Politisasi Agenda Keamanan Siber Pada Era Industri 4.0 di Forum Multilateral

Hino Samuel Jose
Universitas Pembangunan Nasional Veteran Jakarta
abrahamsamueljose@gmail.com

Abstraksi
Keamanan siber dalam forum multilateral masih mengalami perdebatan dan tantangan hingga saat ini di tahun 2021. Forum multilateral selain menjadi sarana kerjasama bagi para negara untuk mencari solusi bersama juga menjadi ruang untuk para aktor mengedepankan politisasi kepentingan mereka dalam agenda multilateral. Isu strategis dan substantif dari keamanan siber hingga saat ini sudah meluas ke konflik geopolitik sehingga terjadi redefinisi dari alam keamanan siber itu sendiri yang berpengaruh ke forum multilateral. Artikel ini menggunakan teori keamanan siber dalam HI serta membahas mengenai peristiwa sebelumnya yang terkait dengan topik. Artikel ini menggunakan penelitian kualitatif menggunakan data sekunder untuk menganalisa berbagai sub konteks yang relevan. Artikel ini akan membahas bagaimana politisasi keamanan siber dilakukan di forum multilateral pada era 4.0. Artikel ini juga membahas mengenai peran pemerintah yang diredefinisi oleh kebutuhan akan peran industri dan non-state actor dalam dinamika multilateral untuk agenda keamanan siber. Penelitian ini menyimpulkan bahwa akan ada terus tantangan karena ruang siber akan menjadi lapangan kontestasi baru dalam keamanan internasional. Pembahasan multilateral tentunya harus menghadapi perubahan yang kompleks ini.

Kata Kunci: Keamanan siber, Multilateral, Politik Siber, Diplomasi, Teknologi

Abstract
Cyber security in multilateral forum is still experiencing debates and challenges until now in 2021. Multilateral forums are not only a means of cooperation for countries to find common solutions, but also a space for actors to politicizee multilateral agenda according to their will. The strategic and substantive issues of cyber security to this date have extended to geopolitical conflicts, resulting in a redefinition of the nature of cyber security itself which has intertwined effects to the dynamics on multilateral forums. This article uses the Cyber security theory in IR and explains correlated events regarding the topic. This artilce employed qualitative analysis through secondary data to analyze multiple relevant subcontext of this topic. This article will discuss how the politicization of cybersecurity is carried out in multilateral forums in the 4.0 era. This article also discusses the role of government which has been redefined by the need for the role of industry and non-state actors in the multilateral dynamics for the cybersecurity agenda. This research conclude that cyber space will become the new contestation field in international security. The multilateral approach to this issue have to withstand these complex changes.

Keywords: Cybersecurity, Multilateral, Cyber politics, Diplomacy, Technology

Pendahuluan

Perkembangan digital merupakan salah satu hal yang paling banyak dibahas ketika mengkaji isu industri 4.0 yang erat dengan konektivitas internet, penggunaan teknologi yang lebih banyak dalam kehidupan sehari-hari, dan kegiatan ekonomi. Dalam tiga dekade belakangan, pertumbuhan penggunaan teknologi informasi dan komunikasi atau *Information and Communications Technology* (ICT) meningkat secara tajam (Castellacci & Tveito, 2018).

Tidak hanya demikian, perkembangan teknologi yang semakin memuncak ini juga diimbangi dengan hadirnya tantangan-tantangan baru yang dinilai substansial. Adapun digitalisasi ini memang menjadi salah satu bukti bahwa pencapaian yang tinggi, progresif, dan efektif dapat dilakukan bahkan dalam sektor ekonomi dan produksi sosial (Johnson, 2018). Isu digitalisasi sendiri yang erat dengan perkembangan ICT membuat dimensi siber beserta perkembangan *internet of things, big data*, keamanan siber, dan kecerdasan buatan (AI) menjadi bagian dalam diskursus HI ditengah perdebatan kemampuan teori HI menjelaskan hal-hal ini (Kiggins, 2018). Ditengah meningkatnya kesadaran manusia dan perkembangan di jaman 4.0, berkurangnya peran buruh karena otomasi serta efisiensi SDM, maka kecerdasan terindustralisasi dan menciptakan sistem otonom yang mengganti peran manusia (Alam, et al, 2019).

Sekuritisasi siber yang dilakukan menjadi tidak terbatas hanya pada ruang fisik namun juga ruang virtual yang terpisah dengan spektrum tradisional dan tidak menggunakan tentara dan persenjataan fisik. Implikasi dari ancaman yang tidak terlihat di ruang siber seperti terorisme dan radikalisme secara langsung berpengaruh besar bagi keamanan nasional (Indrawan & Efriza, 2017). Signifikansi dari ancaman siber ini sudah menjadi hal yang bersifat disruptif, terarah, politis, dan semakin stratejik (Dunn & Wenger, 2019). Situasi ini mendorong berbagai negara harus menjadikan hal ini sebagai konten prioritas kebijakan domestik untuk melindungi kepentingan dan menciptakan *rule of law* dalam ruang siber (Dunn & Wenger, 2019). Dengan dinamika teknologi yang selalu dipengaruhi oleh dorongan dari luar atau suatu variabel "eksogenus" (McCharty, 2018), maka variabel tersebut itu lah yang akan selalu mendorong perubahan sosial dari dinamika di lingkungan siber (Leese & Hoijtink, 2019). Ketika membahas keamanan siber sendiri, dengan pembuatan kebijakannya yang tentu sarat akan kepentingan politik, maka penting untuk diketahui bahwa teknologi menjadi pelaku utama yang mempengaruhi perilaku aktor sosial dan politik dalam diskursus sekuritisasi siber (Behrent, 2013).

Saat ini, perlu diketahui bahwa adanya kepentingan nasional yang sudah menembus dimensi siber, untuk menciptakan *sense of deterrence* semakin nyata, tentu perluasan studi siber ini diikuti dengan perubahan akan alam konflik pada era pasca perang dingin (Buzan, Waever, & Wilde, 1998). Berkembangnya ancamana membuat para negara tentu harus mempertegas dan menghadirkan sekuritisasi yang tentuya senantiasa terpolitisasi oleh tujuan strategis tertentu. Tidak hanya politik dalam konteks melawan kejahatan dan ketidakamanan siber, bahkan peran negara juga diperluas dengan adanya aktor penjahat/ operasi di lingkungan siber yang didukung oleh suatu negara (Brenner & Crescenzi, 2006). Peran negara yang terlibat dalam kejahatan atau ketidakamanan siber ini tidak lain dilakukan untuk melumpuhkan lawan secara spesifik dan untuk menjatuhkan ekonomi maupun situasi politik keamanan, ancaman yang terjadi tentunya tidak bersifat monoton (Akoto, 2021). Dalam lanskap politik internasional kontemporer saat ini di abad ke-21, kekuatan siber suatu negara menjadi salah satu kapabilitas untuk menentang ancaman negara hegemoni sebagai suatu cara ofensif untuk menyerang tanpa adanya prediksi yang riil (Hern, 2018).

