknologi di dalam ruang siber yang terus berkembang tanpa henti, hingga pertimbangan hak asasi manusia untuk menyampaikan pendapat.

Hingga pada baru-baru ini terdapat suatu pemahaman mengenai keamanan siber sosial yang menawarkan pandangan baru mengenai bagaimana informasi dan jaringan di internet diolah menjadi suatu hal yang dapat diamati dan ditanggulangi. Ruang siber sendiri menjadi suatu ladang yang penuh lika-liku dan memerlukan tata kelola yang lebih untuk dapat menghadapi isu-isu yang ada. Oleh karena itu

pemetaan upaya sekuritisasi dan arsitektur keamanan siber sosial pemerintah Indonesia dalam menghadapi ekstremisme berbasis kekerasan yang mengarah pada terorisme di ruang digital dibutuhkan, dimana peneliti melakukan wawancara untuk mendapatkan data langsung dari instansi terkait.

Berdasarkan penelitian yang sudah dilakukan, pemerintah Indonesia melakukan upaya sekuritisasi melalui beberapa aktor yang melakukan tindakan *speech act*. Aktor-aktor tersebut adalah Presiden Republik Indonesia Joko Widodo, BSSN, BNPT, Kominfo, POLRI, dan DPR RI. Kemudian peneliti menemukan bahwa ekstremisme berbasis kekerasan di ruang digital yang mengarah pada terorisme sebagai sebuah *existential threat* dengan dampak yang dihasilkan apabila hal tersebut dibiarkan. Kemudian masyarakat Indonesia sebagai *referent object* karena merupakan tanggungjawab dari pemerintah sendiri untuk melindungi rakyatnya. Lalu hasil dari sekuritisasi ini adalah dua peraturan presiden yang juga menghasilkan Rencana Aksi nasional, yaitu Strategi Keamanan Siber Nasional dan Rencana Aksi Nasional Pencegahan dan Penanggulangan Ekstremisme Berbasis Kekerasan Yang Mengarah Pada Terorisme.

Dalam arsitektur keamanan siber sosial pemerintah Indonesia, terdapat empat komponen yang peneliti temukan. Komponen pertama adalah Strategi Keamanan Siber Nasional (SKSN), dimana strategi ini berupaya untuk meningkatkan penjagaan berkelanjutan terhadap masyarakat Indonesia di ruang siber melalui aspek keamanan siber teknis dan sosial. Dalam pengaplikasian SKSN ini, BSSN juga menerapkan sistem Quadhelix yang melibatkan pemerintah, akademisi, pihak swasta, dan masyarakat umum. Kemudian yang kedua terdapat

pendekatan sistem Pentahelix BNPT yang mana memiliki komponen sama dengan Quadhelix namun menambah pihak media. Lalu yang terakhir kerjasama internasional, dimana kerjasama ini sangat berpengaruh terhadap perkembangan ilmu-ilmu penanggulangan radikalisme di media sosial, serta pemerintah Indonesia juga sudah banyak berinisiatif untuk mendapatkan akses terhadap jaringan penyebaran radikalisme yang lebih besar melalui intelijen dari negara lain.

Dalam penanggulangan radikalisme di media sosial, peneliti mengambil dua perspektif untuk menganalisis upaya dan arsitektur keamanan siber sosial milik pemerintah Indonesia. Perspektif pertama datang dari UNESCO melalui pendekatan *Online Prevention Initiatives* yang menawarkan metode literasi media dan Informasi, serta kontra narasi. Peneliti sendiri menemukan bahwa metode-metode tersebut sudah dilakukan pemerintah Indonesia melalui upaya dan arsitektur keamanan siber sosial berbentuk program-program literasi, kampanye positif, dan penyebaran ilmu positif di berbagai tingkatan pendidikan.

Perspektif kedua peneliti ambil berdasarkan riset dari *International Journal of Conflict and Violence,* yaitu *Counter Strategies Against Online Extremism.* Riset ini sendiri menawarkan dua strategi yaitu strategi reaktif dan proaktif. Pada aspek proaktif sendiri, dikarenakan sejarah Indonesia yang sudah memiliki pengalaman dalam menghadapi radikalisme, strategi-strategi proaktif seperti kontra narasi dan penggunaan teknologi sebagai alat deteksi sudah memiliki pondasi yang cukup kuat untuk dijalankan secara berkelanjutan. Sedangkan, peneliti menemukan bahwa melalui upaya dan arsitektur keamanan siber sosial, Indonesia masih perlu mengembangkan dalam aspek peningkatan kredibilitas sosial-politik dan teologis,

serta penekanan yang lebih terhadap platform-platform internet dan media sosial yang ada di Indonesia. Sementara itu, aspek-aspek lain seperti kerjasama dengan berbagai pihak, pendekatan global, dan penyensoran Pemerintah Indonesia sudah dapat melingkupi strategi tersebut melalui sistem-sistem Quadhelix dan Pentahelix, kerjasama internasional, dan peran kerja Kominfo.

