BAB II

KONDISI KOREA UTARA DI TENGAH TEKANAN INTERNASIONAL

2.1. Sejarah dan Dinamika Kepemimpinan Korea Utara

Pembagian Semenanjung Korea pasca Perang Dunia II menjadi dua zona pengaruh antara Uni Soviet di bagian utara dan Amerika Serikat di bagian selatan menciptakan kondisi politik yang sangat terpolarisasi. Di bawah pengaruh Uni Soviet, Korea bagian utara mengadopsi ideologi komunisme sebagai pondasi kekuatan politik di masa depan. Dalam artikel "*The Making of The North Korean State",* Gwang-Oon Kim menjelaskan bahwa pada periode 1945–1950 merupakan fase kritis reformasi politik di utara, ketika struktur kelembagaan negara mulai disusun oleh pengaruh lokal dan kebijakan Uni Soviet. Kondisi tersebut pada akhirnya menjadikan Korea Utara sebagai negara dengan sistem pemerintahan yang terpusat di bawah kepemimpinan Kim Il-sung (Kim, 2007).

Setelah proklamasi formal *The Democratic People's Republic of Korea* (DPRK), Korea Utara yang berada dibawah kepemimpinan Kim Il-sung mulai menggabungkan kekuasaan dengan mengutamakan monopoli politik, kontrol partai tunggal, dan memperbaiki struktur negara agar selaras dengan visi ideologi negara. Kim Il-sung juga melancarkan kampanye untuk menyingkirkan faksi-faksi internal yang termasuk faksi-faksi pendukung Tiongkok maupun Uni Soviet sehingga rezim menjadi lebih terpusat. Selain itu, militer dan partai disinergikan agar loyalitas terhadap rezim menjadi pilar utama stabilitas negara (Song & Wright, 2018). Adapun salah satu kebijakan Kim Il-sung mengenai industrialisasi dan kolektivitas

ini tidak memberikan dampak pembangunan yang signifikan bagi negaranya, sebaliknya kebijakan ini justru menyebabkan kelaparan di wilayah pedesaan karena kegagalan produksi pertanian dan kebijakan pembangunan yang dipaksakan.

Setelah pemerintahan Kim Il-sung berakhir pada tahun 1994, kepemimpinan Korea Utara digantikan oleh anaknya, yaitu Kim Jong-il pada periode 1994 hingga 2011. Pada masa ini, Korea Utara mengalami tantangan berat dalam sektor ekonomi karena runtuhnya dukungan dari Uni Soviet dan Tiongkok yang telah terpecah. Terlebih adanya bencana alam yang menyebabkan krisis pangan besar dan kondisi ekonomi yang semakin memburuk membuat Korea Utara berada di ambang keruntuhan. Untuk mengatasi permasalahan tersebut, Kim Jong-il menerapkan kebijakan *Songun* atau "*military-first policy"* yang menjadikan kekuatan militer sebagai pilar utama dalam struktur politik dan sumber legitimasi negara (Derochie, 2025). Meskipun kebijakan ini mampu meningkatkan kekuatan militernya karena alokasi sumber daya negara, kondisi sektor sipil dan ekonomi tidak berubah. Jadi Korea Utara hanya berfokus menjaga stabilitas politiknya meskipun kondisi ekonomi dan sipil tetap memprihatinkan.

Pada tahun 2011 setelah kepemimpinan Kim Jong-il berakhir, Korea Utara dipimpin oleh Kim Jong-un yang merupakan anak dari Kim Jong-il. Pada masa kepemimpinan Kim Jong-un, terjadi penyesuaian kebijakan, meskipun masih dalam mempertahankan ideologi dan kontrol rezim. Salah satu contohnya yaitu kebijakan ekonomi yang lebih terbuka, seperti pemberian sedikit keleluasaan manajerial kepada perusahaan negara dan kolektif, dorongan terhadap zona ekonomi khusus, dan pengembangan kebijakan pembangunan daerah pedesaan. Dalam artikel "*From*

Marketization to a Market Economy in North Korea" menjelaskan adanya pergeseran menuju *marketization*, namun tetap dalam kendali ketat pemerintah untuk menjaga stabilitas politik sembari memperbaiki pertumbuhan ekonomi meskipun dampaknya tidak terlalu signifikan (Kim, 2022).

Kondisi Korea Utara yang terlalu menjunjung tinggi kemandirian di setiap aspek kehidupan negara, baik itu politik, ekonomi, militer, dan dengan menekankan rakyat sebagai subjek utama revolusi dan pembangunan bangsa tanpa bergantung terhadap negara lain merupakan buah pokok ideologi *juche* yang dikemukakan oleh Kim Il-sung. Ideologi ini menjadi dasar maupun pondasi utama Korea Utara untuk bertahan di sistem internasional yang anarkis ini. Melalui ideologi yang telah diterapkan sejak kepemimpinan Kim Il-sung, Kim Jong-il, hingga Kim Jong-un, Korea Utara mampu mempertahankan rezim karena para pemimpinnya memiliki kontrol penuh terhadap berbagai dinamika, kebijakan, dan keputusan. Namun kontrol penuh dari pemimpin yang mampu meningkatkan kekuatan Korea Utara ini, juga dapat membawa kehancuran bagi berbagai aspek jika pemimpin hanya berfokus pada aspek tertentu. Seperti yang terjadi ketika kekuatan militernya menjadi kuat, namun kondisi ekonomi dan kesejahteraan warga menjadi isu yang perlu diperbaiki kembali.

2.2. Kondisi Domestik Korea Utara

2.2.1. Struktur Kekuasaan dan Kontrol Politik

Sejak tahun 2011 kepemimpinan Kim Jong-un semakin memperkuat rezim dengan struktur kekuasaan yang sangat terpusat dengan adanya kombinasi antara ideologi,

kontrol partai, dan penekanan pada loyalitas elit. Adapun kekuatan militer tetap menjadi pilar penting rezim meskipun perannya mulai bergeser yang tidak hanya sebagai kekuatan pertahanan tetapi juga sebagai instrumen politik untuk memperkuat supremasi keluarga Kim dan partai atas negara. Dalam penelitian yang dilakukan oleh Sungmin Cho (2020) *"Why North Korea Could Not Implement the Chinese Style Reform and Opening? The Internal Contradiction Between Economic Reform and Political Stability"* menjelaskan bahwa meskipun ada keinginan untuk melakukan reformasi ekonomi dengan membuka peluang bagi investasi asing dan zona ekonomi khusus, langkah ini dianggap berbahaya karena mampu mengancam esensi rezim yang memiliki kontrol penuh (Cho, 2020). Oleh karena itu, untuk tetap menjaga stabilitas politiknya, Kim Jong-un tetap melakukan reformasi ekonomi pragmatis, namun tetap dalam kontrol penuh pemerintah.