Artikel ini membahas politisasi agenda keamanan siber pada level multilateral, di mana dinamika perang dan kejahatan siber yang terjadi antar negara mempengaruhi

modalitas pembahasan multilateral. Dengan adanya pandangan dimana keamanan internasional merupakan hasil konstruksi dari ketergantungan para aktor dalam sekuritisasi dan agresi, maka dapat disimpulkan ada celah keterbatasan kapasitas dan hal-hal lain yang membatasi perilaku suatu aktor dalam konteks keamanan siber (Nugroho, 2018). Hal ini berarti pemerintah tidak serta merta bisa sendirian melakukan sekuritisasi tanpa membawa aktor non-negara dalam deliberasi kebijakan dan menetapkan apa saja kebutuhan dan langkah yang harus dicapai.

Oleh karena dinamika kepentingan politik yang sangat kental, perlu diketahui bahwa perselisihan, peperangan, dan persaingan antara *major power* dalam dimesi siber akan berdampak besar. Mearsheimer (2001) menyatakan bahwa mengelola konflik yang telah terjadi antara dua *major power* bukanlah suatu hal yang mudah, dan bersifat kompleks. Dalam beberapa tahun belakangan, permasalahan seperti kedaulatan negara, kekuatan, interdependensi, dan strategi penanganan (*containment*) masih menjadi perdebatan oleh karena alam studi siber yang unik (Schmidt, 2013). Dengan demikian maka domain keamanan siber dalam studi hubungan internasional menempatkan manusia sebagai pengguna di ruang siber itu sendiri sebagai *referent object*. Namun, walaupun melibatkan manusia, perlu diketahui bahwa kontestasi politik dan konflik internasional di ruang siber cenderung akan menempatkan suatu kontestasi teori dan redefinisi yang terjadi karena tertahannya bukti empiris dalam studi keamanan siber pada konteks HI (Liaropoulos, 2013). Perkembangan domain keamanan siber menurut Maness dan Valeriano (2015) memiliki proposisi yang bertolak belakang dengan konsep peperangan yang benar (*just war*) karena di ruang siber tidak ada pemisahan akan siapa yang tidak bersalah, dan tidak adanya aspek proporsionalitas yang dapat digariskan dalam dimensi siber (Maness & Valeriano, 2015; Basyar, 2020).

Kerangka teori keamanan siber sendiri memang pada tahun 2000-an masih cenderung belum terproliferasi seperti sekarang dimana tidak ada dahulu adanya suatu individu/ praktisi yang memperkenalkan studi siber sebagai suatu fokus (Denning & Frailey, 2011). Secara konseptual, diskursus yang ada dalam keamanan siber belum diakui secara sah dalam sistem internasional dimana para negara belum mencapai kesepakatan mengenai hal ini hingga ketika artikel ini ditulis. Namun, tidak adanya konsensus dalam pemahaman konsep yang diakui oleh negara dalam lingkup global tidak membuat produktivitas akan isu siber tetap terjamin kedepannya dan senantiasa diperdebatkan (Bambauer, 2012). Namun demikian, tidak adanya konsensus membuat hukum internasional tidak dapat terbentuk di lingkup dimensi siber. Adapun menurut Stevens (2016), adanya kebutuhan akan norma internasional dalam konteks ICT juga mendorong kebutuhan akan perlindungan informasi dan keamanan masyarakat secara menyeluruh ditengah digitalisasi. Hal ini menjadi dasar bahwa kepentingan politik dan intensi suatu aktor dalam konteks kebijakan keamanan siber harus dilakukan melalui intervensi di level global, termasuk forum multilateral.

Secara tekstual, keamanan siber menurut Valeriano dan Manes (2018) menjadi kebutuhan penting yang tidak dapat diabaikan, oleh karena itu rezim internasional seperti *International Telecommunications Union* (ITU) memberikan praktek dan mewujudukan institusionalisasi global dalam dunia siber secara strategis. ITU bukan menjadi solusi

permasalahan, melainkan bentuk kesadaran aktor dalam sistem internasional untuk mengoperasionalisasikan kerjasama horizontal maupun vertikal antar negara (ITU, n.d.). Penulis berpendapat bahwa ITU didirkan sebagai suatu organisasi internasional dibawah PBB yang terbentuk oleh karena kebutuhan negara dalam mempertahankan perdamaian dan kerjasama ICT. Namun, perlu diketahui bahwa model tatanan dari rezim siber yang tercipta baik ITU maupun diluar ITU didorong oleh dua faktor utama yaitu: kebutuhan para aktor untuk mempunyai platform pembuatan kebijakan bersama; dan menjadi sarana untuk para aktor yang memiliki kapabilitas dan kepentingan dalam kontrol pembuatan kebijakan yang ada untuk isu siber (Stadnik, 2017).

Metode.

Artikel ini ditulis menggunakan analisa kualitatif yang dikumpulkan dari data sekunder yaitu literatur yang sesuai dengan menggunakan cara *document-based* dan *internet-based research* untuk dibahas dan dikaji sesuai dengan pertanyaan penelitian. Adapun metode kualitatif menurut Lamont (2015) merupakan suatu metode yang dapat memperbolehkan peneliti dalam mengkaji kejadian, fenomena, organisasi, tempat, dan berbagai hal untuk diperdalam. Menurut Bryman (2008) hal ini merupakan suatu cara untuk mengumpulkan data dari sumber primer atau sekunder yang akan digunakan dalam mendekati suatu teori yang akan dijelaskan. Adapun pertanyaan penelitian yang akan dibahas dalam artikel ini adalah: (1) bagaimana keamanan siber dan tantangan terkini dipolitisasi oleh aktor dalam sistem internasional terutama pada level multilateral; dan (2) apa pengaruh dari studi kasus geopolitik dari politik digital terhadap dinamika serta polarisasi dalam pembentukan norma di level multilateral? Pertanyaan penelitian ini akan dijawab dan dikembangkan berdasarkan studi kasus yang disinggung di dalam tulisan ini.

Hasil dan Pembahasan

1. Tinjauan Historis Keamanan Siber Dalam Hubungan Internasional

Adanya kebutuhan akan keamanan siber tentu membawa perubahan dalam pola perilaku para aktor untuk berkompetisi untuk peluang kemajuan dan sekuritisasi terhadap ancaman kontemporer yang semakin nyata. Tanpa adanya perkembangan teknologi dan jaringan yang menghubungkan seluruh dunia, alat seperti peluncur nuklir, satelit, dan berbagai elektronik yang vital untuk kebutuhan manusia tidak akan ada, dan tentu ini mempengaruhi tatanan internasional dan diplomasi secara signifikan. Dalam kasus dunia nyata, kehadiran Stuxnet yang merupakan cacing komputer pada tahun 2010 yang dikembangkan semenjak 2005 oleh AS dan Israel dalam menghadang proliferasi nuklir Iran menjadi bukti bahwa isu siber dipolitisasi sesuai kebutuhan. Ketakutan AS dan Israel terhadap pembangunan nuklir di Iran menunjukan bahwa ruang siber dapat digunakan sebagai senjata untuk menciptakan hegemoni ditengah potensi Iran yang berpengaruh dan dapat membalik situasi di Timur Tengah (Parsi, 2008). Cara ini merupakan solusi yang diambil yang menggunakan kapabilitas siber sebagai langkah untuk mengisolasi lawan agar tidak menemukan solusi yang dapat dicapai dalam suatu peperangan (Ventre, 2011). Pratama (2016) menegaskan bahwa sekuritisasi siber merupakan salah satu usaha di sistem internasional yang anarki. Hal ini membuktikan bahwa eksistensi politik menembus dimensi ruang dan waktu tanpa perlu interaksi fisik. Dapat dipahami pula secara garis besar bahwa

saat ini kontestasi siber yang terjadi menjadi salah satu kekuatan untuk negara yang terbatas dalam opsi perang fisik secara konvensional dalam mempertahankan asersi pengaruhnya untuk mempengaruhi kebijakan negara lain (Sari, 2018).

