BAB 1

PENDAHULUAN

1.1 Latar Belakang

Konsep strategi *cyber warfare* harus ditetapkan dalam aspek strategis, operasional, dan taktis berdasarkan konsep strategi militer (Kim, Cheon, and Eom 2019). Teknologi telah mengubah cara berperang, yang mana jarak dan medan menjadi kurang penting, karena drone dan ruang siber telah mengecilkan pertimbangan-pertimbangan ke tingkat yang lebih besar (Azad and Haider 2022). Hal tersebut menjadikan definisi bahwa *cyber warfare* menjadi ancaman yang mendesak, namun tetap mempertahankan cakupan yang luas (Ashraf 2021).

Berangkat dari penjelasan sebelumnya, dalam karakteristik *cyberspace* terdapat lapisan unik yang mempengaruhi pendekatan taktik pada *cyber warfare*. Terdapat lapisan manusia, bahwa aktivitas keamanan di ruang siber bertujuan untuk mempengaruhi perilaku pengguna. Adapun lapisan logikal, yang melakukan serangan melalui perangkat lunak dengan tujuan seperti spionase, mengganggu komputer musuh, atau menyerang sistem fisik yang dikendalikan melalui siber. Tidak hanya itu, terdapat lapisan fisik, serangan dapat menargetkan perangkat keras dan infrastruktur pendukung ruang siber (Even and Siman Ṭov 2012).

Rusia menjadi salah satu negara adidaya pada abad ke-18, abad ke-19, dan hampir sepanjang abad ke-20. Tentaranya yang menang memasuki Berlin pada abad ke-18 yang dikenal sebagai perang tujuh tahun (1756-1763), Paris pada abad ke-19 yang melawan Napoleon (1814), dan Berlin lagi pada abad ke-20 sebagai akhir Perang Dunia II (1945), telah menunjukkan peran perang sebagai mekanisme seleksi dalam politik internasional. Terlebih dari itu, Rusia secara umum dianggap

telah muncul kembali sebagai kekuatan besar di abad ke-21, meskipun hal tersebut masih kontroversial (Ellman 2022). Hal tersebut didukung dengan kepemimpinan Vladimir Putin, bahwa Rusia modern berani menunjukkan kekuatannya terhadap negara-negara tetangga, serta meluas di luar wilayah pengaruh tradisionalnya, meskipun secara teori kurang memiliki banyak kekuatan tradisional dibandingkan pesaing utamanya, seperti Amerika Serikat dan Tiongkok (Stoner 2021).

Berdasarkan laporan dari situs web Lowy Institute Asia Power Index, Rusia menduduki pada peringkat 3 dengan skor 90.1 tentang *cyber capabilities* pada tahun 2022-2024. Peringkat Rusia mengalami penurunan yang signifikan, namun diperkuat dengan ukuran ketahanan. Rusia meningkatkan skornya untuk kemampuan militer, dengan memobilisasi ekonomi perang untuk mendukung perangnya di Ukraina (Lowy Institute Asia Power Index, n.d.). Adapun laporan dari Universitas Harvard pada 27 September 2022, bahwa Rusia menempati posisi tiga negara teratas dengan kemampuan siber terbesar, mengalahkan Inggris yang menjadi posisi keempat. Dalam laporan tersebut, Rusia telah meningkat sebagian besar karena lebih banyak operasi siber yang telah dilaporkan secara publik pada kekuatan siber (Voo, Hemani, and Cassidy 2022, DiMolfetta 2022).

Cyber warfare menjadi jenis serangan siber (operasi siber) tingkat tertinggi dan paling kompleks yang dilakukan terhadap kepentingan siber nasional suatu negara (Li and Liu 2021). Hal tersebut dapat dikaitkan dengan Rusia yang mulai memprioritaskan pengembangan kemampuan siber sebagai bentuk perang asimetris yang lebih hemat biaya namun mampu menimbulkan kerusakan signifikan. Selama tahun 2010-an, Rusia memperkuat kekuatan siber ofensifnya sebagai pengganti keterbatasan militer konvensional. *Cyber warfare* menjadikan Rusia dapat

mengatasi keterbatasan geografis, populasi yang menurun, dan anggaran militer yang terbatas, sambil mempertahankan elemen kejutan dalam konflik tanpa risiko besar pembalasan langsung. Strategi *cyber warfare* pun sejalan dengan ambisi Presiden Vladimir Putin untuk mengembalikan Rusia sebagai kekuatan dunia, sehingga menjadikan perang siber sebagai pilar utama kekuatan militer modern mereka (Nayar 2021).

