KETERBATASAN STRATEGI *DETERRENCE* AMERIKA SERIKAT TERHADAP SERANGAN SIBER KOREA UTARA

(THE LIMITATION OF UNITED STATES DETERRENCE STRATEGY TOWARDS NORTH KOREA CYBER ATTACKS)

SKRIPSI

Oleh

Kukuh Ugie Sembodho

NIM 150910101007

JURUSAN ILMU HUBUNGAN INTERNASIONAL

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK

UNIVERSITAS JEMBER

2019

KETERBATASAN STRATEGI *DETERRENCE* AMERIKA SERIKAT TERHADAP SERANGAN SIBER KOREA UTARA

(THE LIMITATION OF UNITED STATES DETERRENCE STRATEGY TOWARDS NORTH KOREA CYBER ATTACKS)

SKRIPSI

Diajukan guna melengkapi tugas akhir dan memenuhi salah satu syarat untuk menyelesaikan studi pada jurusan Ilmu Hubungan Internasional (S1) dan mencapai gelar Sarjana Sosial

Oleh

Kukuh Ugie Sembodho

NIM 150910101007

JURUSAN ILMU HUBUNGAN INTERNASIONAL

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK

UNIVERSITAS JEMBER

2019

PERSEMBAHAN

Skripsi ini saya persembahkan untuk:

1. Seluruh keluarga dan kerabat;
2. Bapak dan Ibu Guru sejak Taman Kanak-Kanak hingga Perguruan Tinggi;
3. Almamater Ilmu Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik Universitas Jember;
4. Teman berfikir dan berkembang di Himpunan Mahasiswa Hubungan Internasional (HIMAHI), *University Student English Forum* (USEF), dan *The Center for Human Rights Multiculturalism and Migration* (CHRM2) Universitas Jember;
5. Seluruh keluarga HI UNEJ 2015, dan teman-teman yang tidak dapat disebutkan satu per satu.

MOTTO

"*If you're asking me if I think we're at war, I think I'd say Yes*".. *We're at war right now in cyberspace. We've been at war for maybe a decade. They're pouring oil over the castle every day*[*)]

[*)] Seffers, 2019, Kinetic Weapons Remain a Priority as Cyber War Rages, I

PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama : Kukuh Ugie Sembodho

NIM : 150910101007

Menyatakan bahwa karya tulis ilmiah yang berjudul "Keterbatasan Strategi *Deterrence* Amerika Serikat terhadap Serangan Siber Korea Utara" adalah benar-benar hasil karya saya sendiri, kecuali kutipan yang telah saya sebutkan sumbernya. Sumber yang digunakan dalam skripsi ini berasal dari sumber-sumber yang sah dan diketahui. Skripsi ini belum pernah diajukan pada institusi mana pun, dan bukan karya jiplakan. Saya bertanggung jawab atas keabsahan dan kebenaran isinya sesuai dengan sikap ilmiah yang harus dijunjung tinggi.

Demikian pernyataan ini saya buat dengan sebenarnya, tanpa ada tekanan dan paksaan dari pihak mana pun serta bersedia mendapat sanksi akademik jika ternyata di kemudian hari pernyataan ini tidak benar.

Jember, 9 Juli 2019

Yang menyatakan

Kukuh Ugie Sembodho

NIM 150910101007

SKRIPSI

KETERBATASAN AMERIKA SERIKAT TERHADAP SERANGAN SIBER KOREA UTARA

THE VULNERABILITY OF UNITED STATES TOWARDS NORTH KOREA CYBER ATTACKS

Oleh
KUKUH UGIE SEMBODHO
NIM 15019101007

Pembimbing

Dosen Pembimbing Utama : Agus Trihartono, S. Sos., M.A., Ph.D.
Dosen Pembimbing Anggota : Drs. Abubakar Eby Hara, M.A., Ph.D.

PENGESAHAN

Skripsi berjudul "Keterbatasan Strategi *Deterrence* Amerika Serikat terhadap Serangan Siber Korea Utara" telah diuji dan disahkan pada:

Hari :Rabu
Tanggal :7 Agustus 2019
Waktu :08.30-Selesai
Tempat :Ruang Ujian Bersama Fakultas Ilmu Sosial dan Ilmu Politik
Univeristas Jember

Tim Penguji,
Ketua

Drs. Himawan Bayu Patriadi MA., Ph.D.
NIP 196108281992011001

Sekretaris 1

Sekretaris 2

Agus Trihartono, S.Sos, MA. Ph.D.
NIP 196908151995121001

Drs. Abubakar Eby Hara, MA., Ph.D.
NIP 196402081989021001

Anggota 1

Dr. Muhammad Iqbal, S.Sos., M.Si.
NIP 197212041999031004

Mengesahkan,
Dekan Fakultas Ilmu Sosial dan Ilmu Politik
Universitas Jember

Dr. Hadi Prayitno, M.Kes
NIP. 196106081998021001

RINGKASAN

Keterbatasan Strategi *Deterrence* Amerika Serikat terhadap Serangan Siber Korea Utara; Kukuh Ugie Sembodho, 150910101007; 2019: 99 Halaman; Jurusan Ilmu Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik Universitas Jember.

Penemuan dan perkembangan internet telah berdampak bagi banyak hal termasuk dalam pola hubungan antarnegara baik yang bersifat konstruktif maupun destruktif. Ruang siber oleh banyak pakar disebut sebagai domain kelima peperangan setelah daratan, laut, udara, dan ruang angkasa. Dalam beberapa dekade terakhir telah banyak serangan yang diluncurkan melalui ruang siber seperti *Operation Desert Storn, Stuxnet, Estoman Cyber Attack*, dll. Serangan di ruang siber memiliki banyak variasi dan dapat diluncurkan oleh individu hingga Negara. Salah satu persaingan di ruang siber antarnegara yang menarik untuk dikaji adalah persaingan antara Amerika Serikat dan Korea Utara. Kedua Negara terlibat dalam banyak kasus peperangan siber. Persaingan kedua Negara tersebut menarik ketika Amerika Serikat sebagai salah satu negara dengan system keamanan siber terkuat di dunia justru beberapa kali berhasil diserang oleh Korea Utara dengan medium ruang siber. Beberapa serangan siber seperti *4th of July Cyber Attack, Sony Cyber Attack,* dan *WannaCry Ransomware* menunjukkan kerentanan Amerika Serikat di ruang siber.

Penelitian ini bertujuan untuk mengetahui alasan keterbatasan strategi *deterrence* Amerika Serikat terhadap serangan siber Korea Utara. Permasalahan yang dikaji dalam penelitian ini berkaitan dengan alasan dibalik keterbatasan strategi *deterrence* Amerika Serikat terhadap serangan siber Korea Utara. Sumber data yang digunakan yakni *literature* berupa buku baik cetak maupun *e-book*, artikel dari internet, dan jurnal ilmiah. Analisis data yang dilakukan yakni menggunakan eksplanatif kualitatif.

Hasil penelitian menunjukkan bahwa keterbatasan strategi *deterrence* Amerika Serikat terhadap Korea Utara di ruang siber disebabkan oleh adanya

perbedaan karakteristik ruang siber sebagai sebuah domain perang. Beberapa factor seperti anonimitas, asimetri, *super-empowered individuals*, skalabilitas dan temporalitas dianggap menjadi alasan kunci bagi kerentanan Amerika Serikat di ruang siber. Anonimitas berkaitan dengan sifat serangan di ruang siber dilakukan secara diam-diam dan tidak transparan, sifat ini membuat proses atribusi menjadi terhalang. Walaupun atribusi dapat dilakukan, adanya sifat asimetri juga menjadi faktor dari kerentanan Amerika Serikat terhadap serangan siber. Ketergantungan Amerika Serikat dan Korea Utara terhadap internet yang asimetris membuat satu Negara diuntungkan sedang lainnya dirugikan. Selain itu fakta apabila seorang atau sekelompok dapat meluncurkan serangan siber seperti yang terjadi pada *Sony Cyber Attack* membuat proses retaliasi menjadi sulit. Temuan lain juga menjelaskan dua sifat dari serangan siber yang membuatnya berbeda, yaitu skalabilitas dan temporalitas. Skalabilitas mengacu pada kemungkinan dampak yang dapat ditimbulkan oleh sebuah serangan sedangkan temporalitas mengacu pada sifat serangan yang tiba-tiba tanpa peringatan dini.

PRAKATA

Puji syukur kepada Tuhan Yang Maha Esa atas segala rahmat dan hidayah-Nya sehingga penulis dapat menyelesaikan skripsi yang berjudul "Keterbatasan Strategi *Deterrence* Amerika Serikat terhadap Serangan Siber Korea Utara". Skripsi ini disusun untuk memenuhi salah satu syarat menyelesaikan pendidikan strata satu (S1) pada Jurusan Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Jember.

Penyusunan skripsi ini tidak lepas dari bantuan dan dukungan berbagai pihak. Oleh karena itu, penulis menyampaikan terima kasih sebesar-besarnya kepada:

1. Agus Trihartono, S.Sos., M.A., Ph.D. selaku Dosen Pembimbing Utama dan Drs. Abubakar Eby Hara, M.A., Ph.D. selaku Dosen Pembimbing Anggota yang telah meluangkan waktu, pikiran, perhatian, dan bimbingan dalam penulisan skripsi ini;
2. Drs. Abubakar Eby Hara MA, Ph.D selaku Dosen Pembimbing Akademik atas dorongan dan bimbingannya selama penulis menjadi mahasiswa;
3. Bapak dan ibu dosen di Jurusan Ilmu Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik Universitas Jember yang telah memberikan ilmu dan bimbingan selama penulis menjadi mahasiswa;
4. Semua pihak yang tidak dapat disebutkan satu per satu atas bantuan tenaga dan waktunya dalam penyelesaian skripsi ini.

Dalam penulisan skripsi ini tentu masih terdapat kelemahan, kekurangan serta kesalahan. Oleh sebab itu penulis menerima segala kritik dan saran demi kesempurnaan skripsi ini. Penulis berharap semoga skripsi ini dapat bermanfaat.

Jember, 17 Juni 2019

Penulis

DAFTAR ISI

Halaman

BAB I
PENDAHULUAN

1.1. Latar Belakang

Penemuan dan perkembangan internet telah membuat dunia internasional menjadi akrab dengan istilah ruang siber (inggris: *cyberspace*) (Department of Defense, 2010:79-80). Ruang siber mencakup arsitektur pengorganisasian internet, semua perangkat yang terhubung, serta jaringan kabel dan nirkabel. Beberapa jaringan ini dikelola oleh entitas sektor pemerintah dan swasta, beberapa terhubung ke internet yang lebih luas dan beberapa yang tidak. Walaupun internet secara teknis adalah domain murni pertama yang diciptakan manusia, struktur yang dimiliki membuatnya sulit untuk dipahami. Domain yang diharapkan berada dalam batas tertentu justru berkembang seperti sistem alami lainya seperti koloni bakteri dan galaksi yang meluas ke segala arah (Granger & Lorelei, 2012:99). Dirancangnya ruang siber sebagai domain yang terbuka membuat keamanan menjadi hal yang tidak melekat di dalamnya. Oleh karena itu, fungsi dari internet dan ruang siber menjadi luas dan beragam hingga ruang siber dapat dikatakan sebagai domain kelima peperangan setelah daratan, laut, udara dan ruang angkasa (Kaplan, 2016:6).

Setelah penemuan ruang siber sebagai domain perang yang baru, banyak negara, kelompok maupun individu yang meluncurkan serangan melalui domain tersebut. Tragedi 9/11, serangan siber di Estonia dan *Stuxnet*[1] di Iran dianggap sebagai katalis bagi munculnya diskursus mengenai *cyberwarfare*[2] (Kaiser, 2015: 11), untuk kemudian berusaha memberikan penjelasan bagaimana perang siber

[1] Merupakan sebuah "cacing komputer" berukuran 500 kb yang berhasil menginfiltrasi berbagai komputer termasuk fasilitas nuklir Iran di tahun 2010. Holloway, M. 2015.Stuxnet Worm Attack on Iranian Nuclear Facilities. http://large.stanford.edu/courses/2015/ph241/holloway1/ [Diakses pada 3 Juni 2019]

[2] Aktivitas yang dilakukan oleh individu, kelompok, atau negara yang satu terhadap yang lain yang bersifat destruktif yang berbasis komputer dan jaringan. Kshetri, N. (2014). *The Quest to Cyber Superiority*. Springer. Halaman 5

telah merubah tatanan keamanan nasional. Dalam konteks keamanan, perang siber memiliki pola yang sangat berbeda jika dibandingkan dengan perang yang selama ini kita ketahui. Dahulu, keadaan asimetris dimana sumber daya militer yang berbeda akan terlihat jelas ada di antara pihak-pihak yang bertikai. Melihat hal tersebut, perang siber kemudian menambah nilai strategis yang dalam berbagai kasus menguntungkan pihak yang lebih inferior (Dixit, 2010). Melakukan serangan pada area siber bertujuan untuk mengatasi ketidakmampuan militer suatu kelompok atau negara dengan cara menggunakan cara dan pola yang baru. Upaya tersebut dilakukan untuk melemahkan lawan dan membuat pola perang menjadi berbeda, namun bukan berarti keseluruhan proses perang siber harus dianalisis secara khusus dan terpisah dari konteks keamanan tradisional (Eun & Abmann, 2016), atau menganggap intervensi militer atau bentuk perang lain telah tidak relevan dalam dunia internasional. Sebaliknya, diskursus keamanan siber ini menjadi wacana baru yang memperkaya studi hubungan internasional.

Satu dari banyak serangan siber yang terjadi dalam beberapa tahun terakhir adalah serangan yang dilakukan oleh Korea Utara terhadap Amerika Serikat. Di samping kekuatan nuklir yang selama ini diekspos oleh media, Korea Utara juga memiliki kapabilitas dalam bidang siber. Korea Utara menjadi satu dari empat negara yang mengancam Amerika Serikat dalam bentuk serangan siber di samping Rusia, Tiongkok, dan Iran (Coats, 2018:5). Beberapa pakar keamanan bahkan menyebut jika saat ini kekuatan siber Korea Utara lebih kuat dari yang dimiliki oleh Russia (Hern, 2018). Pyongyang dipercaya memiliki sumber daya yang dapat digunakan untuk memberikan berbagai pendekatan ofensif dengan sedikit atau tanpa peringatan, termasuk serangan siber, penghapusan data, dan penyebaran *ransomware*[3] (Busby, 2018). Korea Utara menjadi sebuah negara yang menarik karena berbeda dengan Tiongkok, Rusia, dan Iran yang memang

[3] Sebuah serangan siber yang pada umumnya dilakukan dengan mengenkripsi data korban, dan meminta tebusan agar data tersebut dapat dikembalikan melalui email. Goldman, Russell. (2014). What We Know and Don't Know About the International Cyber Attack. https://www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html [Diakses pada 22 April 2019]

merupakan negara dengan penetrasi teknologi tinggi (Dhiraj 2019), Korea Utara yang notabene bukan negara yang berfokus pada teknologi bisa duduk setara menjadi 4 negara yang mengancam Amerika serikat. Oleh karena itu Korea Utara dipilih dari 4 negara tersebut.

Serangan siber yang dilakukan oleh Korea Utara bukanlah sebuah teori konspirasi belaka. Korea utara dianggap menjadi aktor di balik berbagai serangan siber yang menyerang Amerika Serikat, seperti: *Fourth of July Incident* pada tahun 2009; *Sony Pictures* pada tahun 2014; serta W*annaCry* pada tahun 2017 (Bing & Lynch, 2018; Busby, 2018). Dampak dari serangan siber tersebut tidak dapat dipandang sebelah mata. Pada *Fourth of July Incident*, serangan siber berhasil membuat berbagai situs web pemerintah lumpuh. Beberapa web yang berhasil diretas pada serangan tersebut antara lain: Departemen Keuangan Amerika Serikat; Dinas Intelijen Rahasia; Departemen Transportasi Amerika Serikat; Komisi Sekuritas dan Bursa Amerika Serikat serta berbagai media besar di Amerika Serikat. Dalam serangan tersebut, peretas melakukan *Distributed Denial of Services* (DDoS)[4] yang membuat situs web yang diretas menjadi lumpuh (Castro, 2009; Shaer, 2009). Serangan siber terhadap *Sony Pictures* juga tak kalah berbahaya. *Guardians of Peace* (GOP)[5] berhasil meretas perusahaan tersebut dan membocorkan berbagai data seperti surel antar pegawai hingga beberapa film yang belum tayang (Siboni & Siman-Tov, 2014: 1). Walaupun *Sony Pictures* merupakan perusahaan swasta, keberhasilan serangan siber tersebut menunjukan bagaimana sistem keamanan siber yang kurang kuat. Tidak hanya serangan yang menyerang satu negara saja, dampak dari serangan siber *WannaCry* berhasil meneror lebih dari 150 negara. Serangan ini menjadi pelajaran dunia

[4] DDos (Bahasa Inggris: *distributed Denial of Service Attacks)* adalah jenis serangan yang dilakukan oleh peretas terhadap sebuah komputer atau server di dalam jaringan internet dengan cara menghabiskan sumber daya yang dimiliki komputer tersebut sampai komputer tersebut tidak lagi dapat menjalankan fungsinya. Beal, V. 2015. DDoS Attack- Distributed Denial of Service. https://www.webopedia.com/TERM/D/DDoS_attack.html [Diakses pada 2 Juni 2019]

[5] Merupakan organisasi peretas yang mengklaim telah memiliki jaringan di seluruh dunia. Kelompok ini menjadi sorotan setelah melakukan serangan terhadap *SONY Pictures* dan menyatakan ingin menyingkirkannya dari bumi. DeSimone, A. 2017. *Sony's Nightmare before Christmas.* John Hopkins. Halaman 4

bagaimana serangan siber bisa sangat berdampak bagi sebuah negara bahkan dunia, dalam serangan itu beberapa sektor seperti kesehatan dan pendidikan dilumpuhkan (Department of Health, 2018: 11).

Setelah mengalami berbagai serangan siber tersebut, Amerika Serikat tidak tinggal diam. Amerika Serikat berusaha mengembangkan sistem keamanan siber untuk dapat mengatasi atau mencegah adanya serangan serupa. Amerika Serikat telah mulai memperhatikan keamanan siber sejak tahun 2002 dengan dibuatnya *The Homeland Security Act of 2002* yang di dalamnya memuat *Cyber Security Enhancement Act of 2002*[6] (Department of Homeland Security, 2002). Setelah itu, perkembangan diskursus mengenai keamanan siber terus berkembang dan menghasilkan berbagai kerangka hukum yang secara khusus mengatur tentang keamanan siber mulai dari *Cyber Intelligence Sharing and Protection Act (CISPA), Strengthening and Enhancing Cybersecurity by Using Research, Education, Information, and Technology Act of 2012 (SECURE IT), the Cybersecurity Act of 2012* hingga yang terbaru adalah *National Cyber Strategy* 2018 (Tirrel, 2012).

Penelitian ini menjadi menarik karena posisi Amerika Serikat yang berada di peringkat kedua atau termasuk dalam kategori *Leading Country* dalam *Global* Cybersecurity *Index*[7] (International Telecommunications Union, 2018) dan peringkat pertama dalam *Cyber Attack Power Ranking by Country* (Celiktas & Unlu, 2018:480) yang mana Korea Utara bahkan tidak masuk kedalamnya. Kedua indeks tersebut setidaknya menggambarkan bagaimana Amerika Serikat memiliki kemampuan baik defensif maupun ofensif yang lebih dari memadai. Di samping itu, Amerika Serikat merupakan negara dengan penetrasi internet tinggi yang penggunanya mencapai 80% dari jumlah populasi (Dillinger, 2019) dan 6,5% dari

[6] Merupakan undang-undang federal Amerika Serikat yang mengatur kejahatan yang terkait komputer maupun internet

[7] GCI merupakan survey yang mengukur komitmen negara terhadap keamanan siber dengan lima pilar (legal, teknis, organisasi, *capacity building,* serta kerjasama). International Telecommunications Union. (2018). Global Cybersecurity Index. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf [Diakses pada 15 Januari 2019]

seluruh GDP Amerika Serikat (1,2 Triliun dollar AS) di tahun 2016 bergantung pada internet (NTIA, 2018). Sedangkan di lain sisi Korea Utara merupakan negara yang memiliki kehadiran terkecil dalam internet global dan bahkan kecilnya kehadiran tersebut disalurkan melalui Tiongkok. Selain itu, oleh pemerintah Korea Utara internet nasional dipisahkan dari internet global (Chanlett-Avery, 2017:1). Kondisi yang kontras di antara kedua negara rasanya membuat kasus yang terjadi antara Korea Utara dan Amerika Serikat ini menjadi menarik. Serangan yang terus menerus dilakukan olehnya menunjukan keterbatasan keamanan siber yang dibangun oleh Amerika Serikat. Penelitian ini kemudian akan menjelaskan bagaimana pergeseran konsep keamanan dalam ruang siber dan bagaimana penerapanya dalam kasus Amerika Serikat dan Korea Utara.

Dari latar belakang dan ketimpangan tersebut, penulis kemudian akan mengangkat penelitian yang berjudul:

Keterbatasan Strategi *Deterrence* Amerika Serikat terhadap Serangan Siber Korea Utara

1.2. Ruang Lingkup Pembahasan

Ruang lingkup pembahasan merupakan salah-satu aspek yang penting dalam sebuah penelitian untuk tetap memastikan penelitian tidak melebar dan menjelaskan sesuatu yang tidak perlu dijelaskan. Dalam penelitian ini terdapat dua ruang lingkup pembahasan, pertama berkaitan dengan batasan materi dan kedua berkaitan dengan batasan waktu.

1.2.1 Batasan Materi

Penelitian ini merupakan studi keamanan (*security studies*) yang akan menggunakan logika berfikir strategi *deterrence* sehingga untuk membuat penelitian ini fokus, penulis membatasi materi yang dibahas dalam tulisan ini meliputi berbagai serangan siber Korea Utara dan berbagai upaya yang dilakukan oleh Amerika Serikat untuk menangkalnya.

1.2.2 Batasan Waktu

Batasan waktu yang ditetapkan dalam tulisan ini adalah dari tahun 2002 hingga 2018. Tahun 2002 dipilih sebagai awal bagi data penelitian dikarenakan pada tahun tersebut muncul strategi keamanan siber pertama oleh Amerika Serikat yang dikenal dengan nama *The Homeland Security Act of 2002*. Mengingat isu perang siber yang masih terus terjadi hingga saat ini, maka 2018 dipilih sebagai akhir batasan waktu penelitian karena pada akhir 2018 penelitian ini dimulai, pembatasan ini ditujukan untuk membuat penelitian memiliki fokus yang jelas dan dimana terjadi kejadian baru maka tidak akan mempengaruhi hasil penelitian.

