BAB VI

KESIMPULAN

6.1 Kesimpulan

Kesimpulan dari analisis operasi siber Rusia dalam konflik Rusia-Ukraina periode 2021-2022 dengan konsep *Information Operations* menunjukkan bahwa Rusia secara efektif memanfaatkan peperangan siber sebagai bagian integral dari strategi militernya. Dalam konflik ini, Rusia menggunakan serangan siber yang disinkronisasi dengan operasi disinformasi, propaganda, dan penguasaan narasi global untuk mencapai tujuan geopolitiknya. Operasi siber Rusia meliputi tiga komponen utama: *Computer Network Attack* (CNA), *Computer Network Defense* (CND), dan *Computer Network Exploitation* (CNE). Rusia menggunakan CNA untuk menyerang infrastruktur vital Ukraina, seperti jaringan listrik, telekomunikasi, dan perbankan, dengan serangan malware seperti NotPetya dan AcidRain yang melumpuhkan sistem penting Ukraina. Serangan-serangan ini tidak hanya bertujuan untuk mengganggu infrastruktur, tetapi juga untuk menciptakan ketidakstabilan sosial dan melemahkan kepercayaan publik terhadap pemerintah Ukraina. Di sisi lain, CND Rusia sangat berhasil mempertahankan sistem komputasi dari serangan siber eksternal, memastikan bahwa operasi militer dan strategi sibernya tidak terganggu. Selain itu, melalui CNE, Rusia mengakses dan mengeksploitasi jaringan komputer Ukraina untuk mencuri data intelijen yang digunakan untuk memperkuat operasi militernya dan mendukung kampanye disinformasi.

Pendekatan Rusia dalam operasi siber tidak dapat dipisahkan dari penggunaan disinformasi dan pengendalian narasi publik di ruang digital. Serangan siber ini bekerja berdampingan dengan konsep operasi informasi yang didukung oleh bot otomatis dan troll untuk menyebarkan narasi pro-Rusia, membingungkan opini publik global, serta mengaburkan fakta tentang tindakan militer di Ukraina. Rusia juga memanfaatkan media tradisional dan sosial, seperti RT dan Sputnik, untuk memperkuat narasinya, yang menggambarkan invasi sebagai upaya defensif melawan ancaman NATO dan Barat.

Dengan demikian, operasi siber Rusia dalam konflik ini merupakan implementasi dari model *Information Operations* yang mencakup manipulasi informasi, penguasaan ruang siber, dan pengendalian narasi global. Serangan siber ofensif dan disinformasi yang terkoordinasi menciptakan ketidakpastian dan kebingungan, sementara Rusia terus membangun narasi yang memperkuat legitimasi tindakannya di mata audiens global. Strategi ini menegaskan bahwa dalam perang modern, kontrol informasi dan persepsi publik sama pentingnya dengan kekuatan militer di medan tempur fisik.

6.2 SARAN

6.2.1 Saran Praktis

Bagi Rusia, diperlukan peningkatan koordinasi yang lebih kuat antara operasi siber dan kampanye informasi agar dampaknya lebih efektif di arena global. Disinformasi yang disebarkan harus lebih fleksibel dan mampu menyesuaikan diri dengan ekosistem informasi yang kini semakin diatur oleh platform media sosial. Dalam hal ini, Rusia perlu mengadopsi strategi yang lebih terfokus dan cerdas untuk menghadapi resistensi dari negara-negara Barat, yang sudah semakin terampil dalam mendeteksi dan menangkal upaya disinformasi. Upaya ini juga harus mencakup peningkatan kualitas operasi siber dengan cara mengembangkan serangan yang lebih sulit dideteksi dan dilawan, terutama yang menyasar infrastruktur penting dari lawan. Mengoptimalkan kecepatan dan efektivitas dalam merespons serangan siber juga akan memberi Rusia keunggulan dalam konflik siber modern, di mana kecepatan tindakan menjadi faktor penentu keberhasilan. Sementara itu, di sisi Ukraina, kolaborasi yang lebih erat dengan negara-negara Barat sangat penting dalam memperkuat sistem pertahanan siber. Ukraina harus fokus pada pengembangan teknologi keamanan yang lebih canggih dan berkelanjutan, memanfaatkan pengalaman dan keahlian Barat untuk meningkatkan ketahanan terhadap serangan siber. Di samping itu, kampanye media sosial Ukraina juga perlu terus diperkuat dengan narasi yang lebih kuat dan emosional, sehingga dapat terus menarik simpati dan

dukungan internasional. Penyampaian pesan yang mampu menggugah hati masyarakat global, terutama di negara-negara yang netral atau skeptis, akan menjadi elemen kunci dalam mempertahankan dukungan jangka panjang terhadap perjuangan Ukraina dalam konflik ini.

6.2.2 Saran Teoritis

Dari perspektif *Information Operations* (IO), analisis menunjukkan bahwa strategi Rusia dalam konflik ini mengintegrasikan berbagai elemen IO seperti disinformasi, pengendalian narasi publik, dan serangan siber untuk mempengaruhi persepsi global dan melemahkan moral musuh. Teorinya, *Information Operations* menggambarkan bahwa kontrol terhadap arus informasi dan kemampuan memanipulasi persepsi publik merupakan kekuatan strategis yang setara dengan keunggulan militer konvensional. Konflik Rusia-Ukraina menegaskan pentingnya penguasaan penuh terhadap lingkungan informasi, baik di ranah domestik maupun internasional, dengan tujuan membentuk opini publik yang mendukung, mengurangi dukungan bagi lawan, dan menciptakan kebingungan di antara audiens global. Keberhasilan IO di sini bukan hanya tentang volume informasi yang disebar, tetapi juga tentang bagaimana negara mampu mempengaruhi keputusan politik dan sosial melalui kontrol narasi. Integrasi serangan siber dengan operasi informasi, seperti yang dilakukan Rusia, menunjukkan bahwa IO yang efektif adalah perpaduan antara disrupsi teknologi dengan kampanye pengaruh yang tepat sasaran, yang berfungsi untuk menciptakan keunggulan strategis dalam medan perang modern.