Journal of International Relations, Volume 4, Nomor 3, 2018, hal. 393-401
Online di http://ejournal-s1.undip.ac.id/index.php/jihi

Pengaruh *Cyber Attack* terhadap Kebijakan *Cyber Security* Amerika Serikat

Kristian Aji Nugroho
Departemen Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik
Universitas Diponegoro
Jalan Prof. H Soedarto, SH, Tembalang, Semarang, Kode Pos 1269
Websiter: http://www.fisip.undip.ac.id Email: fisip@undip.ac.id

ABSTRACT
This research aims to determine how the effect caused by cyber attack on cybersecurity policy in the United States This research is a descriptive study with guided by the framework of the concept of crime of caliber is a transnational crime by UNTOC, public policy theory of Van Meter and Van Horn is a model of process of policy implementation, and constructivism caused by social interaction in society and international political culture make cybersecurity policy implemented in national and international scope. This research is a qualitative research using library research as a data source. The results obtained from the level of cyber attacks experienced by the United States affect the public policy in the United States so that cybersecurity policy is made to maintain the security and national sovereignty of the United States.
Keywords: *cyberattack , public policy, cybersecurity*

Pendahuluan

Proses umum globalisasi dekade terakhir memberikan penjelasan utama bagi munculnya kejahatan transnasional. Karena liberalisasi pasar dan penurunan kepentingan perbatasan antar negara, kejahatan transnasional telah meningkat secara dramatis. Asumsi ini sampai batas tertentu menyederhanakan penyebab dan perkembangan kejahatan transnasional. Hal itu sudah menunjukkan bahwa kejahatan transnasional selalu terjadi. Bagaimanapun, kejahatan transnasional tidak hanya terjadi karena orang, barang dan jasa bisa menyeberang perbatasan. (Kemenkumham, 2012)

Kejahatan lintas batas adalah perilaku yang membahayakan kepentingan yang dilindungi oleh hukum di lebih dari satu yurisdiksi nasional dan yang dikriminalisasi dalam setidaknya satu dari negara yang bersangkutan (Passas, 2003 : 20). Dari pengertian tersebut, kejahatan yang dimaksud tidak hanya sifat nya lintas batas negara, tetapi termasuk juga kejahatan yang dilakuakn di negara tersebut, juga akan berakibat berakibat fatal tehadap negara lain (Intan, 2008:1). Kejahatan transnasional dalam penjelasan oleh kemlu.go.id, saling berhubungan satu sama lain antara 3 kategori *: trafficking crimes, financial crimes, high-tech crime* (kemlu.go.id).

Kejahatan siber mempunyai dampak yang cukup besar karena dampaknya bukan hanya pada individu saja, melainkan juga pada organisasi dan negara. Kejahatan siber yang menyerang negara tentunya menjadi perhatian yang lebih bagi sektor pemerintahan negara bersangkutan karena merugikan dan sudah mengganggu sektor keamanan negara. Amerika serikat sebagai negara yang sudah memanfaatkan teknologi informasi di segala aspek kehidupan disana tidak luput dari serangan siber yang menimbulkan kejahatan siber. Karena sudah menyangkut kemanan negara, maka pemerintah mengambil sikap untuk mengeluarkan kebijakan. Pengambilan kebijakan berkaitan dengan potensi serangan *cyber*,

baik dari postur yang ofensif dan defensif, penuh dengan jenis pertanyaan nilai yang menginformasikan warga negara dapat memberikan kontribusi yang berarti.

Menurut Herbert Lin (2018) dalam pembuatan kebijakan siber yang pada umunya terbagi mejadi 2 dimensi, yaitu dimensi internasional dan domestik. Dalam dimensi internasional seperti keamanan internasional, kerjasama, da hukum yang berlaku. Untuk dimensi domestik seperti infrastruktur vital-terkait keamanan siber; sektor privat; ekonomi; psikologi dan edukasi; sosiologi, antropologi dan organisasi; hukum; implikasi etis dan sosial dalam *cybersecurity*; dan pengadaan alat. Dalam menjelaskan pengaruh *cyber attack* terhadap kebijakan *cyber security*, penulis menggunkan konsep kejahatan transnasional, konsep kebijakan publik dan teori konstruktivisme.