1.3. Rumusan Masalah

Sebuah penelitian yang ideal seharusnya memiliki perumusan masalah untuk mempermudah proses analisis masalah. Di samping itu, rumusan masalah juga membuat penelitian lebih jelas, terutama terkait dengan dari mana penelitian dimulai dan kemana penelitian tersebut akan menuju (Arikunto, 1989: 7). Rumusan masalah diangkat berdasarkan latar belakang yang dihadapi oleh sebuah fenomena. Berdasarkan latar belakang yang telah dijabarkan sebelumnya, maka rumusan yang diangkat dalam tulisan ini adalah: **mengapa strategi *deterrence* Amerika Serikat mengalami keterbatasan terhadap serangan siber Korea Utara?**

1.4. Tujuan Penelitian

Setiap penelitian baik kualitatif maupun kuantitatif selalu memiliki tujuan yang hendak dicapai. Dalam penelitian kualitatif, tujuan penelitian atau *purpose statement* merupakan pernyataan yang menjadi keseluruhan arah penelitian (Creswell, 2003: 15). Penelitian ini bertujuan untuk menjelaskan alasan dibalik keterbatasan strategi *deterrence* Amerika Serikat khususnya dalam menghadapi serangan siber Korea Utara.

1.5. Kerangka Konseptual

1.5.1 Keamanan Siber (Cybersecurity)

Istilah keamanan siber (Inggris: *cybersecurity*) dapat ditelusuri setidaknya dari akhir tahun 1980-an dan bahkan secara konseptual lebih jauh lagi, tetapi penggunaannya saat ini relatif baru. Hingga tahun 2000-an tidak ada praktisi yang mengidentifikasi diri sebagai profesional dalam keamanan siber (Denning & Frailey, 2011:25), ketika dokumen kebijakan nasional juga mulai menggunakan istilah tersebut. Selanjutnya, keamanan siber berkembang sebagai konsep dan praktik dengan begitu cepat, dan berkembang bersama dengan konsep keamanan kontemporer lainnya. Seperti halnya konsep yang lain, terdapat kesulitan dalam mencapai konsensus terkait apa yang disebut sebagai keamanan siber (Bambauer, 2012:587). Kondisi seperti ini disesalkan bagi beberapa orang tetapi juga menawarkan peluang untuk keterlibatan yang produktif dengan keamanan siber .

Keamanan siber secara umum dapat didefinisikan sebagai sebuah sarana yang tidak hanya untuk melindungi dan mempertahankan masyarakat dan infrastruktur informasinya yang penting, tetapi juga cara penuntutan kebijakan nasional dan internasional yang berbasis teknologi informasi (Stevens, 2016: 11). Deskripsi tersebut menyoroti karakteristik ontologis keamanan siber dan hubungannya dengan teknologi informasi, khususnya internet. Selain itu, deskripsi tersebut mengakui bahwa keamanan siber bukan hanya strategi defensif, seperti yang ditujukan pada upaya untuk mencapai kepentingan politik melalui intervensi dan pendekatan internasional yang aktif. Hal tersebut menyiratkan apabila beberapa teori dan metode mungkin cocok untuk mengeksplorasi keamanan siber. Keamanan siber sebagai sebuah teori tidak mengalami perkembangan yang pesat dalam beberapa tahun terakhir dikarenakan studi keamanan siber berorientasi untuk memecahkan masalah kebijakan dengan mengorbankan pengembangan teori dan inovasi metodologi (Eriksson & Giacomello, 2007: 2). Keamanan siber pada dasarnya layak menjadi sebuah pekerjaan akademik — dan ada banyak kontribusi yang sangat bagus — tetapi beberapa pakar keamanan siber belum

melampaui 'kemandulan teoritis' yang mempengaruhi studi keamanan secara umum (Buzan, 2000:3).

Pentingnya keamanan siber dalam ilmu hubungan internasional merupakan fakta yang tidak dapat dihindarkan dan telah menjadi fokus bagi beberapa negara (Valeriano & Maness, 2018:273). Dalam pengembanganya, kemananan siber sebagai sebuah teori maupun praktek mengalami kesulitan utamanya terkait penilaian dan pengukuran, hingga *International Communication Union* (ITU)[8] mengeluarkan beberapa indikator yang membantu mengukur keamanan siber. Dalam kerangka kerjanya, ITU memfokuskan keamanan siber pada lima bidang utama antara lain: langkah hukum; teknis; organisasional; pembangunan kapasitas; dan kerjasama (ITU, 2018:7-8). Kelima indikator tersebut merupakan hal yang penting dalam mengukur kemampuan sebuah negara dalam keamanan siber karena indikator tersebut akan secara tidak langsung menciptakan sistem nasional yang sadar terhadap keberadaan dan pentingnya ruang siber. Keamanan siber memiliki ranah penerapan yang berkaitan dengan segala industri dan sektor baik secara vertikal maupun horizontal. Untuk menciptakan perubahan kemampuan siber di tingkat nasional berarti membutuhkan keterlibatan lembaga politik sosial, dan ekonomi. Hal tersebut dapat diwujudkan dalam penegakan hukum, lembaga pendidikan, kementrian, dan segala bentuk kerjasama publik dan privat di sebuah negara maupun antar negara (ITU 2018:9).

1.5.2 Deterrence

Deterrence dalam studi keamanan internasional mengacu pada upaya strategis untuk mencegah pihak lain mengambil tindakan yang merugikan dengan memberikan gambaran serangan balik apabila tindakan tersebut dilakukan (Morgan, 2010: 55). Dengan kata lain, *deterrence* adalah bujukan kepada, penyerang potensial yang mencoba menyampaikan apabila tidak melakukan

[8] *The International Telecommunication Union* atau yang awalnya bernama *International Telegraph Union* merupakan agensi khusus PBB yang bertanggung jawab atas isu-isu terkait komunikasi dan informasi. ITU. 2019. ITU-T in Brief. https://www.itu.int/en/ITU-T/about/Pages/default.aspx [Diakses pada 12 Juli 2019]

serangan adalah keputusan terbaik yang bisa diambil (Morgan, 1977: 22). Konsep *deterrence* mengacu pada suatu bentuk pengaruh pencegahan yang terutama bertumpu pada insentif negatif (Paul, Morgan, & Wirtz, 2009: 2). Keberadaan strategi ini banyak dibicarakan oleh pakar HI pada era perang dingin dimana terdapat perlombaan senjata nuklir antara Amerika Serikat dan Uni Soviet yang mana terdiri atas tiga komponen antara lain: kemampuan; kredibilitas; dan komunikasi.

Seiring dengan perkembangan teknologi, hubungan antara perang siber dan strategi *deterrence* telah meningkat dan menjadi fokus studi beberapa pakar keamanan. Banyak yang kemudian mencari jawaban mengenai bagaimana cara mengimplementasikan teori *deterrence* klasik untuk kemudian dapat menjadi solusi bagi serangan siber maupun perang siber yang mungkin terjadi (Lupovici, 2011: 49-51). Hal tersebut kemudian menjadi dorongan mengenai munculnya apa yang Goodman kemukakan yang kemudian disebut *cyber deterrence theory*.

Penggunaan strategi *cyber deterrence* dapat dilihat sejak *Operation Desert Storm*[9] pada tahun 1991 ketika ide mengenai revolusi militer menjadi sorotan. Pada awal serangan, Amerika Serikat melancarkan *information war (IW)* yang mana oleh D. Betz didefinisikan sebagai potensi senjata dalam dirinya sendiri (Betz, 2006: 508), kepada pemerintah Irak dengan melumpuhkan sistem komunikasi militernya. Kejadian tersebut kemudian menunjukan pentingnya strategi *cyber deterrence.* Pada tahun 1990-an, para pakar memberikan dasar yang kuat untuk studi *deterrence* dan IW. Setelah berbagai serangan siber pada akhir 2000-an, seperti serangan siber di Estonia pada tahun 2007, perhatian para ahli beralih untuk mencegah serangan siber, atau perang siber, yang memiliki tujuan strategis dan politis (Stevens, 2012: 149-151).

[9] Bagian dari perang teluk yang terjadi dari tanggal 17 Januari 1991 hingga 28 Februari 1991 yang terjadi antara koalisi 35 negara yang dipimpin oleh Amerika Serikat terhadap Irak sebagai respon atas invasi dan aneksasi terhadap Kuwait. Gugliota, G., & Murphy, C. 1991. Jets Roar Off in Darkness at Start of 'Desert Storm'. https://www.washingtonpost.com/wp-srv/inatl/longterm/fogofwar/archive/post011791_2.htm [Diakses pada 4 Juni 2019]

Istilah *cyber deterrence* terdiri dari dua komponen. Pertama yaitu *cyber* atau siber yang mana oleh Joseph S. Nye didefinisikan sebagai awalan yang menggambarkan kegiatan yang berkaitan dengan komputer dan jaringan (Nye, 2011: 122). Komponen kedua adalah *deterrence* yang didefinisikan sebagai usaha untuk mencegah pihak lain melakukan serangan atau tindakan merusak dengan memberikan gambaran tentang kemungkinan pembalasan atau hukuman (Morgan, 2010: 155). Dengan basis tersebut kemudian Goodman mendefinisikan *cyber deterrence* sebagaimana strategi *deterrence* lain yang berusaha mencegah serangan pihak lain, namun hal dasar yang membedakan adalah media serangan yang lebih spesifik pada ranah maya (Goodman, 2010: 107). T. Stevens menawarkan deskripsi yang lebih spesifik tentang *cyber deterrence*, dengan penekanan pada strategi *deterrence* yang umumnya dirasakan di antara negara. Tujuan *cyber deterrence* adalah untuk menghalau serangan siber melalui bujukan dari calon agresor bahwa serangan semacam itu akan berujung dengan hasil yang tidak menguntungkan (Stevens, 2012: 151).

Sebagaimana strategi *deterrence* klasik, komunikasi, kredibilitas, dan kapabilitas merupakan tiga komponen penting dalam teori *cyber deterrence*. Pertama, negara mengimplementasikan strategi *deterrence* untuk melindungi kepentingannya. Dalam upaya mencegah pihak lain melakukan serangan, negara tersebut harus mendeklarasikan penggunaan strategi *deterrence* (Goodman, 2010: 105). Negara yang menggunakan strategi ini harus melakukan komunikasi secara efektif terhadap negara lain terutama negara yang menjadi potensi agresor di masa mendatang. Tak kalah pentingnya, kemampuan negara untuk menunjukan kemauan serta kemampuan yang mana tidak hanya pada masa perang. Kedua, bersamaan dengan komunikasi, kredibilitas menjadi hal yang sama pentingnya. Strategi *deterrence* akan efektif apabila ada kejelasan terkait apa yang akan dilakukan ketika garis merah yang telah ditetapkan tersebut dilewati. Apabila hal tersebut gagal dilakukan maka kredibilitas suatu negara akan kemudian dipertanyakan oleh dunia internasional (Iasiello, 2014: 56). Terakhir, kapabilitas

adalah cara negara untuk menghukum penantang atau menyangkal manfaat yang dapat diperoleh dari serangan, atau keduanya (Goodman, 2010: 105-106).

Apabila menggunakan penjelasan diatas, *cyber deterrence* akan dianalisis menggunakan teori *deterrence* klasik yang mana menggunakan dua strategi utama yaitu: *deterrence by denial;* dan *deterrence by punishment or retaliation* (Geers, 2010: 7; Libicki, 2009: 29).

a. Deterrence by Denial

Secara sederhana, *deterrence by denial* merupakan usaha untuk mencegah calon agresor untuk mendapatkan atau mencapai tujuanya melalui serangan siber, sebaliknya strategi ini berusaha menunjukan bagaimana berbagai jenis serangan akan berujung pada hasil yang sebenarnya tidak diharapkan oleh agresor (Kugler, 2009: 327). Strategi ini berusaha meminimalisir peluang lawan untuk mendapatkan keuntungan dengan melakukan serangan melalui perlindungan komputer dan jaringan (Jasper, 2015: 69). Dengan demikian, tujuan *deterrence by denial* adalah persuasi musuh bahwa dengan pertahanan yang kuat, maka serangan tidak akan mendapatkan manfaat yang setara dengan biaya usaha dan biaya yang dikeluarkan (Philbin, 2013: 2-5). *Deterrence by denial* dianggap sebagai aspek pertahanan dari strategi pencegahan dan, menurut Goodman, terdiri dari dua elemen mendasar: kesia-siaan dan pencegahan. Sementara yang pertama adalah untuk menunjukkan bahwa agresi tidak akan memiliki "dampak seperti yang diharapkan," dan yang kedua adalah untuk menunjukkan bahwa langkah-langkah berbasis pertahanan akan menyebabkan gangguan kejahatan dunia maya, sehingga menghambatnya dari mencapai tujuannya (Goodman, 2010: 106).

Dari berbagai literatur terkait *deterrence by denial*, beberapa diantaranya membaginya menjadi *deterrence by resistance* dan *deterrence by resilience*. *Deterrence by resistance* pada dasarnya merupakan strategi defensif (Thijssen, 2016: 6), derajat keberhasilan tergantung pada peningkatan pertahanan sebelum adanya serangan (Bendiek, 2015: 560-561). Strategi ini dimaksudkan untuk menyakinkan penyerang siber jika seranganya tidak akan efektif (Thijssen, 201:

6). Meskipun selalu dapat diperbaiki, parameter defensif tidak dapat disempurnakan. Artinya, negara mungkin dapat menyulitkan, dalam hal jumlah waktu dan upaya yang diperlukan, bagi penyerang untuk menyusup ke jaringan, namun ia tidak dapat mencegah penyerang untuk memasuki sistem pada akhirnya (Solomon, 2011: 20). Karena alasan itu, berbagai cendekiawan dan pakar menekankan keharusan untuk beralih dari postur benteng (*fortress*) ke ketahanan *(resilience)* dalam mencegah serangan siber dan perang siber (Bologna, Fasani, & Martellini, 2013: 53). Menurut J. L. Caton, pentingnya beralih ke pendekatan ketahanan terbukti dalam kebijakan *cyber deterrence* Gedung Putih dan Kebijakan NATO terbaru untuk pertahanan siber (Caton, 2013: 155-156). Kedua yaitu deterrence by resilience. Strategi ini menunjukkan ketahanan sistem siber sebuah negara negara; kemampuan dan sistem alternatif, dan pemulihan sistem yang cepat (Tran, Campos-Nanez, Fomin, & Wasek, 2016: 29). Bertolak belakang dengan strategi sebelumnya yang lebih berfokus pada pengembangan perangkat lunak *antivirus*, *firewall*, dan *patch* (Murdrinich, 2012: 181) deterr*ence by resilience* adalah pendekatan holistik yang dapat beradaptasi dengan berbagai jenis serangan siber (Bologna et al., 2013: 53).

b. Deterrence by Punishment or Retaliation

Strategi utama lainya adalah *deterrence by punishment or retaliation*. Metode ini merupakan metode yang ofensif (Goodman, 2010: 106), yang mana menunjukan ancaman, kerugian, serta resiko yang besar apabila negara tersebut diserang. Tujuan utamanya adalah untuk meyakinkan musuh apabila kerugian yang akan diterima melebihi apa yang dapat dicapai dari melakukan serangan siber. Seperti halnya dalam teori *deterrence* klasik, *cyber deterrence* menuntut tindakan hukuman yang bersifat segera, pasti, dan berat. Dengan kata lain, konsekuensi dari tindakan retribusi harus mutlak atau tidak dapat disangkal. Pada akhirnya, tingkat efektivitas mengacu pada seberapa besar serangan balik akan diterima oleh agresor. Untuk dapat mencegah secara efektif, pencegah harus memastikan bahwa pelaku siber diyakinkan apabila segala aksi akan

diidentifikasi, ditangkap, dan kemudian dihukum dengan cepat dan keras. (Taipale, 2010: 18).

Munculnya istilah *cyber deterrence* kemudian memunculkan perdebatan terkait relevansi strategi *deterrence* klasik dalam ranah maya. Di satu sisi, sebagaimana dijelaskan sebelumnya, beberapa ilmuwan berpendapat jika strategi *deterrence* yang selama ini ada masih relevan dan dapat diaplikasikan dalam ranah maya (Rice, Butts, & Shenoi, 2011). Sebagai contoh, studi yang dilaksanakan oleh Militer Amerika Serikat yang tidak memberikan perbedaan signifikan antara strategi *deterrence* yang digunakan di ruang kinetik seperti daratan dan lautan dengan ranah maya (Philbin, 2013:6). Di lain sisi, para peneliti mempertanyakan kembali terkait kemampuan teori *deterrence* klasik dalam menjawab permasalahan siber. Mereka mengidentifikasi beberapa faktor teknologi, politik, dan hukum yang berbeda di ranah siber yang menunjukkan bahwa teori *deterrence* klasik tidak lagi cocok untuk diaplikasikan. Faktor-faktor tersebut termasuk volatilitas teknologi,[10] anonimitas, kebingungan, ambiguitas, sifatnya asimetrisnya, serta batasan hukum dan norma internasional. Ciri khas ranah siber ini kemudian membentuk pola baru dalam mencapai sebuah strategi deterrence yang efektif (Gartzke & Lindsay, 2015: 320; Geers, 2010; Kello, 2013: 33; Lupovici, 2011:49-51). Perbedaan tersebut kemudian dikelompokan menjadi dua oleh Michael Schearer, antara lain:

a. Atribusi, struktur internet, dan anonimitas

Dalam *cyber deterrence* atribusi merupakan hal yang berkaitan dengan kemampuan untuk menentukan identitas dan lokasi pelaku yang melakukan serangan siber atau segala bentuk aktivitas lain di ranah maya (Schearer, 2016). David D. lark dan Susan landau mengatakan apabila atribusi merupakan hal yang mendasar dalam strategi *deterrence* karena pada akhirnya kemampuan untuk menyerang balik akan sangat bergantung pada siapa dan dimana lokasi penyerang suatu negara (Clarke & Knake, 2010). Oleh karenanya, menjadi penting bagi

[10] Sifat internet atau komputer yang dapat dengan mudah berganti dan tidak dapat diprediksi

sebuah negara untuk memperhatikan masalah atribusi agar strategi *cyber deterrence* menjadi lebih efektif.

Berbeda dengan perang tradisional yang mana terlihat jelas siapa lawan kita, atribusi di ranah maya merupakan hal yang cukup sulit untuk dilakukan (Monaco, 2016). Struktur internet membuat serangan siber menjadi *multi-steps* dan *multi-stages* yang mana seolah diciptakan untuk menyulitkan proses atribusi (Clarke & Knake, 2010). Bagaimana struktur serta sistem internet telah menunjukan bagaimana realitas atribusi telah berkembang seiring dengan perkembangan teknologi. Hal ini kemudian menunjukan bagaimana strategi klasik sudah tidak dapat digunakan.

Anonimitas juga menjadi permasalahan baru dalam ranah maya. Dalam berbagai kasus, serangan siber dilakukan dengan menggunakan kriptografi yang sulit dipecahkan sehingga membuat identitas pelaku sulit diungkap (US Department of Defense, 2015). Sulitnya mengungkap identitas penyerang membuat proses komunikasi menjadi tidak berjalan lancar. Dalam hal ini, terdapat dua hal yang dapat dilakukan: komunikasi unilateral yang mana tidak dapat efektif sebagaimana komunikasi langsung; serta menunggu serangan untuk dapat melihat identitas penyerang yang mana tidak sejalan dengan definisi *deterrence* di awal pembahasan.

b. Asimetri, aktor non-negara, dan rendahnya hambatan

Perbedaan lainya adalah pada sifat asimetri dalam ranah siber yang tidak menjadi permasalahan penting dalam *deterrence* klasik. Dalam *deterrence* klasik, kekuatan sebuah dapat dengan jelas dilihat seberapa besar kekuatan militernya, semakin besar kekuatan militer maka semakin besar pula *deterrence* negara tersebut. Namun demikian, dalam ranah maya negara besar tidak dapat serta merta menyimpulkan apabila negara kecil akan memiliki kekuatan siber yang lebih kecil terlebih apabila negara kecil tersebut memiliki sedikit atau tidak memiliki sama sekali asset untuk diserang (Libicki, 2009: 70; Schearer, 2016).

Melihat berbagai perbedaan karakter ranah maya, para pakar kemudian membuat saran yang berkaitan dengan bagaimana cara meningkatkan efektivitas *cyber deterrence* untuk dapat mengatasi berbagai serangan siber maupun perang siber. Beberapa telah mengusulkan aplikasi *cyber deterrence* mulai dari *serial deterrence*, *expanded deterrence*, dan *tailored deterrence*, yang merupakan perluasan dari konsep *deterrence* klasik (Kugler, 2009; Libicki, 2009; Lupovici, 2016; Morgan, 2010). Pertahanan siber yang aktif, mencegah serangan siber dengan menggunakan cara kinetik, dan *cyber deterrence* terhadap jenis senjata cyber tertentu juga sedang dipertimbangkan (Denning, 2001; Graham, 2010; Keen, 2015; Murdrinich, 2012). Bahkan, konfigurasi ulang struktur internet telah ditawarkan sebagai sarana untuk meningkatkan keamanan siber (Murdrinich, 2012). Peneliti lain telah mencari solusi di luar domain teknis ranah maya. Mereka menyarankan pendekatan berbasis norma di bawah strategi *deterrence by denial*, dengan penekanan pada faktor manusia dalam membentuk ide dan identitas di ranah siber, dan konstruksi sosial dari ancaman siber yang dirasakan (Lupovici, 2016; Stevens, 2012).

Dari berbagai penjelasan diatas kemudian disimpulkan apabila logika berpikir strategi *cyber deterrence* pada dekade sebelumnya tampaknya tidak mampu mengatasi ancaman serangan siber dan perang siber yang tidak pasti dan tidak transparan. Para ahli berpendapat bahwa prinsip-prinsip *deterrence* klasik Perang Dingin yang memainkan peran penting dalam pencegahan perang nuklir tidak dapat ditransfer ke ranah maya karena strategi tidak membawa nilai yang sama ketika berbicara pada ranah maya (Iasiello, 2014: 54). RAND Corporation menyatakan, "karena ruang siber adalah media yang sangat berbeda, konsep *deterrence* dan perang mungkin tidak memiliki dasar logis yang dimiliki oleh bidang nuklir dan konvensional." Dari sini, ranah siber harus didekati melalui pendekatan nya sendiri (Libicki, 2009: 5). Akibatnya, para ilmuwan, pakar, dan pejabat pemerintah masih memiliki keraguan signifikan tentang efektivitas *cyber deterrence* dalam menghadapi tantangan perang siber. Teori atau pendekatan apa

yang dapat memberikan kerangka kerja penjelasan yang lebih baik untuk menginformasikan *cyber deterrence* dan memahami efektivitasnya dalam menghadapi ancaman siber atau mencegah perang siber, khususnya antara Amerika Serikat dan Korea Utara, adalah pertanyaan yang tampaknya tetap belum terjawab dalam literatur. Studi ini akan fokus pada memberikan jawaban yang relevan untuk pertanyaan ini dalam konteks cyber war antara Amerika Serikat dan Korea Utara.

1.6. Argumentasi Utama

Strategi *deterrence* digunakan oleh Amerika Serikat di ruang siber terbukti dengan pembangunan infrastruktur siber yang begitu masif, namun dalam pelaksanaanya strategi *deterrence* Amerika Serikat mengalami beberapa keterbatasan khususnya dalam menghadapi serangan siber Korea Utara. Hal tersebut disebabkan oleh perbedaan proses atribusi dimana dulu negara dapat dengan mudah mengetahui siapa lawannya sedangkan di ruang siber proses atribusi bisa memakan waktu berbulan-bulan. Selain itu, keterbatasan juga terjadi karena sulitnya melakukan retaliasi/pembalasan yang seimbang mengingat ketimpangan yang dimiliki antara Amerika Serikat dan Korea Utara.