Kejahatan transnasional termasuk isu siber salah satunya, tentunya membahayakan dan dalam penegakan hukum nasional akan dihadapi oleh tantangan dalam proses kriminalisasinya karena bergantung pada negara lain (Passas, 2003). Fatalnya dampak dari ancaman siber yang dilakukan oleh sindikat penjahat transnasional memang beragam, tapi yang pasti berdampak besar karena praktik kejahatan yang saling multidimensional. Berlanjut mengenai dilema dalam keamanan siber, perlu memang secara umum penjagaan perdamaian dan keamanan global dilakukan oleh aktor negara dalam suatu rezim internasional (termasuk forum multilateral). Nmaun, untuk memaksimalkan preservasi perdamaian dan keamanan internasional dalam dimensi siber harus melibatkan industri IT dan aktor non-negara yang menggunakan teknologi sebagai jiwa mereka (Stadnik, 2017). Namun, peran multilateralisme masih penting disini karena norma yang terbentuk di level domestik mengalami difusi dalam level global melalui proses institusionalisasi yang terjadi (Finnemore & Sikkink, 1998). Difusi norma yang terjadi dari level domestik tentu tidak terlepas dari terlepas dari peristiwa dan dinamika ancaman siber yang direfleksikan menjadi evaluasi bagi kebijakan domestik negara. Bagian selanjutnya dari artikel ini akan membahas lebih lanjut mengenai hal tersebut. Tabel dibawah ini akan menggambarkan beberapa timeline historik mengenai perkembangan perang siber dari masa ke masa.

Tabel 1. Selintas Data Peretasan Siber yang Terjadi dari Tahun 1998 - 2020

Tahun	Kejadian/ Deskripsi Peristiwa
1998	Sebuah virus bernama "Morris Worm" ditemukan yang menjadi salah satu virus berbahaya yang dapat membelah diri dalam beberapa periode waktu dan menyerang infrastruktur secara keseluruhan. Morris Worm berhasil menginfeksi komputer host dan memperlambat performa komputer (Kehoe, 1992). Virus ini diciptakan oleh Robbert Morris ketika sedang bereksperimen dengan komputernya dan ia kemudian ditangkap oleh pemerintah AS dengan tuduhan penipuan dan penyalahgunaan teknologi.
2005	Sel-sel jejaring penjahat siber Tiongkok meretas jaringan NASA milik AS yang dikelola oleh Lockheed Martin yang dipercaya sebagai salah satu konspirasi pemerintah Tiongkok yang menargetkan fasilitas siber Departemen Pertahanan AS, walaupun para sel-sel hacker ini menyatakan bahwa mereka beroperasi sendirian (CSIS, 2021).
2006	• Selama tahun 2006, berbagai serangan siber dilakukan dan menargetkan fasilitas siber pertahanan militer berbagai negara (CSIS, 2021). • Pada tahun 2006, NASA terpaksa mengamankan peluncuran roket mereka dari peretasan dengan mengamankan seluruh jaringan email dan koneksi agar tidak ada virus yang mensabotase peluncuran roket (NATO, 2013). • Peretas Tiongkok melakukan serangan ke jaringan sistem IT parlemen Inggris.

2007	• Data tempur rahasia jet F-35 dan proyek pesawat tempur dicuri oleh peretas China dan kejadian ini diikuti dengan penutupan jaringan email Universitas Pertahanan Nasional di AS karena peretas asing yang tidak dikenal meninggalkan banyak spyware di sistem (CSIS, 2021). • Pada pertengahan tahun 2007, pemerintah Estonia terpaksa mempertahankan jaringan IT-nya setelah beberapa serangan dilakukan oleh hacker asing yang tidak dikenal, pemerintah Rusia difitnah meskipun tidak ada bukti kuat dari Rusia yang ditemukan (NATO, 2013). Sebelum serangan terhadap Estonia, Menteri Pertahanan AS juga mengumumkan bahwa jaringan Pentagon menerima percobaan peretasan asing untuk mengeksploitasi database melalui jaringan email yang tidak aman (CSIS, 2021). • Kementerian Keamanan Nasional Tiongkok juga menuduh bahwa ada beberapa jaringan peretasan yang berasal dari Tiongkok dan Taiwan (NATO, 2013).
2008	• Perusahaan yang berasal dari Amerika, Eropa, dan Jepang mengalami serangan siber yang luar biasa terhadap jaringan TI properti dan bisnis mereka. Diduga bahwa ini adalah bagian dari spionase industri dan kegiatan teror. • Kelompok peretas yang berbasis di Shanghai yang terkait dengan departemen TI tentara rakyat Tiongkok dituduh mencuri informasi rahasia dan juga pesan email berukuran 50 MB beserta lampirannya (NATO, 2013). Namun laporan publik tidak mengungkapkan agensi AS mana yang diserang oleh kelompok ini karena sensitivitasnya informasi tersebut terhadap kekhawatiran publik. • Pada musim panas 2008, database Partai Demokrat dan Republik di AS diretas oleh banyak peretas asing. Kemudian peretasan ini diikuti oleh serangan terhadap situs web pemerintah Georgia oleh peretas yang berasal Rusia (NATO, 2013).
2009	• Seorang hacker Israel dipenjara selama 6 bulan setelah mencuri 10 juta USD dari bank-bank Amerika (CSIS, 2021). • Internet Israel diretas pada Januari 2009 oleh penyusup asing yang tidak dikenal, Hamas dan Hizbullah dituduh melakukan serangan ini (NATO, 2013).
2010 - 2013	• Terjadi serangan siber yang begitu besar terhadap Google, Adobe, dan perusahaan online besar barat lainnya yang dilakukan oleh beberapa peretas asing yang tidak dikenal dengan menggunakan celah dan celah keamanan lainnya dalam sistem bingkai cyberwall (CSIS, 2021). • Sebuah kelompok bernama "Tentara Cyber Iran meretas mesin pencari terkenal China 'Baidu'. • Serangan siber “Oktober Merah” pada tahun 2012 menargetkan beberapa negara bekas Uni Soviet, khususnya sistem TI pemerintahnya. Virus ini berhasil mengumpulkan data sensitif dan vital tentang pangkalan militer, kedutaan besar, proyek penelitian pemerintah, sistem nuklir, dan basis data infrastruktur lainnya (CSIS, 2021). • Pada Juni 2013, NATO untuk pertama kalinya bertemu untuk membahas masalah keamanan siber dan sepakat untuk membentuk Aliansi Pertahanan Siber NATO untuk melakukan serangan balik dan mencegah hilangnya data penting terhadap peretas asing (NATO, 2013). • NATO meningkatkan aliansinya melawan serangan siber melalui implementasi *NATO Computer Incident Response Capability* (NCIRC) yang bernilai lebih dari 58 juta Euro (CSIS, 2021).