Kebijakan *cybersecurity* yang dibuat oleh pemerintah federal Amerika Serikat tentuya berawal dari permasalahan siber yang dialami Amerika Serikat sepeeti serangan yang ditujukan terhadap Amrika Serikat hingga berujung pada kejahatan siber yang ditujukan ke Amerika Serikat sehingga menimbulkan kerugian di berbagai sektor. Amerika Serikat sebagai negara yang memegang peranan penting dalam perkembangan teknologi dunia menjadi sasaran serangan siber oleh negara – negara lain seperti Cina, Rusia, Korea Utara, Iran dan juga oleh kelompok teroris seperti ISIS. Maka dari itu penulis ingin menunjukkan bagaimana pengaruh *cyber attack* terhadap kebijakan cuber security Amerika Serikat.

Pembahasan

Dimensi Siber Amerika Serikat dan Upaya Penanggulangan Cyber Attack

Perkembangan teknologi di Amerika serikat sangat pesat. Bahkan Amerika Serikat bisa dikatakan sebagai pionir dalam perkembangan teknologi di dunia. Banyak penemuan teknologi berasal dari Amerika Serikat yang berpengaruh ke seluruh dunia. Termasuk dengan ditemukannya internet. Hampir semua aspek kehidupan sudah terkomputerisasi dan tehubung dengan internet di Amerika Serikat akibat dari pesatnya perkembangan teknologi. Berdasarkan data dari statista.com, 290 juta penduduk Amerika Serikat tercatat sebagai pengguna internet atau 74.5% dari seluruh penduduk Amerika Serikat pada tahun 2016. 70% dari seluruh pengguna internet di Amerika Serikat menggunakan smartphone untuk mengakses internet. Dari data tersebut bisa diketahui jika masyarakat Amerika Serikat tidak bisa lepas dari penggunaan internet di kehidupan sehari – harinya, terlebih dengan akses internet hanya dengan genggaman tangan yaitu dengan smartphone.

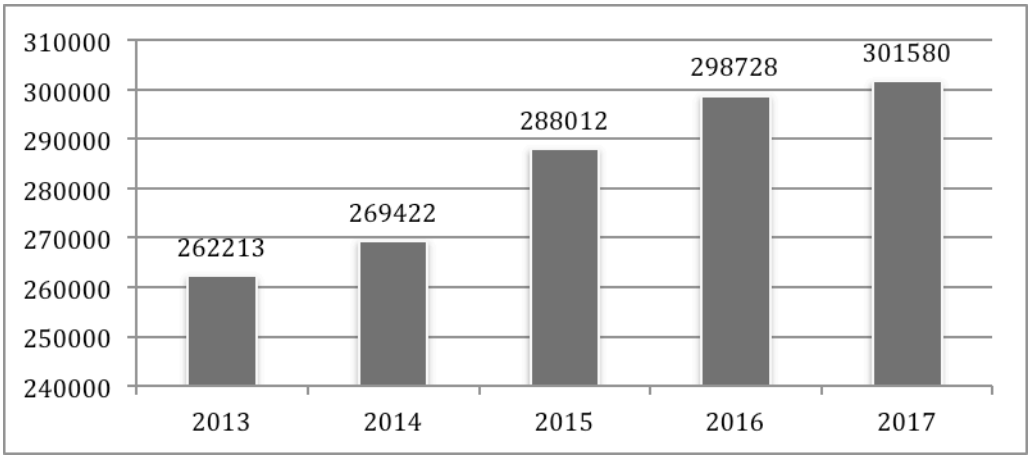
Kemajuan teknologi dirasakan warga Amerika Serikat di semua sektor. Berikut beberapa sektor vital yang terdampak kemajuan teknologi seperti kesehatan, pendidikan, informasi publik,perbankan, transpotasi, industri, pemerintahan, pertahanan. Dari sektor kesehatan, kemajuan teknologi di bidang kesehatan berdampak pada pencegahan penyakit dan penyebaran informasi penyakit yang lebih cepat. Data kesehatan yang terkumpul akan dikembangkan untuk memperoleh hasil penelitian lebih lanjut. Bidang pendidikan menjadi sektor yang sangat diuntungkan dengan kemajuan teknologi dan informasi karena dapat secara mudah mencari informasi dan materi untuk menunjang bidang pendidikan. Proses belajar mengajar juga menjadi lebih mudah dan fleksibel karena informasi dapat didapatkan secara gratis maupun berbayar di internet dan mulai mengubah cara pandang dalam belajar yang sebelumnya *teacher-centris* ke *student-centris*. Teknologi mengantar perubahan struktural mendasar yang dapat menjadi bagian integral untuk mencapai peningkatan produktivitas yang signifikan. Bidang jurnalisme juga merasakan dampak yang besar dari kemajuan teknologi. Semua informasi sudah terdigitalisasi akibat internet dan memunculkan bentuk baru dari media seperti *social media* dan *blog*. Cepatnya informasi yang diberikan, sering menimbulkan isu dan kontroversi yang ditimbulkan dari pemberitaan. Hampir semua kantor berita memiliki website dan akses media internet