Stabilitas politik dan rezim di Korea Utara mampu tetap terjaga karena adanya loyalitas terhadap keluarga Kim secara turun temurun. Loyalitas elit ini menjadi landasan utama stabilitas rezim karena struktur elit dibangun sedemikian rupa agar anggotanya memiliki kepentingan langsung atas pemerintahan. Selain itu, elit-elit ini lebih memilih untuk menjaga sistem apa adanya meskipun harus menerima pengorbanan material dibandingkan mengambil posisi yang mampu mengancam status dan nyawa mereka sendiri. Terlebih adanya kesatuan antar elit, jalur karir yang diwariskan secara politis dan kekerabatan, serta keterbatasan akses ke kekuasaan bagi mereka yang tidak loyal mampu memperkuat rezim (Carothers, 2022). Meskipun begitu, dampak dari dinamika internasional dan lokal yang yang berupa sanksi internasional, korupsi, kelangkaan pangan, dan keterbatasan energi

menjadi tantangan bagi rezim untuk mengatasi permasalahan tersebut, seperti memberikan izin operasional yang terbatas bagi usaha informal, dan mengizinkan *pseudo-state enterprises* (perusahaan yang secara resmi milik negara tetapi dalam prakteknya dikendalikan oleh elit atau pihak swasta) demi menjaga keutuhan rezim dan stabilitas politik .

2.2.2. Kondisi Ekonomi dan Tekanan Struktural

Dalam aspek ekonomi, Korea Utara menghadapi tantangan akibat isolasi dan sanksi internasional yang hal ini dipicu oleh program nuklir yang mengancam stabilitas internasional dan berbagai pelanggaran HAM terhadap warganya. Meskipun demikian, berdasarkan data Bank of Korea, perekonomian Korea Utara pada tahun 2024 mengalami pertumbuhan sebesar 3,7% dari 3,3% pada tahun 2023 yang hal ini menunjukkan pertumbuhan yang signifikan dalam delapan tahun terakhir. Pertumbuhan ini tidak mengindikasikan perbaikan struktural karena masih ditopang oleh hubungan terbatas dengan mitra, seperti Rusia dan aktivitas perdagangan tertentu dengan Tiongkok. Namun tingkat pendapatan nasional perkapita Korea Utara pada tahun 2024 hanya mencapai 1.239 dolar Amerika Serikat atau sekitar 3,4% dari pendapatan perkapita Korea Selatan yang hal ini menunjukkan adanya kesenjangan ekonomi yang signifikan antara kedua Korea (Reuters, 2025).

Adapun perdagangan di Korea Utara menunjukkan penurunan sebesar 2,4% pada tahun 2024 menjadi sekitar 2,7 miliar dolar Amerika Serikat, namun nilai ekspor meningkat 10,8% menjadi 360 juta dolar Amerika Serikat. Komoditas ekspor Korea Utara yang mendominasi tidak berasal dari sektor industri berat melainkan produk-produk seperti wig, bulu mata palsu, dan jam tangan bahkan

pada tahun 2023 ekspor produk rambut dan wig ke Tiongkok mencapai 167 juta dolar Amerika Serikat dengan total sekitar 1.680 ton yang hal ini menjadikan salah satu sumber devisa penting bagi Korea Utara di tengah sanksi internasional. Selain itu, sanksi perdagangan dari PBB mengakibatkan penurunan output manufaktur sebesar 12,9% serta penurunan pendapatan sebesar 15,3% yang hal ini mempersempit ruang gerak rezim dalam menopang kesejahteraan masyarakat sehingga negara semakin bergantung pada aktivitas ekonomi ilegal dan non konvensional, termasuk serangan siber terhadap sektor keuangan global (Kim et al., 2023). Dengan demikian, meskipun terdapat pertumbuhan positif dalam beberapa tahun terakhir, perekonomian Korea Utara tetap rapuh dan sangat bergantung pada celah perdagangan.

Kondisi struktural dengan sistem ekonomi yang terpusat membuat pemerintah Korea Utara memiliki kontrol penuh terhadap aktivitas ekonomi. Hal ini ditandai dengan hampir seluruh aktivitas produksi dan distribusi berada di bawah kendali negara melalui perusahaan milik negara, sedangkan kepemilikan swasta dan investasi asing dibatasi secara ketat. Struktur ini sejak lama telah bertumpu pada pertanian kolektif dan industrialisasi berat. Namun karena teknologi dan fasilitas yang kuno serta inefisiensi alokasi energi dan bahan baku mengakibatkan tingkat produktivitas yang lambat meskipun Korea Utara memiliki cadangan sumber daya mineral yang signifikan dan potensi industri yang besar. Jadi permasalahan struktural dan ekonomi dapat terjadi karena Korea Utara terlalu memusatkan anggaran untuk meningkatkan kekuatan militer dan stabilitas rezim dibandingkan pembangunan ekonomi produktif.

Tingkat kemiskinan di Korea Utara yang mencapai 60% dari 26 juta warga dan 11,8 juta warga atau sekitar 45% mengalami malnutrisi merupakan hasil dari sistem ekonomi yang terpusat dan tekanan struktural (Cuaresma et al., 2020). Meskipun Korea Utara memiliki potensi sumber daya yang baik, ambisi untuk menstabilkan rezim dengan berfokus pada peningkatan militer belum dapat mensejahterakan warganya, sebaliknya hal ini justru meningkatkan kesenjangan antara elit politik-militer dengan masyarakat umum. Jadi situasi ini memperkuat gambaran bahwa pertumbuhan ekonomi yang tercatat secara agregat tidak mampu menunjukkan perbaikan fundamental dalam kualitas hidup penduduk, melainkan lebih menunjukkan kemampuan rezim untuk bertahan melalui mekanisme adaptif, salah satunya dengan menguatkan ekonomi bayangan yang ditandai dengan aktivitas non-konvensional sebagai sumber devisa negara.