1.7. Metode Penelitian

Metode penelitian merupakan suatu langkah yang sistematis dalam suatu penelitian. Penggunaan suatu metode dalam suatu penelitian bertujuan untuk menciptakan pola berpikir dari data-data yang ada. Dari segi kaidah penulisan, metode penelitian juga dianggap sebagai hal yang penting terlebih untuk membantu proses penelitian agar penelitian dapat menjadi sistematis, ilmiah dan kronologis.

1.7.1 Teknik Pengumpulan Data

Penelitian ini menggunakan data sekunder *(secondary data)* yang mana data diperoleh dari hasil pengamatan pihak lain bukan melalui pengamatan secara langsung. Hal tersebut berarti penulis tidak melakukan interaksi langsung dengan objek penelitian (Moleong, 1995: 62). Dalam dunia penulisan karya ilmiah, metode seperti ini kerap disebut sebagai studi kepustakaan *(library research)*. Untuk mendapatkan data yang valid, penulis menggunakan data dari:

a. Perpustakan Universitas Jember
b. Ruang baca Fakultas Ilmu Sosial dan Ilmu Politik
c. Portal Jurnal
d. Situs Web Resmi Negara

Sedangkan bentuk sumber-sumber yang akan dijadikan sebagai sumber bagi penulis antara lain:

a. Buku;
b. Media Cetak maupun Elektronik;
c. Jurnal;
d. Berita;
e. Laporan Resmi.

1.7.2 Teknik Analisis Data

Teknik analisis data menjelaskan bagaimana data yang diperoleh kemudian diolah untuk dapat menjawab pertanyaan penelitian (Pertiwi, 2009: 51). Dalam penelitian ini, penulis menggunakan metode eksplanatif kualitatif (Mas'oed, 1990). Penelitian eksplanatif merupakan penelitian yang berusaha mencari alasan terjadinya suatu fenomena termasuk di dalamnya untuk menjelaskan suatu keberhasilan maupun kegagalan. Penelitian kualitatif merupakan sebuah tradisi dalam ilmu sosial yang secara fundamental bergantung pada pengamatan pada manusia dalam kawasanya sendiri dan berhubungan dengan orang-orang tersebut dalam bahasanya dan dalam peristilahan**.** Pada metode ini, peneliti akan mengumpulkan berbagai data yang relevan dan terpercaya yang kemudian

dianalisis dan diinterpretasikan untuk mencari sebuah kesimpulan atas suatu fenomena.

1.8. Sistematika Penulisan

Bab 1 Pendahuluan

Bab pertama dalam tulisan ini merupakan proposal penelitian dimana penulis akan menjelaskan latar belakang, rumusan masalah, ruang lingkup pembahasan, tujuan penelitian, kerangka konseptual, argumentasi utama, metode penelitian serta sistematika penulisan.

Bab 2 Keamanan Siber Amerika Serikat dan Kaitanya dengan Studi Hubungan Internasional

Bab ini akan menjelaskan perkembangan strategi keamanan Amerika Serikat dari masa ke masa. Dalam bab ini pula dijelaskan alasan mengapa kemudian ruang siber menjadi alternatif pilihan untuk melaksanakan sebuah serangan.

Bab 3 Perkembangan Kekuatan Siber Amerika Serikat dan Korea Utara

Bab ini akan memberikan gambaran terkait persaingan Amerika Serikat dan Korea Utara dari masa ke masa serta membandingkan kekuatan siber Amerika Serikat dan Korea utara.

Bab 4 Kerentanan Amerika Serikat di Ruang Siber

Bab ini akan menjelaskan faktor-faktor yang mempengaruhi kerentanan Amerika Serikat terhadap berbagai serangan siber khususnya dari Korea Utara.

Bab 5 Kesimpulan

Bab ini akan menyimpulkan keseluruhan pembahasan yang sebelumnya telah dijelaskan di bab- bab sebelumnya.

BAB II
KEAMANAN SIBER AMERIKA SERIKAT DAN KAITANYA DENGAN STUDI HUBUNGAN INTERNASIONAL

2.1 Era Informasi dan Pergeseran Tren dalam Studi Hubungan Internasional

Era Informasi yang sering disebut pula era digital merupakan periode bersejarah di abad ke-21 yang ditandai oleh pergeseran cepat dari apa yang dihasilkan oleh era industri, ke ekonomi baru yang didasarkan pada teknologi informasi (Torr, 2003:20). Awal Era Informasi dapat dikaitkan dengan William Shockley, Walter Houser Brattain dan John Bardeen, penemu dan insinyur transistor pertama yang menjadi titik balik bagi revolusi teknologi modern. Dengan revolusi digital, seperti halnya Revolusi Industri menandai awal Era Industri (Ohmae, 1995:143). Definisi apa yang disebut digital (atau informasi) terus berubah dari waktu ke waktu seiring dengan ditemukanya teknologi baru, perangkat pengguna, metode interaksi dengan manusia lain.

Dampak dari era informasi terhadap perubahan pada strategi perang telah menjadi perdebatan dalam dua dekade terakhir khususnya di kalangan pembuat kebijakan, lembaga militer maupun aktor non pemerintah lain untuk kemudian menelaah bagaimana dapat cara yang efektif untuk menghadapi apa yang kemudian disebut sebagai perang siber. Tidak seperti senjata pada masa lalu, teknologi yang diperlukan untuk memulai sebuah perang siber tidak terbatas pada seseorang/sekelompok aktor pada suatu sistem. Kemampuan untuk menyerang sebuah sistem yang penting dapat dilakukan baik oleh negara maupun non negara yang mana keduanya sama-sama dapat mengacaukan tatanan masyarakat yang bergantung pada informasi.

Dalam beberapa tahun terakhir dunia telah melihat bukti nyata terjadinya perang siber. Berbagai serangan termasuk serangan siber 2007 di Estonia, serangan 2008 di negara bagian Georgia, virus *Stuxnet* tahun 2009 yang menyerang program nuklir Iran, dan tindakan oleh kelompok peretas "Anonim"

terhadap perusahaan seperti *Visa, Mastercard, Paypal,* dan *Amazon* melalui *Wikileaks*[11]. Setiap serangan menggambarkan potensi kehancuran yang dapat ditimbulkan oleh perang siber. Oleh karena perang siber adalah perang yang tidak konvensional dan asimetris, negara-negara yang lemah dalam kekuatan militer konvensional juga cenderung berinvestasi di dalamnya sebagai cara untuk mengimbangi kekuatan konvensional (Geers, 2011:114). Ke depan pembuat kebijakan akan diminta untuk mengembangkan strategi yang mengatasi masalah keamanan siber. Kesulitan mengembangkan strategi yang efektif akan diperparah oleh banyak masalah termasuk; apa yang memenuhi syarat sebagai perang siber, apakah respon harus sama ketika mendapat dari serangan oleh aktor negara atau non-negara, apakah negara merespon hal yang sama jika elemen-elemen sektor sipilnya diserang daripada sektor publik, dan apakah sikap ofensif atau pertahanan diperlukan?

Sementara banyak hal telah ditulis pada topik tersebut, perlu ada pemeriksaan yang lebih kuat tentang bagaimana kombinasi senjata siber dengan pendekatan strategis tradisional dapat mempengaruhi pilihan strategis terkait dengan perang siber. Apakah pendekatan perang masa lalu cocok dengan konteks perang siber yang terus berkembang atau haruskah generasi baru ahli strategi dikembangkan untuk secara khusus menangani ide-ide perang siber. Meneliti kemungkinan penerapan ide-ide klasik perang untuk perang siber harus mempertimbangkan kemungkinan konsekuensi kebijakan berdasarkan potensi hasil. Sementara bom atau misil mungkin tidak cocok dengan perang dunia maya, dampak dari jenis konflik ini sebenarnya mungkin lebih dahsyat dalam hal mengganggu masyarakat. Dalam konteks keamanan siber, semakin tergantung aktor secara elektronik, semakin rentan pula (Liaropoulos, 2011:4).

[11] Merupakan organisasi nirlaba internasional yang mempublikasikan kebocoran berita oleh media tanpa diketahui siapa pengirimnya. Leigh, D. & Harding, L. 2011. *Wikileaks: Inside Julian Assange's War on Secrecy.* London: Guardian Books. Halaman 16

2.2 Nilai Strategis Ruang Siber dalam Studi Hubungan Internasional

2.2.1 Karakteristik Ruang Siber

Kata siber (inggris: *cyber*) berasal dari kata sibernetika yang makna literalnya adalah melalui penggunaan komputer. Penggunaan istilah ruang siber mencakup gabungan dari semua jaringan komunikasi, basis data, dan sumber informasi ke dalam suatu ruang yang tidak terhingga. Ruang siber dapat juga diartikan sebagai ekosistem jaringan yang virtual dan tidak material serta lingkungan bio-elektronika yang bersifat universal (Cavelty, 2012:155). Beberapa penulis, seperti Matt Murphy dari *the Economist*, menganggap ruang siber sebagai domain kelima peperangan, setelah daratan, udara, laut, dan ruang angkasa (Murphy, 2010). Walaupun mulai banyak diperbincangkan, hingga saat ini belum ada suatu definisi ruang siber yang dapat menjelaskannya secara keseluruhan. Oleh karena tidak adanya definisi yang memadai, sering terjadi kesalahpahaman dalam mendefinisikan ruang siber. Kesalahpahaman yang paling umum adalah membandingkannya dengan World Wide Web, padahal konsep ruang siber jauh lebih kompleks daripada membuka *Internet Explorer* di gawai atau komputer.

Secara fisik, ruang siber terdiri dari komponen perangkat keras yang digunakan dalam membangun jaringan, seperti router, server, dan komputer, dan infrastruktur yang memungkinkan komponen-komponen ini untuk dihubungkan, seperti kabel serat optik, kabel jaringan area lokal (LAN), atau teknologi nirkabel. Komponen perangkat keras ini didefinisikan secara geopolitik dan biasanya tunduk pada yurisdiksi nasional. Meskipun sering tidak dimasukkan dalam definisi ruang siber, dalam konteks keamanan nasional beberapa negara juga akan mempertimbangkan infrastruktur yang memungkinkan seperti sistem telekomunikasi dan jaringan listrik. Komponen perangkat keras ini terhubung dalam jaringan dengan komponen perangkat lunak yang memungkinkan informasi dikirim dan diterima dalam paket sesuai dengan protokol jaringan, seperti Model Referensi ISO/OSI atau model TCP / IP (Kuehl, 2009:9).

Deskripsi fungsional ruang siber hingga saat ini masih diperdebatkan di berbagai negara dan organisasi. Dalam pengertian yang paling mendasar, ruang siber berkaitan dengan informasi dalam atau ditransfer melalui sistem komputer jaringan dan interaksi manusia dengan manusia lain atau informasi melalui jaringan ini. Dari perbedaan definisi tersebut, negara ataupun organisasi memiliki gagasan yang berbeda tentang kegiatan dalam dan yang melalui ruang siber yang harus diatur dan/atau dikendalikan. Beberapa akan menggambarkan dunia maya hanya sebagai lingkungan jaringan, menempatkan penekanan pada infrastruktur dan konektivitas, sementara yang lain akan secara eksplisit memasukkan pentingnya konten informasi yang terdapat di ruang siber dalam definisi mereka, yang kemudian berfungsi untuk mengatur atau mempengaruhi konsep terkait seperti kekayaan intelektual, kebebasan berpendapat, dan privasi (Hathaway & Klimburg, 2012:9). Terlepas dari perbedaan tersebut, untuk tujuan tulisan ini baik konten dan lingkungan dianggap sebagai fitur fungsional penting dari ruang siber.

Beberapa karakteristik utama ruang siber membuatnya berbeda dengan media lain. Pertama, dunia maya memungkinkan pengguna untuk mengirimkan sejumlah besar informasi secara efisien dan cepat. Komunikasi tidak hanya *point-to-point* atau *broadcast* tetapi menggunakan paket *switching*, di mana informasi dipecah menjadi blok-blok kecil berdasarkan alamat tujuan dan kemudian dikirim melalui beberapa jalur. Fitur ini memungkinkan adanya paradigma baru pertukaran informasi. Kedua, pengguna sejauh ini menikmati anonimitas, terbukti dengan jumlahnya yang masif. Banyak sistem jaringan, termasuk Internet, belum dirancang dengan mempertimbangkan keamanan atau identitas. Terlepas dari adanya beberapa fitur identifikasi seperti *IP address* (alamat IP)[12] dan alamat *media access control* (MAC)[13], seringkali sulit untuk

[12] Merupakan serangkaian nomor yang disematkan ke setiap perangkat yang tersambung ke jaringan internet dengan fungsi untuk mengetahui pemilik suatu perangkat atau jaringan. Postel, J. 1981. *Internet Protocol, DARPA Internet Program Protocol Specification*. California: University of Southern California. Halaman 7

[13] Bagian dari jaringan komputer yang berfungsi untuk menyediakan mekanisme penentuan alamat sehingga setiap titik yang tersedia pada sebuah jaringan dapat berkomunikasi. Techopedia. 2019. Media Access Control (MAC).

melacak sumber aktivitas di ruang siber. Juga sulit untuk membangun hubungan antara identitas fisik / hukum seseorang dan personanya di ruang siber. Namun baru-baru ini, berbagai alat dan teknik telah muncul untuk mengelola masalah atribusi dengan lebih baik. Tingkat pentingnya masalah atribusi bervariasi tergantung pada aktor dan jenis aktivitas siber yang dilakukan (House Science and Technology Committee, 2010). Namun, karena tren umum, atribusi masih tetap memakan waktu, mahal, dan seringkali membutuhkan kerja sama antara pihak berwenang di berbagai negara. Ketiga, tidak seperti domain operasional lainnya, ruang siber adalah domain buatan manusia di mana banyak blok bangunan perangkat keras dan perangkat lunak dapat dimodifikasi dan dikonfigurasi ulang. Fakta tersebut berarti bahwa jaringan dan sistem dapat dibangun kembali dan dirancang ulang dengan lebih dari satu cara tergantung pada prioritas dan kebutuhan organisasi, meskipun ketergantungan biaya dan jalur tetap menjadi hambatan.

2.2.2 Operasi Dalam dan Melalui Ruang Siber

Sejarah operasi siber masih sulit dipahami dan tidak jelas, karena operasi siber sendiri sebagian besar masih bersifat diam-diam. Tidak hanya sarana-sarana siber yang digunakan sebagai bagian dari operasi militer yang masih tertutup, bahkan kasus-kasus yang paling terkenal pun belum diangkat secara masif di media. Mengkategorikan perang siber ke dalam *framework* yang ada juga masih sulit, selain karena alasan perang siber yang terbagi ke beberapa garis waktu mulai dari perang formasi (IW) dan peperangan elektronik (EW), potensi ruang siber juga telah digunakan dalam konteks strategis yang sepenuhnya berbeda, termasuk sabotase dan serangan strategis terbatas. Beberapa kejadian yang terjadi dalam beberapa dekade terakhir telah secara konsisten memberikan dampak signifikan terhadap pemahaman tentang perang siber. Kejadian yang dibahas di bawah ini

---

https://www.techopedia.com/definition/25059/media-access-control-mac. [Diakses pada 12 Juli 2019]

umumnya dianggap sebagai kasus penting yang berkontribusi pada konsep perang siber.

Salah satu kerangka kerja yang berguna untuk menjelaskan bagaimana operasi di dalam dan melalui ruang siber telah dilakukan adalah untuk menentukan fitur dari ruang siber apa yang telah ditargetkan dan untuk tujuan militer atau politik apa serangan tersebut dilakukan. Secara umum, operasi siber telah menargetkan sistem komputer itu sendiri, informasi penduduk di dalamnya, atau keduanya. Gangguan atau penghancuran target-target ini telah menjadi tujuan akhir militer atau dijadikan sasaran untuk mendukung cara-cara militer konvensional lainnya untuk mencapai tujuan lain.

Perang siber, yang biasa disebut perang informasi atau perang *net-centric* pada tahun 1990-an, memiliki akar strategis dalam perang informasi. *Operation Desert Storm* menunjukkan keuntungan luar biasa dari sebuah kepemilikan kekuatan militer yang terkoneksi dan memiliki kesadaran situasional waktu (Freedman, 2013:215). Komunikasi digital menghasilkan C4ISR[14] yang unggul, dikombinasikan dengan operasi EW yang luas dan superioritas pasukan udara sejak awal awal, pasukan koalisi dengan mudah menghancurkan pasukan Irak. Kolonel John Warden, perancang strategi selama *Operation Desert Storm*, mengklaim bahwa dengan kurang dari satu persen bom dijatuhkan di Vietnam, tim gabungan berhasil menciptakan kelumpuhan strategis dan operasional di Irak (Rattray, 2001:91). Keberhasilan tim gabungan begitu besar sehingga peperangan yang berbasis internet segera dijuluki sebagai revolusi dalam urusan militer (Freedman, 2013:216). Sebagian besar dari keberhasilan ini adalah karena peran ganda dari *Precision-Guided Munitions* (PGM)[15] yang dipadukan dengan akses ke informasi penargetan yang tepat waktu dan akurat. Informasi dalam perang selalu

[14] C4ISR (Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance) merupakan istilah umum yang berkaitan dengan sistem, tata cara, dan teknik terkait diseminasi informasi. Novel Engineering. What is C4ISR?. http://blog.novel.engineering/what-is-c4isr. [Diakses pada 12 Juli 2019]

[15] Bom gravitasi berpemandu dan rudal jelajah. Acton, J. M. 2017. Cyber Weapons and Precision-Guided Munitions. *Dalam Perkovich, G., & Levite A. E. Understanding Cyber Conflict* (45-60). Washington, DC: Georgetown University Press. Halaman 45.

penting, tetapi setelah *Operation Desert Storm* itu menjadi bagian yang lebih integral dari peperangan modern.

Di antara negara-negara lain yang memulai studi yang lebih mendalam tentang peran ruang siber dalam peperangan, Tentara Pembebasan Rakyat (PLA) Tiongkok secara khusus mencari informasi terkait bagaimana memanfaatkan informasi (Krekel, Adams, & Bakos, 2012:14). Untuk melengkapi strategi tersebut perlu juga untuk melemahkan pemanfaatan ruang siber musuh dalam konflik. *Unrestricted Warfare* (Qiao & Wang, 1999:4), yang ditulis pada tahun 1999 oleh dua perwira PLA, menjelaskan bagaimana negara dapat mengatasi militer yang berteknologi tinggi dan konvensional dengan menggunakan senjata dan taktik di luar aturan konflik tradisional, termasuk perang siber. Jenis-jenis karya ini menunjukkan pentingnya penggunaan strategi siber dalam peperangan modern, dan pada akhirnya kebutuhan untuk mengamankan komando domain ini sebagai tujuan militer menjadi tidak dapat dihindarkan. Konseptualisasi Tiongkok terhadap domain siber, bagaimanapun, sedikit berbeda dari konseptualisasi Amerika Serikat karena kemampuan siber jatuh di bawah konsep yang lebih besar dari "*information operations*" yang meliputi perang elektronik dan operasi psikologis (Chang, 2014:13). Pertahanan dan serangan jaringan tentu saja merupakan bagian dari strategi siber Tiongkok, tetapi informasi yang ada di jaringan dan sistem juga dianggap sebagai elemen penting dari peperangan.

Terdapat pula beberapa kasus masa lalu di mana perang siber telah digabungkan dengan strategi konvensional dalam operasi militer. Contoh yang dapat menggambarkan kasus ini secara komprehensif adalah penggunaan kemampuan siber Rusia selama Perang Rusia-Georgia tahun 2008, yang diintegrasikan dengan kemampuan penyerangan konvensional. Serangan dimulai dengan DDoS dan perusakan situs media dan pemerintah, yang kemudian diperluas ke daftar target yang lebih luas termasuk situs web dari lebih banyak agen pemerintah, institusi keuangan, institusi pendidikan, dan forum peretas Georgia (Bumgarners & Borg, 2009:5). Tujuan dari serangan semacam ini,

terutama selama fase awal konflik, tampaknya untuk mengganggu pengambilan keputusan nasional dan komunikasi yang efektif antara pemerintah dan masyarakat. Gangguan ini disebabkan oleh kemampuan siber, walaupun terbatas dalam kerusakan dan relatif tidak canggih dari sisi metode, namun hal tersebut dapat mendukung pasukan tempur perang utama untuk memiliki kebebasan operasional yang lebih besar dengan mengganggu siklus keputusan lawan (Banner, 2014:108). Hingga saat ini tidak ada parameter yang bisa menjelaskan apakah operasi siber Rusia sebenarnya merupakan bagian integral dari keberhasilan keseluruhan operasi militer.

Operation Orchard adalah kasus yang lebih spesifik di mana strategi siber merupakan bagian integral dari keberhasilan operasi militer. Pada bulan September 2007, Angkatan Udara Israel melakukan serangan udara terhadap reaktor nuklir di Suriah (Follath & Stark, 2009). Dalam operasi ini, beberapa pesawat Israel berhasil terbang ke wilayah udara Suriah tanpa hambatan dalam koordinasi dengan unit pasukan darat khusus (Rid, 2013:42). Kemudian ditemukan bahwa Israel mungkin menembus jaringan pertahanan udara Suriah sebelum penyerangan dan meretas sistem radarnya. Meskipun metode pasti serangan siber tidak diketahui, ada kemungkinan bahwa kombinasi sarana elektronik dan serangan siber digunakan untuk membuat radar Suriah tidak berfungsi. Pelajaran penting dari operasi ini adalah bahwa Suriah tidak menyadari bahwa radar mereka telah diretas, yang memungkinkan pesawat Israel untuk beroperasi di wilayah udara Suriah tanpa hambatan. Seandainya Israel menggunakan cara lain untuk menonaktifkan radar, misalnya, dengan menembakkan rudal atau mengirimkan sinyal gangguan, tentu hal tersebut akan membuat pertahanan Suriah sadar memperingatkan operasi itu. *Operation Orchard* menunjukkan bahwa mengganggu C4ISR musuh, terutama secara diam-diam melalui sarana siber, dapat menjadi bagian integral dari misi militer.

Hal yang sama terjadi pula selama Perang di Afghanistan, Amerika Serikat dapat menggunakan jenis serangan siber yang tidak terdeteksi untuk mendapatkan

keuntungan atas lawan-lawannya, meskipun ada beberapa detail yang dibuka untuk umum. Sebuah pernyataan singkat dari Letnan Jenderal Richard Mills memberikan beberapa wawasan tentang operasi siber di Afghanistan. Pada konferensi tahun 2012, ia menyatakan bahwa timnya dapat masuk ke dalam jaringan musuh, menginfeksi perintah dan kendali musuh, untuk memudahkan jalanya operasinya (Gjelten, 2013). Pernyataan ini menunjukkan bahwa Militer Amerika Serikat secara aktif mendukung dan mengintegrasikan kegiatan tempur langsungnya dengan dukungan dalam bentuk penetrasi dan eksploitasi jaringan, menunjukkan bahwa kemampuan perang siber dapat menjadi sangat penting di medan perang di mana kesadaran situasional adalah kuncinya.