karena merupakan cara yang murah, mudah, dan cepat daripada media cetak. Jurnalisme di era digital membuat perubahan berupa hal – hal baru seperti cara, kecepatan, suara, akuntabilitas, budaya, etika, dan mobilitas

Dari bidang transportasi, *Intelegent Transportation System* (ITS) yang merupakan sebuah ekosistem yang terbentuk karena kemajuan teknologi dimana kendaraan dan hal lain yang berkaitan dengan transportasi dapat diarahkan dengan sebuah sistem. Dari dunia perbankan, kegiatan transaksi keuangan semakin mudah dengan *e-banking* dan akses hanya dengan melalui *smartphone* yang tersambung dengan koneksi internet. kemudahan tersebut membuat orang enggan untuk melakukan transaksi di cabang terdekat. ATM, Internet banking, mobile banking, alat pembayaran elektronik merupakan contoh penggunaan teknologi dalam dunia perbankan AS. Untuk bidang kepemerintahan, kemajuan teknologi membuat interaksi pemerintah dengan warganya menjadi lebih dekat,pelayanan publik yang lebih cepat, penyebaran informasi mejadi lebih mudah. Bagi pemerintah, kemajuan teknologi mampu membantu dalam mewujudkan *good governance*, seperti dalam hal akuntabilitas dan transparansi. Pada bidang pertahanan, Amerika serikat tidak bisa lepas dari perannya dalam peperangan di dunia. Mulai dari perang dunia I dan II hingga peperangan modern, Amerika Serikat mengalami kemajuan teknologi di bidang pertahanan yang sangat pesat.

Amerika serikat merupakan negara yang paling sering menjadi sasaran *cyber attack*. Perkembangan teknologi yang sangat pesat menjadi alasan utama *cyber attack*. Serangan yang dilakukan bukan hanya menyerang industri maupun pemerintahan, warga sipil pun menjadi target serangan.