2.2.3. Militerisasi Negara dan Perluasan ke Ranah Siber

Selain aspek ekonomi, aspek militer memegang peran yang dominan dalam kehidupan politik maupun sosial Korea Utara. Dengan menggunakan doktrin *Songun* atau *military first policy*, Korea Utara menempatkan kekuatan militer sebagai prioritas utama pembangunan negara. Angkatan bersenjata Korea Utara juga merupakan salah satu yang terbesar di dunia dari segi jumlah personel yang ada, meskipun kemampuan teknologi konvensionalnya tertinggal dibandingkan negara-negara maju. Untuk mengatasi hal tersebut, Korea Utara berfokus pada pengembangan senjata nuklir dan misil balistik yang hal ini menimbulkan kekhawatiran bagi komunitas internasional dan mengancam stabilitas internasional. Terlebih dalam dekade terakhir, strategi pertahanan Korea Utara diperluas dengan

menjadikan ruang siber sebagai bagian utama dari kekuatan militer sehingga ancaman yang ditimbulkan tidak hanya bersifat konvensional saja, tetapi juga bersifat digital (Derochie, 2025).

Pembangunan rudal balistik, nuklir, serta peningkatan kekuatan militer tradisional yang agresif mengakibatkan Korea Utara mendapat tekanan internasional. Dalam kondisi ini, pengembangan kapabilitas sier menjadi salah satu strategi alternatif bagi Korea Utara untuk mempertahankan kepentingan nasional di tengah keterbatasan ekonomi dan isolasi global. Meskipun beberapa sektor berstatus stagnan atau bahkan dalam keterlambatan, kemampuan siber Korea Utara dapat dikatakan mampu berkembang secara signifikan dan menjadi salah satu instrumen strategis negara. Terlebih investasi jangka panjang pemerintah Korea Utara dalam mengembangkan sumber daya manusia di bidang teknologi, termasuk pelatihan individu berbakat sejak muda yang kemudian ditempatkan di lembaga teknis khusus sebelum bergabung dengan unit siber negara. Para peretas yang tergabung dalam unit Lazarus Group mampu melakukan operasi siber tingkat lanjut, mulai dari infiltrasi jaringan, pencurian data dan aset kripto bernilai jutaan dolar, hingga serangan destruktif menggunakan malware terhadap institusi internasional. Contohnya pada tahun 2014 Lazarus Group menyerang Sony Pictures Entertainment yang menyebabkan kebocoran data besar-besaran dan kerugian finansial yang signifikan bagi perusahaan tersebut (NCC Group, 2022).

2.3. Korea Utara dalam Sistem Internasional

Korea Utara memainkan peran penting di panggung internasional melalui pendekatan diplomasi yang adaptif dan diversifikasi aliansi yang strategis. Setelah Perang Dunia II, Korea Utara mengatur desain aliansi secara strategis dengan negara-negara sekutu tanpa mengubah identitas bangsa yang merupakan negara yang mandiri dan tertutup. Selain itu, Korea Utara juga mengembangkan diplomasi baru dalam isu non tradisional seperti perubahan iklim sebagai sarana untuk mendapatkan bantuan teknologi dan ekspresi kepedulian terhadap keamanan manusia yang hal ini menunjukkan bahwa Korea Utara tidak hanya fokus pada kekuatan militer saja, tetapi juga pada isu global kontemporer (Scartozzi & Kang, 2023).

Salah satu aspek penting dalam dinamika Korea Utara di ranah internasional adalah upayanya untuk memperkuat militernya sebagai respon terhadap ketidakpastian keamanan di sekitar kawasan Asia Timur yang hal ini berdampak pada stabilitas keamanan regional. Pada tahun 2025 ini, Korea Utara menguji kekuatan rudal dari kapal barunya yang merupakan kapal *destroyer* dengan berat sekitar 5.000 ton yang dilengkapi dengan sistem persenjataan canggih, seperti rudal jelajah dan supersonik, sistem anti-pesawat, serta perlengkapan peredam elektronik (Al Jazeera, 2025). Pengembangan kapal perang ini tentu memperluas proyeksi kekuatannya di laut dan memunculkan keprihatinan bahwa wilayah maritim di Korea dan jalur pelayaran internasional menjadi terancam. Selain itu, Korea Utara juga memperdalam kerjasama militer dengan Rusia termasuk pengiriman artileri dan personil yang tidak hanya memberikan Korea Utara pengalaman perang nyata

tetapi juga adanya potensi pertukaran teknologi dan akses ke sistem pertahanan yang lebih modern (McCurry & Graham, 2024). Presiden Kim Jong-un menyatakan bahwa penambahan aset strategis ini dilakukan sebagai reaksi terhadap peningkatan kehadiran militer Amerika Serikat di Korea Selatan dan latihan bersama sekutu seperti Jepang yang dapat mempertegang kawasan regional (Kim, 2025). Dengan demikian, modernisasi militer konvensional Korea Utara bukan hanya isu domestik atau pertahanan nasional semata, melainkan bagian dari sistem keamanan regional yang dapat memicu perlombaan senjata, meningkatnya ketegangan antar negara, dan potensi kesalahpahaman yang memperbesar peluang konflik antarnegara.

Korea Utara tidak hanya berfokus dalam pengembangan senjata militer, seperti rudal balistik dan nuklir saja, akan tetapi Korea Utara juga berfokus dalam pengembangan siber sebagai salah satu alternatif. Korea Utara memperkuat kapabilitasnya dalam serangan dunia maya sebagai bentuk "senjata asimetris" yang mampu menutup kesenjangan militer tradisional dengan musuhnya. Korea Utara juga melakukan berbagai serangan siber, seperti *phising, malware*, serta pencurian aset digital dengan target yang bervariasi dari lembaga pemerintahan hingga sektor keuangan di negara-negara lain (Kim, 2022). Selain itu, Korea Utara juga memanfaatkan infrastruktur jaringan global untuk operasi pengintaian siber dan visualisasi ancaman sehingga tidak hanya menyerang, tetapi juga memetakan targetnya secara lebih sistematis.

Motif strategis di balik tindakan diplomasi dan operasi siber Korea Utara dapat dipahami dalam kerangka politik rezim dan kebutuhan untuk bertahan di tengah sistem internasional yang anarkis. Korea Utara memandang operasi siber

sebagai instrumen untuk mencapai tiga tujuan utama: pertama, untuk mengimbangi superioritas militer tradisional dari aliansi musuh; kedua, menyebabkan disrupsi sosial di negara sasaran dengan resiko langsung yang lebih rendah; ketiga, untuk memperoleh sumber daya finansial bagi rezim yang terisolasi dan meningkatkan kekuatan militernya. Selain itu, Korea Utara juga memanfaatkan negara-negara pihak ketiga sebagai jalur infrastruktur dan jaringan dukungan bagi operasi sibernya yang didasari oleh analisis pola penggunaan jaringan teknologi dan interkoneksi antar negara (Perdana et al., 2024).