2014	• Banyak kampanye serangan siber dilakukan oleh peretas Iran terhadap pangkalan militer dan jaringan industri AS. • Peretas militer China menargetkan beberapa perusahaan AS untuk mencuri informasi perdagangan rahasia. • Berbagai serangan dilakukan terhadap basis data pemerintah NATO dan Uni Eropa baik melalui situs web/sertifikat online palsu dan atau menggunakan pelanggaran server untuk mendapatkan data pengguna.
2015	• Situs ICJ dimatikan dan diretas saat sidang arbitrasi Laut China Selatan sedang dilakukan, pelacakan IP menunjukkan bahwa itu berasal dari China. • Beberapa situs web pemerintah Pakistan diretas oleh kelompok yang diidentifikasi sebagai Tim Cyber Mallu. • Sebuah serangan Cina dilakukan terhadap industri AS dalam penelitian sel surya. • Beberapa pejabat pemerintahan di kabinet Obama diretas oleh Pengawal Revolusi Iran. Dan akses akun email Direktur CIA John Brennan berhasil diretas.
2016-2018	• Pada 2016, Microsoft mendeteksi peretasan yang canggih dan terampil yang menargetkan lembaga pemerintah (termasuk badan intelijen), pusat penelitian pertahanan, dan penyedia layanan telekomunikasi di Asia Selatan dan Tenggara sejak 2009 (CSIS, 2021). • Campur tangan Pemilihan Presiden AS 2016 oleh Rusia dituduh oleh komunitas intelijen AS setelah kekalahan Hillary Clinton dan kemenangan Donald Trump pada pilpres AS. • Yahoo diretas dan mengungkapkan bahwa 500 juta data pengguna telah disusupi dan diklaim sebagai penyusupan serangan siber yang didukung oleh suatu negara. • Pada 2017, pemerintah situs dan jaringan pemerintah Arab Saudi dan sektor energinya diserang oleh serangan siber buatan Iran. • Pada tahun 2017, kampanye spyware yang didukung suatu negara yang tidak diketahui menyerang jaringan militer dan pemerintah India dan Pakistan. • Pada tahun 2018, akun email pribadi anggota dewan panel PBB diretas oleh Korea Utara karena sanksi perdagangan yang diberlakukan oleh PBB berdasarkan usulan panel tersebut (CSIS, 2021).
2019-2020	• Jaringan hotel AS diretas oleh peretas China yang menyebabkan lebih dari 500 juta data pelanggan dicuri. • Dewan Keamanan PBB pada 2019 mengungkapkan bahwa Korea Utara melalui jaringan siber ilegalnya mencoba mencuri 670 juta dolar AS dalam mata uang kripto antara 2015 dan 2018 (CSIS, 2021). • Pada 2019, database pemilih pemilu legislatif dan presiden Indonesia diretas oleh aktor yang berasal dari China dan Rusia. • Kementerian luar negeri Australia diserang pada Januari 2020 selama beberapa minggu. • Akun staf WHO dicoba diretas oleh peretas Iran di tengah pandemi Covid-19

Dari data diatas dapat disimpulkan bahwa serangan siber sangatlah terpolitisasi dan bagaimana cara menghadapinya akan tergantung dari postur yang direfleksikan oleh para aktor ketika ingin mencegah serangan siber lainnya. Dari perspektif hukum internasional, adanya keterkaitan antara konflik post-modern dengan hukum perang (*law of war*), serangan siber yang dijelaskan pada tabel 1 merupakan wujud peperangan apabila dilakukan pada alam

perang yang kinetik (Valuch, Gabris, & Hamulak, 2017). Pada periode pasca perang dingin, tentunya subjek keamanan siber harus di-redefinisikan oleh karena perubahan alam konflik yang sangat kompleks, dan tidak dapat disetujui secara konsensus dalam berbagai diskursus hukum, politik, keamanan, diplomasi, dan relasi-tensi para aktor dalam studi HI, ICT, dan politik secara menyeluruh.

2. Politik Multilateral dan Keamanan Siber

Setiap negara yang menggunakan forum multilateral untuk mengancam keamanan dan keselamatan orang banyak dengan menggunakan serangan siber dapat dianggap sebagai sebuah pelanggaran terhadap piagam PBB. Walaupun demikian, tidak dapat dipungkiri bahwa politik di level multilateral saat ini mengenai keamanan siber masih terpolarisasi antara blok barat dan timur. Walaupun memang hal ini tidak separah dan seintens dengan apa yang terjadi di perang dingin, namun operasi yang semakin rapid, serta perdebatan dan tidak adanya kesamaan pandangan di forum multilateral menjadikan solusi untuk masalah ini cenderung lumpuh. Seperti contoh AS yang menekankan bahwa aktor jahat harus dilawan secara gamblang dalam isu siber (White House, 2011), dan Rusia yang menegaskan kekuasaan otoriter pemerintah hingga ke dimensi siber untuk mencegah apapun yang bertentangan dengan keamanan negara (MoFA of the Russian Federation, 2016). Hingga fenomena regional ketika Uni Eropa mengadopsi *EU Cybersecurity Act* mengedepankan nilai demokrasi dan perlindungan kepentingan masyarakat UE dari segala potensi ancaman siber (European Commission, 2021). Ketiga contoh ini menjadi induksi pembahasan bagaimana implikasi politis terhadap dinamika kerja sama multilateral untuk penetapan norma keamanan siber.

Menurut penelitian dari Butler dan Lachow (2012), organisasi internasional sebagai fasilitator forum multilateral memiliki beberapa peran kunci dalam mengatasi permasalahan keamanan siber seperti: (1) perluasan dan pengembangan kerangka hukum internasional di ruang siber; (2) perjanjian dan ketetapan mengenai tanggung jawab para aktor swasta seperti penyedia layanan internet dan para aktor pemerintahan untuk memastikan keamanan jaringan siber dari peretas; dan koordinasi keamanan siber harus dilakukan secara kolektif yang dipermudah dengan jejaring politik dan aliansi militer yang sudah terbentuk untuk mencapai kepentingan bersama (Bulter & Lachow, 2012). Narasi ini terdengar naif dan seperti gagasan kosong semata karena politisasi yang sangat kental di ruang siber, kritik ini senada karena semakin besar aktor yang berpartisipasi dalam norma, maka akan semakin samar/ ambigu norma yang dibentuk dalam proses penetapan norma multilateral. Hal ini akan menghasilkan dua kemungkinan, yang pertama dimana norma yang ditetapkan dalam dimensi keamanan siber akan digunakan tidak sebagaimana mestinya/ berdasarkan tujuan holistik yang ada; atau ketetapannya bersifat lumpuh dan tidak mampu mengikat para aktor yang mengelabui kewajiban mereka.