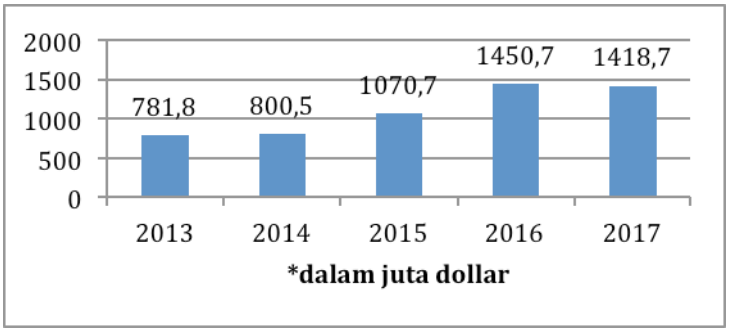
Grafik 1 Keluhan Kasus Kejahatan Siber 2013-2017



Sumber : www.ic3.gov, 2017

Dari grafik di atas, jumlah pelanggaran data terus meningkat dari tahun ke tahun. Pada tahun 2013 tercatat ada 262.213 laporan kejahatan siber. Lalu pada 2014 naik menjadi 269.422 laporan. Di tahun berikutnya juga mengalami peningkatan pada tahun 2015 dan 2016 yaitu ada 288.012 laporan pada 2015 dan 298.728 laporan pada 2016. Di tahun 2017 juga mengalami peningkatan dengan jumlah laporan mencapai 301.580. Bila ditotal, dalam kurun waktu 5 tahun tersebut antara 2013 sampai 2017 tercatat ada 1.420.555 laporan masuk ke IC3.

Grafik 2 Kerugian akibat Kejahatan Siber AS 2013-2017



Sumber : www.ic3.gov, 2017

Grafik di atas memberikan informasi terkait kerugian yang diakibatkan oleh serangan kejahatan siber yang dialami Amerika Serikat dalam kurun waktu 5 tahun antara 2013 sampai 2017. Dari grafik diatas, kerugian selalu meningkat dari tahun 2013 sampai tahun 2016 dan pada tahun 2017 mengalami sedikit penurunan. Bila ditotal, kerugian finansial akibat kejahatan siber yang dialami Amerika Serikat dari 2013 sampai 2017 ditaksir mencapai 5,52 miliar dollar AS.

Serangan siber yang dialami Amerika Serikat sudah merugikan negara AS secara keseluruhan karena sudah berdampak pada sektor – sektor vital yang mempengaruhi kehidupan warga negara Amerika Serikat dan tentunya berdampak pada kerugian finansial akibat serangan siber. Dibutuhkan peran pemerintah dalam menangani kasus serangan siber yang sudah mempengaruhi kehidupan warga negara AS. Upaya pemerintah AS bisa dilihat dengan peraturan yang dibuat oleh pemerintah AS dalam menanggulangi kasus kejahatan siber yang semakin marak.

Sejarah undang – undang AS yang terkait dengan kejahatan teknologi sudah dibuat sejak tahun 1956. Undang-undang pertama yang digunakan untuk mengadili kriminal komputer di AS adalah undang-undang kecurangan kawat-kawat yang melarang penggunaan kabel komunikasi yang digunakan dalam perdagangan antar negara bagian atau internasional dalam setiap upaya untuk melakukan penipuan. Bahkan undang-undang penipuan kawat masih digunakan untuk secara efektif mengadili kejahatan terkait komputer bahkan hari ini (law.cornell.edu, 2018).

Setelah ditemukannya komputer dan pesatnya perkembangan teknologi, pemerintah AS menyadari akan dampak negatif yang akan didapat. Kongres menanggapi masalah kejahatan komputer dengan memberlakukan beberapa undang-undang. Undang-undang kejahatan komputer federal pertama adalah *Computer Fraud and Abuse Act of 198.* Lalu setelah disetujui pada tahun 1986, *Electronic Communications Privacy Act* (ECPA) merupakan amandemen terhadap hukum penyadapan federal, Undang-Undang tersebut tidak melegalkan komunikasi elektronik yang disimpan atau dikirim tanpa otorisasi. Setelah itu muncul beberapa undang – undang karena semakin berkembangnya teknologi dan pada akhirnya dikeluarkanlah kebijakan *cybersecurity* sebagai pedoman keamanan

cyber pada 2003 yaitu *National Stategy to Secure Cyberspace* yang berisi 5 prioritas keamanan nasional, seperti : peningkatan keamanan sistem respon, peningkatan keamanan dari ancaman dan kerentanan siber, peningkatan keamanan kepedulian dan program latihan, pengamanan dunia siber pemerintah, dan keamanan nasional serta kerjasama internasioal terkait keamanan siber (us-cert.gov, 2003).