Dalam konteks pemanfaatan *cyber capabilities*, berbagai strategi telah diidentifikasi oleh para ahli, termasuk Ralph Thiele, yang dalam bukunya menyebutkan 13 strategi utama yang dapat digunakan oleh aktor dengan *cyber capabilities*. Strategi tersebut meliputi pemahaman peluang dan tantangan operasional siber, pengumpulan data dan pemodelan target, serta manipulasi informasi dan sistem jaringan. Strategi lainnya termasuk sabotase infrastruktur kritis, serangan pada jaringan komando dan kontrol, hingga konvergensi siber dengan perang elektromagnetik, kecerdasan buatan, dan aset ruang angkasa. Adapun strategi-strategi yang juga mencakup operasi ofensif untuk mencuri rahasia, mengganggu data, serta merusak kepercayaan pada kepemimpinan politik atau militer target (Thiele 2021).

Negara-negara besar, khususnya Rusia, berusaha menggunakan strategi *cyber warfare* untuk mempengaruhi keseimbangan kekuatan internasional demi keuntungan mereka (Noel and Reith 2021). Hal tersebut dikarenakan strategi *cyber warfare* mencerminkan ambisi Rusia untuk mempertahankan pengaruh geopolitik nya dengan memanfaatkan kekuatan teknologi siber sebagai alat utama dalam perang modern (Mueller et al. 2023). Pada tahun 2010-an, Rusia melakukan serangan siber bersamaan dengan bentuk-bentuk gangguan dan spionase siber

lainnya, untuk melakukan serangan siber yang terus menerus dengan menargetkan pemerintah, militer, telekomunikasi, dan infrastruktur teknologi informasi sektor swasta di Ukraina. Tidak hanya itu, serangan siber yang sangat ditargetkan di Ukraina (dan lebih luas lagi) telah terlihat sejak tahun 2014 (Stoddart 2024).

Dalam perang melawan Ukraina, Rusia memanfaatkan *cyber warfare* sebagai alat untuk mendukung operasi informasi dan propaganda global yang dirancang untuk mengurangi dukungan terhadap Kyiv, terutama di negara-negara *Global South*. Dapat dijelaskan bahwa Rusia memiliki pendekatan pada *cyber warfare* sebagai instrumen strategis yang dapat menciptakan gangguan, mendukung spionase, dan menyebarkan disinformasi dengan biaya rendah dibandingkan dengan serangan fisik langsung. Rusia menjadi negara yang sering menghadapi keterbatasan dalam mencapai tujuan militer konvensional, sehingga menggunakan *cyber warfare* untuk memperkuat pengaruh politiknya, melemahkan semangat musuh, dan menciptakan ketidakstabilan. Namun, efektivitasnya terbatas oleh kemampuan pertahanan siber Ukraina yang didukung oleh mitra internasional, serta sifat dari ranah siber yang cenderung lebih mendukung strategi defensif daripada ofensif (Mueller et al. 2023).

Rusia umumnya tidak berfokus pada istilah *cyber* atau *cyber warfare*, tetapi lebih memilih fokus pada istilah *information wars* (*информационные войны*) yang mencakup operasi jaringan komputer, perang elektronik, operasi psikologis, dan informasi. Cakupan tersebut menjadi bagian dari strategi dominasi lanskap informasi dalam kerangka perang informasi yang holistik (Connell and Vogler 2017, Krasovskaya and Gulyaev 2019). Para analis menilai pada implementasi operasi siber Rusia yang menjadi operasi berskala besar, efektif secara taktis, dan

selaras dengan tujuan militer Moskow untuk mengacaukan pemerintah, militer, serta warga sipil Ukraina (Bateman 2022). Dalam konteks invasi Rusia Ukraina 2022, Rusia melakukan penyebaran narasi palsu dan menyesatkan serta taktik lain, menciptakan kedok dukungan terhadap kelompok separatis di Ukraina Timur, dan menggoyahkan pemerintah Ukraina dengan kekuatan militer. Rusia melakukan pendekatan pada sejarah sebagai alat propaganda yang mencoba untuk menjelaskan pada sengketa atas warisan sejarah antara Rusia dan Ukraina (Aleksejeva 2023).