Pembahasan di PBB mengenai keamanan siber dilakukan saat ini banyak oleh kelompok kerja *United Nations Group of Governmental Experts* (GGE) yang bekerja di isu tekonologi komunikasi dan informasi selama 10 tahun. GGE ini dibuat untuk negosiasi alat dan norma keamanan siber selama masa perdamaian (*peacetime*) dan menjaga agar tidak ada perang siber yang mengancamn infrastruktur vital dan kepentingan masyarakat banyak (Pope, 2018). Tantangan dalam arsitektur keamanan siber internasional masih cukup besar, karena ketika pada tahun 2017, negara-negara belum sepakat untuk ketentuan aplikasi hukum internasional pada ruang siber. AS dalam hal ini mendorong bahwa kegiatan membela diri

(*self-defense*), usaha pertahanan siber, dan hukum humaniter internasional harus dilakukan di ruang siber, sementara itu Rusia dan Tiongkok berpendapat berbeda dengan AS dan negara barat serta mendorong norma di mana harus ada identifikasi ancaman terlebih dahulu (Grigsby, 2018; Pope, 2018).

Ketidakamanan siber juga mengancam proses demokrasi di suatu negara, karena banyak peretasan yang dilakukan untuk merubah hasil pemilu, tentunya ini akan berdampak ke situasi politik suatu negara – yang berpengaruh pada dinamika di forum multilateral (Pope, 2018). Contohnya yang bisa dilihat adalah pada isu konflik AS-Rusia dalam intervensi siber pemilu 2016 yang memenangkan Donald Trump, pada level multilateral permasalahan ini menimbulkan disintegrasi pandangan negara-negara karena agenda ini terpolitisasi atas pengaruh yang dibawa oleh AS. Pada forum multilateral AS beberapa kali berselisih dengan Rusia, seperti apa yang terjadi sidang Dewan Keamanan PBB (DK PBB) mengenai keamanan siber pada 29 Juni 2021 ketika AS menginginkan pembahasan mengenai infrastruktur siber, sedangkan Rusia meminta membuat kerangka baru, hal ini tentu kontraproduktif (CNA, 2021). Hal seperti ini juga di advokasikan oleh negara anggota G-7 pada tahun 2017 melalui Deklarasi Lucca yang menetapkan bahwa intervensi siber yang dilakukan terhadap proses politik demokrasi harus di respons oleh negara melalui *enabling policy* dan langkah yang terarah. Diseminasi norma ini menurut penulis adalah suatu bentuk sistematis bahwa supremasi demokrasi dan hak untuk menentukan nasibnya sendiri harus bebas dari berbagai ancaman, termasuk isu intervensi siber oleh pihak asing (Pope, 2018).

Pada level multilateral, perbedaan pendapat menjadi permasalahan, seperti apa yang terjadi antara AS dan Rusia dalam pembahasan sidang PBB. Walaupun secara unilateral komunitas intelijen AS sudah menetapkan intervensi Rusia, tetap saja pihak seperti Rusia masih membantah karena ini dilakukan oleh sekelompok orang yang terasosiasi dalam tujuan yang sama dan masih cenderung politis (ODNI, 2017). Studi sebelumnya menyatakan bahwa apabila ada celah asing yang terbuka memanfaatkan fragmentasi opini publik dan tidak adanya keamanan, maka akan berdampak negatif pada opini publik dan stabilitas nasional (Miller, Nakashima, & Entous, 2017). Hal ini menurut penulis tentu vital karena di tengah era revolusi industri 4.0 masih ada kesadaran kolektif untuk menyelesaikan masalah yang sangat rawan apalagi di tengah digitalisasi dan membentuk partisipasi dalam norma internasional. Untuk menciptakan hal yang konkret, tentu dibutuhkan usaha yang keras dan besar untuk menetapkan solusi kolektif terhadap ancaman keamanan siber dan modus kejahatan transnasional (Gultom, 2017). Operasi kontra-intelijen yang dilakukan pemerintah sebenarnya memperparah implikasi bagi negara berkembang, walaupun hal ini belum terdengar ke publik dari forum multilateral seperti pembahasan di PBB dan pendapat kontradiktif antara AS dan Rusia. Bahkan negara-negara maju menanggapi hal ini serius seperti apa yang dilakukan AS untuk menambah dana pertahanan siber dalam mencegah intervensi asing (Volz, 2018). Meskipun negara maju dan *major power* dalam keamanan siber belum memiliki mekanisme spesifik untuk perang siber antar negara, bisa dilihat bahwa fokus keamanan siber sebenarnya adalah tindakan untuk menciptakan *sense of deterrence* (Fidler, 2017). Hal ini membuat MU PBB pada tahun 2017 mengadopsi resolusi A/RES/70/174 untuk memperkuat penetapan norma pencegahan tindakan kriminal hingga ke ruang siber.

Pada konteks politik internasional, merupakan suatu jaringan kompleks yang terbentuk dengan berbagai unsur yang unik yang terproses secara kompleks yang terus menembus batas-batas wilayah negara ditengah ancaman kontemporer (Kim, 2014). Maka itu tingkat kompleksitas dari ancaman serta usaha untuk sekuritisasi berhubungan erat dengan relasi sosial dan ekonomi yang memiliki kekutasaan dan ide agar para aktor berhasil

mengenalkan norma baru yang secara substansial dan radikal bisa menyembuhkan (Hamonangan & Assegaff, 2020). Politisasi yang terjadi dalam diskursus keamanan siber akan dibahas dalam artikel ini dengan mempertimbangkan bagaimana dinamika hubungan antar negara pada forum multilateral mengenai agenda keamanan siber. Aktor negara akan senantiasa mendefinisikan keuntungan komparatif yang dapat mereka peroleh dari kerjasama di suatu rezim internasional, dan apabila suatu proses pembentukan norma di level multilateral tidak memberikan keuntungan terhadap kepentingan pengembangan siber suatu negara – maka akan terjadi disfungsi dari rezim tersebut. Negara berkembang yang ada di wilayah bumi bagian selatan (*global south*) contohnya, akan memprioritaskan akses yang aman dan muktahir di ruang siber untuk kebutuhan mereka, namun kurang kuatnya kerangka hukum dan stabilitas institusi yang mengatur hal siber membuat akses yang diperoleh ke internet akan memberikan lebih banyak keburukan ketimbang kebaikan (Muller, 2015). Sementara, dengan situasi geopolitik saat ini tentu *major power* baru akan mendorong bahwa kerja sama siber dari level multilateral harus melibatkan peningkatan transfer teknologi dan pendanaan proyek diperlukan oleh negara berkembang (Farrell & Newman, 2019). Gagasan geopolitik yang terintegrasi dengan diskursus keamanan siber memang hingga saat ini belum secara formal dibahas pada level multilateral. Namun yang pasti adalah ini menjadi kontestasi baru dalam politik digital yang akan berimplikasi ke permasalahan geopolitik (Tekir, 2020). Diseminasi informasi saat ini akan fokus pada penciptaan konektivitas siber yang menghubungkan sektor manufaktur dengan rantai suplai global dan untuk mendiseminasi informasi melalui jaringan yang menghubungkan masyarakat (Castells, 2000).