Cyber Attack sebagai Pengaruh Pembentukan Kebijakan Cyber Security

Dampak yang diakibatkan oleh *cyber attack* telah mempengaruhi kehidupan masyarakat Amerika Serikat di segala aspek. Hal ini menuntut negara untuk menangani permasalahan ini karena menyangkut kehidupan warga negara yang bergantung pada dunia siber. Untuk mengakomodir kemauan publik, diperlukan kebijakan yang bisa menjaga keamanan warga masyarakatnya dari serangan siber yang bisa saja termasuk kejahatan siber. Kebijakan tersebut harus diimplementasikan terhadap warga negara, organisasi, maupun pemerintah untuk bersinergi agar kebijakan yang dibuat bisa tepat sasaran dan dilaksanakan oleh seluruh semua aktor didalamnya. Dalam kasus ini, pubik menentukan kebijakan yang seharusnya dibuat, karena dampaknya dirasakan oleh masyarakat dan hal tersebut terkait dengan kemanan warga negara yang juga lingkup nasional mengenai maslaah searangan siber ini. Maka dari itu, jika dihubungkan dengan teori implementasi kebijakan publik adalah *a model of the policy implemantation procces* yang dikemukakan oleh Donald van Meter dan Carl van Horn , yang meliputi : standar /ukuran dan tujuan kebijakan; sumber-sumber kebijakan ; karakteristik badan/instansi pelaksana ; komunikasi antar organisasi terkait dan kegiatan-kegiatan pelaksanaan; sikap para pelaksana; dan lingkungan ekonomi, sosial, dan politik. Kebijakan *cybersecurity* yang dibuat Amerika Serikat tersebut bisa dijelaskan dengan teori implementasi kebijakan publik tersebut.

Kenaikan Anggaran Cybersecurity

Semakin tingginya tingkat intensitas serangan siber yang ditujukan ke Amerika Serikat dari tahun ke tahun, membuat pemerintah Amerika Serikat semkain serius untuk memberikan porsi lebih terhadap bidang *cyber security* sebagai respon dari serang siber yang dialami Amerika Serikat. Sejak kebijakan *cyber security* dibahas pemerintah secara komprehensif pada 2003 (White House, 2003), alokasi anggaran untuk menjalankan kebijakan ini naik setiap tahunnya. Hal itu juga dampak dari serangan siber yang semakin banyak juga terhadap Amerika Serikat.

Dalam mengimplementasikan sebuah kebijakan, menurut Van Horn dan Van Meter dalam salah satu poinnya dijelaskan jika implementasi kebijakan juga harus memperhatikan lingkungan, entah itu lingkungan sosial, politik, ekonomi, maupun lingkungan yang lain. Dalam hal ini, lingkungan ekonomi menjadi salah satu kunci dalam implementasi kebijakan ekonomi karena dengan alokasi dana yang semakin besar, maka implementasi kebijakan *cybersecruity* diharapkan bisa lebih tepat sasaran.

Angka yang didapat dari tahun 2014 menunjukkan anggaran sebesar 5,8 miliar dollar. Pada 2015, terjadi peningkatan anggaran yang sangat signifikan. Hal itu diketahui dari anggaran *cybersecurity* yang dihabiskan pemerintah federal AS mencapai angka 12 miliar dollar AS. Biaya yang dianggarakan padan tahun 2016 sebesar 14 miliar dollar AS. Di tahun 2017, anggaran *cybersecurity* kembali meningkat dari tahun sebelumnya sebesar 35% atau sekitar 19 miliar dollar AS. Selalu terjadi peningkatan anggaran *cybersecurity* dari tahun ke tahun, menunjukkan sektor *cybersecurity* semakin mendapat perhatian lebih oleh pemerintah AS.