Selama bertahun-tahun, Rusia telah menjadi pengguna yang gigih dalam spionase siber untuk pengumpulan intelijen maupun persiapan medan perang di Ukraina, wilayah lain di luar negeri, dan di negara-negara barat (Stoddart 2024). Rusia yang memainkan peran teknologi canggih dapat memberikan keunggulan strategis dan taktis yang signifikan dalam berbagai aspek (McGuire 2021). Militer Rusia pun menganggap siber ofensif sebagai sarana penting untuk memberikan dampak strategis di lingkungan geopolitik yang penuh ancaman, sehingga banyak kemampuan siber ofensif yang dapat dilakukan oleh militer Rusia (Thornton and Miron 2022). Maka sebagai limitasi, dalam penelitian ini memfokuskan pada strategi serangan siber berbasis *Computer Network Attack* (CNA), sebagai pendukung dalam operasi militer yang diterapkan oleh Rusia dalam invasi ke Ukraina pada periode 2022–2024. Pemilihan periode 2022-2024 pun didasarkan pada konflik yang terjadi dan perkembangan yang signifikan oleh militer Rusia dalam peningkatan strategi siber dalam perang modern, yang bersamaan dengan meningkatnya kapasitas teknologi militer.

1.2 Rumusan Masalah

Bagaimana Rusia menerapkan strategi serangan siber berbasis *Computer Network Attack* (CNA) dalam invasi ke Ukraina pada tahun 2022-2024?

1.3 Tujuan Penelitian

Riset ini memiliki tujuan sebagai berikut:

1. Untuk menganalisis bagaimana strategi serangan siber berbasis *Computer Network Attack* (CNA) menjadi komponen strategis dalam mencapai tujuan operasional Rusia selama invasi ke Ukraina pada tahun 2022-2024.

1.4 Cakupan penelitian

Adapun cakupan dari penelitian ini yaitu strategi serangan siber berbasis *Computer Network Attack* (CNA) yang diterapkan oleh Rusia dalam invasi ke Ukraina pada periode 2022–2024. Penelitian ini menganalisis bagaimana strategi CNA digunakan untuk mendukung operasi militer Rusia, melumpuhkan infrastruktur kritis Ukraina, dan keamanan di tengah konflik tersebut.

Periode 2022–2024 dipilih karena mencerminkan puncak peningkatan strategi siber Rusia dalam perang modern, yang bersamaan dengan meningkatnya kapasitas teknologi militer dan respons signifikan dari Ukraina serta komunitas internasional. Penelitian ini juga mencakup kronologi dari dimulainya invasi, sebagai landasan perkembangan eskalasi konflik dan teknologi Rusia. Lebih dari itu, dengan adanya landasan dalam penelitian ini, maka dapat dikaitkan dengan bagaimana kemampuan Rusia mencapai tujuan geopolitik dengan strategi siber berbasis CNA.

1.5 Tinjauan Pustaka

Kajian mengenai strategi siber Rusia dalam invasi ke Ukraina menunjukkan bahwa *Computer Network Attack* (CNA) menjadi instrumen strategis yang diintegrasikan dengan operasi militer konvensional. Berdasarkan kerangka Winterfeld dan Andress (2012), CNA dipahami sebagai upaya mengganggu, menurunkan, atau menghancurkan sistem dan informasi melalui jaringan komputer. Dalam konteks mendukung dan memahami proses penelitian ini, yang berfokus pada tahun 2022-2024 dan dianalisis menggunakan kerangka pemikiran Steve Winterfeld dan Jason Andress, terdapat sejumlah penelitian lainnya yang cukup relevan sebagai tinjauan pustaka.

Pada dimensi jenis serangan, literatur menyoroti kombinasi *physical*, *electronic*, dan *logical warfare*. Khoirunnisa dan Cristy Sugiati (2024) dalam jurnal yang berjudul "Cyber Warfare Strategies in the Russia-Ukraine Conflict (2021-2022): Implications for National Security and Modern Warfare", menunjukkan bahwa Rusia memanfaatkan *logical warfare* melalui penyebaran malware seperti WhisperGate yang merusak data, serta *electronic warfare* dengan serangan DDoS yang melumpuhkan komunikasi pemerintah Ukraina (Khoirunnisa and Sugiati 2024). Ian A. Clark (2023) dalam jurnal yang berjudul "The Ethical Character of Russia's Offensive Cyber Operations in Ukraine", memperkuat temuan ini dengan menambahkan contoh gangguan satelit Viasat KA-SAT sebagai *electronic warfare* yang memengaruhi jaringan sipil dan militer (Clark 2023). Keir Giles (2023) dalam jurnal penelitian yang berjudul "Russian Cyber and Information Warfare in Practice", juga menekankan integrasi *logical warfare* dengan operasi informasi,

yang menciptakan efek psikologis pada publik sekaligus mengacaukan komunikasi militer (Giles 2023).