Penemuan operasi yang dijuluki *Olympic Games* menjadi kasus publik pertama yang menggunakan kemampuan siber itu untuk tujuan strategis. Penemuan cacing Stuxnet yang tidak disengaja pada tahun 2010 mengungkapkan sebuah operasi ekstensif yang menargetkan fasilitas pengembangan nuklir Natanz Iran (Sanger, 2012). Di antara banyak fungsinya, Stuxnet mengeksploitasi kerentanan dan secara khusus menargetkan sistem Siemens SCADA yang digunakan di Natanz, menunjukkan perencanaan dan organisasi yang signifikan di belakang operasi ini. Selama bertahun-tahun cacing Stuxnet mengeluarkan perintah palsu ke PLC yang mengendalikan sentrifugal, menyebabkan mereka lepas kendali. Tujuannya bukan untuk menghancurkan semua sentrifugal tetapi untuk diam-diam menyebabkan sebagian dari mereka gagal, untuk kemudian membuat peneliti Iran percaya bahwa kerusakan tersebut adalah kegagalan sistem. Kegunaan operasi ini menjadi perdebatan; beberapa mengklaim bahwa operasi ini telah berdampak signifikan terhadap program nuklir Iran selama beberapa tahun, sementara yang lain mengklaim bahwa dampak strategisnya sangat minimal. Berlawanan dengan kebijakan konvensional, operasi itu tidak murah dan tidak mudah. Ini menunjukkan bahwa operasi siber paling canggih membutuhkan organisasi teknis dan kemampuan intelijen yang memadai. Meskipun demikian,

insiden tersebut adalah kasus pertama di mana senjata siber menyebabkan kehancuran fisik dalam konteks strategis.

Insiden yang dibahas di atas menggambarkan bahwa meskipun sejarahnya relatif singkat, aktor di seluruh dunia telah melakukan upaya sengaja untuk menggunakan ruang siber untuk tujuan politik dan/atau militer. Namun, sebagian besar diskusi berfokus pada cara — analisis malware, vektor serangan, dampak serangan, atribusi teknis. Ada upaya terbatas untuk membahas strategi si pelaku — bagaimana pelaku menggunakan sarana siber untuk mencapai apa yang diinginkannya, dan bagaimana hal ini cocok dengan sasaran strategis pelaku yang lebih besar. Seperti konflik tradisional, pemahaman tentang motivasi di balik insiden ini sangat penting untuk menggambarkan pola, menganalisis bagaimana kemampuan dapat berkembang, dan mencari cara untuk melakukan serangan balik.

2.2.3 Keuntungan Asimetris dan Kemampuan Siber

Seperti yang ditunjukkan oleh kasus-kasus sebelumnya, kemampuan untuk mengganggu atau menghancurkan satu atau lebih elemen yang terdiri dari ruang siber, termasuk informasi, perangkat lunak, dan infrastruktur fisik, telah digunakan secara strategis oleh aktor negara dan non-negara. Meskipun yang kuat dan yang lemah telah memanfaatkan dan menggabungkan kemampuan siber dalam konflik, untuk tujuan tulisan ini, perlu ditelusuri bagaimana kemampuan siber dapat menimbulkan ancaman asimetris, terutama oleh aktor dengan kekuatan militer konvensional yang lebih rendah.

Secara umum, strategi penyerangan memiliki kelebihan atas pertahanan di ruang siber, meskipun ini tidak selalu benar dalam semua kasus. Kerugian utama bagi strategi pertahanan adalah asimetri informasi yang besar. Penyerang memiliki kebebasan besar untuk memilih kapan dan bagaimana mengkompromikan suatu sistem sementara yang diserang dipaksa untuk terus menerus mempertahankan semua sektor dan aset yang mungkin menjadi objek serangan. Hal tersebut membuat strategi pertahanan cenderung mahal dan rumit,

dan biasanya sampai pada titik bahwa tidak semua orang mampu membelinya. Selain itu, keamanan siber masih sering statis, mengandalkan *firewall* dan sistem deteksi intrusi yang gagal menyaring serangan menggunakan malware yang tidak dikenal atau yang mencuri kredensial yang sah. Kurangnya berbagi informasi di antara para pihak yang diserang, meskipun baru-baru ini menjadi lebih baik, memungkinkan penyerang untuk menggunakan kembali alat dan taktik serupa pada target lain. Meskipun serangan yang paling canggih seperti *Stuxnet* membutuhkan waktu, biaya, dan organisasi yang cukup besar, banyak serangan yang tidak mencapai ambang ini relatif murah, mudah, dan dapat diulang.

Kemampuan dunia maya dapat menjadi cara yang efektif untuk menetralisir atau menekan manfaat persenjataan canggih dan senjata gabungan. Karena sistem militer modern sangat bergantung pada komunikasi digital dan penyimpanan data. Gangguan atau penghancuran fungsi-fungsi ini dapat menjadi sangat penting dalam suatu operasi. Misalnya, operasi udara modern sering mengandalkan sistem dan sensor luar jangkauan visual (BVR), dan radar peringatan dini sangat penting untuk pertahanan rudal. Sama seperti kemacetan di EW, untuk kekuatan militer yang lemah akan menjadi sangat diuntungkan untuk mencoba menetralkan fungsi-fungsi ini daripada berinvestasi dalam sistem senjata modern. Misalnya, pelajaran dari *Operation Orchard* memberi tahu bahwa penindasan yang efektif terhadap pertahanan udara musuh dengan cara siber memungkinkan tujuh pesawat udara untuk mencapai target tanpa hambatan. Aplikasi untuk situasi lain, seperti peretasan fungsi radar dalam sistem pertahanan rudal, berpotensi memitigasi kebutuhan untuk menembakkan sejumlah besar rudal untuk menekan satu target.

Kemampuan siber juga telah digunakan sebagai kasus yang terisolasi dalam serangan strategis. Contoh-contoh seperti *Shamoon* dan *Dark Seoul* (Symantec, 2013) telah menunjukkan bahwa mungkin untuk mengganggu suatu organisasi tanpa infiltrasi atau serangan fisik. Insiden seperti *Project Aurora* dan *Stuxnet* telah menunjukkan bahwa dalam beberapa kasus serangan siber dapat

secara fisik menghancurkan target. Hal tersebut menyiratkan bahwa jika kemampuan digunakan dengan cara yang tepat, dapat mencapai target strategis secara langsung. Seperti teori awal tentang pengeboman udara strategis, *malware* dengan fungsi destruktif dapat memungkinkan penyerang untuk melewati apa yang disebut John Warden sebagai "cincin konsentris" (UKEssays, 2018) dan secara langsung mencapai target yang diinginkan tanpa memasang operasi kompleks mulai dari pinggiran. Ini mungkin sangat menarik bagi entitas yang lebih lemah, yang tidak dapat meluncurkan operasi yang sedemikian kompleks. Hal yang paling penting, ruang siber memberikan kekuatan militer yang lebih lemah sarana yang lebih kredibel untuk memaksa lawan yang lebih kuat daripada ancaman kekuatan militer konvensional.

Pembahasan ini menjadi lebih menarik bagi kekuatan militer yang lebih lemah terutama jika aparat militer dan politiknya sendiri tidak mengandalkan jaringan dan kemampuan siber. Jika kerentanan saling menguntungkan dan kedua belah pihak memiliki kemampuan untuk mengeksploitasi mereka, mungkin keduanya akan mencari cara untuk menahan diri. Jika kerentanannya asimetris, di mana satu pihak sangat bergantung pada ruang siber untuk kegiatan militer, ekonomi, dan politik sementara pihak lain nyaris tidak menggunakannya maka pihak yang lebih bergantung akan kehilangan kemampuan pembalasan. Dalam kasus ini, pihak pertama tidak bisa merespon hanya dengan membalas sama dengan yang ia dapatkan, tetapi harus menemukan cara alternatif untuk merespon, yang mungkin atau mungkin tidak layak secara politik.

Ketidakseimbangan ini bahkan lebih parah ketika mempertimbangkan bahwa ada beberapa norma internasional yang diterima tentang tanggapan negara yang tepat atau tindakan balasan terhadap serangan siber, yang menambah kebingungan bagi para pembuat kebijakan. Meskipun teknik atribusi telah menjadi lebih baik baru-baru ini, untuk sebagian besar serangan lanjutan masih sulit untuk menyelidiki asal serangan. Bahkan jika kesuksesan tercapai, sulit untuk mengikat pencetusnya ke negara. Kerjasama penegakan hukum

internasional dalam hal ini lebih baik untuk kejahatan dunia maya untuk kegiatan jahat lainnya yang bersifat sementara dan dipengaruhi secara politis. Hukum internasional saat ini belum mencapai kesepakatan tentang isu-isu mendasar seperti tindakan apa di dunia maya yang membentuk berbagai tingkat perilaku negara yang agresif —yaitu, serangan bersenjata atau penggunaan kekuatan—, apa yang akan menjadi respons yang sah dan proporsional dalam setiap kasus, dan apa yang tugas pasir pihak ketiga adalah. Dalam kondisi ini, pembela HAM akan mengalami kesulitan mengkomunikasikan batasan dan ancaman yang mengindikasikan bahwa tindakan tertentu di dunia maya akan secara konsisten dan tidak dapat disangkal dikembalikan dengan biaya yang sesuai.

2.3 Penggunaan Strategi Berbasis Ancaman Sebagai Strategi Keamanan Amerika Serikat

Strategi berbasis ancaman merupakan salah satu hal yang menjadi pusat dari studi hubungan internasional. Dalam banyak kasus *deterrence* dan *compellence* dianggap sebagai gambaran strategi berbasis ancaman agar lebih dapat dimengerti di level teoritis dan lebih dapat efektif di lever praktis. Usaha tersebut, yang mulai banyak diperbincangkan sejak berakhirnya Perang Dunia II, hingga saat ini masih banyak diperdebatkan. Tidak ada kesepakatan bersama di antara para peneliti maupun pembuat kebijakan tentang efektifitas strategi tersebut atau kondisi dimana strategi tersebut dapat dilaksanakan dengan baik. Amerika Serikat sebagai salah satu negara yang sering menggunakan strategi tersebut telah mengalami baik keberhasilan maupun kegagalan, beberapa contoh penggunaan strategi berbasis ancaman akan kemudian digunakan untuk mencari karakteristik terkait siapa yang dilawan dan seberapa berhasil strategi tersebut.

2.3.1 Nuclear Deterrence Era Perang Dingin

Nuclear deterrence merupakan sebuah contoh dari strategi berbasis ancaman yang dapat dikatakan paling berhasil yang didemonstrasikan oleh Amerika Serikat dan Uni Soviet pada masa Perang Dingin. Pada intinya, *nuclear deterrence*

merupakan strategi yang diarahkan pada negara-negara yang sudah dipersenjatai dengan senjata nuklir dengan tujuan untuk menghalangi penggunaannya (Record, 2004:1). Pada awal 1970-an, teori "*mutually assured destruction*" berlaku dan baik Amerika Serikat maupun Uni Soviet tidak termotivasi untuk menerima resiko dari perang nuklir (Payne & Walton, 2002: 169). Hasil dari *nuclear deterrence* telah menjadi sebuah gambaran keberhasilan, karena tidak ada negara bangsa sejak saat itu yang pernah menggunakan senjata nuklir terhadap target, karena ancaman akan kehancuran, pemulihan, prestise internasional, dan sumber daya alam jauh melebihi manfaat untuk menggunakan senjata nuklir dalam konflik apa pun.

Keberhasilan *nuclear deterrence,* kemudian menjadi sebuah optimisme bagi pakar *deterrence* yang kemudian berusaha menggunakanya di bidang lain termasuk ruang siber. Dalam beberapa literatur ditemukan apabila terdapat beberapa persamaan dan perbedaan antara konflik nuklir dan konflik siber. Persamaan pertama adalah keduanya beroperasi pada tiga level operasi militer yang sama yaitu strategi, operasional dan taktikal yang mana keduanya memiliki potensi membahayakan mulai dari individu hingga masyarakat luas. Kedua, baik konflik nuklir maupun konflik siber sama-sama mampu menciptakan kerusakan yang besar dan membuatnya menjadi ancaman yang serius bagi negara. Ketiga, keduanya dapat dilakukan oleh berbagai macam aktor mulai dari negara, kelompok, hingga individu. Terakhir, keduanya baik secara sengaja maupun tidak dapat menimbulkan dampak diluar dari yang diperkirakan oleh serangan tersebut, pada senjata nuklir, kerusakan reaktor mungkin dapat merusak ekosistem sedangkan pada ruang siber dampak dari sebuah serangan mungkin jauh lebih besar dari apa yang sebelumnya direncanakan (Mulvenon & Rattray, 2004:18).

Disamping beberapa persamaan karakteristik yang muncul dari kedua konflik, terdapat pula beberapa perbedaan yang menonjol antara keduanya. Pertama, dalam banyak kasus serangan siber dilakukan oleh individu maupun kelompok yang membuat negara tidak bertanggung jawab atas kekacauan yang

ditimbulkan, berbeda dengan senjata nuklir yang dalam banyak kasus dilakukan oleh negara. Kedua, berbeda dengan perkembangan senjata nuklir yang dapat dimonitor, perkembangan senjata siber bersifat lebih tertutup dan tidak transparan dan juga tidak ada lembaga yang secara khusus mengawasinya. Terakhir, adalah atribusi di ruang siber yang begitu sulit yang membuat negara sulit untuk mengetahui siapa di balik serangan dan siapa yang harus diwaspadai (Iasiello, 2013: 398). Oleh perbedaan tersebutlah kemudian akan sulit untuk mengaplikasikan strategi yang sama seperti saat Perang Dingin.

2.3.2 Perang Melawan Terorisme

Beberapa penulis percaya bahwa perang melawan terorisme menggunakan strategi berbasis ancaman dapat berhasil pada tingkat tertentu, terutama jika organisasi teroris terasosiasi kepada sebuah negara/bangsa, ketika terdapat aset nyata yang dapat dirusak untuk mempengaruhi kepemimpinan teroris dan membatasi kebijakannya untuk menjaganya (Bar, 2008:12). Penulis yang lain berpendapat bahwa pembunuhan para pemimpin tingkat tinggi dan komandan operasional akan memiliki efek jera sementara, jika hanya untuk memberikan waktu jeda di mana kelompok-kelompok ini harus mengatur kembali diri mereka sendiri (Bar, 2008:14). Di lain sisi ada pula yang menganjurkan *deterrence* untuk mencapai keberhasilan terhadap target teroris, pihak yang terancam harus memahami ancaman (implisit atau eksplisit), dan pengambilan keputusan oleh musuh harus cukup dipengaruhi oleh perhitungan biaya dan manfaat (Trager & Zagorcheva, 2005:87). Penulis lain menyatakan bahwa meskipun teroris pada umumnya tidak dapat ditangkal, beberapa tindakan teroris tertentu mungkin dapat ditangkal bahkan hingga hari ini (Davis & Jenkins, 2002:59). Meskipun demikian, terdapat lebih banyak hambatan daripada keuntungan dalam perang melawan terorisme terutama apabila musuh tidak berada pada satu lokasi yang sama.

Faktor lain yang mempersulit upaya pencegahan adalah motivasi. Sementara kepemimpinan teroris mungkin menghargai kehidupan mereka sendiri, terdapat kelompok-kelompok penuh dengan individu yang bersedia mati untuk suatu

alasan. Ahli keamanan nasional Inggris John Gearson beranggapan apabila konsep tradisional *deterrence* tidak akan bekerja melawan musuh teroris dengan taktik yang diakui bersifat destruktif dan menargetkan orang yang tidak bersalah, hal tersebut diperparah dengan fakta bahwa orang/kelompok yang disebut prajurit yang mengaku bertarung di jalan tuhan dan bersedia untuk mati sebagian besar tidak memiliki kewarganegaraan (Gearson, 2012:171). Jika diperhatikan, bagian pertama dari pernyataan Gearson juga berlaku bagi para pelaku serangan siber. Aktor yang termotivasi oleh suatu sebab, apakah politik, ideologis, atau finansial, sulit sekali untuk dihalangi kecuali jika beberapa tindakan formatif dapat menyebabkan dampak fisik, emosional, atau finansial yang signifikan untuk mengekang keterlibatan dalam aktivitas lebih lanjut di ruang.

Sisi lain yang menantang strategi *deterrence* untuk sukses adalah secara konsisten memengaruhi perilaku teroris. Agar berhasil, ancaman pencegah respons langsung harus dibuat bersyarat pada perilaku musuh; jika individu dan kelompok politik percaya bahwa mereka akan ditargetkan sebagai bagian dari perang melawan teror Amerika Serikat terlepas dari tindakan mereka, mereka memiliki lebih sedikit insentif untuk menunjukkan penolakan (Kroenig & Pavel, 2012:21). Sampai saat ini, belum ada insiden yang diamati secara publik atau bukti di mana perang melawan terorisme dengan penyangkalan atau hukuman yang telah berhasil digunakan untuk mengurangi aktivitas terorisme, atau memengaruhi para aktor yang mengarahkan atau melakukan kegiatan tersebut. Oleh karena persamaanya dengan konflik siber, dapat dikatakan pula apabila memerangi serangan siber dengan strategi serupa akan menjadi sulit.

BAB III
PERKEMBANGAN KEKUATAN SIBER AMERIKA SERIKAT DAN KOREA UTARA

3.1 Hubungan Amerika Serikat dan Korea Utara dari Masa ke Masa

Perilaku mengancam Korea Utara, pengembangan kemampuan senjata nuklir, kimia, dan biologi yang dilarang, dan pengejaran berbagai aktivitas terlarang, telah menjadi salah satu masalah yang terus-menerus muncul dalam kebijakan luar negeri Amerika Serikat khususnya pasca Perang Dingin (Chanlett-Avery, 2018:1). Sejak terbentuknya Korea Utara pada tahun 1948, Amerika Serikat tidak pernah memiliki hubungan diplomatik resmi dengan negara tersebut. Administrasi Amerika Serikat berturut-turut sejak awal 1990-an telah berupaya menggunakan kombinasi negosiasi, bantuan, dan sanksi bilateral maupun internasional untuk mengakhiri program senjata Korea Utara, namun usaha tersebut hingga saat ini belum membatasi kemampuan Korea Utara yang justru semakin meningkat (Kwon, 2016:150).

Kepentingan Amerika Serikat di Korea Utara mencakup masalah keamanan, politik, dan hak asasi manusia. Aliansi militer bilateral dengan Korea Selatan dan Jepang mewajibkan Amerika Serikat untuk mempertahankan sekutu-sekutu ini dari serangan apapun dari Korea Utara. Puluhan ribu tentara Amerika Serikat yang berbasis di Korea Selatan dan Jepang, serta puluhan ribu warga sipil Amerika Serikat yang tinggal di negara-negara itu, berada dalam jangkauan serangan rudal jarak menengah Korea Utara (Sigal, 2003). Kemajuan Korea Utara yang cepat dalam kemampuan nuklirnya dan rudal jarak jauhnya dapat membuat Amerika Serikat berisiko terhadap serangan Korea Utara. Konflik di semenanjung Korea atau runtuhnya pemerintah di Pyongyang akan memiliki implikasi parah bagi ekonomi regional — atau bahkan global. Negosiasi dan diplomasi seputar program senjata nuklir Korea Utara memengaruhi hubungan

Amerika Serikat dengan semua kekuatan utama di kawasan itu, terutama dengan Tiongkok dan Korea Selatan (Park, 2013:4).

Selain masalah geostrategis, Amerika Serikat juga berurusan dengan rezim totaliter yang tidak terikat oleh banyak norma yang mengatur hubungan internasional. Sebuah negara berpenduduk sekitar 25 juta orang, yang didirikan oleh Kim Il-sung ini memiliki filosofi resmi *juche* (kemandirian) yang telah membuatnya menentang pengaruh luar, yang umumnya dilihat oleh rezim sebagai ancaman potensial terhadap pemerintahannya (Lee, 2003:105). Kontrol keluarga Kim telah membantu memungkinkan Korea Utara untuk menentang pengaruh luar, serta untuk masuk ke dalam dan kemudian melanggar perjanjian diplomatik dan komersial, sampai pada tingkat yang mengejutkan bagi negara yang relatif kecil yang dikelilingi oleh tetangga yang lebih kuat secara material. Selama 70 tahun terakhir, Korea Utara telah menciptakan salah satu kekuatan militer terbesar di dunia, yang bertindak sebagai pencegah terhadap intervensi militer luar dan memberikan Pyongyang posisi tawar yang tinggi. Akan tetapi, militerisasi yang terjadi —digabungkan dengan perilaku Korea Utara yang provokatif, sistem pembuatan kebijakan yang buram, dan kesediaan untuk menentang konvensi internasional— juga sangat menghambat pertumbuhan ekonomi Korea Utara dengan minimnya interaksi dengan Korea Utara dunia luar (Reuters, 2018).

Disamping berbagai perselisihan yang terjadi antara Amerika Serikat dan Korea Utara yang telah disebutkan diatas, saat ini kedua negara dapat dikatakan memasuki babak baru. Seiring dengan perkembangan media baru yang dapat dimanfaatkan sebagai arena dari konflik internasional, Korea Utara pun mengikuti perkembangan tersebut. Selain mengembangkan kekuatan nuklir dan rudalnya, Korea Utara juga terus mengembangkan kemampuan sibernya. Saat ini banyak peneliti yang menyatakan apabila kekuatan siber Korea Utara jauh lebih berbahaya dari kekuatan konvensionalnya (Patrick, 2019). Amerika serikat juga memandang Korea Utara sebagai salah satu dari empat negara yang mengancam dalam hal ruang siber. Adanya konflik di ruang siber ini tentunya menuntut

adanya perhatian khusus untuk mengantisipasi kemungkinan terburuk yang dapat terjadi.

Konflik yang terjadi antara Amerika Serikat dan Korea Utara di ruang siber tidak bisa dipandang sebelah mata. Walaupun tidak terjadi kontak fisik antar kedua negara namun kerugian yang dirasakan benar-benar nyata. Pada tahun 2016, Amerika Serikat kehilangan sekitar 109 $ AS dari ruang siber saja (CEA, 2018:2). Kegiatan yang dilakukan sangatlah beragam, mulai dari *denial of service* hingga pembajakan *cryptocurrency*[16]. Besarnya kerugian yang ditimbulkan atas konflik yang terjadi di ruang siber ini kemudian membuat Amerika Serikat khususnya memulai untuk mengidentifikasi bagaimana menangani berbagai serangan di ruang siber tersebut.

3.2 Perkembangan Kekuatan Siber Amerika Serikat

3.2.1 Gambaran Umum Keamanan Siber Amerika Serikat

Sejak beberapa dekade terakhir, Amerika Serikat semakin bergantung pada dunia maya sebagai sarana untuk memfasilitasi arus barang dan jasa global, mendorong dialog politik yang bebas dan terbuka, dan mendukung berbagai layanan penting seperti kontrol listrik, air, dan kegunaan lainnya (Harrinson, 2012; Konana, 2017). Sementara internet telah membawa peluang sosial dan ekonomi yang begitu besar, internet juga telah memperkenalkan tantangan yang sulit bagi keamanan nasional, ekonomi, serta keamanan informasi perusahaan dan pribadi yang sensitif. Di dunia dimana semua terhubung secara global, keamanan siber adalah salah satu masalah keamanan nasional paling serius yang dihadapi Amerika Serikat dan sebagian besar negara di dunia.