5.2 Saran

Dengan arsitektur keamanan siber sosial milik pemerintah indonesia, dimana di dalamnya terdapat sistem Quadhelix milik BSSN dan sistem Pentahelix milik BNPT. Izinkan peneliti sebagai seorang akademisi untuk menyarankan sebuah kerangka kerja untuk membaca dan menanggulangi manuver-manuver informasi yang sekiranya dilakukan oleh pelaku penyebaran radikalisme di Indonesia. Kerangka kerja ini merupakan sebuah pengelompokan jenis-jenis manuver infomasi dan jaringan yang dilakukan oleh Kathleen M. Carley bernama BEND *Framework.* BEND *Framework* ini menggambarkan bagaimana suatu entitas dapat memanipulasi keyakinan, ide, dan informasi (K. M. Carley, 2020). Bentuk-bentuk manuver ini dibangun berdasarkan paradigma *dismiss*, *distort*, *dismay*, dan *distract* yang diperkenalkan oleh Ben Nimmo (K. Carley & Beskow, 2019). BEND mengkategorikan bentuk-bentuk manuver berdasarkan polaritas serta apakah targetnya adalah informasi atau objek. Dimana penjelasan lebih jelasnya dapat dilihat melalui gambar 5.1.

	Information Maneuver		Network Maneuver	
	Knowledge network manipulation		Social network manipulation	
	Things you can do by affecting what is being discussed		Things you can do by affecting who is talking/listening to whom	
Positive	**Engage**	Discussion that brings up a related but relevant topic	**Back**	Actions that increase the importance of the opinion leader
	Explain	Discussion that provides details on or elaborates the topic	**Build**	Actions that create a group or the appearance of a group
	Excite	Discussion that brings joy/happiness/cheer/enthusiasm to group	**Bridge**	Actions that build a connection between two or more groups
	Enhance	Discussion that encourages the group to continue with the topic	**Boost**	Actions that grow the size of the group or make it appear that it has grown
Negative	**Dismiss**	Discussion about why the topic is not important	**Neutralize**	Actions that limit the effectiveness of opinion leader such as by reducing the number who can or do follow or reply or attend to
	Distort	Discussion that alters the main message of the topic	**Nuke**	Actions that lead to a group being dismantled
	Dismay	Discussion about a topic that will bring worry/sadness/anger to group	**Narrow**	Actions that lead to the group becoming sequestered from other groups
	Distract	Discussion about a totally different topic and irrelevant	**Neglect**	Actions that reduce the size of the group or make it appear that the group has grown smaller

Gambar 5.1 BEND *Framework*

Sumber: (K. Carley & Beskow, 2019)

Seperti yang sudah terlihat, gambar 5.1 memisahkan antara *information maneuver* dan *network maneuver*. Manuver informasi sendiri adalah manipulasi informasi dan aliran atau relevansi informasi di dunia maya, sedangkan manuver jaringan adalah manipulasi dari jaringan sosial daring yang sudah terbentuk (K. Carley & Beskow,

2019). Berikut penjelasan dari masing-masing manuver baik yang positif maupun negatif.

- Manuver infomasi
  - Positif
    - *Engage*: pesan yang mengangkat topik terkait namun relevan
    - *Explain*: pesan yang memberikan rincian atau menguraikan topik
    - *Excite*: pesan yang menimbulkan emosi positif seperti kegembiraan atau kegembiraan
    - *Enhance*: pesan yang mendorong kelompok topik untuk melanjutkan topik tersebut
  - Negatif
    - *Dismiss* : pesan tentang mengapa topik tersebut tidak penting
    - *Distort* : pesan yang mengubah pesan utama topik
    - *Dismay*: pesan yang menimbulkan emosi negatif seperti kesedihan atau kemarahan
    - *Distract*: diskusi tentang topik yang sama sekali berbeda dan tidak relevan

- Manuver jaringan
  - Positif
    - *Back*: Tindakan yang meningkatkan pentingnya pemimpin opini atau menciptakan pemimpin opini baru
    - *Build*: tindakan yang membuat grup atau tampilan grup
    - *Bridge*: tindakan yang membangun hubungan antara dua kelompok atau lebih
    - *Boost*: Tindakan yang memperbesar ukuran grup atau membuatnya tampak berkembang
  - Negatif
    - *Neutralize*: Tindakan yang mengurangi pentingnya pemimpin opini
    - Nuke: Tindakan yang menyebabkan suatu kelompok dibubarkan atau dibubarkan, atau terkesan terpecah
    - *Narrow*: Tindakan yang menyebabkan suatu kelompok menjadi terasing dari kelompok lain atau terpinggirkan
    - *Neglect*: Tindakan yang mengurangi ukuran kelompok atau membuat kelompok tampak semakin kecil.

Dengan adanya *BEND Framework* peneliti mengharapkan adanya pemahaman lebih lanjut oleh pemerinta Indonesia terkait manipulasi informasi dan jaringan yang dilakukan oleh entitas-entitas yang ingin melakukan operasi informasi, dimana salah satu jenis operasi tersebut adalah penyebaran radikalisme di media sosial Indonesia. Dimana dengan pemahaman tersebut pemerintah Indonesia akan lebih mudah memahami bagaimana kontra narasi yang harus dilakukan melalui kerangka kerja dari keamanan siber sosial Ini.