Kebijakan Cybersecurity yang Dibuat Pemerintah Amerika Serikat

Pemerintah AS menunjukkan keseriusannya dalam menjaga sistem keamanan informasi. Hal itu dikarenakan hampir seluruh data yang ada di Amerika Serikat sudah terkomputerisasi dan Amerika Serikat sebagai negara adidaya yang sudah sangat maju teknologinya tentunya rentan dengan serangan siber yang dilakukan oleh pihak lain. Sistem keamanan yang dibangun pemerintah Amerika Serikat mencakup semua aspek vital dalam masyarakat seperti di bidang kesehatan, ekonomi, pendidikan, energi, transportasi, dan lain-lain. Apabila salah satu dari aspek tersebut terdampak serangan siber, maka akan menimbulkan kerusakan sistem.

Melalui perspektif konstruktivisme, keamanan merupakan hasil dari konstruksi sosial karena keamanan bergantung pada aktor yang merasa perlu ada pengamanan dari kejahatan siber, apalagi jika sudah berdampak sampai tingkat negara. Keamanan nasional diakui sebagai kependudukan pemerintah dan tergantung pada kebijakan luar negeri, komunitas intelijen dan kemampuan militer. Namun demikian, hari ini infrastruktur penting dipahami sebagai tanggung jawab bersama di mana pemerintah sendiri tidak dapat menawarkan keamanan yang diperlukan (Eriksson dan Giacomello, 2004). Dengan demikian, mempertahankan keterlibatan aktor swasta, lokal atau individu dalam jaringan keamanan memiliki kepentingan yang sama dengan upaya nasional atau internasional dalam melindungi lingkungan digital. Maka dari itu, pemerintah Amerika Serikat melalui departemen terkait membuat beberapa kebijakan *cybersecurity* dengan tujuan menjaga keamanan nasional yang didalamnya berisi strategi untuk mengatur apa yang seharusnya dilakukan dan koordinasi berbagai sektor demi menjaga keamanan nasional.

Pemerintah Amerika Serikat mulai serius terhadap *cybersecurity* dari Pemerintahan Barack Obama. Tidak hanya keamanan dalam negeri, Pemerintah Amerika Serikat juga menginisiasi penting nya *cybersecurity* terhadap dunia internasional. Walaupun pada 2003 sudah dikeluarkan berupa kebijakan yang mengatur mengenai *cyberspace*, pada saat itu laporan serangan siber terhadap Amerika Serikat belum terlalu berdampak pada pembuatan kebijakan mengenai *cybersecurity* karena serangan siber yang diberitakan tidak sebanyak saat ini. Kebijakan yang dikeluarkan oleh Presiden Bush, *The National Strategy to Secure Cyberspace* berupa kebijakan untuk menjaga sistem keamanan dalam negeri dengan tujuan menjaga obyek vital milik negara dan juga sudah menananmkan pondasi kerjasama internasional dalam membangun kebijakan *global cybersecurity.* (White House, 2003)

Tabel 1 Daftar Kebijakan *Cyber Security* Amerika Serikat

Tahun	Nama Dokumen	Lembaga Penerbit
2003	*The National Strategy to Secure Cyberspace*	Gedung Putih
2009	*Cyberspace Policy Review*	Gedung Putih
2011	*International Strategy for Cyberspace*	Gedung Putih
2011	*Departement of Defense Strategy for Operating Cyberspace*	Departemen Pertahanan Amerika Serikat
2015	*The Departement of Defense Cyber Strategy*	Departemen Pertahanan Amerika Serikat
2016	*Departement of State International Cyberspace Policy Strategy*	Departemen Luar Negeri Amerika Serikat