Pertumbuhan teknologi berbasis internet di seluruh dunia saat ini berjalan beriringan dengan ancaman terhadapnya. Aktor yang memiliki kemampuan teknis

[16] Aset digital yang diciptakan sebagai media pertukaran seperti halnya uang yang menggunakan bahasa digital yang rumit. Greenberg, A. 2011. Crypto Currency. https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html#59f90a61353e. [Diakses pada 12 Juli 2019]

dapat melakukan penipuan, pencurian, gangguan, manipulasi dan, dalam beberapa kasus, kerusakan pada sistem komputer, jaringan, atau data (Fischer, 2016:2). Penjahat, teroris, dan musuh negara-bangsa dapat mengeksploitasi ketergantungan Amerika Serikat yang meluas pada teknologi yang rentan untuk mengubah, mencuri, atau menghancurkan informasi; mengalihkan atau mencuri uang; mendapatkan keunggulan kompetitif melalui pencurian kekayaan intelektual; mengganggu layanan; dan berpotensi melumpuhkan infrastruktur kritis (Wilson, 2013:11).

Dampak dari ancaman siber sangatlah beragam, sebagian besar di antaranya tidak menimbulkan ancaman yang signifikan terhadap keselamatan pribadi, publik atau terhadap fungsi pemerintah, ekonomi, dan masyarakat. Pada saat yang sama, serangan di ruang siber dan beberapa jenis aktivitas siber lainya dapat dikatakan berbahaya terutama apabila dilakukan oleh negara atau aktor non negara yang ahli di bidang tersebut dan yang menargetkan infrastruktur kritis di Amerika Serikat (Ablon, 2018:4). Ketika dua parameter tersebut dipenuhi maka serangan siber dapat menjadi ancaman signifikan bagi keamanan nasional dan kepentingan ekonomi Amerika Serikat. Ancaman yang berbahaya inilah yang ingin ditangani oleh Pemerintah Amerika Serikat melalui kebijakannya untuk menghalau musuh yang beroperasi di ruang siber.

Pemerintah Amerika Serikat sedang berupaya mengimplementasikan berbagai kebijakan untuk meningkatkan semua instrumen kekuatan nasional untuk melawan aktivitas di ruang siber yang menimbulkan ancaman signifikan bagi dunia, serta untuk mencegah negara dan aktor non-negara yang berusaha untuk menyerang. Upaya tersebut dilakukan dengan tanpa mengganggu keterbukaan dan konektivitas negara yang menjadikan internet sedemikian penting bagi kemajuan ekonomi dan sosial negara (United States, 2018:24). Dalam pelaksanaannya, pemerintah berkomitmen untuk terus memperbaiki kemampuan yang dimiliki saat ini dan mengembangkan kemampuan baru yang akan meningkatkan biaya dan

mengurangi manfaat melakukan aktivitas siber yang berbahaya terhadap Amerika Serikat dan kepentingannya.

3.2.2 Peran Negara dalam Ruang Siber

Sebagai negara yang berlandaskan atas hukum, peran negara menjadi kunci bagi perkembangan sistem keamanan siber di Amerika Serikat. Setiap bagian dari pemerintah bekerja sama guna menciptakan kerangka hukum yang dapat mengatasi permasalahan yang ditimbulkan akibat serangan di ruang siber. Oleh karenanya terdapat berbagai produk hukum yang menjadi landasan bagi strategi keamanan siber Amerika Serikat yang mulai muncul sejak tahun 2002 dan terus mengalami perkembangan hingga saat ini. Beberapa diantaranya sebagai berikut.

a. *Cyber Security Enhancement Act 2002*

Pada tahun 2002, untuk pertama kalinya pemerintahan Amerika Serikat memiliki kerangka hukum yang mengatur tentang keamanan siber negara yang disebut C*yber Security Enhancement Act.* Aturan ini mencoba untuk meningkatkan hukuman pada kejahatan siber yang mana ingin menunjukan keseriusan negara pada kejahatan ini; memperbaiki usaha penegakan hukum melalui koordinasi yang baik; memberikan otoritas dan sumber daya bagi *National Infrastructure Protection Center* untuk menjadi sarana penilaian, peringatan, investigasi, dan respon terhadap serangan bagi infrastruktur penting negara baik dari serangan fisik maupun siber; serta memberikan bantuan teknologi bagi penegak hukum baik di tingkat federal maupun lokal (Department of Defense, 2002:6).

Sebagai peraturan pertama terkait keamanan siber, C*yber Security Enhancement Act* masih melihat keamanan siber sebagaimana keamanan tradisional lainya. Satu-satunya perbedaan yang dilihat adalah medium terjadinya kejahatan atau serangan. Oleh karena anggapan tersebut maka strategi yang digunakan untuk melawan kejahatan siber juga masih sangat tradisional menggunakan instrumen keamanan yang digunakan pada perang dunia maupun

perang dingin. Salah satu strategi yang menjadi basis bagi C*yber Security Enhancement Act* adalah strategi *deterrence* dimana dalam strategi ini *deterrence* di ruang siber diasumsikan memiliki karakteristik yang sama dengan apa yang terjadi di perang dingin.

b. National Strategy for Securing Cyberspace

Pada tahun 2003, Pemerintahan Presiden Bush mengeluarkan upaya sistematis pertama yang mengatur tentang keamanan siber Amerika Serikat yang disebut *National Strategy for Securing Cyberspace.* Dokumen ini mengidentifikasi apabila di era informasi saat itu, ancaman telah berubah termasuk di dalamnya melalui ruang siber. Oleh karenanya pemerintah menekankan pentingnya kerjasama guna menanggulangi kerentanan yang disebabkan oleh serangan siber. Dalam penjelasanya, keamanan siber yang dimaksud dalam dokumen ini meliputi dua hal: pertama, pentingnya logika *deterrence* pada era Perang Dingin untuk menyelesaikan masalah keamanan siber, dan kedua pentingnya mekanisme *bottom-up* guna membentuk kebijakan keamanan siber (United States, 2003:11). Seperti halnya dokumen terkait keamanan siber sebelumnya, dokumen ini beranggapan apabila strategi *nuclear deterrence* dapat diterapkan dalam kasus keamanan siber. Dengan menggunakan logika *cost and benefit* pemerintahan Bush menganggap apabila ancaman akan dapat diminimalisir. Oleh karenanya, saat itu muncul tren pengembangan infrastruktur siber untuk memperkuat pertahanan siber Amerika Serikat.

Di lain sisi, keunikan ancaman siber telah membawa pemerintahan Bush menjadi lebih inklusif dan membuka selebar-lebarnya kesempatan berdialog bagi antara Pemerintah Federal, Pemerintah Negara Bagian, maupun Masyarakat sipil untuk kemudian merumuskan kebijakan terkait keamanan siber (United States, 2003: 37). Keterbukaan terhadap masukan ini secara jelas disampaikan dalam *National Strategy for Securing Cyberspace* dimana dikatakan apabila keamanan siber harus diwujudkan melalui *public-private partnership (PPP).* PPP memungkinkan pihak terkait untuk memberikan masukan kebijakan kepada

pemerintah untuk kemudian ditindaklanjuti. Kerjasama semacam ini dirasa sangat penting mengingat sebagian besar sumber daya siber dikuasai oleh aktor non negara.

c. *The Comprehensive National Cybersecurity Initiative*

Pada akhir masa kepemimpinanya, tepatnya tahun 2008, President Bush meluncurkan *The Comprehensive National Cybersecurity Initiative. S*ebagai respon terhadap kekurangan dari beberapa dokumen sebelumnya, dokumen ini kemudian menawarkan beberapa fokus baru dalam proses keamanan siber (Arcaspicio, 2009). Pertama, menciptakan garis depan pertahanan untuk melawan serangan tiba-tiba dengan membentuk atau memperkuat kesadaran situasional terkait kerentanan dan ancaman yang mungkin terjadi di ruang siber oleh pemerintah federal. Kedua, melindungi keseluruhan jenis ancaman siber dengan meningkatkan kemampuan intelijen Amerika Serikat dan meningkatkan keamanan dalam sektor informasi. Ketiga, menguatkan lingkungan keamanan siber masa depan dengan meningkatkan kualitas maupun kuantitas pendidikan serta pengembangan penelitian terkait keamanan siber (United States, 2008:2).

Dalam proses pembuatan *The Comprehensive National Cybersecurity Initiative,* segera disadari apabila tujuan daripada dokumen ini tidak akan tercapai apabila tidak disertai dengan upaya penguatan sektor-sektor strategis dalam pemerintahan. Oleh karenanya, dokumen ini kemudian memasukan aspek pendanaan dalam penegakan hukum federal untuk meningkatkan kualitas investigasi kasus kejahatan, pengumpulan intelijen, serta hal-hal lain terkait dengan keamanan siber. Disamping itu, strategi ini juga memberikan perhatian kepada privasi dan hak-hak sipil.

d. *Cyber Policy Review*

Di bawah pemerintahan Presiden Obama, Amerika Serikat melakukan review terkait strategi, kebijakan, standar, dan hal lain yang terkait dengan keamanan siber. Dalam proses pengerjaanya, *cyber policy review* mempertemukan pemerintah dengan berbagai pihak seperti pemilik industri,

akademisi, masyarakat sipil, mitra internasional, serta pihak lain yang terkait untuk melihat bagaimana selama ini masalah keamanan siber coba diselesaikan. Dalam dokumen ini dapat ditemukan beberapa informasi penting terkait keamanan siber seperti halnya beberapa kekurangan dari kebijakan yang ada serta rencana aksi jangka pendek.

Menyadari tantangan dan peluangnya, presiden kemudian mengidentifikasi keamanan siber sebagai salah satu prioritas utama dalam masa kepemimpinanya. Dalam review ini, terdapat dua rekomendasi utama yang berusaha dikembangankan oleh pemerintah (United States, 2009:17). Pertama, pentingnya kerjasama dari berbagai pemangku kepentingan baik dari dalam maupun pemerintah federal. Ancaman siber yang begitu luas membuatnya sulit untuk dilacak dan diidentifikasi, dalam kasus ini melibatkan banyak orang tidak pernah menjadi keputusan yang salah. Kedua, pemerintah menyadari pentingnya pengembangan infrastruktur teknologi informasi.

e. Strategi Internasional untuk Dunia Maya

Pada bulan Mei 2011 Gedung Putih mengeluarkan *"International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World."* Strategi ini dimaksudkan untuk memberikan peta jalan bagi departemen dan lembaga AS untuk menentukan dan mengkoordinasikan peran dalam kebijakan ruang siber internasional, mengidentifikasi cara-cara yang hendak dilakukan ke depan, dan merencanakan implementasi akhir dari sebuah kebijakan. Di level nasional dokumen tersebut menyerukan kepada masyarakat sipil dan sektor swasta untuk memperkuat sektor siber melalui kemitraan, kesadaran, dan tindakan dan di level global mengundang negara lain untuk bergabung (Seger, 2012:25). Fokus dari strategi ini adalah pada masa depan ruang siber, membangun kebijakan ruang siber, dan mengidentifikasi prioritas kebijakan. Dokumen tersebut menegaskan bahwa Amerika Serikat berkomitmen untuk melestarikan dan meningkatkan manfaat jaringan digital dan akan mengejar kebijakan ruang siber internasional

yang memberdayakan inovasi yang menggerakkan AS dan ekonomi global. Amerika Serikat akan menghadapi tantangan tak terhindarkan yang ditimbulkan oleh pertumbuhan jaringan digital sambil menjaga kebebasan mendasar, privasi, dan arus informasi yang bebas.

International Strategy for Cyberspace menyatakan bahwa Amerika Serikat akan membangun dan mempertahankan lingkungan dimana norma perilaku memandu tindakan negara, mempertahankan kemitraan, dan mendukung aturan hukum di ruang siber. Beberapa prinsip mendasar termasuk: menjunjung tinggi kebebasan mendasar, menghormati hak kepemilikan, menghargai privasi, perlindungan terhadap kejahatan, dan hak beladiri (United States, 2011:8). Selain itu, norma-norma yang muncul dapat mencakup: interoperabilitas global, stabilitas jaringan, akses yang dapat dipertanggungjawabkan, tata kelola multi-*stakeholder*, dan uji tuntas keamanan ruang siber. Diplomasi, pertahanan, dan pengembangan akan dimasukkan ke dalam peran AS di masa depan di ruang siber. Amerika Serikat akan berusaha untuk memasukkan sebanyak mungkin pemangku kepentingan, akan mempertahankan jaringannya, dan akan mendorong aktor-aktor yang baik sambil mencegah dan menghalangi para aktor yang menggunakan ruang siber untuk mengancam perdamaian dan stabilitas. Amerika Serikat akan bekerja secara bilateral dan multilateral untuk memfasilitasi pengembangan kapasitas siber di luar negeri dan akan membantu negara-negara lain dalam pengembangan kemampuan keamanan siber yang relevan dengan tingkat perkembangan teknologi mereka (Nakashima, 2011).

Dokumen ini mengidentifikasi tujuh bidang prioritas (United States, 2011:17) kebijakan yang berbeda yang membentuk kerangka kerja strategis antara lain: 1) Ekonomi - mempromosikan standar internasional dan pasar terbuka yang inovatif; 2) Perlindungan jaringan - meningkatkan keamanan, keandalan, dan ketahanan; 3) Penegakan hukum - memperluas kolaborasi dan penegakan hukum; 4) Militer - mempersiapkan tantangan keamanan abad ke-21; 5) Tata kelola Internet - mempromosikan struktur yang efektif dan inklusif; 6) Pembangunan

internasional - membangun kapasitas, keamanan, dan kemakmuran; dan 7) Kebebasan Internet - mendukung kebebasan mendasar dan privasi.

f. *Executive Order* 13636: Meningkatkan Infrastruktur Kritis Keamanan Cyber

Executive Order 13636, Meningkatkan Cybersecurity Infrastruktur Kritis (EO 13636), yang dikeluarkan pada bulan Maret 2013, berupaya untuk meningkatkan keamanan dan ketahanan infrastruktur kritis melalui upaya sukarela yang melibatkan lembaga federal serta pemilik dan operator infrastruktur kritis milik pribadi (Fischer, 2014:6). Perintah eksekutif ini menggunakan otoritas hukum dan konstitusi untuk memperluas proses berbagi informasi dan kolaborasi antara pemerintah dan sektor swasta, mengembangkan kerangka kerja sukarela dalam keamanan siber dan praktik terbaik untuk melindungi infrastruktur kritis, membangun proses konsultasi untuk meningkatkan keamanan siber infrastruktur kritis, mengidentifikasi infrastruktur kritis prioritas tinggi untuk perlindungan, membuat program insentif untuk adopsi kerangka kerja secara sukarela, meninjau persyaratan peraturan keamanan, dan memasukkan perlindungan privasi dan kebebasan sipil.

Sebuah pertanyaan penting mengenai berbagi informasi adalah bagaimana menyeimbangkan persyaratan untuk peningkatan keamanan siber dengan keharusan lain seperti perlindungan privasi, hak-hak sipil, dan kepentingan bisnis dan ekonomi yang sah. Beberapa sektor infrastruktur kritis sudah masuk dalam peraturan keamanan siber federal, tetapi perlindungan sektor lain masih tergantung pada upaya regulasi sendiri. Keberadaan perintah eksekutif ini dalam pelaksanaanya menimbulkan debat. Beberapa berpendapat bahwa peraturan sukarela yang selama ini dilaksanakan tidak memberikan perlindungan yang memadai; sedangkan sebagian lainnya berpendapat bahwa menerapkan persyaratan federal tambahan akan mahal dan tidak efektif. Perintah Eksekutif ini tidak mengesahkan peraturan infrastruktur kritis federal selain dari apa yang sudah ada di undang-undang, tetapi mengharuskan *National Institutes of Standards and Technology* (NIST) untuk memimpin pengembangan Kerangka

Keamanan Siber, Sekretaris Keamanan Dalam Negeri untuk membentuk tujuan kerja bagi keamanan siber, badan-badan khusus sektor untuk mengkoordinasikan peninjauan kerangka kerja, mengembangkan panduan khusus, dan melaporkan setiap tahun tentang partisipasi oleh sektor infrastruktur kritis (Department of Homeland Security, 2019).

Beberapa pengamat keamanan melihat perintah eksekutif ini sebagai langkah yang diperlukan dalam upaya untuk mengamankan aset penting terhadap ancaman keamanan, namun demikian terdapat pula beberapa kritik(Congressional Research Service, 2014:16). Beberapa kritikus berpikir bahwa proses untuk mengembangkan kerangka kerja terlalu terburu-buru, yang lain berpikir itu terlalu lambat. Beberapa khawatir bahwa kerangka kerja berisiko menjadi bentuk regulasi faktor, yang lain khawatir bahwa kerangka kerja itu tidak dapat diberlakukan karena sifatnya yang sukarela.

g. National Cyber Security Strategy

Kesejahteraan dan keamanan Amerika bergantung pada bagaimana pemerintah merespon peluang dan tantangan yang menjadi dampak dari era informasi. Infrastruktur kritis, pertahanan nasional, dan kegiatan sehari-hari masyarakat Amerika Serikat selalu berkaitan dengan teknologi yang berbasis internet dan terhubung secara global. Oleh karena segala bidang semakin bergantung pada internet, maka pemerintah menyadari apabila terdapat kerentanan baru yang muncul. *National Cyber Security Strategy* ini kemudian menjadi kerangka kerja untuk pemerintah untuk kemudian dapat memanfaatkan ruang siber sebaik-baiknya dan juga untuk meminimalisir kemungkinan terjadinya kejahatan.

Dengan diluncurkanya strategi ini, pemerintah Amerika Serikat meng-klaim apabila untuk pertama kalinya setelah 15 tahun terdapat sebuah strategi siber yang terartikulasi secara jelas (United States, 2018:1). Strategi ini menjelaskan bagaimana pemerintah akan melindungi negara melalui proteksi jaringan, sistem, fungsi, dan data. Mempromosikan kesejahteraan masyarakat

dengan memelihara keamanan, mengembangkan ekonomi digital dan inovasi domestik yang kuat. Menciptakan perdamaian dan keamanan dengan menguatkan kemampuan negara untuk mencegah dan jika perlu menghukum pihak yang menggunakan ruang siber untuk tujuan kejahatan. Serta mengembangkan pengaruh Amerika Serikat dalam mewujudkan internet yang lebih terbuka dan terpercaya.

Pada strategi ini, terdapat satu bagian yang menjelaskan strategi *cyber deterrence.* Dijelaskan apabila sejalan dengan proses identifikasi terkait hal yang dapat disebut sebagai kejahatan di ruang siber, pemerintah Amerika Serikat juga terus memastikan adanya konsekuensi apabila terdapat pihak yang melakukan tindakan yang tidak bertanggung jawab yang membahayakan. Dengan kata lain, Amerika Serikat mencoba untuk membentuk strategi *deterrence* melalui kekuatanya (Lohrmann, 2018). Segala instrumen pemerintah memiliki tugas untuk mencegah dan merespon segala bentuk aktivitas yang membahayakan. Aktivitas tersebut termasuk aktivitas diplomatik, informasi, militer (baik kinetik maupun siber), finansial, hukum dan lainya. Namun demikian, strategi dalam dokumen ini tidaklah diuraikan secara detail yang membuat langkah-langkah kedepan tidak dapat diketahui. Bahkan, *cyber deterrence* tidak menjadi aksi prioritas dalam strategi ini.

3.2.3 Strategi Siber Amerika Serikat

Sebuah artikel pada *Air & Space Power Journal* yang berjudul *"Policy for US Cybersecurity"* memberikan gambaran umum terkait otoritas, peran, dan tanggung jawab agen-agen Amerika Serikat yang bertanggung jawab atas keamanan siber dan merekomendasikan modifikasi yang dapat meningkatkan keamanan siber dan melindungi kepentingan keamanan nasional AS (Roesener, Bottolfson, & Fernandez, 2014:39). Atas dasar kemudahan, rendahnya biaya, dan dimungkinkanya anonimitas operasi siber kemudian menjadi masif dan sama berbahayanya dengan serangan dalam domain fisik. Artikel tersebut juga menyatakan bahwa —karena keterkaitan domain siber,— serangan siber yang

sukses di Amerika Serikat dapat mempengaruhi semua aspek masyarakatnya. Potensi serius untuk dampak negatif yang signifikan terhadap kepentingan nasional Amerika Serikat memaksa pemerintah untuk menginisiasi persiapan dan perlindungan pemerintah dalam domain virtual yang setara dengan yang ada di domain fisik (Department of Defense, 2011:4).

Beberapa agen Amerika Serikat ditugaskan dengan tanggung jawab atas keamanan siber. Departemen Keamanan Dalam Negeri (DHS) adalah agen utama untuk perlindungan infrastruktur penting, baik yang berwujud maupun tidak. Sekretaris Keamanan Dalam Negeri bertanggung jawab atas manajemen krisis dan koordinasi respon terhadap kejadian di ruang siber yang signifikan (Fischer, 2014:2). Departemen Kehakiman (DOJ) bertanggung jawab untuk memitigasi ancaman teroris domestik, menyelidiki insiden, dan menuntut serangan teroris, sabotase, serangan infrastruktur kritis yang sebenarnya maupun yang bersifat percobaan. Biro Investigasi Federal (FBI) mengoperasikan Gugus Tugas Gabungan Investigasi Ruang Siber Nasional. Institut Nasional untuk Standar dan Teknologi (NIST), sebuah lembaga non-regulasi di bawah yurisdiksi Departemen Perdagangan (DOC), menetapkan standar untuk keamanan infrastruktur kritis tetapi tidak memiliki wewenang untuk memaksakan atau menegakkan standar dunia maya di sektor swasta. Departemen Pertahanan (DOD) bertanggung jawab atas keamanan infrastruktur kritisnya sendiri dan ketika diberi wewenang oleh presiden atau Kongres, melakukan kegiatan di ruang siber untuk membela Amerika Serikat dan kepentingan nasionalnya. Dalam DOD, Komando Strategis AS (USSTRATCOM) bertanggung jawab atas operasi siber, *US Cyber Command* (USCYBERCOM) bertanggung jawab atas sebagian besar kemampuan dunia maya, dan *US Northern Command* (USNORTHCOM) bertanggung jawab atas perencanaan, pengorganisasian, dan pelaksanaan misi pertahanan negara (Department of Homeland Security, 2016:6).

3.3 Perkembangan Kekuatan Siber Korea Utara

3.3.1 Gambaran Umum Ruang Siber Korea Utara

Terisolasinya Korea Utara dari komunitas internasional dalam waktu yang lama telah berdampak pada minimnya diskusi tentang negara tersebut termasuk dalam hal kemampuan sibernya. Walaupun Korea Utara termasuk kedalam negara yang paling tidak terhubung dalam jaringan internet global (Jose, 2014) dan ditambah dengan fakta apabila perkembangan teknologinya juga masih tertinggal, sebuah penelitian justru menunjukan apabila negara tersebut telah mengembangkan basis teknologi yang memungkinkan Korea Utara melakukan operasi disruptif di ruang siber (Choi, 2010). Basis teknis semacam ini menunjukan apabila terdapat upaya sistematis guna menciptakan ahli dibidang teknologi dan informasi. Tren semacam ini diperkirakan akan terus berkembang dan menerima perhatian pemerintah di masa mendatang.