2.3.1. Korea Utara di Tengah Tekanan Internasional

Berbagai tindakan maupun tanggapan kontroversial yang dilakukan oleh Korea Utara adalah cara untuk bertahan di sistem internasional yang anarkis dan tekanan dari negara lain yang pada akhirnya menempatkan Korea Utara pada posisi yang sulit, yaitu sanksi internasional. Sanksi internasional ini sangat merugikan Korea Utara karena mampu membatasi ruang geraknya untuk meningkatkan kekuatan negaranya. Sanksi internasional yang dijatuhkan oleh PBB sebagian besar mengincar sektor ekonomi Korea Utara sehingga menyulitkan pembangunan negaranya. Adapun sanksi ekonomi ini berupa pembatasan perdagangan dan impor input antara industri yang mampu menurunkan output manufaktur negara sebesar 12.9% sera menurunkan pendapatan riil sekitar 15,3% (Kim et al., 2023). Selain itu, harga barang impor juga mengalami kenaikan yang signifikan karena pembatasan pada rantai pasok barang dan bahan baku yang mengganggu produksi domestik. Kondisi ini juga diperburuk jika banyak negara mitra dagang besar Korea Utara juga memperketat kepatuhan terhadap sanksi.

Selain dampak ekonomi makro, Korea Utara secara sistematis memperbaiki kembali jaringan perdagangan bilateral dan multilateralnya untuk mengurangi efek negatif dari tekanan internasional. Korea Utara juga mengalihkan rute perdagangannya ke negara maupun jaringan lainnya yang tidak terlalu mengindahkan sanksi internasional, sehingga meskipun ada pembatasan formal, perdagangan informal dapat tetap berlangsung. Korea Utara juga menggunakan hubungan diplomatik dan kerjasama dengan pihak ketiga untuk menjaga sektor industri dan militer yang ditunjukkan dengan adanya praktik penyelundupan, penggunaan perusahaan perantara, dan komponen "*dual-use*" sebagai cara beradaptasi (Preble, 2024). Disisi lain, Korea Utara juga berhasil mempertahankan beberapa kapasitas dalam negeri melalui penguatan sektor informal dan jaringan lokal yang memungkinakn kebutuhan strategis tetap terpenuhi meskipun aktivitas resmi terhambat. Dengan begitu langkah yang diambil Korea Utara ini mampu menunjukkan kemampuan adaptasi, fleksibilitas dalam jaringan ekonomi, dan diplomasi di tengah tekanan sanksi internasional yang merugikan Korea Utara.

2.4. Kepedulian Pemerintah Korea Utara Terhadap Warganya

Kebijakan *people-first principle* menunjukkan bahwa meskipun sedang mengalami isolasi dan sanksi internasional, Korea Utara tidak hanya berfokus untuk meningkatkan kekuatan militer dan siber saja, tetapi Korea Utara juga menunjukkan kepedulian terhadap warganya. Kebijakan ini merupakan strategi yang digunakan Korea Utara untuk menunjukkan citra peduli rakyat setelah dunia melihat Korea Utara merupakan negara yang hanya berfokus pada kekuatan siber maupun militer saja, tidak peduli terhadap rakyatnya bahkan telah membuat rakyatnya hidup dalam

krisis. Melalui kebijakan ini, Korea Utara merubah arah geraknya dari prinsip *Songun* yang menempatkan militer sebagai prioritas utama menjadi kesejahteraan rakyat lebih penting daripada kekuatan militer. Meskipun dalam prosesnya untuk menyejahterakan rakyat masih dikontrol ketat oleh negara dimana partai dan negara menentukan apa yang dimaksud dengan "kepentingan rakyat". Kebijakan ini juga menunjukkan bahwa langkah untuk menyejahterakan rakyat bukan semata karena tekanan internasional memaksa Korea Utara untuk lebih memikirkan rakyatnya, tetapi juga karena Korea Utara sendiri ingin memperbaiki keadaan rakyatnya ditengah isolasi dan menunjukkan legitimasi domestiknya (Jung, 2024).

Dalam menunjukkan kepedulian terhadap rakyatnya, Korea Utara mengubah bekas situs uji coba rudal menjadi lahan pertanian rumah kaca yang bernama *Ryonpho Greenhouse Farm*. Proyek ini dibuat untuk memperingati ulang tahun Partai Pekerja Korea dan diproyeksikan sebagai model bagi peradaban pedesaan dengan tujuan untuk mencapai target *improving people's lives* dalam kebijakan utama rezim. Proyek ini memiliki luas sekitar 280 hektar dengan lebih dari 850 blok rumah kaca modern dan adanya rencana integrasi dengan fasilitas sosial, seperti rumah, sekolah, dan fasilitas layanan. Proyek ini dibuat juga berdasarkan kondisi masyarakat Korea Utara yang kekurangan gizi akibat krisis pangan dengan persentase hampir 46% warga Korea Utara atau sekitar 11,8 juta warga. Meskipun demikian, hasil dari *greenhouse* ini tidak langsung didistribusikan kepada warga, melainkan dikirim terlebih dahulu kepada pemerintah di ibu kota (Shin & Coghill, 2022). Meskipun proyek ini memiliki lahan yang luas serta potensi yang besar, jika hasilnya tidak didistribusikan secara merata dan lebih

memprioritaskan kepada pemerintah terlebih dahulu maka perbaikan gizi masyarakat secara umum tetap terbatas.

Korea Utara juga melaksanakan proyek pembangunan besar-besaran berupa penyediaan 50.000 unit perumahan di Pyongyang. Proyek ini merupakan bagian dari kebijakan domestik pemerintahan Kim Jong Un untuk meningkatkan kesejahteraan sosial di tengah keterbatasan ekonomi nasional. Pada tahap awal di tahun 2022, pembangunan 10.000 unit rumah di Distrik Songsin dan Songhwa telah berhasil diselesaikan. Selanjutnya, sebanyak 30.000 unit rumah tambahan di wilayah timur laut Distrik Hwasong juga telah selesai, sementara 10.000 unit terakhir telah memasuki tahap akhir pembangunan pada tahun 2025 (Boram, 2025). Secara keseluruhan, proyek ini mencerminkan upaya rezim Korea Utara untuk mempertahankan legitimasi politik melalui peningkatan fasilitas sosial, meskipun negara tersebut masih berada dalam kondisi isolasi dan menghadapi tekanan sanksi internasional.