Studi sebelumnya mengungkapkan bahwa permasalahan baru-baru ini seperti 5G apabila dilakukan pendekatan dalam konteks multilateral akan terus mengalami ketidakpastian karena tekanan sanksi dan politisasi agenda pada dimensi lain (Reiter, 2021). Pergantian kepemimpinan yang terjadi di level nasional di AS juga berpengaruh pada posisi negara adi daya di forum multilateral untuk isu siber. Contohnya adalah ketika AS memberikan sinyal kepada sekutunya di Eropa (NATO) bahwa AS telah kembali dan siap untuk bermain sebagai *jazz player* di level multilateral ketimbang usaha unilateral yang digalakkan oleh Presiden Trump sebelumnya. Hal ini tentu akan membuat AS bersama para sekutunya lebih solid lagi di PBB dalam menentang usaha-usaha Rusia, Tiongkok, dan teman-temanya untuk mendorong norma yang mereka percayai lebih solutif. Usaha ini juga penulis nilai merupakan suatu solusi yang *feasible* mengingat tidak adanya sumber hukum internasional yang berhasil menjadi kiblat norma multilateral dalam isu siber. Sifat anonimitas dari suatu serangan siber serta ketidakpastian siapa yang mengirim serangan dan darimana lokasinya membuat aplikasi hukum internasional sulit diterapkan. Perlu diketahui bahwa hukum internasional secara umum tidak dapat secara langsung memaksa pertanggung jawaban aktor non-negara sebagai pelaku kejahatan siber (*accounting non-state actor responsible*).

Lebih spesifik dalam level multilateral, kejadian pada tahun 2017 dimana *United Nations Group of Government Experts on Developments in the Field of Information and Telecommunications in the Context of International Security* (UNCGE) gagal melakukan finalisasi konsensus untuk laporan tahun 2017 memberikan sinyal bahwa ada disfungsi kerjasama. Seharusnya memang lebih baik untuk mengembangkan konsensus dalam bentuk resolusi PBB ketimbang perluasan laporan pada tahun 2015 (Chernenko, Demidov, & Lukyanov, 2018). Usaha untuk membangkitkan negosiasi multilateral yang mandek dilakukan dan pada tahun November 2019 Rusia menjadi sponsor dari resolusi A/C.1/73/L.27/Rev 1 menetapkan pendirian *Open Ended Working Group* (OEWG) membuka pintu untuk aktor non-negara seperti NGO untuk berpartisipasi. Namun, memang berbagai

tuduhan kembali dijatuhkan oleh para negara barat seperti AS, Canada, Inggris, Australia, Belanda, dan lainnya menuduh bahwa Rusia memplintir beberapa ketetapan dari laporan UN CGE pada tahun 2013 dan 2015 yang dianggap dapat mempengaruhi kemajuan konsensus yang telah dicapai untuk beberapa hal sebelumnya. Namun, tetap saja beberapa "konsensus" tersebut kehilangan sosok pemimpin seperti AS saat sudah beberapa tahun absen dalam kontestasi politik siber, hal ini dimanfaatkan oleh Rusia untuk memanfaatkan ketentuan proseduran di MU PBB untuk menguntungkan diplomasi siber mereka (Sherman & Raymond, 2019). Hasil voting dengan 88 negara setuju, 58 menolak, dan 34 abstain bukan merupakan sinyal bagus untuk pencapaian konsensus siber kedepannya.

3. Selintas Pemahaman Tekanan di Forum Multilateral Dari Sisi Negara Anggota PBB

Tidak semua negara anggota di seluruh dunia dianggap mampu dan efektif dalam hal menjaga dan memperkuat supremasi hukum pada level domestik melawan seluruh aktor penjahat siber. Dengan demikian, tidak adanya instrumen hukum internasional mengenai keamanan siber membuat negara tidak memiliki acuan untuk mensinergikan ketetapan hukum mereka sesuai *best practices* yang dianjurkan. Kelemahan ini juga dimanfaatkan sebagai salah satu agenda politik para negara-negara besar (*major power*) dalam mempolitisasi agenda siber demi kepentingan pengaruh geopolitik dan geostrateginya, yang berimbas secara luas ke negara-negara lain dalam negosiasi multilateral. Dapat disimpulkan bahwa diperlukan pandangan *bottom up* ketika menyelesaikan isu terorisme dan perang siber karena sifat lintas yurisdiksi dan transnasional dari aktivitas sibernya tidak benar-benar tercakup dalam tata dan ketertiban hukum domestik (Walker, 2019). PBB dalam hal ini telah mengakui bahwa ada banyak norma internasional yang tumpang tindih dan tidak jelas dalam hal memerangi ancaman terorisme siber. Untuk membahas lebih lanjut, ada 3 tantangan sistemik yang menjadi hal mendesak dalam menyelesaikan ancaman cyberterrorism.

Pertama, ada banyak keberatan di antara negara-negara anggota mengenai pandangan mereka mengenai penerapan hukum internasional dan tata kelolanya di dunia maya. Negara dengan tatanan serta manajemen perlindungan siber mungkin dapat memberikan implementasi kebijakan yang praktis. Namun, banyak negara anggota yang berpandangan bahwa norma dan proses normatif masih dapat menjadi solusi utama, namun tindakan normatif tersebut terbukti kurang dan tidak mampu menghadapi dinamika perubahan ancaman siber – semua karena kurangnya kesadaran di antara pemangku kepentingan pemerintah (UNIDIR, 2017). Kedua, ada banyak situasi ketidakpatuhan terhadap langkah-langkah regulasi siber yang ada dalam banyak kondisi nasional. Misalnya, kurangnya kepercayaan di antara pemangku kepentingan pemerintah merusak kolaborasi dan kerja sama yang dapat menguatkan keadilan dan perlindungan terhadap terorisme dan kejahatan siber (UNIDIR, 2017). Ketiga, kurangnya kerangka kerja bagi pemerintah untuk menyesuaikan pengungkapan dan klasifikasi data sensitif dan jaringan siber (Zerzri, 2017). Kondisi ini diperparah dengan keterlibatan aktor non-negara itu sendiri – karena terorisme siber banyak dilakukan oleh aktor non-negara, hal ini membuat intervensi dari komunitas internasional kepada aktor-aktor ini yang beroperasi di wilayah nasional dibatasi oleh kerangka hukum dan pendekatan kebijakan tradisional lainnya untuk memerangi ancaman terhadap terorisme siber (Klein, 2015). Dan ini masih menjadi perdebatan panas di forum multilateral seperti PBB dan OEWG yang dijelaskan sebelumnya karena banyak negara memiliki garis berbeda dalam pengerahan tindakan represif maupun yang lebih ringan.