Walaupun Korea Utara mulai investasi terhadap industri teknologi informasi pada awal tahun 1980an, upaya aktif Korea Utara baru dapat dilihat pada akhir tahun 1990an. Tahun 1999, yang kemudian disebut sebagai tahun ilmu pengetahuan di Korea Utara merupakan tahun saat pemerintah membentuk institusi pendidikan yang bergerak di bidang ilmu komputer dan kemudian mendeklarasikan teknologi sebagai salah satu pilar guna mencapai apa yang mereka sebut sebagai negara yang kuat dan berdaulat. Sejak saat itu, pemerintah mengeluarkan empat rencana jangka pendek untuk pengembangan teknologi khususnya di bidang ilmu komputer (ROK Ministry of Unification, 2015).

Korea Utara secara sistematis telah mengembangankan kemampuan teknologi informasinya terutama dalam pengembangan perangkat lunak. Universitas Kim Il-sung, Universitas Kim Chaek, Universitas Sains Pyongsung, Universitas Teknologi Komputer Pyongyang, dan sekolah yang berbasis teknologi bekerja bersama untuk melakukan pelatihan bagi siswanya dalam mengembangkan teknologi perangkat lunak (Kang, 2018). Salah Satu pencapaian Korea Utara dalam teknologi perangkat lunak adalah penemuan teknologi

computer numerical control yang berfungsi untuk menguji satelitnya (Kolawole, 2011). Usaha Korea Utara dalam teknologi informasi telah sampai pada level dimana pemerintah dapat mendapatkan keuntungan dengan mengirimkan tim ke Shenyang untuk berpartisipasi dalam pengembangan program untuk perusahaan Korea Selatan.

Korea Utara telah secara konsisten mempersiapkan baik alat maupun infrastruktur yang dibutuhkan untuk kepentingan meretas. Korea Utara memiliki akses ke dua blok alamat IP. Pertama, terdapat 1024 alamat yang disediakan oleh *Star Joint Venture Co* yang merupakan kerjasama antara *Korea Post and Telecommunication Co* (KPTC) dan *Loxley Pacific,* firma yang bergerak di bidang telekomunikasi di Thailand. Alamat-alamat IP tersebut menjadi pusat bagi banyak situs resmi Korea Utara. Kedua, KPTC saat ini juga menggunakan 256 alamat dari *China Unicom* (Williams, 2011).

3.3.2 Peran Negara dalam Ruang Siber

Berbeda dengan kemampuan perang konvensional, mengukur kemampuan dunia maya suatu negara sangat sulit, mengingat senjata yang digunakan dalam perang dunia maya sulit dipahami dan dalam banyak kasus tidak berwujud. Meskipun mengalami kesulitan, upaya terus dilakukan untuk mengukur kemampuan siber Korea Utara, seperti yang ditunjukkan dalam perkiraan pemerintah Korea Selatan tahun 2015 bahwa pada tahun tersebut terdapat 6.800 peretas yang berasal dari Korea Utara (Oh, 2015). Angka tersebut, jika benar, dapat memberikan pandangan sekilas kepada pengamat Korea Utara tentang seberapa besar kekuatan siber Korea Utara. Kecanggihan organisasi yang melaksanakan operasi siber dan basis teknologi yang menopang kegiatan mereka menjadi indikator yang lebih baik dari prospek jangka panjang terkait kemampuan siber Korea Utara.

Bagian ini berfokus pada organisasi, struktur pendukung dan unit-unit di Korea Utara yang berfokus pada kemampuan siber. Penjelasan dalam bagian ini akan membentuk konteks dasar tentang bagaimana unit siber diorganisasikan dan

rantai komando umum dilaksanakan. Hal ini menjadi sangat penting untuk memprediksi motivasi, tujuan, dan misi berbagai organisasi yang menjalankan bidang siber di Korea Utara.

a. Biro Pengintaian Umum *(Reconnaissance General Bureau/RGB)*

Biro Pengintaian Umum Korea Utara (selanjutnya disebut RGB), merupakan pusat aktivitas siber Korea Utara. Dengan memahami sejarah organisasi, garis keturunan, dan organisasi internal RGB maka kemudian dapat dipahami tendensi Korea Utara dalam menggunakan dan mengkonseptualisasikan kemampuan sibernya (Bermudez Jr, 2010:4). Keterkaitan RGB dengan kegiatan di ruang siber serta kegiatan teroris secara diam-diam dan kegiatan terlarang lainya mengindikasikan bahwa Korea Utara kemungkinan melihat kemampuan siber sebagai media yang kuat untuk strategi nasional. Sekitar 2009 dan 2010, Korea Utara melakukan re-strukturisasi beberapa organ intelijennya, yang mengubah organisasi aset perang siber mereka dan memindahkan sejumlah besar unit yang terkait dengan kegiatan di ruang siber dan spionase di bawah satu atap. Unit-unit yang tersebar antara Partai Pekerja Korea (KWP) dan Kementerian Angkatan Bersenjata Rakyat (MPAF) digabungkan ke dalam RGB, yang juga mencakup sejumlah pasukan khusus dan unit terkait spionase.

RGB adalah kunci dari operasi siber Korea Utara, serta operasi diam-diamnya. RGB adalah organisasi yang relatif baru, dibentuk pada 2009 dari reorganisasi skala besar yang terbentuk dari berbagai unit dan departemen yang ada dalam struktur pemerintah Korea Utara. Unit-unit ini dikaitkan dengan berbagai kegiatan termasuk perang politik, pengumpulan intelijen asing, penculikan, operasi khusus, dan pembunuhan (ROK Ministry of National Defense, 2014:276). Ketika pemerintah AS atau Korea Selatan mengatribusikan operasi siber ke organisasi Korea Utara tertentu, nama yang muncul adalah RGB atau Sub-Unitnya. Sementara RGB bertanggung jawab atas operasi siber Korea Utara, termasuk penelitian, pengumpulan intelijen, dan operasi, Tentara Rakyat Korea (KPA) bertugas mempertahankan kemampuan siber. Organisasi komponen

RGB memiliki sejarah terlibat dalam terorisme, spionase, serta perdagangan senjata terlarang.

Dalam struktur RGB terdapat beberapa departemen/biro yang secara khusus mengurus masalah terkait ruang siber. Biro 121 adalah unit siber paling penting di DPRK. Berbagai misi ruang siber meliputi operasi siber ofensif dan defensif, spionase siber, eksploitasi jaringan, dan kejahatan siber merupakan misi yang dilakukan oleh Biro 121. Sumber berbeda menyebutnya dengan nama yang berbeda, termasuk Unit 121, Biro 121, dan Biro Pengintaian Elektronik. Tidak ada laporan yang mengungkap pemimpin Biro 121, meskipun Kim Yong-chol, direktur RGB, dilaporkan memiliki andil besar dalam mengawasi aktivitas Biro 121, seperti laporan bahwa ia secara pribadi memerintahkan operasi siber ofensif terhadap Sony Pictures (MK News, 2015). Biro 121 juga dilaporkan di media Korea Selatan memiliki nama alternatif, Biro Bimbingan Perang Siber di bawah biro Pengintaian Elektronik. Penggunaan nama alternatif oleh Korea Utara untuk organisasi politik dan militer bukanlah fenomena yang baru. Strategi ini digunakan sebagai bagian dari operasi penyangkalan dan penipuan negara (Lee, 2014).

Selain itu, terdapat pula Lab Riset Teknologi Komputer RGB. Keberadaanya sangatlah dirahasiakan terlihat dari sedikitnya yang telah dilaporkan tentang lab tersebut. Pelaporan publik terakhir tentang unit ini adalah pada tanggal 20 Maret 2013, selama audiensi konfirmasi untuk Nam Jae-joon, yang mana mengidentifikasi unit ini bersama dengan Lab No.110 sebagai unit yang memiliki teknik peretasan yang cukup canggih untuk melakukan serangan destruktif pada lembaga keuangan Korea Selatan (Park, 2013). Tidak diketahui apakah unit ini masih ada, telah digabungkan atau dibubarkan. Disamping minimnya informasi, unit ini layak dijelaskan karena satu artikel berita mengenai operasi Lab Riset Teknologi Komputer menjelaskan apabila lab ini merupakan tempat dimana banyak *ransomware* maupun virus diproduksi. Virus yang terkenal disebut virus JML (Shin, 2012).

Selanjutnya dikenal pula Biro Operasi Pertama. Media dan laporan penelitian Korea Selatan sering mengutip apabila biro ini merupakan unit siber utama di bawah RGB (Yoo, 2012:55). Deskripsi fungsi mereka, setidaknya dalam sumber terbuka, hanyalah sebatas pada spionase siber guna mencari informasi terkait musuh-musuhnya. Saat ini Biro Operasi pertama semakin bergantung pada sarana siber, mengingat risiko rendah dan biaya yang terlibat, dan bahwa beberapa alat dan teknik yang dikembangkan dalam proses dibagi dengan unit RGB lain. Namun tampaknya berlebihan untuk mengkarakterisasi unit ini sebagai unit operasi siber utama setingkat dengan biro 121.

b. Departemen Staf Umum Tentara Rakyat Korea *(General Staff Department)*

Departemen Staf Umum Tentara Rakyat Korea Utara (selanjutnya disebut GSD), seperti kebanyakan staf umum dalam organisasi militer lainnya, bertanggung jawab atas komando operasional serta perencanaan dan manajemen pasukan militer Korea Utara. Ketika MPAF biasanya lebih terkait dengan politik dan administrasi, GSD dikaitkan dengan perencanaan operasional. GSD bertugas untuk melapor langsung ke NDC khusus untuk Kim Jong-un, komandan tertinggi Tentara Rakyat Korea (North Korea Leadership Watch, 2011). Selain pengawasannya yang bersifat konvensional, GSD mengawasi aspek militer umum dari operasi siber Korea Utara serta misi terkait lainnya seperti perang elektronik, perang informasi, dan operasi psikologis. GSD memiliki beberapa organisasi bawahan yang memiliki misi umum yang berbeda di ruang siber. Informasi publik tentang unit siber GSD kurang relatif minim dibandingkan dengan RGB yang membuat informasi terkait peran dan fungsinya menjadi terbatas.

Seperti yang dijelaskan sebelumnya, terdapat beberapa unit yang bekerja di ranah siber. Pertama, dikenal dengan istilah biro operasi. Tugas dari biro ini adalah untuk melaksanakan perencanaan militer, strategi, dan manajemen umum. Dengan demikian, walaupun biro umum tidak terlibat langsung dengan operasi siber, keberadaanya masih dianggap penting dalam perkembangan kemampuan siber Korea Utara dikarenakan biro operasi lah yang pada akhirnya yang berperan

dalam pembuatan kebijakan terkait operasi siber (Gause, 2006:18). Dibawah biro operasional inilah untuk pertama kalinya dilaksanakan latihan militer gabungan yang menitikberatkan pada kekuatan siber (North Korea Intellectuals Solidarity, 2014).

Selanjutnya, dikenal pula Biro Komando. Biro Komando bertugas untuk melakukan operasi jaringan komputer (CNO) dan memiliki tanggung jawab untuk mengembangkan *malware*. Biro tersebut didirikan pada awal 1990-an, melalui analisis Perang Teluk, menyadari pentingnya memiliki kekuatan militer yang terhubung dengan internet dan bahwa elemen-elemen siber dapat menghadirkan kerentanan musuh yang kemudian dapat dieksploitasi. Kim Heung-kwang menjelaskan Biro Komando merupakan unit yang bekerja di bawah Komando Angkatan Darat, Angkatan Laut, dan Angkatan Udara (Kim, 2010). Menurut laporan tahun 2009, Biro Komando memiliki sekitar 50 hingga 60 petugas di Unit 31, yang bertanggung jawab untuk pengembangan *malware*. Unit 32, bertanggung jawab untuk pengembangan perangkat lunak untuk penggunaan militer; dan Unit 56, yang bertanggung jawab untuk mengembangkan perangkat lunak komando dan kontrol militer (North Korea's Internal State ofAffairs, 2009:15). Deskripsi laporan menunjukkan bahwa misi utama unit-unit ini adalah penelitian dan pengembangan, namun secara rutin ditarik untuk misi-misi tertentu.

Berbagai media Korea Selatan serta para ahli seperti Yoo Dong-yul sering mengutip apabila terdapat sebuah unit bernama Biro Sabotase yang diyakini sebagai salah satu unit siber di Korea Utara (Yoo, 2013:65). Unit ini lebih dikenal sebagai unit perang psikologis atau informasi daripada unit sabotase. Misi utama biro ini digambarkan untuk memanfaatkan internet guna menyebarkan propaganda anti-Korea Selatan dan selanjutnya akan melakukan eksploitasi jaringan untuk tujuan propaganda dan informasi yang salah, namun unit ini tidak melakukan serangan jaringan komputer atau berfungsi sebagai unit perang siber operasional. Lebih jauh lagi, biro ini juga berperan aktif dalam melakukan gangguan jaringan bagi musuh-musuhnya (Choi, 2013).

Unit selanjutnya di bawah GSD adalah Biro Komunikasi. Biro Komunikasi bertanggungjawab atas semua administrasi dan operasi mengenai komunikasi dalam KPA, termasuk pemantauan telekomunikasi domestik dan asing dan mengamankan komunikasi KPA (Bermudez, 2001:34). Sedikit informasi baru yang dilaporkan tentang organisasi ini. Menurut Joseph bermudez, biro Komunikasi bekerja erat dengan Departemen Keamanan Negara dan biro Pengintaian yang sekarang direorganisasi (dipindahkan sebagai unit bawahan RGB) dalam sinyal operasi intelijen dan juga bekerja dengan biro Informasi Rahasia, terutama bertanggung jawab untuk enkripsi data. Setidaknya terdapat satu batalion komunikasi, yang terletak di Pyongsong, dilaporkan berada di bawah biro Komunikasi, namun tidak ada informasi lebih lanjut mengenai berapa unit di bawah biro ini atau seberapa besar biro ini (Yoo, 2009).

Unit terakhir dikenal dengan nama Biro Perang Elektornik. Tugas dari biro ini adalah bertanggungjawab dalam melatih seluruh intelejen di bawah KPA (Bermudez, 2001:35). Dilaporkan apabila biro ini terbentuk pada pertengahan tahun 1980an dibawah komando Kim Jong-il dengan tujuan modernisasi militer. Berdasarkan laporan Departemen Pertahanan Korea Selatan, Biro Perang elektronik memiliki satu resimen yang terdiri dari empat batalion yang siap untuk ditempatkan di garda depan(News Can, 2005). Tujuan dari biro ini dipercaya untuk menggangu atau merusak komando militer dan sistem kontrol musuh melalui ruang siber. Biro ini tidak bekerja sendiri, melainkan menjadi pelengkap bagi biro-biro lain. Keberadaan biro ini dapat dilihat dalam beberapa kasus yang terjadi di antara Korea Utara dan Korea Selatan dimana pada tahun 2010 Biro Perang Elektronik melakukan gangguan terhadap sistem radar Korea Selatan yang membuat Korea Selatan menembak ke lokasi yang salah (Shin, 2010).

3.3.3 Strategi Siber Korea Utara

Strategi siber Korea Utara pada dasarnya merupakan kelanjutan dari strategi asimetris yang telah lama dijalankan. Melihat bagaimana lawan utama Korea Utara secara ekonomi maupun politik lebih kuat, maka perlu dilakukan

penyesuaian yang dapat menguntungkan negaranya. Dalam pembahasan ini akan dijelaskan dua strategi utama yang dilakukan Korea Utara di ruang siber guna meningkatkan nilai strategisnya.

a. Strategi Asimetris

Seiring dengan kejelasan bahwa Korea Utara tidak dapat secara konvensional mengalahkan musuh-musuh utamanya (Korea Selatan dan Amerika Serikat), Korea Utara kemudian mulai berinvestasi dalam kemampuan militer asimetris untuk digunakan di luar wilayah militer konvensional (Bechtol Jr., 2012:163). Termasuk dalam strategi ini antara lain: perluasan pasukan khusus, investasi dalam teknologi rudal balistik, pengembangan nuklir, dan yang terbaru kemampuan siber. Kemampuan ini tidak hanya memungkinkan peningkatan posisi tawar Korea Utara terhadap musuh-musuhnya selama masa damai, tetapi juga berfungsi sebagai senjata yang efektif saat masa perang. Selama Semenanjung Korea masih didominasi oleh keunggulan konvensional Korea Selatan dan Amerika Serikat, Korea Utara akan terus termotivasi untuk mendiversifikasi senjata asimetris dan non-konvensional. Korea Utara akan menemukan kemampuan yang sangat berharga yang memberikan kesempatan untuk mempertahankan diri, mengurangi keuntungan, atau dengan kata lain membahayakan musuh tanpa menghadapi pembalasan yang sebanding. Pada dasarnya, kemampuan ini memungkinkan Korea Utara untuk melawan Amerika Serikat dan musuh-musuh lainya tanpa pernah benar-benar melawan mereka.

Kemampuan asimetris yang paling banyak dipublikasikan yang menjadi strategi Korea Utara adalah kemampuan rudal balistik dan senjata nuklir. Meskipun keduanya tidak dapat diklasifikasikan dalam strategi siber, namun dapat memberikan gambaran perihal strategi asimetris Korea Utara dengan cukup baik (Park, 2016). Dengan menginvestasikan sejumlah dana ke dalam beberapa sektor yang sangat efektif dan sangat mengancam yang menargetkan titik lemah lawan atau mengancam untuk meningkatkan biaya perang untuk lawan, Korea Utara memanfaatkan sebaik-baiknya anggaran tersebut. Dengan memilih sektor yang

dapat menggandakan efektivitas kinerjanya sendiri atau secara signifikan mengurangi efektivitas lawan, baik melalui ancaman/pencegahan atau penggunaan aktual, Korea Utara secara teoritis melakukan investasi yang bijak dalam banyak kasus (Fish, 2017).

Sementara senjata nuklir tidak secara khusus berhubungan linear dengan perang siber, namun logika di baliknya dapat dikatakan sama. Kemampuan perang siber dapat digunakan untuk mengganggu dan menghancurkan jaringan informasi musuh, dan banyak militer negara maju sekarang memiliki kebergantung pada jaringan. Meskipun Korea Utara mungkin tidak mendapatkan pengganda kekuatannya sendiri dari kemampuan sibernya, ia mungkin mendapatkan penggandan kekuatan ketika melawan musuh-musuhnya.

Korea Utara saat ini telah menganggap apabila kemampuan siber sama pentingnya dengan program nuklirnya. Kim Jong-un diduga mengatakan apabila perang siber bersama dengan senjata nuklir dan rudal adalah ‘pedang serba guna’ yang menjamin kemampuan militer Korea Utara untuk menyerang tanpa henti (Kim, 2013). Pernyataan penting penting karena dengan ini dapat disimpulkan apabila Korea Utara menganggap kemampuan siber sebagai senjata strategis, sebagai sesuatu yang lebih dari sekadar alat pengintaian pada level taktis. Lebih jauh lagi, kemampuan siber mungkin telah mengambil peran sentral dalam mendukung strategi militer Korea Utara.

b. Serangan Tiba-Tiba

Bagian utama dari upaya Korea Utara untuk mengoptimalkan kemampuan perang sibernya adalah perkembangan alami dari minatnya untuk terlibat dalam perang informasi dan elektronik untuk mengganggu komando dan kontrol dalam operasi militer. Bahkan pada pertengahan 1980-an, konsep yang biasa disebut sebagai "*electronic information warfare*" dikembangkan di berbagai lembaga penelitian dan pendidikan di Korea Utara (Bermudez, 2005:241). Militer Amerika Serikat memiliki kemampuan perang elektronik yang unggul dan ketergantungan yang semakin besar pada teknologi dan jaringan komunikasi elektronik. Korea Utara melihat perlunya beradaptasi untuk mempertahankan

sistem komunikasinya sekaligus mengganggu komunikasi dan jaringan Amerika Serikat dan Korea Selatan. Peperangan elektronik Amerika Serikat dan pengembangan elektronik umum kemungkinan disorot oleh pakar militer Korea Utara ketika kapal-kapal angkatan laut Korea Utara menangkap *Pueblo AS* pada tahun 1968 dan memeriksa teknologi di atas kapal. *Pueblo* digunakan untuk komunikasi dan pengumpulan sinyal sinyal intelijen. Ketika komputer dan jaringan digital menjadi kebutuhan nyata untuk perintah dan kontrol dan logistik yang efisien, mereka menjadi sumber daya yang jelas untuk dikejar.

Secara historis, strategi dan doktrin militer Korea Utara, sejauh apa yang telah dipelajari dalam sumber terbuka, pada awalnya dipahami sebagai kombinasi dari Uni Soviet dan Republik Rakyat Tiongkok. Konsep dan kerangka teoritis USSR untuk seni operasional, mekanisasi berat, dan sejenisnya dicampur dengan konsep perang gerilya RRC dan perang infanteri ringan untuk membentuk landasan doktrin dan pemikiran Korea Utara (Minich, 2005:22). Walaupun Korea Utara tidak memiliki tingkat tentara yang sama besarnya dengan USSR atau potensi Kekuatan Republik Rakyat Tiongkok, unsur-unsur dari doktrin kedua negara sangat berpengaruh karena kedua negara memiliki andil besar dalam melatih tentara Korea Utara. Selain itu, baik Uni Soviet dan RRC memiliki pengalaman bertarung dan mengalahkan lawan yang dipersenjatai dan didanai lebih baik.

Korea Utara belajar dari Perang Korea bahwa perang yang berkepanjangan melawan Amerika Serikat tidaklah menguntungkan dan perlu mengadopsi strategi untuk memenangkan perang yang cepat dan strategis di semenanjung Korea. Perang yang cepat dan strategis dapat dicapai dengan serangan pertama yang mengejutkan yang menyerang dari depan dan belakang secara bersamaan. Strategi ini akan memungkinkan Korea Utara berada dalam kondisi militer dan politik yang menguntungkan sebelum bala bantuan AS dapat tiba, dan mungkin menempatkan Korea Utara dalam posisi yang menguntungkan untuk mendapatkan konsesi lebih lanjut melalui negosiasi. Agar ini berhasil, kecepatan dan perintah

serta kontrol yang akurat adalah hal yang penting, seperti halnya gangguan yang mungkin dicapai dalam logistik dan informasi musuh.

Pelajaran strategis paling penting yang relevan dengan kemampuan siber Korea Utara saat ini, terutama untuk militer tradisional, berasal dari kasus Perang Teluk dan Perang Irak. Operasi-operasi Amerika Serikat kemungkinan telah mengajarkan kepada Korea Utara bahwa Amerika Serikat dapat mengalami kesulitan untuk menggalang pendapat domestik dan internasional (Minich, 2005:76), tetapi juga bahwa pasukan yang sangat maju dan terkoneksi dapat sangat efektif terhadap kekuatan konvensional musuh.