Dalam mengelola dan mempertahankan kepercayaan publik, Korea Utara tidak hanya mengandalkan proyek-proyek kesejahteraan, tetapi juga secara aktif memanfaatkan propaganda sebagai instrumen politik domestik. Propaganda ini berfungsi sebagai respon untuk melawan stigma internasional terhadap Korea Utara, khususnya label *state-sponsored activism.* Adapun bentuk propaganda ini diwujudkan melalui narasi media negara yang menekankan keberhasilan pembangunan, kemandirian nasional, serta penggambaran kepemimpinan Kim Jong Un. Selain itu, berbagai proyek kesejahteraan seperti pembangunan infrastruktur sosial direpresentasikan sebagai bukti nyata komitmen negara

terhadap rakyatnya (Black et al., 2022). Dengan demikian, propaganda dan kebijakan kesejahteraan saling melengkapi dalam memperkuat legitimasi rezim dan menjaga loyalitas masyarakat di tengah tekanan eksternal.

Sebagai negara dengan sistem pemerintahan yang terpusat, kebijakan Kim Jong Un yang menunjukkan kepedulian terhadap kesejahteraan rakyat dapat dipahami sebagai strategi politik untuk mempertahankan kepercayaan publik terhadap pemerintah. Selama ini, Korea Utara sering dipersepsikan sebagai negara yang hanya memprioritaskan penguatan militer dan kapabilitas siber, sementara kesejahteraan masyarakat umum tertinggal dan elit politik menikmati kondisi yang jauh lebih baik. Dalam konteks tersebut, kebijakan kesejahteraan berfungsi tidak hanya sebagai instrumen domestik untuk meredam potensi ketidakpuasan masyarakat, tetapi juga sebagai upaya pembangunan citra positif di panggung internasional (Jung, 2024). Melalui citra tersebut, Korea Utara berusaha menentang stigma global, khususnya tuduhan *state sponsored activism* yang dikaitkan dengan aktivitas Lazarus Group dalam mendanai rezim. Dengan demikian, kebijakan kesejahteraan ini dapat dipandang sebagai bagian dari strategi rezim untuk mempertahankan legitimasi sekaligus membingkai narasi bahwa tekanan internasional merupakan faktor utama yang menghambat berkembangnya Korea Utara.

2.5. Kekuatan Siber Sebagai Langkah Alternatif Korea Utara

Korea Utara mengambil langkah untuk meningkatkan kekuatan siber sebagai langkah alternatif untuk mengatasi keterbatasan akses teknologi konvensional dan

sumber daya strategis oleh tekanan diplomatik dan ekonomi. Korea Utara telah mengembangkan kapabilitas siber dengan tiga tujuan utama, yaitu menyeimbangkan kemampuan militer tradisional terhadap aliansi Amerika Serikat dengan Korea Selatan, mengganggu struktur sosial dan ekonomi musuh dengan resiko minimal, dan menghasilkan sumber daya finansial alternatif. Adapun kelompok siber Korea Utara seperti Lazarus Group, Kimsuky, dan APT 37 telah melakukan berbagai tindakan seperti, *phising*, malware, dan pencurian aset kripto di berbagai belahan dunia (Kim, 2022). Langkah ini diambil Korea Utara karena untuk mengembangkan kekuatan siber relatif murah jika dibandingkan dengan peningkatan kekuatan militer konvensional dan juga sebagai jalur yang lebih efisien untuk memperkuat posisinya dalam keamanan regional tanpa harus menghadapi konfrontasi militer secara langsung.

Pendekatan siber ini tidak hanya bersifat ofensif, tetapi juga sebagai bagian dari bentuk adaptasi Korea Utara terhadap sanksi internasional dan isolasi. Hal ini ditunjukkan melalui pola serangan siber yang dilakukan oleh kelompok-kelompok hacker Korea Utara tidak dilakukan secara acak, melainkan terstruktur, sesuai sasaran, dan sejalan dengan tujuan geopolitik Korea Utara. Kelompok siber Korea Utara terbukti memanfaatkan data arsip *Border Gateway Protocol* (BGP) dan jaringan untuk merancang serangan yang lebih sulit terdeteksi dan berdampak signifikan bagi korban (Youn et al., 2022). Dengan begitu, strategi siber Korea Utara mampu menghasilkan keuntungan langsung seperti dari pencurian aset maupun informasi dan juga untuk membentuk posisi tawar dalam dinamika keamanan regional.

2.5.1. Kekuatan Siber dan Serangan Siber

Kekuatan siber atau *cyber power* dalam pandangan Joseph Nye menegaskan bahwa kekuasaan dalam era digital bukan hanya mengenai dominasi militer atau ekonomi tradisional, melainkan melibatkan kemampuan aktor internasional untuk mencapai hasil yang diinginkan melalui pemanfaatan teknologi digital atau siber. Adapun karakteristik siber, seperti anonimitas, rendahnya hambatan untuk mendapatkan informasi dibandingkan dengan cara tradisional, dan kerentanan siber simetris mampu memberikan peluang yang besar bagi aktor untuk memberikan pengaruh yang signifikan. Joseph Nye beranggapan bahwa dalam ranah siber ini, kekuasaan mengalami pergeseran, bukan hanya negara kuat yang mendominasi, tetapi mulai banyak aktor lainnya yang juga memainkan peran penting dalam dominasi (Nye, Jr, 2010). Oleh karena itu, negara harus mempertiimbangkan kapasitas teknis, regulasi, reputasi digital, dan pengaruh informasi sebagai bagian penting untuk tetap mempertahankan kekuasaannya.

Dalam kerangka berpikir Joseph Nye, *cyber power* mencangkup perpaduan antara aspek *hard power* seperti kemampuan ofensif dan defensif dalam siber dan *soft power* seperti kemampuan dalam beropini, menyebarkan informasi maupun ide, maupun mempengaruhi melalui jaringan digital. Joseph Nye juga menekankan bahwa aktor yang mampu mempertahankan infrastruktur siber nasional sekaligus juga mengendalikan arus informasi dan memanfaatkan jaringan global akan memiliki keunggulan kompetitif dalam sistem internasional yang modern ini (Nye, Jr, 2010). Selain itu, ranah siber bersifat lintas batas dan terdesentralisasi yang ini menunjukkan bahwa hanya dengan mengandalkan kemampuan tradisional, seperti

militer dan ekonomi dinilai kurang memadai. Namun siber juga memberikan tantangan dan hambatan, seperti adanya aktivitas spionase, penyebaran berita palsu, bahkan serangan siber.