Strategi CNA Rusia juga dapat dipahami melalui kategori serangan operasional proaktif dan reaktif. Khoirunnisa dan Sugiati (2024) menilai serangan DDoS dan infiltrasi jaringan sebelum invasi fisik sebagai *proactive attack* yang bertujuan melemahkan sistem Ukraina sejak awal (Khoirunnisa and Sugiati 2024). Clark (2023) mengidentifikasi penggunaan *reactive attack* ketika Rusia memanfaatkan celah keamanan yang ditemukan pasca pemantauan, seperti dalam praktik *exfiltrate* terhadap data sensitif untuk tujuan strategis (Clark 2023). Giles (2023) menggambarkan bahwa Rusia memadukan kedua pendekatan tersebut secara adaptif, menyesuaikan intensitas serangan berdasarkan respon Ukraina dan dukungan internasional (Giles 2023).

Dalam proses serangan CNA, delapan proses serangan dari kerangka Winterfeld dan Andress (2012) dapat digunakan untuk memetakan pola Rusia. Khoirunnisa dan Sugiati (2024) mengaitkan *recon* dan *scan* dengan pengumpulan informasi awal melalui pemantauan jaringan dan teknik *phishing* (Khoirunnisa and Sugiati 2024). Tahap *access* dan *escalate* terlihat pada pemanfaatan kredensial curian serta eksploitasi sistem untuk memperluas kontrol. Clark (2023) menyoroti tahap *exfiltrate* dan *obfuscate* dalam pencurian data pribadi dan penyamaran jejak digital guna menghindari atribusi (Clark 2023). Giles (2023) menekankan *sustain* sebagai tahap strategis, yang mana Rusia mempertahankan akses jangka panjang untuk mengaktifkan serangan kembali sesuai situasi medan perang (Giles 2023).

Perbandingan ketiga sumber menunjukkan adanya konsistensi dalam melihat serangan siber dengan pendekatan CNA sebagai bentuk kekuatan Rusia.

Semua penulis sepakat bahwa serangan siber menjadi inti karena dampaknya langsung pada infrastruktur digital dan kemampuan komunikasi Ukraina. Tetapi terdapat perbedaan yang terletak pada fokus analisis, yaitu Khoirunnisa dan Sugiati (2024) menitikberatkan pada daftar aktor dan jenis serangan, Clark (2023) menambahkan perspektif etika serta pengendalian informasi, sedangkan Giles (2023) melihat hubungan erat propaganda dan adaptasi taktis. Perbedaan fokus tersebut dapat membantu dalam memberikan gambaran utuh tentang spektrum penggunaan CNA Rusia.

Kekuatan CNA Rusia dalam invasi ini juga terletak pada integrasi dengan domain lain. Clark (2023) dan Giles (2023) menunjukkan bahwa serangan siber sering dilakukan beriringan dengan operasi rudal atau pergerakan pasukan, sehingga efeknya berlapis. Hal tersebut sejalan dengan penekanan Winterfeld dan Andress (2012) bahwa CNA paling efektif jika disinergikan dengan metode perang lain. Lebih dari itu, efektivitas serangan proaktif Rusia terkadang terhambat oleh respons cepat Ukraina yang didukung sektor teknologi global, sebagaimana dicatat Giles (2023).

Walaupun terdapat variasi dalam keberhasilan taktis, literatur menunjukkan bahwa CNA tetap menjadi instrumen strategis yang relevan bagi Rusia. Integrasi CNA dengan propaganda dan operasi fisik menunjukkan pemahaman Rusia terhadap perang multidomain yang memadukan aspek teknis dan psikologis. Hal tersebut menegaskan bahwa CNA bukan sekadar pendukung, tetapi komponen inti yang membentuk strategi siber Rusia pada periode invasi 2022–2024.