Pada forum multilateral juga tentunya konteks ketidakamanan siber seperti terorisme siber dan perang siber tidak terlepas dari dorongan politis. Oleh karena itu pembahasan di

level multilateral tentu apabila melibatkan *state sponsored cyber terrorism* akan semakin ruwet karena sang pelaku akan menyembunyikan perbuatannya. Tuduhan yang dilontarkan tentu tidak akan memberikan iklim baik, apalagi ditengah tidak adanya ketetapan hukum internasional mengenai siber. Menjadi suatu refleksi bahwa telah terjadi redefinisi konteks transnasional dari kegiatan terorisme siber itu sendiri (Weiss, 1996). Dalam perspektif hubungan internasional, kita dapat melihat bahwa ada 2 jenis daro alam/ *nature* terorisme siber, yaitu "terorisme siber hibrida/ *hybrid cyberterrorism*" dan "terorisme siber murni/ *pure cyberterrorism*" (Pradnyana & Rofii, 2020). Tindakan yang berkorelasi dan multidimensi dari aktivitas terorisme siber ini dikonfigurasikan dengan sangat baik untuk meningkatkan kemampuan dan kekuatan pelaku di luar kepentingan cyber mereka (Zerzri, 2017). Hal ini akan mengarah pada situasi lain yang lebih buruk ketika publik terancam dan inkapabilitas negara akan menjadi sejarah kelam karena korban terus berjatuhan. Serangan langsung terhadap individu mempunyai pola langsung dan konsisten serta meresahkan karena penggunaan digital menjadi bagian dari masyarakat (Pradnyana & Rofii, 2020). Dunia multilateral tidak dapat menyelesaikan permasalahan ini karena akan sangat bergantung pada hukum nasional, dan saat ini tidak ada norma yang disepakati secara kuat sebagai landasan dari PBB. Tentunya hal ini membuat rezim internasional hanya bisa menjadi ajang untuk para negara dalam melakukan institusionalisasi masing-masing tanpa adanya sinergi yang seharusnya dibutuhkan.

Kesimpulan

Keamanan siber merupakan agenda non-tradisional yang dinamis dalam politik internasional, serta peran institusi internasional dalam level kerja sama multilateral dibutuhkan untuk penanganan permasalahan siber yang merupakan implikasi dari fenomena perang siber pada level bilateral. Kompetisi antara para negara yang memiliki kekuatan siber tentu menjadi penentu bagaimana mereka menjaga rakyatnya ditengah meningkatnya kebutuhan siber, serta bagaimana negara berproses dalam dinamika multilateral untuk penyusunan norma-norma siber yang saat ini masih cenderung politis. Pembahasan forum multilateral berkorelasi dengan aksi-reaksi negara-negara dan kebutuhan tersebut harus dipenuhi secara strategis apabila mempunyai sumber daya yang mumpuni, dan secara politis untuk bekerjasama dengan negara lain yang lebih mampu. Dengan tidak adanya norma konsensus pada level multilateral, maka politisasi agenda keamanan siber akan menjadi cara negara untuk mencari solusi ditengah tidak adanya ketetapan yang diterima. Serta pembahasan akan cenderung tidak murni untuk kebutuhan holistik, dan ruang siber akan menjadi arena baru dari kontestasi geopolitik. Organisasi multilateral tentu akan menghadapi tantangan besar apabila perang siber terjadi dan penyelesaiannya akan lebih kompleks ketimbang konflik tradisional.

Daftar Pustaka

Akoto, W. (2021). International trade and cyber conflict: Decomposing the effect of trade on state-sponsored cyber attacks. *Journal of Peace Researc*. doi:10.1177%2F0022343320964549

Alam, T., Antony, A., Hotama, K., & Kuswandi, S. (2019). Revolusi Industri Keempat: Akhir Dari Buruh di Seluruh Dunia. *Jurnal Hubungan Internasional, 12*(2), 229-244. doi:10.20473/jhi.v12i2.13311

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

Basyar, M. (2020). Etika Perang Dalam Islam dan Teori Just War. *Jurnal Penelitian Politik, 17*(1), 17-30. doi:10.14203/jpp.v17i1.854

Behrent, M. (2013). Foucault and technology. *History and Technology, 29*(1), 54-104. doi:10.1080/07341512.2013.780351

Brenner, S., & Crescenzi, A. (2006). State-sponsored crime: The futility of the economic espionage act. *Houston Journal of International Law, 28*(2), 389-465.

Bryman, A. (2008). *Social research methods.* New York: Oxford University Press.

Bulter, R., & Lachow, I. (2012, Desember). *Multilateral Approaches For Improving Global Security in Cyberspace.* Retrieved Juni 18, 2021, from MITRE: https://www.mitre.org/publications/technical-papers/multilateral-approaches-for-improving-global-security-in-cyberspace

Buzan, B., Waever, O., & Wilde, J. (1998). *Security: A New Framework for Analysis.* Boulder: Lynne Rienner Publisher.

Castellacci, F., & Tveito, V. (2018). Internet use and well-being: A survey and a theoretical framework. *Research Policy, 47*(1), 308-325. doi:10.1016/j.respol.2017.11.007

Castells, M. (2000). The Contours of the Network Society. *Foresight, 2*(2), 151-157. doi:10.1108/14636680010802591

Chernenko, E., Demidov, O., & Lukyanov, F. (2018, Februari 23). *Increasing International Cooperation in Cybersecurity and Adapting Cyber Norms*. Retrieved Juni 19, 2021, from Council on Foreign Relations: https://www.cfr.org/report/increasing-international-cooperation-cybersecurity-and-adapting-cyber-norms

CSIS. (2021). *Significat Cyber Incidents Since 2006.* Retrieved February 12, 2021, from Center for Strategic and International Studies: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents

Denning, P., & Frailey, D. (2011). The Profession of IT: Who Are We-Now? *Communications of the ACM, 54*(6), 25-27. doi:10.1145/1953122.1953133

Dunn, M., & Wenger, A. (2019). Cyber security meets security politics: Complex technology, fragmented politics, and networked science. *Contemporary Security Policy, 41*(1), 5-32. doi:10.1080/13523260.2019.1678855

European Commission. (2021, Maret 8). *The EU Cybersecurity Act brings a strong agency for cybersecurity and EU-wide rules on cybersecurity certification*. Retrieved Juni 18, 2021, from European Commission: https://digital-strategy.ec.europa.eu/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity

Farrell, H., & Newman, A. (2019). *Weaponized Globalization: Huawei and the Emerging Battle over 5G Networks*. Retrieved Juni 19, 2021, from Global Asia: https://www.globalasia.org/v14no3/cover/weaponized-globalization-huawei-and-the-emerging-battle-over-5g-networks_henry-farrellabraham-newman

Fidler, D. P. (2017). The U.S. Election Hacks, Cybersecurity, and International Law. *Maurer School of Law Repository*. Retrieved from https://www.repository.law.indiana.edu/cgi/viewcontent.cgi?article=3607&context=facpub

Finnemore, M., & Sikkink, K. (1998). International Norm Dynamics and Political Change. *International Organization, 52*(4), 887-917. doi:10.1162/002081898550789

Hamonangan, I., & Assegaff, Z. (2020). Cyber Diplomacy: Menuju Masyarakat Internasional yang Damai di Era Digital. *Padjadjaran Journal of International Studies, 12*(2), 342-352.