Salah satu cara yang mungkin dilakukan Korea Utara untuk mengembangkan strategi perang siber mungkin merupakan kombinasi dari informasi dan elektronik, dengan strategi jangka panjangnya dalam memerangi perang gaya-*blitzkrieg* di semenanjung Korea. Serangkaian serangan siber pada tahap awal perang dapat menciptakan berbagai efek. Seperti *Operation Orchard*, serangan dapat mengganggu atau menghancurkan radar dan sensor yang diperlukan untuk pertahanan rudal. Seperti Perang Rusia-Georgia 2008, Korea Utara dapat memperkenalkan kekacauan dan menghambat pengambilan keputusan pada tahap awal konflik melalui serangan DDoS. Tujuannya strategi seperti ini adalah untuk memperlambat komando dan kontrol lawan.

Sejarah strategis Korea Utara telah menunjukkan kemampuan yang dapat mengalahkan musuh yang lebih kuat. Bagi Korea Utara, lawan utamanya —Amerika Serikat dan Korea Selatan— memiliki kekuatan modern yang bergantung pada jaringan. Dengan logika yang sama bahwa perang elektronik membuat sebuah negara sangat bergantung pada jaringan, maka sangat penting untuk mengganggu pasukan yang sangat bergantung pada teknologi tersebut melalui ruang siber pula. Dengan demikian, Korea Utara akan memiliki keunggulan yang strategis dibanding musuh-musuhnya.

BAB V
KESIMPULAN

Penemuan dan perkembangan internet telah menciptakan berbagai perubahan, termasuk dalam pola interaksi negara —baik yang bersifat konstruktif maupun destruktif. Perang yang dulu dilaksanakan di darat, laut, udara dan ruang angkasa kini telah berkembang hingga ke ruang siber. Setelah ruang siber dianggap sebagai sebuah domain perang yang strategis, banyak negara yang kemudian memanfaatkan keberadaanya. Peristiwa 9/11, *Operation Desert Storm,* dan *Stuxnet* di Iran menjadi beberapa peristiwa penting yang menjadi gambaran apabila ruang dan kemampuan siber merupakan dua hal yang tidak dapat dipisahkan dalam perang modern.

Salah satu persaingan di ruang siber yang menjadi sorotan saat ini adalah persaingan antara Amerika Serikat dan Korea Utara. Kedua negara pada dasarnya tidak pernah memiliki hubungan yang baik dan ketika ruang siber muncul, persaingan pun menjadi melebar. Amerika Serikat oleh banyak penelitian dianggap sebagai negara yang memiliki sistem keamanan siber yang kuat, dan oleh karenanya Amerika Serikat dapat dikatakan memenuhi parameter untuk *deterrence* yang baik. Menjadi menarik apabila melihat realita yang menunjukan apabila dalam beberapa tahun terakhir Korea Utara mau dan mampu melaksanakan serangan siber ke Amerika Serikat. Beberapa peristiwa penting antara lain: *4th of July Cyber Attacks* tahun 2009, *Sony Cyber Attack* tahun 2014 dan *WannaCry Ransomware* tahun 2017.

Di samping segala upaya yang dilakukan oleh Amerika Serikat, ruang siber rupanya memiliki sifat tersendiri yang dalam kasus ini merugikan Amerika Serikat. Sifat-sifat tersebut antara lain: adanya kontestasi akan banyak konsep di ruang siber, utamanya terkait anonimitas, asimetri dan munculnya *super-empowered individual*; kedua, berbeda dengan serangan konvensional,

serangan di ruang siber memiliki dampak yang beragam yang kemudian membuat sulit untuk mengukur dampak dan retaliasi yang harus dilakukan; ketiga, sifat serangan di ruang siber bersifat tiba-tiba sehingga negara menjadi kesulitan untuk mempersiapkan aksi respon terhadap serangan tersebut. Ketiga faktor tersebut merupakan faktor yang secara spesifik menjelaskan persaingan siber antara Amerika Serikat dan Korea Utara sehingga besar kemungkinan apabila faktor-faktor tersebut tidak relevan apabila digunakan dalam kasus lain.

Daftar Pustaka

Buku

Acton, J. M. 2017. Cyber Weapons and Precision-Guided Munitions. Dalam Perkovich, G., & Levite A. E. *Understanding Cyber Conflict* (45-60). Washington, DC: Georgetown University Press.

Arikunto, S. 1989. *Prosedur Penelitian, Suatu pendekatan Praktek*. Jakarta: PT. Bima Aksara.

Bermudez Jr, Joseph S. E. 2001. *The Armed Forces of North Korea*. London: I. B. Tauris.

Bermudez Jr, Joseph S. E. 2013. SIGINT, EW, and EIW in the Korean People's Army: An Overview of Development and Organization. Dalam Mansourov, A.Y. *Bytes and Bullets: Information Technology Revolution and National Security on the Korean Peninsula* (240-245). Hanolulu: Asia-Pacific Center for Security Studies.

Blank, Stephen. 2001. Can Information Warfare be Deterred?. Dalam Alber, D. S., & Papp, D. D., *Information Age Anthology, Volume III: The Information Age Military* (125-157). Washington, DC: Command and Control Research Program.

Bologna, S., Fasani, A., & Martellini, M. 2013. From fortress to resilience. Dalam *Cyber security: Deterrence and IT protection for critical infrastructures*. New York: Springer.

Bumgarner, J., & Borg, S. 2009. *Overview by US-CCU of the Cyber Campaign Against Georgiain August of 2008*. Washington, DC: U.S. Consequences Unit

Buzan, B. 2000. 'Change and insecurity' reconsidered. Dalam S. Croft & T. Terriff, *Critical reflections on security and change* (1–17). Abingdon: Routledge.

Caton, J. L. 2013. Exploring the prudent limits of automated cyber attack. Dalam *Cyber Conflict*. Tallin: NATO Publications.

Cavelty, Dunn M. 2012. Cyber Security. Dalam Collins, *Contemporary Security Studies*. New York: Oxford University Press.

Chang, Amy. 2014. *Warring State: China's Cybersecurity Strategy*. Washington, DC: Center for New American Security

Clarke, R. A., & Knake, R. K. 2010. *Cyber war: The next threat to national Security and what to do about it*. New York: Harper Collins.

Conway, M. 2008. Media, fear and the hyperreal: The construction of cyberterrorism as the ultimate threat to critical infrastructures. Dalam M. Dunn Cavelty & K. S. Kristensen, *Securing 'the homeland': Critical infrastructure, risk and (in)security* (109–129). Abingdon: Routledge.

Cresswell, J. 2003. *Research Design: Qualitative, Quantitative and Mixed Methods Approaches Second Edition*. London and New Delhi: SAGE Production.

Davis, Paul K., & Jenkins, Brian M. 2002. *Deterrence and Influence in Counterterrorism: A component in the War on al-Qaeda*. Santa Monica: Rand.

Dunn Cavelty, M. 2008. *Cyber-security and Threat Politics: U.S. Efforts to Secure the Information Age*. Abingdon: Routledge.

Eriksson, J., & Giacomello, G. 2007. Introduction: Closing the gap between International Relations theory and studies of digital-age security. Dalam J. Eriksson & G. Giacomello , *International relations and security in the digital age* (1–28). Abingdon: Routledge.

Freedman, Lawrence. 2013. The Revolution in Military Strategy. Dalam *Strategy: A History* (215-236). New York: Oxford University Press.

Gause, Ken E. 2006. *North Korean Civil-Military Trends Military-First Politics to A Point*. Carlisle: Strategic Studies Institute.

Geers, K. 2011. *Sun Tzu and Cyberwar*. Cooperative Cyber Defence Centre of Excellence.

Granger, S., & Kelly, L. 2012. Cybersecurity and Modern Grand Strategy. Dalam Kalathil, S., *Diplomacy development and Security in the Information Age* (99-112). Georgetown University School of Foreign Affairs: Institute for the Study of Diplomacy

Greathouse, Craig B. 2014. Cyber War and Strategic Thought: Do the Classic Theorists Still Matter?. Dalam Kremer, Jan-Frederik, & Muller, Benedikt, *Cyberspace and International Relations* (21-40). New York & London: Springer.

Hathaway, M. E., & Klimburg, A. 2012. 1.2 Cyber Terms and Definition. Dalam Klimburg, A., *National Cyber Security Manual* (8-19). Tallinn: NATO CCD COE Publications.

Iasiello, E. 2013. *Cyber Attack: A Dull Tool to Shape Foreign Policy.* Tallin: NATO CCD COE Publications

Kaplan, F. 2016. *Dark territory: the secret history of cyber war*. New York: Simon & Schuster.

Kello, L. 2017. *The virtual weapon and international order*. New Haven, CT: Yale University Press.

Krekel, B., Adams, P., & Bakos G. 2012. *Occupying the Information High Ground: Chinese Capabilities for Computer Network Operations and Cyber Espionage*. Washington, DC: Northrop Grumman Corp

Kshetri, N. 2014. *The Quest to Cyber Superiority*. Springer.

Kuehl, Daniel T. 2009. Chapter 2: From Cyberspace to Cyberpower: Defining the Problem. Dalam Kramer, F. D., Starr, S. H., & Wentz, L. K., *Cyberpower and National Security* (3-23). Washington, DC: National Defense University.

Kugler, R. L. 2009. Deterrence of cyber attacks. Dalam *Cyberpower and national security* (pp. 309–340). Washington DC: Poyomac Books.

Kugler, R. L. 2012. Deterrence of Cyber Attacks. Dalam Kramer, F.D., Starr, S. H., & Wentz, L. K., *CyberPower and National* (309-340). Lincoln: University of Nebraska Press.

Leigh, D. & Harding, L. 2011. *Wikileaks: Inside Julian Assange's War on Secrecy.* London: Guardian Books.

Lewis, James A. 2018. *Rethinking Cybersecurity: Strategy, Mass Effect and States*. New York: CSIS.

Libicki, M. C. 2009. *Cyberdeterrence and Cyberwar*. Santa Monica: RAND Corporation.

Mas'oed, M. 1990. *Ilmu Hubungan Internasional: Disiplin dan Metodologi*. Jakarta: LP3ES.

Minich, James M. 2005. *The North Korean People's Army: Origin and Current Tactics*. Annapolis: U.S. Naval Institute Press.

Moleong, L. J. 1995. *Metodologi Penelitian Kualitatif*. Bandung: PT Remaja

Rosdakarya.

Morgan, P. M. 1977. *Deterrence : A Conceptual Analysis*. Beverly Hills, CA: SAGE Publications.

Morgan, P. M. 2010. Applicability of traditional deterrence concepts and theory to the cyber realm. Dalam *Proceedings of a workshop on deterring cyberattacks: Informing strategies and developing options for U.S. policy*. Washington DC: The National Academies Press.

Ohmae, Kenichi. 1995. *The End of the Nation State: The Rise of Regional Economies*. New York: The Free Press.

Payne, K.B, & Walton, D. 2002. Deterrence in the Post Cold War World. Dalam Baylis, J., Cohen, E., & Gray, C., *Strategy in the Contemporary World, An Introduction to Strategic Studies.* New York: Oxford University Press

Pertiwi. 2009. *Panduan Penulisan Skripsi*. Yogyakarta: Tugu Publisher.

Postel, J. 1981. *Internet Protocol, DARPA Internet Program Protocol Specification*. California: University of Southern California

Qiao, L., & Wang, X. 1999. *Unrestricted Warfare*. Beijing: PLA Literature and Art Publishing

Rattray, Gregory, J. 2001. *Strategic Warfare in Cyberspace*. Cambridge: MIT Press.

Rid, Thomas. 2013. *Cyber War Will Not Take Place*. London: Oxford University Press

Stevens, T. 2016. *Cyber security and the politics of time*. Cambridge: Cambridge University Press.

Taipale, K. 2010. Cyber-deterrence. Dalam Reich, P. C., & Gelbstein, E., *Law, Policy, and Technology: Cyberterrorism,* Information *Warfare, and Internet Immobilization.* Hershey: IGI Global.

Torr, James D. 2003. *The Information Age*. Michigan: Greenhaven Press.

Valeriano, B. & Mannes, R. C. 2018. International Relations Theory and Cyber Security: Threats Conflicts and Ethics in an Emergent Domain. Dalam Brown, C. & Eckersley, R. *The Oxford Handbook of International Political Theory* (273-289). Oxford: Oxford University Press.

Wilson, C. 2013. Cybersecurity and Cyber Weapons: Is Nonproliferation Possible? Dalam M. Martellini, *Cyber Security, Deterrence, and IT*

Protection for Critical Infrastructures (11-24). New York & London: Springer.

Yoo, Dong-ryul. 2013. *Cyberspace and National Security*. Seoul: Korean Institute of Liberal Democracy.

Jurnal

Adams, James. 2001. Virtual Defense. *Foreign Affairs*, *80*(3): 98-112. DOI: 10.2307/20050154

Aradau, C. 2010. Security that matters: Critical infrastructure and objects of protection. *Security Dialogue*, 41(5): 491–514.

Balzacq, T., & Dunn Cavelty, M. 2016. A theory of actor network for cyber-security. *European Journal of International Security*, 1(2): 176–198.

Bambauer, D. E. 2012. Conundrum. *Minnesota Law Review*, 96(2): 584–674

Barnard-Wills, D., & Ashenden, D. 2012. Securing virtual space: Cyber war, cyber terror, and risk. *Space & Culture*, 15(2): 110–123.

Barnett, Roger W. 1998. Information Operations, Deterrence, and the Use of Force. *Naval War College Review*, *51*(2).

Bechtol Jr., Bruce E. 2012. Maintaining a Rogue Military: North Korea's Military Capabilities and Strategy at the End of the Kim Jong-il Era. *International Journal of Korean Studies*, *16*(1): 160–191.

Betz, D. J., & Stevens, T. 2013. Analogical reasoning and cyber security. *Security Dialogue* 44(2): 147–164.

Bonner III, E. L. 2014. Cyber Power in 21st-century Joint Warfare. *Join Force Quarterly 74*: 102-109.

Deibert, R. J., & Rohozinski, R. 2010. Risking security: Policies and paradoxes of cyberspace security. *International Political Sociology*, 4(1): 15–32.

Denning, P. J., & Frailey, D. J. 2011. Who are we—now? *Communications of the ACM,* 54(6): 25–27.

Dunn Cavelty, M. 2013. From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review* 15(1): 105–122.

Eun, Y. S., & Abmann, J. S. 2016. Cyberwar: Taking Stock of Security and Warfare in the Digital Age. *International Study Perspectives*, *17*(3):

343–360. https://doi.org/10.1111/insp.12073

Gartzke, E., & Lindsay, J. R. 2015. Weaving tangled webs: Offense, defense, and deception in cyberspace. *Security Studies*, *24*(2): 316–348. https://doi.org/10.1080/09636412.2015.1038188

Gearson, J. 2012. Deterring Conventional Terrorism: From Punishment to Denial and Resilience. *Contemporary Security Policy,* 33(1):171-198. https://doi.org/10.1080/13523260.2012.659600

Geers, K. 2010. The challenge of cyber attack deterrence. *Computer Law & Security Review*, *26*(3): 298–303. https://doi.org/10.1016/j.clsr.2010.03.003

Goodman, W. 2010. Cyber deterrence: Tougher in theory than in practice? *Strategic Studies Quarterly*, *4*(3): 102–135.

Hansen, L., & Nissenbaum, H. 2009. Digital disaster, cyber security, and the Copenhagen school. *International Studies Quarterly* 53(4): 1155–1175.

Iasiello, E. 2014. Is cyber deterrence an illusory course of action? *Journal of Strategic Studies*, *7*(1): 54–67. https://doi.org/10.5038/1944-0472.7.1.5

Jasper, S. 2015. Deterring malicious behavior in cyberspace. *Strategic Studies Quarterly 2*, *9*(1): 60–85.

Kaiser, R. 2015. The Birth of Cyberwar. *Political Geography*, *46*: 11–20. https://doi.org/https://doi.org/10.1016/j.polgeo.2014.10.001

Kello, L. 2013. The meaning of the cyber revolution: Perils to theory and statecraft. *International Security*, *38*(2): 7–40. https://doi.org/10.1162/ISEC_a_00138

Kroenig, M., & Pvel, B. 2012. How To Deter Terrorism. *The Washington Quarterly,* 5(2):21-36. https://doi.org/10.1080/0163660X.2012.665339

Kwon, Bo Ram. 2016. The Condition for Sanction Success: A Comparison of the Iranian and North Korea Cases. *The Korean Journal of Defense Analysis*, *28*(1): 139–161. https://doi.org/10.1080/01402390600765900

Lawson, S. 2013. Beyond cyber-doom: Assessing the limits of hypothetical scenarios in the framing of cyber-threats. *Journal of Information Technology & Politics* 10(1): 86–103.

Liaropoulos, A. 2011. Cyber-Security and the Law of War: The Legal and Ethical Aspects of Cyber-Conflict. *GPSC working paper.*

Lee, Grace. 2016. The Political Philosophy of Juche. *Stanford Journal of East Asian Affairs*, *3*(1): 105–112.

Lupovici, A. 2016. The "attribution problem" and the social construction of "violence": Taking cyber deterrence literature a step forward. *International Study Perspectives*, *17*(3): 322–342. https://doi.org/10.1111/insp.12082

Murdrinich, E. M. 2012. Cyber 3.0: The Department of Defense strategy for operating in cyberspace and the attribution problem. *Air Force Law Review*, *68*: 167–206.

Record, J. 2004. Nuclear Deterrence, Preventive War, and Counterproliferation. *Policy Analysis,* 519:1-31

Rice, M., Butts, J., & Shenoi, S. 2011. A signaling framework to deter aggression in cyberspace. *International Journal of Critical Infrastructure Protection*, *4*(2): 57–65. https://doi.org/10.1016/j.ijcip.2011.03.003

Roesener, L. C., Bottolfson, M. C., & Fernandez, C. G. 2014. Policy for US Cybersecurity. *Air & Space Power Journal:* 38-54.

Schearer, M. 2016. The short life and quick death of cyber deterrence (How I learned to stop worrying and love cyber). https://doi.org/10.2139/ssrn.2766017

Solomon, J. 2011. Cyberdeterrence between nation-states: Plausible strategy or a pipe dream? *Strategic Studies Quarterly*, *5*(1): 1–25.

Stevens, T. 2015. Security and surveillance in virtual worlds: Who is watching the warlocks and why? *International Political Sociology*, 9(3): 230–247.

Traeger, R. F., & Zagorcheva D.P. 2002. Deterring Terrorism. *International Security,* 30(3):87-123.

Tran, H., Campos-Nanez, E., Fomin, P., & Wasek, J. 2016. Cyber resilience recovery model to combat zero-day malware attacks. *Computer & Security*: 19–31. https://doi.org/10.1016/j.cose.2016.05.001

Internet

Associated Press. 2015. Sony CEO Breaks down Hack Response, Google Role in 'The Interview' Release. http://www.mercurynews.com/2015/01/09/sony-ceo-breaks-down-hack-response-google-role-in-the-interview-release/. [Diakses pada 17 April 2019]

Arcaspicio. 2009. The Comprehensive National Cybersecurity Initiative. https://www.arcaspicio.com/insights/2009/6/30/the-comprehensive-national-cybersecurity-initiative.html. [Diakses pada 26 April 2019]

Arce, Nicole. 2014. Sony Was Warned of Impending Cyber Attack in Extortion Email, Reveal Leaked Messages from Inboxes of Top Executives. http://www.techtimes.com/articles/21770/20141209/sony-was-warned-of-impending-cybertattack-in-extortion-email-leaked-email-boxes-of-top-executives-reveal.htm. [Diakses pada 17 April 2019]

BBC. 2017. Cyber-attack: Europol Says it was Unprecedented in Scale. https://www.bbc.com/news/world-europe-39907965. [Diakses pada 22 April 2019]

Bing, C., & Lynch, S. 2018. U.S. charges North Korean hacker in Sony, WannaCry cyberattacks. https://www.reuters.com/article/us-cyber-northkorea-sony/u-s-charges-north-korean-hacker-in-sony-wannacry-cyberattacks-idUSKCN1LM20W. [Diakses pada 28 Desember 2018]

Bisson, David. 2015. Sony Hackers Used Phishing Emails to Breach Company Networks. https://www.tripwire.com/state-of-security/latest-security-news/sony-hackers-used-phishing-emails-to-breach-company-networks/. [Diakses pada 17 April 2019]

Brandom, Russel. (2017). Almost All WannaCry Victims Were Running Windows 7. https://nakedsecurity.sophos.com/2017/05/17/wannacry-the-ransomware-worm-that-didnt-arrive-on-a-phishing-hook/. [Diakses pada 22 April 2019]

Brenner, Bill. 2017. WannaCry: The Ransomware Worm that Didn't Arrive on a Phising Hook. https://www.theverge.com/2017/5/19/15665488/wannacry-windows-7-version-xp-patched-victim-statistics. [Diakses pada 22 April 2019]

Busby, M. 2018. North Korean 'hacker'charged over cyber attacks against NHS. https://www.theguardian.com/world/2018/sep/06/us-doj-north-korea-sony-hackers-chares. [Diakses pada 2 Januari 2019]

Castro, D. 2009. Thoughts on 4th of July Cyber Attacks. https://www.innovationfiles.org/thoughts-on-4th-of-july-cyber-attacks/. [Diakses pada 8 Januari 2019]

Choi, Bongsik. 2010. The North Korea Industry 2010. http://nkinfo.unikorea.go.kr/nkp/main/portalMain.do. [Diakses pada 20 Mei 2019]

Choi, In-soo. 2013. Detailed Report on North Korea's Cyber Psychological Warfare. http://article.joins.com/news/article/article.asp?Total_Id=13047219. [Diakses pada 21 Mei 2019]

Clapper, James R. 2015. National Intelligence, North Korea, and the National Cyber Discussion. https://www.dni.gov/index.php/newsroom/speeches-interviews/speeches-interviews-2015/item/1156-remarks-as-delivered-by-dni-james-r-clapper-on-national-intelligence-north-korea-and-the-national-cyber-discussion-at-the-international-conference-on-cyber-security. [Diakses pada 21 April 2019]

Comey, James B. 2015. Sony Was Warned of Impending Cyber Attack in Extortion Email, Reveal Leaked Messages from Inboxes of Top Executives. https://www.fbi.gov/news/speeches/addressing-the-cyber-security-threat. [Diakses pada 21 April 2019]

Cox, Joseph. 2016. NHS Hospitals Are Running Thousands of Computers on Unsupported Windows XP. https://www.vice.com/en_us/article/jpgb3y/nhs-hospitals-are-running-thousands-of-computers-on-unsupported-windows-xp. [Diakses pada 22 April 2019]

Department of Defense. 2010. United States Department of Defense, Joint Publication 1-02: Department of Defense Dictionary of Military and Associated Terms. http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf. [Diakses pada 12 Juni 2019]

Department of Health. 2018. Investigation: WannaCry cyber attack and the NHS. United Kingdom. https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf. [Diakses pada 2 Januari 2019]

Department of Homeland Security. 2019. Einstein. https://www.dhs.gov/cisa/einstein. [Diakses pada 23 April 2019]