Maka sebagai pembeda dari ketiga literatur tadi, penelitian ini berfokus pada analisis *Computer Network Attack* (CNA) karya Steve Winterfeld dan Jason

Andress sebagai komponen strategis dalam strategi serangan siber Rusia. Adapun celah penelitian yang muncul adalah minimnya kajian yang memetakan kedelapan proses CNA Rusia selama 2022–2024 secara sistematis dalam konteks operasi militer luas. Melalui pendekatan teoritis CNA, penelitian ini akan mengeksplorasi bagaimana Rusia memanfaatkan *physical*, *electronic*, dan *logical warfare* dengan langkah yang reaktif atau proaktif untuk mengevaluasi dampak geopolitik dari penerapan perang siber terhadap stabilitas internasional.

1.6 Kerangka Pemikiran

Computer Network Attack

Dalam buku karya Steve Winterfeld dan Jason Andress (2012) berjudul *The Basics of Cyber Warfare*, dijelaskan konsep strategi serangan ofensif melalui *Computer Network Attack* (CNA). Dalam konteks tersebut, CNA dipahami sebagai tindakan untuk mengganggu, menurunkan, atau menghancurkan informasi maupun sistem melalui jaringan komputer. Sebagai bagian dari strategi perang siber modern, CNA diposisikan sebagai instrumen vital dalam melumpuhkan kemampuan pertahanan musuh secara non-fisik. Penelitian ini menggunakan pendekatan teoritis dari CNA untuk menjelaskan strategi Rusia selama invasi ke Ukraina 2022–2024, dengan fokus pada tiga dimensi utama: jenis serangan, serangan operasional, dan proses serangan.

1. Jenis Serangan

Jenis serangan dalam CNA terbagi menjadi tiga kategori utama, yaitu *physical*, *electronic*, dan *logical warfare*. *Physical warfare* menunjukkan dampak langsung *cyber warfare* terhadap dimensi fisik, seperti gangguan logistik dan

komunikasi yang berdampak pada efektivitas operasi militer. Dijelaskan bahwa serangan siber dapat menargetkan infrastruktur fisik seperti jaringan listrik yang menjadi penopang sistem digital. Maka dari itu, aspek fisik tidak dapat diabaikan dalam strategi siber karena menentukan daya serang dan daya rusak secara langsung (Winterfeld and Andress 2012, 74).

Electronic warfare menargetkan spektrum elektromagnetik untuk mengacaukan sistem berbasis sinyal elektronik seperti komunikasi dan sensor. Dalam dimensi ini, serangan dilakukan tanpa kerusakan fisik namun cukup untuk membuat sistem musuh tidak berfungsi. Dapat dijelaskan juga bahwa peperangan elektronik dan siber sering dilakukan bersamaan dalam strategi yang menyasar kebergantungan lawan pada sistem teknologi (Winterfeld and Andress 2012, 74).

Logical warfare berfokus pada serangan digital murni yang menyasar perangkat lunak dan infrastruktur logis, seperti manipulasi data, sabotase, dan penghancuran sistem digital. Tidak bergantung pada sinyal atau fisik, dimensi ini menjadi inti serangan siber melalui cara-cara pengintaian atau manipulasi sistem. Efektivitas *logical warfare* akan meningkat apabila dikombinasikan dengan elemen dari warfare lainnya dalam satu strategi terpadu (Winterfeld and Andress 2012, 74-75).

2. Serangan Operasional

Serangan operasional CNA mencakup pendekatan reaktif dan proaktif dalam merancang serangan siber terhadap lawan. *Reactive attacks* dilakukan sebagai respons terhadap serangan atau ancaman yang telah terjadi, dengan diawali pengumpulan informasi dan pemetaan sistem musuh. Serangan ini menggunakan data dari pemantauan sebelumnya untuk mengidentifikasi titik lemah musuh

sebelum melancarkan aksi balasan yang terarah dan efisien (Winterfeld and Andress 2012, 75).

Proactive attacks merupakan pendekatan strategis untuk menyerang lebih dahulu sebelum musuh melancarkan serangan. Penyerang dapat menyiapkan serangan yang diaktifkan hanya pada waktu tertentu, seperti *logic bombs* atau malware yang tertanam dalam sistem lawan. Strategi ini memungkinkan pihak penyerang untuk memperoleh keunggulan secara diam-diam tanpa harus menunjukkan intensi agresi secara eksplisit (Winterfeld and Andress 2012, 75).