Serangan siber atau *cyber attack* merupakan tindakan yang dilakukan secara sadar untuk memasuki sistem komputer, jaringan, atau perangkat digital lainnya tanpa memerlukan otorisasi dan dengan tujuan untuk mencuri, mengubah, merusak, atau bahkan memusnahkan data dan fungsi sistem tersebut. Adapun aktor yang melakukan serangan ini dapat berupa individu, kelompok kriminal maupun ideologis, bahkan hingga aktor negara yang memanfaatkan kerentanan teknis maupun kelemahan manusia sebagai rekayasa sosial. Serangan siber dapat diklasifikasikan menurut motifnya,seperti kriminal untuk mendapatkan keuntungan finansial atau berupa politik maupun ideologi untuk mempengaruhi opini publik. Hal ini dapat terjadi karena ruang siber bersifat lintas batas dan sangat dinamis serta berdampak signifikan, mulai dari gangguan operasional ringan hingga kerusakan infrastruktur kritis yang dapat mempengaruhi banyak orang. Dalam konteks *cyber power* seperti yang dibahas oleh Joseph nye, serangan siber menjadi salah satu bukti konkrit bagaimana aktor-aktor siber dengan *cyber power*-nya dapat mempengaruhi dan menekan aktor lain baik secara langsung maupun tidak langsung (Nye, Jr, 2010).

Seiring dengan perkembangan teknologi yang semakin modern, metode serangan siber semakin beradaptasi dan beragam sehingga dapat menemukan celah baru yang dapat mempersulit lawan maupun korban untuk melakukan pertahanan sistem. Contohnya serangan yang menggunakan malware dapat mengunci dan

merusak sistem maupun data korban. Adapun metode seperti *phising* yang bertujuan untuk mengelabui dan mencuri data pribadi korban dengan merekayasa semirip mungkin akun, link, ataupun web resmi. Selain itu, juga ada serangan yang menargetkan ketersediaan sistem seperti serangan *Denial of Service* (DoS) atau *Distributed Denial of Service* (DDoS) juga umum terjadi sebagai alat untuk mengganggu layanan secara massal. Jika dilihat dari perspective *cyber power*, kemampuan untuk menguasai dunia maya hingga melakukan serangan atau menciptakan sistem defensif terhadap serangan siber yang kuat menjadi penentu posisi aktor dalam persaingan siber global (Biju et al., 2019).

2.5.2. Lazarus Group

Salah satu kelompok siber yang berafiliasi dengan Korea Utara dan telah melakukan berbagai serangan serta menciptakan teror dalam dunia maya yaitu Lazarus Group. Sebagai aktor ancaman siber tingkat lanjut (*Advanced Persistent Threat*), Lazarus Group telah melakukan berbagai serangan siber, spionase, peretasan, pencurian aset digital, dan setiap serangan yang telah dilancarkan oleh Lazarus Group pasti memberikan dampak destruktif yang ini membuat para korban mengalami kerugian besar dan kesulitan untuk pulih dari serangannya. Aktivitas kelompok ini menunjukkan kombinasi antara taktik *social engineering* dan kapabilitas malware canggih yang dapat memberikan akses dari sistem kritis di berbagai negara (Perdana et al., 2024). Keberadaan Lazarus Group menjadi salah satu tantangan terbesar dalam keamanan siber global karena sifatnya yang lintas batas dan sulit untuk diadili secara langsung.

Aktivitas Lazarus Group ini berdampak signifikan dalam skala global, khususnya dalam sektor keuangan yang setelah terjadi serangan akan menyebabkan kerugian finansial yang sangat besar, gangguan dan kerusakan sistem operasional organisasi korban, hingga implikasinya terhadap stabilitas keamanan dunia maya. Selain itu, karena aksinya bersifat lintas negara dan melibatkan penyalahgunaan teknologi modern seperti mata uang kripto dan infrastruktur keuangan global, maka respons internasional menjadi sangat kompleks bahkan menjatuhkan tuduhan yang memberatkan bagi Korea Utara (Sartika & Idris, 2025). Namun dugaan mengenai Lazarus Group yang merupakan *state sponsored activism* oleh Korea Utara belum dapat dipastikan kebenarannya, akan tetapi satu hal yang pasti bahwa negara Barat banyak yang menuduh bahwa serangan dari Lazarus Group merupakan strategi dari Korea Utara untuk bisa bertahan dalam kondisi isolasi dan sanksi internasional.

03/2007	According to cybersecurity experts working on Operation Blockbuster, the Lazarus Group starts to develop its first generation of malware;
2009	The Lazarus Group starts its Operation Troy and its wiper malware.
07/2009	Lazarus Group conducts Distributed Denial of Service (DDoS) attacks against 17 South Korean and U.S. government websites.
03/2011	Lazarus Group conducts a DDoS attack on 40 South Korean media outlets, critical infrastructures and financial websites, as well as on U.S. military entities in South Korea, in an operation named Ten Days of Rain.
03/2013	Lazarus Group shuts down 32,000 computers in South Korean broadcast and financial companies.
06/2013	DPRK is attributed with a DDoS attack against 69 South Korean media outlets and government websites.
09/2013	Kaspersky Lab discovers a cyberespionage campaign named the Kimsuky campaign against South Korean think tanks and industries.
2014	DPRK is attributed to a cyber-attack on 140,000 South Korean government and business computers and tries to penetrate the control system for the South Korean transportation network. APT37, a cyberactor associated with the DPRK government, targets South Korean media and websites on DPRK refugees with watering hole attacks.
08/2014	DPRK hackers attack the British TV broadcaster Channel 4. The channel had planned to release a TV show on a nuclear scientist being kidnapped by the DPRK. The TV show was

	cancelled after the cyberattack.
11/2014	Lazarus Group targets Sony Entertainment Pictures with wiper malware. The group identifies itself as the Guardians of Peace and demands that a comedy movie about a plot to assassinate Kim Jong-un not be released. The group also steals information from Sony and leaks it on the internet.
10/2015	Lazarus Group is linked to cyberattacks against banks in the Philippines.
12/2015	Lazarus Group is linked to cyberattacks against the Tien Phong Bank in Vietnam.
02/2016	Lazarus Group conducts a cyberattack on the Bangladesh Central Bank through the SWIFT messaging system and steals US$81 million.
04/2016	DPRK hackers penetrates the South Korean Defense Integrated Data Center and steal classified documents.
11/2016	APT37 targets South Korean government and financial institutions as part of a cyberespionage campaign.
2017	Lazarus Group infiltrates the website of the Polish financial regulator and infects visitors with malware.
02/2017	DPRK hackers steal US$7 million worth of cryptocurrency from the South Korean cryptocurrency exchange Bithumb.
04/2017	A series of spear phishing emails targeting US defense contractors is attributed to the Lazarus Group.
05/2017	Ransomware WannaCry infects approximately 200,000 computers in over 150 countries. Cybersecurity companies Kaspersky Lab and Symantec affirm that the Lazarus Group is behind WannaCry. The NSA attributes the ransomware WannaCry to the DPRK.
09/2017	Lazarus Group targets users of the cryptocurrency exchange Coinlink with spear phishing emails.
2018	Operation Sharpshooter - cyber operations to access critical infrastructure in the United States and other countries around the world, a cyber-exploitation attack designed to probe military, financial, energy, telecommunications, healthcare and other networks for potential vulnerabilities.