Department of Homeland Security. 2019. Fact Sheet: Executive Order (EO) 13636 Improving Critical Infrastructure Cybersecurity and Presidential Policy Directive (PPD) 21 Critical Infrastructure Security and Resilience. https://www.dhs.gov/publication/eo-13636-ppd-21-fact-sheet. [Diakses pada 24 April 2019]

Derian, J. D. 1994. Cyber-Deterrence. http://www.wired.com/wired/archive/2.09/cyber.deter_pr.html. [Diakses pada 12 Februari 2019]

Dillinger, J. 2019. List of Countries by Internet Users. https://www.worldatlas.com/articles/the-20-countries-with-the-most-internet-users.html. [Diakses pada 11 Juli 2019]

Dixit, K. 2010. The Challenges of Asymmetric Warfare. https://idsa.in/idsacomments/TheChallengesofAsymmetricWarfare_kcdixit_090310. [Diakses pada 28 Desember 2018]

Einav, Yohai. 2017. WannaCry: Views from the DNS Frontline. https://blogs.akamai.com/sitr/2017/05/wannacry-views-from-the-dns-frontline.html. [Diakses pada 22 April 2019]

Elkind, Peter. 2015. Inside the Hack of the Century. Part 1: Who Was Manning the Ramparts at Sony Pictures?. http://fortune.com/sony-hack-part-1/. [Diakses pada 17 April 2019]

Elkind, Peter. 2015. Inside the Hack of the Century Part 2: The Storm Builds. http://fortune.com/sony-hack-part-two/. [Diakses pada 17 April 2019]

Essays, UK. 2018. Warden's Five Rings: Overview and Analysis. https://www.ukessays.com/essays/anthropology/wardens-five-rings-theory.php?vref=1. [Diakses pada 11 Februari 2019]

FBI National Press. 2014. Updat on Sony Investigation. https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation. [Diakses pada 20 April 2019]

Fish, Isaac Stone. 2017. Let's Stop Calling North Korea 'Crazy' and Understand Their Motives. https://www.theguardian.com/commentisfree/2017/apr/13/stop-calling-north-korea-crazy-understand-motives. [Diakses pada 22 Mei 2019]

Fleming, Mike, Jr., & Warren, Christina 2015. Hackers Sent Extortion Email to Sony Executives 3 Days Before Attack. http://deadline.com/2014/12/north-korea-thriller-gore-verbinski-steve-carell-canceled-new-regency-1201328532/. [Diakses pada 19 April 2019]

Franceschi-Bicchierai, Lorenzo., & Warren, Christina. 2015. Hackers Sent Extortion Email to Sony Executives 3 Days Before Attack. http://mashable.com/2014/12/08/hackers-emailed-sony-execs/. [Diakses pada 17 April 2019]

Follath, E., & Start, H. 2009. The Story of 'Operation Orchard': How Israel Destroyed Syria's Al Kibar Nuclear Reactor. https://www.spiegel.de/international/world/the-story-of-operation-orchard-how-israel-destroyed-syria-s-al-kibar-nuclear-reactor-a-658663.html. [Diakses pada 12 Februari 2019]

Ge, Linda. 2014. 5 Major Theater Chains Pull 'The Interview' after Sony Hack Threat. https://www.thewrap.com/major-theater-chains-pull-the-interview-after-sony-hack-threat/. [Diakses pada 19 April 2019]

Gjelten, Tom. 2013. Pentagon Goes on the Offensive against Cyberattacks. https://www.npr.org/2013/02/11/171677247/pentagon-goes-on-the-offensive-against-cyber-attacks. [Diakses pada 12 Februari 2019]

Goldman, Russell. 2014. What We Know and Don't Know About the International Cyber Attack. https://www.nytimes.com/2017/05/12/world/europe/international-cyberattack-ransomware.html. [Diakses pada 22 April 2019]

Gorman, Siobhan. 2009. Troubles Plague Cyberspy Defense. https://www.wsj.com/articles/SB124657680388089139. [Diakses pada 23 April 2019]

Greenberg, A. 2011. Crypto Currency. https://www.forbes.com/forbes/2011/0509/technology-psilocybin-bitcoins-gavin-andresen-crypto-currency.html#59f90a61353e. [Diakses pada 12 Juli 2019]

Harrinson, Robert. 2012. Are We Becoming Too Dependent on the Internet?. https://www.austinwilliams.com/blog/are-we-becoming-too-dependent-on-the-internet/. [Diakses pada 28 April 2019]

Hern, A. 2018. North Korea is a bigger cyber-attack threat than Russia, says expert. https://www.theguardian.com/technology/2018/feb/26/north-korea-cyber-attack-threat-russia. [Diakses pada 21 Januari 2019]

Hesseldahl, Arik. 2014. FireEye's Kevin Mandia Talks about the World after the Sony Hack (Full Video). https://www.recode.net/2015/4/30/11562068/fireeyes-kevin-mandia-talks-about-the-world-after-the-sony-hack-full. [Diakses pada 20 April 2019]

Imgur. 2014. I used to work for Sony Pictures. My friend still works there and sent this to me. All of Sony has been hacked. https://imgur.com/qXNgFVz

[Diakses pada 17 April 2019]

International Telecommunication Union (ITU). 2019. ITU-T in Brief. https://www.itu.int/en/ITU-T/about/Pages/default.aspx [Diakses pada 12 Juli 2019]

Jose, Pagliery. 2014. A Peek Into North Korea's Internet. https://money.cnn.com/2014/12/22/technology/security/north-korean-internet/index.html. [Diakses pada 20 Mei 2019]

Kang, Tae-jun. 2018. North Korea's High-Tech Pursuits. https://thediplomat.com/2018/06/north-koreas-high-tech-pursuits/. [Diakses pada 20 Mei 2019]

Kedmey, Dan. 2014. Hackers Reportedly Warn Sony Pictures Not to Release The Interview. http://time.com/3624994/hackers-sony-the-interview-seth-rogen/. [Diakses pada 17 April 2019]

Kim, Heung-kwang. 2010. Responses and Strategies Against North Korea's Cyber Information Warfare. http://www.nkis.kr/board.php?board=nkisb501&page=1&sort=hit&command=body&no=3. [Diakses pada 20 Mei 2019]

Kim, Hyungsoo. 2013. Kim Jong-un Says 'Cyber Warfare is an All-Powerful Tool,' Utilizes it as One of Three Major Means of Warfare. http://nk.joins.com/news/view.asp?aid=12640100. [Diakses pada 22 Mei 2019]

Kim, Hyung-Jin. 2009. Korean, US Websites Hit by Suspected Cyber Attack. https://web.archive.org/web/20090711142028/https://www.google.com/hostednews/ap/article/ALeqM5jvH8X8qojQgzc1R8X_5PceTd1nWQD99A5BQ81. [Diakses pada 23 April 2019]

Kolawole, Emi. 2011. North Korea Quietly Enters the Digital Age. https://www.washingtonpost.com/blogs/innovations/post/north-korea-quietly-enters-the-digital-age/2011/07/25/gIQAN7sAZI_blog.html?utm_term=.1508b847030a. [Diakses pada 20 Mei 2019]

Konana, Prabhudev. 2017. The Economy is Too Dependent on the Internet. https://www.psychologytoday.com/us/blog/the-fundamentals/201711/the-economy-is-too-dependent-the-internet. [Diakses pada 28 April 2019]

Lang, Brent. 2014. Sony Hack 'Unparalleled and Well Planned Crime,' Cyber Security Firm Says. http://variety.com/2014/film/news/sony-hack-unparalleled-cyber-security-fir

m-1201372889/. [Diakses pada 17 April 2019]

Lawler, Richard. 2017. FedEx Estimates Ransomware Attack cost $300 Million. https://www.engadget.com/2017/09/21/fedex-ransomware-notpetya/. [Diakses pada 22 April 2019]

Lee, Young-jong. 2014. Cyber Warfare is KPA's 'Ruthless Sword'. http://www.sisapress.com/news/articleView.html?idxno=140623. [Diakses pada 20 Mei 2019]

Lohrmann, Dan. 2018. New National Cyber Strategy Message: Deterrence Through U.S. Strength. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/new-national-cyber-strategy-message-deterrence-through-us-strength.html. [Diakses pada 2 Mei 2019]

McGee, Marianne K. 2017. WannaCry: What's the Impact on U.S. Healthcare?. https://www.bankinfosecurity.com/wannacry-healthcare-reax-a-9921. [Diakses pada 22 April 2019]

Monaco, L. O. 2016. Administration Efforts on Cybersecurity: The Year in Review and Looking Forward to 2016. https://obamawhitehouse.archives.gov/blog/2016/02/02/administration-efforts-cybersecurity-year-review-and-looking-forward-2016. [Diakses pada 21 Januari 2019]

MK News. 2015. The Head of North Korea's General Reconnaissance Bureau Kim Yong-choi Directly Ordered Sony Hacking. https://www.mk.co.kr/news/politics/view/2015/03/220454/?utm_source=facebook&utm_medium=sns&utm_campaign=share. [Diakses pada 20 Mei 2019]

Mulvenon, J. C., & Rattray, G. J. 2004. Addressing Cyber Instability: Executive Summary. The Atltantic Council http://static1.1.sqspcdn.com/static/f/956646/19193589/1341880349257/CCSA+-+Addressing+Cyber.

Murphy, M. 2010. War in the Fifth Domain. https://www.economist.com/briefing/2010/07/01/war-in-the-fifth-domain [Diakses pada 28 Desember 2018]

Nakashima, Ellen. 2011. Obama Administration's Outlines International Strategy for Cyberspace. https://www.washingtonpost.com/world/obama-administration-outlines-inte

rnational-strategy-for-cyberspace/2011/05/16/AFokL54G_story.html?utm_term=.466b6a607e65. [Diakses pada 28 April 2019]

Nakashima, Ellen. 2017. The NSA Has Linked the WannaCry Computer Worm to North Korea. https://www.washingtonpost.com/world/national-security/the-nsa-has-linked-the-wannacry-computer-worm-to-north-korea/2017/06/14/101395a2-508e-11e7-be25-3a519335381c_story.html?utm_term=.58cca6ac838e. [Diakses pada 22 April 2019]

Newman, Lily H. 2017. The Ransomware Meltdown Experts Warned About is Here. https://www.wired.com/2017/05/ransomware-meltdown-experts-warned/. [Diakses pada 22 April 2019]

News Can. 2005. North Korea's Electronic/Cyber Warfare Capabilities (Questionnaires from the Ministry of National Defense). http://www.newscani.com/news/articleView.html?idxno=3375. [Diakses pada 21 Mei 2019]

North Korea Intellectuals Solidarity. 2014. Kim Jong Un's Instructions From March 8, 2014.http://www.nkis.kr/board.php?board=nkisb201&body_only=y&button_view=n&command=body&no=523 [Diakses pada 20 Mei 2019]

North Korea Leadership Watch. 2011. General Staff Department. https://nkleadershipwatch.wordpress.com/dprk-security-apparatus/general-staff-department/. [Diakses pada 20 Mei 2019]

Novel Engineering. What is C4ISR?. 2018. http://blog.novel.engineering/what-is-c4isr. [Diakses pada 12 Juli 2019]

NTIA. 2018. Initial Estimates Show Digital Economy Accounted for 6.5Percent of GDP in 2016. https://www.ntia.doc.gov/blog/2018/initial-estimates-show-digital-economy-accounted-65-percent-gdp-2016. [Diakses pada 11 Juli 2019]

Obama, Barrack. 2014. Remarks by the President in Year-End Press Conference. https://www.whitehouse.gov/the-press-office/2014/12/19/remarks-president-year-end-press-conference. [Diakses pada 19 April 2019]

Oh, Seok-min. 2015. N. Korea Boosts Cyber Operations Capabilities. https://en.yna.co.kr/view/AEN20150508006900315. [Diakses pada 20 Mei 2019]

Park, Donghui. 2016. North Korea Cyber Attack: A New Asymmetrical Military Strategy. https://jsis.washington.edu/news/north-korea-cyber-attacks-new-asymmetrical-military-strategy/. [Diakses pada 22 Mei 2019]

Park, Soonpyo. 2013. North korea Responsible for Most of 70.000 Cases of Cyberattacks during the Last Five Years. https://www.ytn.co.kr/_ln/0101_201303211024217337?ems=12714. [Diakses pada 20 Mei 2019]

Patrick, Kate. 2019. Cyber Attacks, Not Nukes, May Be North Korea's Most Dangerous Weapon. https://www.insidesources.com/cyber-attacks-not-nukes-may-be-north-koreas-most-dangerous-weapon/. [Diakses pada 28 April 2019]

Philbin, M. J. 2013. Cyber deterrence: An old concept in a new domain. http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA589940. [Diakses pada 28 Desember 2018]

Reuters. 2018. North Korean Economy Sees Sharpest Decline in 20 Years as Sanctions Bite. https://nautilus.org/publications/books/dprkbb/uspolicy/dprk-briefing-book-u-s-interests-and-goals-on-the-korean-peninsula/. [Diakses pada 30 April 2019]

Risk Based Security. 2014. A Breakdown and Analysis of the December, 2014 Sony Hack. https://www.riskbasedsecurity.com/2014/12/a-breakdown-and-analysis-of-the-december-2014-sony-hack/. [Diakses pada 17 April 2019]

Roettgers, Janko. 2017. No, the HBO Hack Wasn't Seven Times Bigger Than the Sony Hack. http://variety.com/2017/digital/news/hbo-hack-no-sony-hack-1202515967/. [Diakses pada 17 April 2019]

ROK Ministry of Defense. 2014. 2014 Defense White Paper. http://www.mnd.go.kr/user/mnd/upload/pblictn/PBLICTNEBOOK_201506120237036840.pdf. [Diakses pada 20 Mei 2019]

ROK Ministry of Unification. 2015. North Korean Encyclopedia: 5-Year Science Technology Development Plan. http://nkinfo.unikorea.go.kr/nkp/term/viewNkKnwldgDicary.do?pageIndex=2&koreanChrctr=&dicaryId=8. [Diakses pada 20 Mei 2019]

Roose, Kevin. 2014. Sony Pictures Hackers Make Their Biggest Threat Yet: 'Remember the 11th of September 2001'.

http://fusion.net/story/34344/sony-pictures-hackers-make-their-biggest-threat-yet-remember-the-11th-of-september-2001/. [Diakses pada 19 April 2019]

San-hun, Choe, & Markoff, John. 2009. Cyberattacks Jam Government and Commercial Web Sites in U.S. and South Korea. https://www.nytimes.com/2009/07/10/technology/10cyber.html?mtrref=en.wikipedia.org&gwh=DD230F7AD9E6B4AFAB4B0418478D04CE&gwt=pay. [Diakses pada 23 April 2019]

Sanger, D. E.. 2012. Obama Order Sped Up Wave of Cyberattacks against Iran. http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html?_r=0. [Diakses pada 12 Februari 2019]

Sanger, D. E., & Fackler, Martin. 2015. N.S.A. Breached North Korean Networks before Sony Attack, Officials Say. https://www.nytimes.com/2015/01/19/world/asia/nsa-tapped-into-north-korean-networks-before-sony-attack-officials-say.html?mcubz=1&_r=0. [Diakses pada 17 April 2019]

Schneier, Bruce 2017. Who Are The Shadow Brokers?. https://www.theatlantic.com/technology/archive/2017/05/shadow-brokers/527778/. [Diakses pada 22 April 2019]

Seal, Mark. 2015. An Exclusive Look at Sony's Hacking Saga. https://www.vanityfair.com/hollywood/2015/02/sony-hacking-seth-rogen-evan-goldberg. [Diakses pada 17 April 2019]

Seger, Alexander. 2012. The Budapest Convention on Cybercrime 10 Years On: Lesson Learnt or the Web is a Web. https://www.coe.int/en/web/cybercrime. [Diakses pada 7 April 2019]

Shaer, M. 2009. North Korean hackers blamed for sweeping cyber attack on US networks.https://www.csmonitor.com/Technology/Horizons/2009/0708/north-korean-hackers-blamed-for-sweeping-cyber-attack-on-us-networks. [Diakses pada 6 Januari 2019]

Shin, Jook-sik. 2012. Information Regarding Jo Myung-Lae, Person in Charge of North Korea's Hacker Unit. http://www.newdaily.co.kr/site/data/html/2012/07/10/2012071000029.html. [Diakses pada 20 Mei 2019]

Shin, Suk-ho. 2010. South Korea's Military Helpless Fighting Electronic Warfare. http://news.donga.com/BestClick/3/all/20101203/33035628/1. [Diakses pada 21 Mei 2019]

Sigal, Leon. 2003. DPRK Briefing Book: U.S. Interests and Goal on The Korean Peninsula. https://nautilus.org/publications/books/dprkbb/uspolicy/dprk-briefing-book-u-s-interests-and-goals-on-the-korean-peninsula/. [Diakses pada 30 April 2019]

Symantec. 2013. Four Years of DarkSeoul Cyberattacks Against South Korea Continue on Anniversary of Korean War. https://www.symantec.com/connect/blogs/four-years-darkseoul-cyberattacks-against-south-korea-continue-anniversary-korean-war. [Diakses pada 12 Februari 2019]

Symantec. 2016. Internet Security Threat Report. https://www.symantec.com/content/dam/symantec/docs/security-center/archives/istr-16-april-volume-21-en.pdf. [Diakses pada 17 April 2019]

Taipale, K. A. 2010. Cyber-deterrence. Law, policy and technology: Cyberterrorism, information, warfare, digital and internet immobilization. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1336045. [Diakses pada 8 Januari 2019]

. Techopedia. 2019. Media Access Control (MAC). https://www.techopedia.com/definition/25059/media-access-control-mac. [Diakses pada 12 Juli 2019]

Thijssen, B. 2016. The cyber triad: Towards effective deterrence in cyberspace. https://www.researchgate.net/publication/306013562_The_Cyber_Triad_Towards_effective_deterrence_in_cyberspace. [Diakses pada 2 Januari 2019]

US Department of Defense. 2015. The Department of Defense Cyber Strategy. Retrieved from http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf. [Diakses pada 6 Januari 2019]

Warren, Tom. 2017. Microsoft Issues 'Highly Unusual' Windows XP Patch to Prevent Massive Ransomware Attack. https://www.theverge.com/2017/5/13/15635006/microsoft-windows-xp-security-patch-wannacry-ransomware-attack. [Diakses pada 22 April 2019]

Weaver, Matthew. 2009. Cyber Attackers Target South Korea and US. https://www.theguardian.com/world/2009/jul/08/south-korea-cyber-attack. [Diakses pada 23 April 2019]

Weinsten, Sheli. 2014. No Active Plot against Movie Theaters, Says Department of Homeland Security. http://variety.com/2014/film/news/no-active-plot-against-movie-theaters-says

-department-of-homeland-security-1201380993/. [Diakses pada 19 April 2019]

Williams, Martyn. 2011. North Korea's Chinese IP Addresses. http://www.northkoreatech.org/2011/06/26/north-koreas-chinese-ip-addresses/. [Diakses pada 20 Mei 2019]

Yoo, Kwan-hee. 2009. The Truth about North Korea's 'Storm Corps,' in Charge of Creating Disturbance behind the Scenes during Wartime. http://www.dailynk.com/korean/read.php?cataId=nk04500&num=69150. [Diakses pada 20 Mei 2019]

Zetter, Kim. 2014. Experts Are Still Divided on Whether North Korea Is behind Sony Attack. https://www.wired.com/2014/12/sony-north-korea-hack-experts-disagree/. [Diakses pada 19 April 2019]

Laporan

Ablon, Lilian. 2018. *Data Thieves: The Motivations of Cyber Threat Actors and Their Use and Monetization of Stolen Data.* Santa Monica: Rand Corporation.

Bar, Shmuel. 2008. *Deterring Terrorist* (Hoover Institution Policy Review no 5674). Diakses dari 28 http://www.hoover.org/publications/policy-review/article/5674.

Bendiek, A. 2015. Deterrence theory in the cyber-century: Lessons from a state-of-the-art literature review.

Bermudez Jr, Joseph S. 2010. *38 North Special Report: A New Emphasis on Operations Against South Korea?*.

Chanlett-Avery, Emma. 2017. *North Korea Cyber Capabilities: In Brief* (CRS Report no R44912). Diakses dari https://fas.org/sgp/crs/row/R44912.pdf.

Chanlett-Avery, Emma. 2018. *North Korea: U.S Relations, Nuclear Diplomacy, and Internal Situation* (CRS Report no R41259). Diakses dari http://www.fas.org/sgp/crs/nuke/R41259.pdf.

Coats, D. 2018. *Statement for the Record: Worldwide Threat Assessment of the US Intelligence Community*.

Council of Economic Advisers. 2018. *The Cost of Malicious Cyber Activity to The U.S Economy*.

Fischer, Eric A. 2014. *Federal Laws Relating to Cybersecurity: Overview and Discussion of Proposed Revisions* (CRS Report no R42114). Diakses dari http://www.fas.org/sgp/crs/natsec/R42114.pdf.

Fischer, Eric A. 2014. *The 2013 Cybersecurity Executive Order: Overview and Considerations for Congress* (CRS Report no R42984). Diakses dari http://www.fas.org/sgp/crs/misc/R42984.pdf.

Fischer, Eric A. 2016. *Cybersecurity Issues and Challenges: In Brief* (CRS Report no R43831). Diakses dari http://www.fas.org/sgp/crs/misc/R43831.pdf.

International Telecommunications Union (ITU). 2018. *Global Cybersecurity Index*. Diakses dari https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf.

North Korea's Internal State of Affairs. 2009. Korea Institute for National Unification Monthly North Korea Review 3.

Park, Jae-kyung. 2013. *China-U.S. Relations in East Asia: Strategic Rivalry and Korea's Choice*. Seoul: CSIS

Siboni, G., & Siman-Tov, D. 2014. *Cyberspace Extortion: North Korea Versus the United States*.

Symantec. 2016. Internet Security Threat Report.

United Nations. 2014. *National accounts main aggregates database*.

Peraturan, Undang-Undang, dan sejenisnya

Department of Defense. *Department of Defense Strategies for Operating in Cyberspace*. Juli 2011. Washington, DC.

Department of Homeland Security. *Homeland Security Act of 2002*. 25 November 2002. 116 STAT 2135. Washington, DC.

Department of Homeland Security. *National Cyber Incident Response Plan.* Desember 2016. Washington, DC.

United States. 2003. *The National Strategy to Secure Cyberspace.* Washington: Presiden Amerika Serikat

United States. 2008. *The Comprehensive National Cybersecurity Initiative.* Washington: Presiden Amerika Serikat

United States. 2009. *Cyberspace Policy Review: Assuring a Trusted and Resilent Information and Communications Infrastructure.* Washington: Presiden Amerika Serikat

United States. 2011. *The International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World.* Washington: Presiden Amerika Serikat

United States. 2018. *The National Cyber Strategy of The United States of America.* Washington: Presiden Amerika Serikat

Skripsi, Tesis, dan Disertasi

Beeker, Kevin R. 2009. *Strategic Deterrence in Cyberspace.* Tesis. Ohio: Air Force Institute of Technology.

Tirrel, W. 2012. *United States Cybersecurity Strategy, Policy, and Organization: Poorly Postured to Cope with a Post-9/11 Security Environment?*. Tesis. Kansas: The George Washington University.