3. Proses Serangan

Proses serangan dalam CNA terdiri dari delapan tahapan yang saling berkaitan dan berurutan, dimulai dari *recon* hingga *obfuscate*. Tahap *recon* merupakan proses pengintaian awal yang bertujuan mengumpulkan informasi rinci mengenai target menggunakan teknik seperti rekayasa sosial, pemantauan fisik, atau penggunaan alat seperti *keylogger* (perekaman). Informasi ini dikumpulkan tanpa memicu alarm sistem dan menjadi dasar penting untuk tahapan berikutnya dalam serangan (Winterfeld and Andress 2012, 76-77).

Scan adalah tahap yang berfokus pada identifikasi kerentanan spesifik dari sistem atau aplikasi target dengan cara memindai dan mencatat informasi seperti versi software, nama pengguna, atau pesan kesalahan. Teknik seperti injeksi *Structured Query Language* (SQL) sering digunakan untuk mengekspos detail penting dari antarmuka web. Data hasil pemindaian ini kemudian didokumentasikan untuk digunakan dalam eksploitasi lebih lanjut (Winterfeld and Andress 2012, 77-78).

Tahap *access* dilakukan untuk memperoleh akses masuk ke sistem target,

baik dengan kredensial sah yang diperoleh sebelumnya melalui rekayasa sosial, maupun melalui eksploitasi terhadap celah sistem. Metode lain seperti serangan sisi klien juga digunakan, yang memanfaatkan kerentanan perangkat pengguna dari email, web, atau USB. Eksploitasi umum terhadap sistem operasi atau aplikasi memungkinkan penyerang untuk memperluas akses awal yang telah didapatkan (Winterfeld and Andress 2012, 78).

Pada tahap *escalate*, penyerang berusaha meningkatkan hak aksesnya dalam sistem melalui teknik *vertical* atau *horizontal privilege escalation*. Proses ini dapat dilakukan dengan mengeksploitasi kelemahan konfigurasi sistem, celah aplikasi, atau fitur tertentu dalam sistem operasi. Target utamanya adalah aplikasi atau layanan yang berjalan dengan hak akses tinggi, karena dapat dimanfaatkan untuk membuka akses shell atau menjalankan perintah sistem (Winterfeld and Andress 2012, 78-79).

Tahap *exfiltrate* merupakan proses pengambilan dan pemindahan data bernilai dari sistem target ke lokasi penyerang, yang menyerang aspek kerahasiaan dan kadang juga ketersediaan dalam model *Confidentiality, Integrity, and Availability* (CIA). Penyerang memanfaatkan protokol seperti *File Transfer Protocol* (FTP), *Secure Copy Protocol* (SCP), dan *Extensible Messaging and Presence Protocol* (XMPP), atau *Hypertext Transfer Protocol* (HTTP) jika protokol lain diblokir. Bahkan dalam lingkungan sistem yang sangat aman, penyerang sering kali masih menemukan jalur keluar untuk mentransfer data secara tersembunyi (Winterfeld and Andress 2012, 79).

Assault merupakan tahap pembeda antara CNA dan uji penetrasi biasa, karena fokusnya adalah menciptakan kekacauan pasca akses dan eksfiltrasi berhasil

dilakukan. Serangan ini dilakukan dengan tujuan menyebabkan efek seperti *deception*, *disruption*, *denial*, *degradation*, dan *destruction* (5D). Aksi pada tahap ini menyerang aspek integritas dan ketersediaan dalam kerangka *Confidentiality*, *Integrity*, *and Availability* (CIA) untuk melumpuhkan sistem target (Winterfeld and Andress 2012, 79).

Tahap *sustain* berfungsi untuk mempertahankan akses ke sistem secara berkelanjutan agar dapat digunakan kembali di kemudian hari. Penyerang dapat menciptakan akun baru, membuka port tambahan, memasang *backdoor*, atau menginstal *command and control* yang tersembunyi. Keberhasilan sustain tergantung pada kemampuan menyamarkan metode akses agar tidak terdeteksi oleh sistem keamanan (Winterfeld and Andress 2012, 80).