Hern, A. (2018, Februari 26). *North Korea is a bigger cyber-attack threat than Russia, says expert*. Retrieved Juni 18, 2021, from The Guardian: https://www.theguardian.com/technology/2018/feb/26/north-korea-cyber-attack-threat-russia

Indrawan, R., & Efriza. (2017). Bela Negara Sebagai Metode Pencegahan Ancamana Radikalisme di Indonesia. *Jurnal Pertahanan dan Bela Negara, 7*(3), 1-17. doi:10.33172/jpbh.v7i3.226

ITU. (n.d.). *ITU-T in Brief*. Retrieved Juni 18, 2021, from International Telecommunication Union: https://www.itu.int/en/ITU-T/about/Pages/default.aspx

Johnson, M. (2018). Inclusion and exclusion in the digital economy: disability and mental health as a live streamer on Twitch.tv. *Information, Communication & Society, 22*(3), 506-520. doi:10.1080/1369118X.2018.1476575

Kehoe, B. P. (1992). *Zen and the Art of the Internet: A Beginner's Guide to the Internet* . Englewood Cliffs, NJ: Prentice Hall .

Kiggins, R. (2018). Big Data, Artificial Intelligence, and Autonomous Policy Decision Making: A Crisis in International Relations Theory? In R. Kiggins (Ed.), *The Political Economy of Robots: Prospects for Prosperity and Security in the Automated 21st Century.* London: Palgrave Macmillan. doi:10.1007/978-3-319-51466-6_10

Kim, S. (2014). Cyber Security and Middle Power Diplomacy: A Network Perspective. *The Korean Journal of International Studies, 12*(2), 323-352.

Lamont, C. (2015). *Research Methods in International Relations.* Thousand Oaks: Sage Publishing.

Leese, M., & Hoijtink, M. (2019). Technology and agency in international relations. London: Routledge.

Liaropoulos, A. (2013). Great Power Politics in Cyberspace: U.S. And China Are Drawing the Lines Between Confrontation and Cooe. In M. Majer, & R. Ondrejcsak (Eds.), *PANORAMA of global security environment* (pp. 155-166). Bratislava: Centre for European and North Atlantic Affairs.

Maness, R., & Valeriano, B. (2015). *Russia's Coercive Diplomacy - Energy, Cyber and Maritime Policy as New Sources of Power.* London: Palgrave Macmillan.

Marsheimer, J. (2001). *The Tragedy of Great Power Politics.* New York: W. W. Norton.

McCharty, D. (Ed.). (2018). *Technology and world poltiics: An Introduction.* London: Routledge.

Miller, G., Nakashima, E., & Entous, A. (2017, June 23). *Obama's Secret Struggle To Punish Russia for Putin's Election Assault*. Retrieved December 15, 2020, from The Washington Post: https://www.washingtonpost.com/graphics/2017/world/national-security/obama-putin-election-hacking/?utm_term=.1042ee4d8dcf

MoFA of the Russian Federation. (2016, Desember 5). *Doctrine of Information Security of the Russian Federation*. Retrieved Juni 18, 2021, from The Ministry of Foreign Affairs of the Russian Federation: https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163

Muller, L. (2015). *Cyber Security Capacity Building in Developing Countries: Challenge and Opportunities* (Vol. 3). Oslo: Norwegian Institute of International Affairs.

NATO. (2013). *Cyber Timeline*. Retrieved February 12, 2021, from North Atlantic Treaty Organization: https://www.nato.int/docu/review/2013/cyber/timeline/en/index.htm

Nugroho, K. (2018). Pengaruh Cyber Attack terhadap Kebijakan Cyber Security Amerika Serikat. *Journal of International Relations, 4*(3), 393-401.

ODNI. (2017). *Assessing Russian Activities and Intentions in Recent US Elections.* Intelligence Community Assessment . Retrieved from http://www.dni.gov/files/documents/ICA_2017_01.pdf

Parsi, T. (2008). *Treacherous Alliance: The Secret Dealings of Israel, Iran and the United States.* New Haven: Yale University Press.

Passas, N. (2003). Cross-border crime and the interface between legal and illegal actors'. *Security Journal, 16*(1), 19-38. doi:10.1057/palgrave.sj.8340123

Pope, A. E. (2018). Cyber-securing our elections. *Journal of Cyber Policy, 3*(1), 24-38. doi:DOI: 10.1080/23738871.2018.1473887

Pradnyana, I. P., & Rofii, M. S. (2020). Cyberterrorism Threats in Indonesia and State Responses. *Literatus Journal, 2*(2), 181-192. doi:https://doi.org/10.37010/lit.v2i2.92

Pratama, R. (2016). Penggunaan Cyberwar Melalui Stuxnet Project Oleh Amerika Serika Dalam Merespon Perkembangan Proyek Nuklir Iran di Natanz. *Jurnal Analisis Hubungan Internasional, 5*(2), 378-386.

Reiter, J. (2021, Maret 2021). *A Multilateral Approach to 5G Safety*. Retrieved Juni 19, 2021, from Real Clear Policy: https://www.realclearpolicy.com/articles/2021/03/29/a_multilateral_approach_to_5g_safety_770138.html

Sari, L. (2018). Bentuk Kebijakan Amerika Serikat Terhadap Ancaman Cyber Crime China Sebagai Bentuk Upaya Proteksianisme Terhadap Keamanan Nasional. *Jurnal Kajian Pemerintah, 4*(1). doi:10.25299/jkp.2018.vol4(1).5307

Schmidt, M. (Ed.). (2013). *Talilinn Manual on the International Law Applicable to Cyber Warfare.* New York: Cambridge University Press.

Sherman, J., & Raymond, M. (2019, Desember 4). *The U.N. passed a Russia-backed cybercrime resolution. That's not good news for Internet freedom*. Retrieved Juni 19, 2021, from Washington Post: https://www.washingtonpost.com/politics/2019/12/04/un-passed-russia-backed-cybercrime-resolution-thats-not-good-news-internet-freedom/

Stadnik, I. (2017). What is an International Cybersecurity Regime and How We Can Achieve It? *Masaryk University Journal of Law and Technology, 11*(1), 129-154. doi:10.5817/MUJLT2017-1-7

Tekir, G. (2020). Huawei, 5G Networks, and Digital Geopolitics. *International Journal of Politics and Society, 2*(4), 113-135.

UNIDIR. (2017). *The United Nations, Cyberspace and International Peace and Security: Responding to Complexity in the 21st Century* . Geneva: UNIDIR .

Valuch, J., Gabris, T., & Hamulak, O. (2017). Cyber Attacks, Information Attacks, and Postmodern Warfare. *Baltic Journal of Law & Politics, 10*(1), 64-89. doi:10.1515/bjlp-2017-0003

Ventre, D. (2011). *Cyberwar and Information Warfare.* London: ISTE.

Volz, D. (2018, March 22). *U.S. spending bill to provide $380 million for election cyber security*. Retrieved December 15, 2020, from Reuters: https://www.reuters.com/article/us-usa-fiscal-congress-cyber-idUSKBN1GX2LC

Walker, S. (2019). *CYBER-INSECURITIES? A Guide to the UN Cybercrime Debate* . Geneva: Global Initiative Against Transnational Organized Crime .

Weiss, G. (1996). The Farewell Dossier: Duping the Soviets. *CIA Studies in Intelligence*. Retrieved from https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/

White House. (2011, Mei). *International Strategy for Cyberspace.* Retrieved Juni 18, 2021, from Obama White House: https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf

Zerzri, M. (2017). *The Threat of Cyber Terrorism and Recommendations for Countermeasures.* Center for Applied Policy Research. Retrieved from https://www.cap-lmu.de/download/2017/CAPerspectives-Tunisia-2017-04.pdf