Tabel 2.1. Timeline Serangan Lazarus Group

Sumber: (Raska, 2020)

2.6. Ambisi Korea Utara di Panggung Internasional

2.6.1. Pengakuan sebagai Negara Nuklir

Ambisi Korea Utara dibawah kepemimpinan Kim Jong Un tidak tidak hanya meningkatkan senjata nuklir untuk keamanan semata, melainkan juga sebagai alat tawar menawar bagi Korea Utara untuk mendapatkan status negara nuklir. Status

ini merupakan status yang sangat penting karena Korea Utara menyadari bahwa pengakuan secara formal dalam *Non Proliferation Treaty* (NPT) mustahil untuk dicapai, sehingga Korea Utara mengambil langkah bahwa pembuatan nuklir tanpa mengikuti peraturan internasional yang ada adalah langkah yang tepat meskipun berbentuk paksaan. Dengan serangkaian uji coba nuklir yang berhasil, seperti uji coba bom hidrogen keenam pada tahun 2017 serta peluncuran rudal Hwasong-17, Korea Utara mampu menunjukkan kemampuannya dalam membuat senjata nuklir di panggung internasional (Smith & Maler, 2022). Hal ini membuat Korea Utara mendapat pengakuan dari internasional, meskipun pengakuan tersebut berupa reaksi waspada, ancaman, tekanan, dan sanksi yang dijatuhkan kepada Korea Utara, terlebih biaya untuk melucuti dianggap terlalu tinggi dan berisiko perang terbuka (Barannikova, 2025).

Upaya Korea Utara yang selalu menekan untuk meningkatkan kekuatan nuklirnya ini bukan hanya uji coba militer semata, akan tetapi juga merupakan cara Korea Utara untuk menyusun hukum domestiknya kembali secara agresif mengenai senjata nuklir dan menutup kemungkinan celah diplomasi denuklirisasi. Puncak dari strategi ini terjadi pada September 2022 ketika Majelis Rakyat Tinggi Korea Utara mengesahkan undang-undang baru yang secara resmi mendeklarasikan status negara sebagai negara senjata nuklir dan menyebut bahwa status ini *irreversible* atau tidak dapat diubah. Undang-undang ini secara eksplisit melarang segala bentuk upaya baik dari dalam maupun luar negeri untuk melucuti senjata nuklir bahkan memberikan kewenangan militer untuk menggunakan serangan nuklir terlebih dahulu jika kepemimpinan rezim terancam (Al Jazeera, 2022). Selain itu, langkah

ini juga dirancang untuk mematikan harapan Korea Selatan dan Amerika Serikat mengenai *Complete, Verifiable, and Irreversible Dismantlement* (CVID) (Korea JoongAng Daily, 2023). Jadi upaya legitimasi senjata nuklir Korea Utara bukan semata untuk kekuatan militer saja, melainkan sebagai identitas konstitusional negara yang melekat pada keberlangsungan rezim.

Berakar dari jatuhnya rezim otoriter negara lain yang menyerahkan program senjata mereka, Korea Utara berupaya maksimal untuk mengejar status *de facto* sebagai negara nuklir dan memaksa aktor internasional untuk mengakuinya meskipun melalui ancaman. Korea Utara belajar dari kejatuhan rezim Muammar Gaddafi yang karena menyerahkan ambisi nuklirnya kepada Barat pada tahun 2003, rezim yang dibangun dalam waktu yang lama jatuh secara cepat (Hecker, 2023). Oleh karena itu, legitimasi sebagai negara nuklir dipandang sebagai satu-satunya cara Korea Utara untuk mencegah intervensi dari pihak asing yang ingin menjatuhkan Korea Utara. Kondisi yang diciptakan Korea Utara ini mampu membuat aktor internasional lainnya mempertimbangkan kembali sebelum melakukan provokasi militer, mengingat Korea Utara memiliki senjata nuklir, rudal balistik antarbenua hingga rudal taktis jarak pendek yang jika terjadi peperangan akan menyebabkan kerusakan yang signifikan.

Melalui legitimasi kekuatan nuklirnya, Korea Utara ingin merubah paradigma denuklirisasi menjadi pengendalian senjata. Korea Utara juga ingin diperlakukan setara dengan negara-negara nuklir non-NPT lainnya seperti Pakistan dan India dimana aktor internasional menerima bahwa senjata nuklirnya untuk stabilitas regional. Dalam skenario ini, Korea Utara merencanakan bahwa negosiasi

yang mungkin terjadi dimasa depan bukan sebatas penyerahan senjata, melainkan pembatasan jumlah nuklir sebagai imbalan untuk pencabutan sanksi yang dijatuhkan. Dengan demikian keputusan dan strategi Korea Utara ini menunjukkan bahwa tidak ada kedaulatan yang lebih tinggi diatas negara, sehingga apa yang Korea Utara lakukan melalui kekuatan nuklir ini bertujuan untuk bertahan di sistem internasional yang anarki.

2.6.2. Kekuatan Siber, Alat yang Mampu Mengancam Stabilitas

Seiring dengan perkembangan zaman, perlombaan kekuasaan tidak hanya ditandai dengan kekuatan tradisional saja, melainkan juga bagaimana aktor internasional memanfaatkan berbagai cara meskipun itu non konvensional atau cara terbaru untuk mendapatkan kekuasaan, memperkuat keamanan, ataupun mencapai kepentingan. Dalam konteks ini, siber mampu menjadi kekuatan vital di tengah zaman digital ini. Berbeda dengan kekuatan tradisional, kekuatan siber bersifat asimetris artinya negara yang memiliki keterbatasan sumber daya mampu memberikan kerusakan signifikan atau bahkan bangkit dari keterpurukan karena kekuatan siber memanfaatkan kecepatan distribusi informasi rahasia maupun data digital lainnya yang hal ini bergantung dari keterampilan dan sumber daya aktor. Selain itu, kekuatan siber bisa menjadi alat diplomasi koersif dan proyeksi kekuatan aktor internasional.