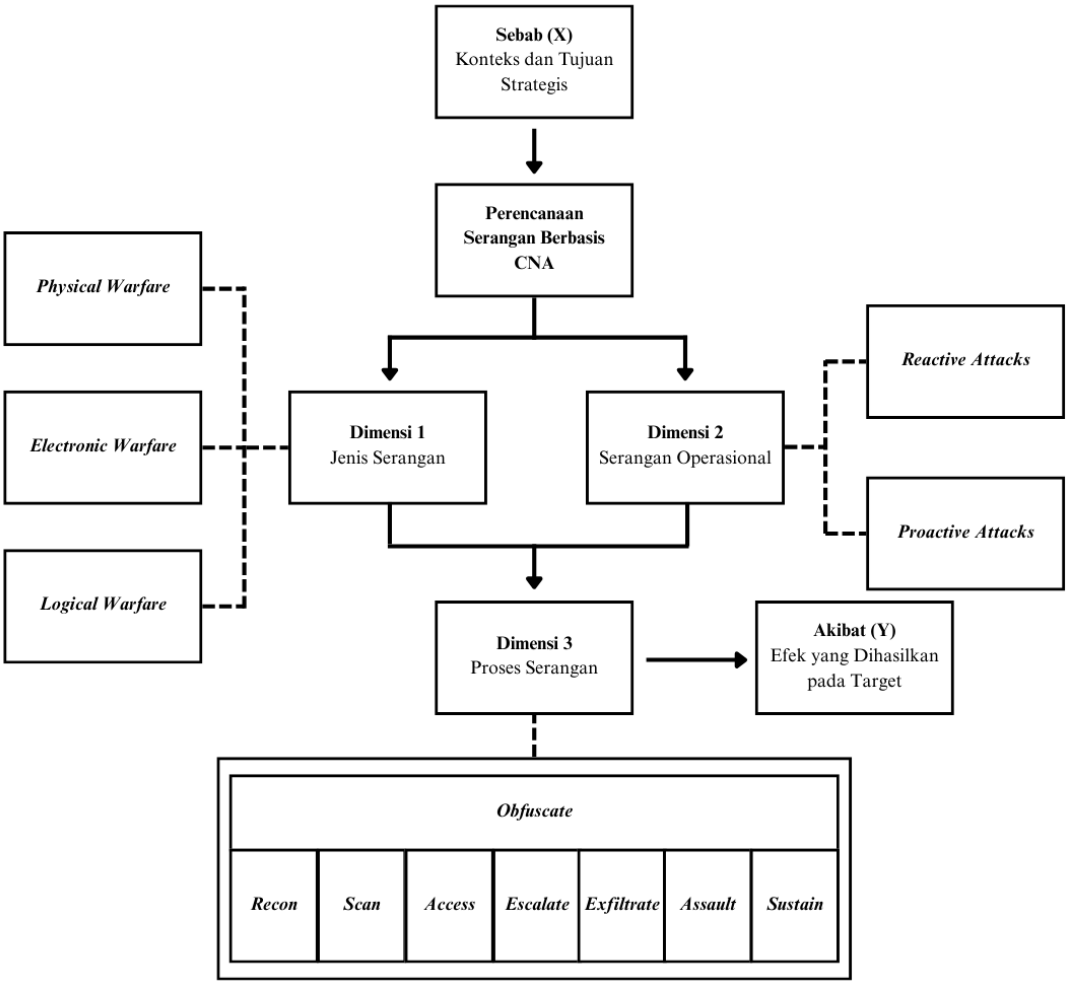
Terakhir, *obfuscate* adalah tahap penyamaran jejak serangan untuk menghindari pelacakan oleh pihak target atau forensik digital. Teknik yang digunakan mencakup penghapusan log, manipulasi timestamp, penggunaan *proxy* atau *IP spoofing*, serta penyisipan bukti palsu. Tujuannya adalah mengalihkan perhatian penyelidik dan menyulitkan proses atribusi terhadap pelaku asli serangan (Winterfeld and Andress 2012, 80-81).

1.7 Argumen Sementara

Penelitian ini menguraikan secara komprehensif tahapan dan dimensi serangan siber Rusia yang berfokus pada aspek teknis dan operasional dengan konsep *Computer Network Attack*. Analisis berisikan tentang penjelasan jenis serangan antara lain *physical warfare, electronic warfare,* dan *logical warfare* dengan proses serangan yang mencakup *recon*, *scan*, *access*, *escalate*, *assault*,

sustain, *exfiltrate*, hingga *obfuscate*, sesuai kerangka Winterfeld dan Andress (2012). Setiap proses dijabarkan dengan contoh implementasi nyata seperti serangan terhadap jaringan energi Ukraina, satelit KA-SAT, dan sistem komunikasi Kyivstar, yang menggambarkan pendekatan proaktif maupun reaktif secara strategis.

Grafik 1. Kerangka Konseptual Analitis Strategi CNA



Sumber: Disusun oleh penulis berdasarkan kerangka CNA Winterfeld dan Andress (2012)

Penelitian ini juga menekankan pentingnya operasi berlapis yang melibatkan aktor siber seperti kelompok Sandworm dan Solntsepeк, yang melakukan infiltrasi jangka panjang untuk tujuan spionase dan sabotase. Strategi

CNA memperlihatkan pemanfaatan malware seperti Industroyer2, AcidRain wiper, dan eksfiltrasi data menjadi bagian terintegrasi dari rencana operasi Rusia. Keseluruhan analisis menunjukkan bahwa pemahaman mendalam atas teknik dan taktik dengan pendekatan CNA sangat penting untuk mencapai tujuan militer dalam konflik modern.

1.8 Metode Penelitian

1.8.1 Jenis Penelitian

Dalam penelitian ini menggunakan jenis penelitian kualitatif deskriptif, yang mana penelitian ini membahas dengan secara deskripsi mengenai topik penelitian, yang didasari bahwa topik ini membutuhkan gambaran mengenai permasalahan yang ada.

1.8.2 Subjek dan Objek Penelitian

Subjek penelitian berfokus pada Rusia, yang mencakup militer dan kelompok peretas Rusia selama invasi ke Ukraina pada 2022-2024. Objek penelitian berfokus pada penggunaan *Computer Network Attack* (CNA) oleh Rusia sebagai strategi utama dalam mendukung operasi militer untuk melumpuhkan infrastruktur kritis Ukraina, dengan waktu penelitian yang mencakup pada periode invasi Rusia ke Ukraina dari tahun 2022-2024.

1.8.3 Metode Pengumpulan Data

Penelitian ini melakukan pengumpulan data dengan menggunakan data sekunder yang meliputi berbagai sumber seperti publikasi akademis, laporan berita, analisis kebijakan, dokumen resmi, dan literatur yang relevan dengan topik penelitian.

1.8.4 Proses Penelitian

Dalam melakukan proses penelitian, yaitu dengan mengumpulkan berbagai sumber yang relevan dengan topik penelitian lalu dianalisis serta diolah data-data yang sudah didapat, sehingga menjadi satu rangkaian pembahasan deskripsi mengenai topik penelitian.

1.9 Sistematika Pembahasan

Terdapat 4 bab utama dalam penelitian ini

1. Bab 1: Pendahuluan

Bab ini membahas dengan rincian yaitu latar belakang menjelaskan secara mendasar mengenai permasalahan yang akan diangkat, rumusan masalah sebagai acuan pertanyaan penelitian, kerangka pemikiran sebagai dasar pembahasan penelitian, argumen sementara sebagai perkiraan pembahasan penelitian, metode penelitian sebagai cara dalam melakukan penelitian, dan sistematika pembahasan untuk mengkategorikan pembahasan.

2. Bab 2: Transformasi Konflik dan Teknologi Rusia dalam Invasi ke Ukraina 2022-2024

Menjelaskan kronologi invasi Rusia ke Ukraina selama 2022-2024, dengan menandai fenomena penting selama invasi tersebut. Bab ini juga menjelaskan kronologi perkembangan teknologi Rusia di bidang militer selama invasi ke Ukraina 2022-2024.

3. Bab 3: Implementasi *Computer Network Attack* oleh Rusia dalam Invasi ke Ukraina 2022-2024

Bab ini membahas analisis dengan data-data yang telah ditemukan dengan menggunakan konsep *Computer Network Attack* oleh Steve Winterfeld dan Jason Andress guna menjawab rumusan masalah.

4. Bab 4: Kesimpulan

Bab ini membahas tentang ringkasan dari latar belakang, kerangka pemikiran, dan bab 3 guna menjawab rumusan masalah. Adapun pembahasan rekomendasi yang diberikan sebagai celah dari penelitian ini, agar dapat dilanjutkan dengan penelitian terbaru.