Kekuatan siber di Korea Utara mulai dikembangkan sejak masa kepemimpinan Kim Jong-Il melalui doktrin “perang segala cara” hingga pada masa kepemimpinan Kim Jong Un kekuatan siber mulai meningkat signifikan. Secara struktural, operasi siber Korea Utara dikendalikan secara terpusat oleh

Reconnaissance General Bureau (RGB) yang di dalamnya terdapat unit-unit khusus, salah satunya yaitu Lazarus Group yang melakukan serangan agresif terhadap aktor internasional (Kim, 2022). Serangan-serangan yang dilakukan Lazarus Group bertujuan untuk menunjukkan kepada internasional bahwa negara yang terisolasi dan ditekan oleh sanksi internasional, mampu memiliki kapabilitas siber yang setara dengan negara maju. Fokus utama serangan yang dilakukan Lazarus Group yaitu sektor ekonomi, namun dalam prosesnya tidak menutup kemungkinan bahwa Lazarus Group juga melakukan spionase atau merusak sistem digital korban. Akibat dari serangan Lazarus Group ini, banyak aktor internasional yang mengalami kerugian signifikan, seperti kasus pencurian terhadap Bangladesh Bank dan bursa kripto seperti *Ronin Bridge* dan *Bybit*, perusakan sistem melalui *malware* atau virus WannaCry yang melumpuhkan layanan kesehatan Inggris, dan spionase (Yun, 2025). Dengan demikian Korea Utara ingin menunjukkan bahwa kekuatan siber memungkinnya tetap bertahan ditengah sanksi dan isolasi, sembari mendapatkan dana untuk menunjang rezim dan peningkatan ekonomi, militer, dan siber.

2.7. Kerangka Hukum Internasional Lingkup Siber

Lingkup siber hingga saat ini masih belum memiliki dasar hukum yang jelas dan pasti sehingga menciptakan ambiguitas dalam menegakkan hukum terhadap pelaku kejahatan siber. Adanya ambiguitas ini tidak hanya dimanfaatkan oleh individu maupun kelompok, namun beberapa juga mulai memanfaatkan hal ini. Korea Utara, salah satu contohnya memanfaatkan ketidakpastian ini untuk terus melancarkan

serangan agar dapat bertahan di tengah tekanan sanksi internasional dan isolasi. Meskipun demikian, komunitas internasional berusaha menerapkan norma-norma hukum internasional yang sudah ada kedalam lingkup siber untuk menjaga stabilitas dan mengadili para pelaku kejahatan siber.

2.7.1. Piagam PBB Pasal 2(4)

Piagam PBB Pasal 2(4) yang berbunyi

> *All Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.*

menjadi fondasi hukum internasional yang melarang setiap warga negara anggota untuk menggunakan ancaman atau kekerasan terhadap integritas wilayah atau kemerdekaan politik negara lain. Namun kondisi ini hanya berfungsi pada ancaman maupun kekerasan fisik, sebaliknya serangan siber tidak menunjukkan faktor fisik karena hanya menyerang sistem digital. Hal ini tentu memunculkan perdebatan apakah setiap serangan siber yang tidak menunjukkan faktor fisik namun menyebabkan kerugian finansial yang besar dapat dihukum atau tidak. Namun jika kondisi bahwa serangan siber ini menyebabkan kerusakan fisik dan hilangnya nyawa, maka tindakan tersebut dapat dianggap sebagai pelanggaran terhadap Pasal 4(2) (United Nations, n.d.). Melihat kondisi ini, ketika Korea Utara melakukan serangan siber melalui Lazarus Group, serangan hanya mengincar sistem keuangan tanpa menyebabkan kerusakan fisik yang hal ini membuat aktor internasional, khususnya Barat kesulitan untuk menindak tindakan yang dilakukan Korea Utara ini. Sehingga salah satu cara untuk menekan Korea Utara melalui tuduhan *state sponsored activism.*

2.7.2. Piagam PBB Pasal 51

Piagam PBB Pasal 51 yang berbunyi

> *Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.*

mengakui hak inheren setiap negara untuk melakukan pembelaan diri (*self defense*) jika terjadi serangan bersenjata. Pasal ini dapat ditegakkan apabila sebuah negara menjadi korban dari serangan bersenjata (*armed attack*). Namun dalam lingkup siber, pasal ini belum dapat sepenuhnya dapat ditegakkan karena batasan serangan bersenjata yang dimaksud masih belum ada sehingga serangan siber bukan termasuk bagian dari serangan bersenjata. Akan tetapi, jika serangan siber ini melumpuhkan infrastruktur kritis secara masif sehingga mengancam eksistensi atau keamanan nasional suatu negara, maka negara tersebut secara hukum berhak melakukan tindakan balasan sebagai bentuk pembelaan diri (United Nations, n.d.).

2.7.3. Tallinn Manual 2.0

Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations merupakan panduan komprehensif yang disusun oleh para ahli hukum internasional untuk menafsirkan bagaimana hukum internasional yang ada berlaku di lingkup siber. Tallinn Manual 2.0 menjelaskan bahwa setiap negara memiliki kedaulatan atas infrastruktur siber yang berada di wilayahnya, namun dalam batasan bahwa infrastruktur siber tidak boleh digunakan untuk menyerang atau segala hal yang

melanggar hak negara lain dan jika ada operasi siber yang mampu menimbulkan kerusakan fisik maka akan dianggap sebagai penggunaan kekuatan yang dalam hal ini melanggar prinsip *non-use of force.* Selain itu, juga menjelaskan bahwa negara tidak boleh mengintervensi urusan dalam negeri negara lain melalui operasi siber (Schmitt, 2017).

Kondisi realita menunjukkan bahwa meskipun Tallinn Manual 2.0 memberikan panduan dan aturan terhadap penggunaan kekuatan siber, Tallinn Manual 2.0 bukan merupakan sebuah aturan resmi yang harus disetujui oleh aktor internasional. Kembali pada fakta bahwa Tallinn Manual 2.0 ini hanya merupakan panduan dari ahli hukum, maka tidak bisa menindak pelaku serangan siber. Hal ini dimanfaatkan oleh aktor internasional untuk tetap melakukan serangan maupun operasi siber yang sebisa mungkin mendapatkan keuntungan sebesar-besarnya dan meninggalkan kerusakan pada sistem tanpa memicu kerusakan fisik.