Sumber : Dewi & Tine, 2016

Dilihat dari tabel di atas, Pemerintah Amerika Serikat menunjukkan keseriusannya terhadap kebijakan *cybersecurity* untuk melindungi keamanan di Amerika Serikat dengan

mengeluarkan beberapa kebijakan mengenai *cybersecurity*. Mulai dari kebijakan yang dikeluarkan presiden Bush pada 2003, pada kebijakan tersebut mengatur mengenai 5 proritas keamanan *cyberspace* nasional. Pertama, mengatur mengenai sistem yang merespon kemananan *cyberspace* nasional. Kedua, mengatur mengenai program untuk mereduksi ancaman dan kerentanan kemananan *cyberspace* nasional. Ketiga, mengenai kesadaran dan program pelatihan kemananan *cyberspace* nasional. Keempat mengenai pengamanan *cyberspace* pemerintahan. Kelima adalah keamanan nasional dan kerjasama keamanan *cyberspace* internasional. Secara keseluruhan kebijakan tersebut untuk skala nasional untuk menjaga infrastruktur vital nasional dan untuk skala internasional dengan melakukan kerjasama dengan negara lain. (White House, 2003)

Dengan dikeluarkannya kebijakan *The National Strategy to Secure Cyberspace* pada 2003, kebijakan *cybersecurity* selanjutnya selalu berpedoman terhadapp kebijakan yang dikeluarkan oleh Presiden Bush, karena poin-poin dalam kebijakan tersebut mewakili apa yang menjadi prioritas dalam berperilaku di dunia siber dan kebijakan selanjutnya merupakan pengembangan dari kebijakan sebelumnya untuk mengimbangi pesatnya perkembangan teknologi yang sangat dinamis.

Dalam melaksanakan strategi kebijakan *cyber security* entah dalam negeri maupun luar negeri, harus mendahulukan kepentingan dalam negeri terlebih dahulu untuk memperkuat pertahanan siber nasional untuk melindungi dari serangan siber yang menyerang data rahasia entah sektor privat maupun pemerintah dan melindungi infrastruktur vital yang menyangkut kehidupan warga negara Amerika Serikat. Undang – undang terkait *cybersecurity* dibuat pemerintah federal Amerika Serikat untuk menjaga kestabilan keamanan siber nasional. Berikut undang – undang terkait *cybersecurity* yang digunakan oleh Pemerintah Federal AS. (1)*Protecting Cyber Networks Act* (PCNA, H.R. 1560) : Undang – undang ini adalah batu loncatan untuk Undang-Undang *Cybersecurity* tahun 2015 karena menetapkan sistem pembagian informasi antara perusahaan swasta dan antara perusahaan swasta dan pemerintah federal. (2) *National Cybersecurity Protection Advancement Act* (NCPAA) : sama seperti PCNA, UU ini menetapkan peran NCCIC yang juga tercantum pada *Cybersecurity Act* 2015. NCCIC dibawah DHS menganalisis infromasi keamanan *cybersecurity* dan berbagai informasi tentang *cybersecurity* dengan sektor pemerintah, publik dan privat. NCCIC juga diberi wewenang untuk bebrbagi informasi dengan pihak swasta. (3) *Cyber Threat Sharing Act* 2015 (CTSA) : diperkenalkan oleh senator Thomas R, untuk menetapkan undang-undang yang memungkinkan perusahaan swasta untuk berbagi informasi ancaman *cyber* dengan entitas swasta dan pemerintah secara lebih baik. Dalam CTSA menempatkan DHS sebagai pusat data sharing ancaman *cyber*. (4) *Cybersecurity Intelligence Sharing and Protection Act* (CISPA) : menyoroti pentingnya kejelasan dalam bahasa legislatif ketika mengacu pada privasi informasi warga negara. Perkembangan undang-undang untuk melindungi perusahaan swasta telah dibawa ke dalam *Cybersecurity Act* tahun 2015 sebagai agenda utama bagi perusahaan swasta untuk menyetujui pembagian informasi secara sukarela. (5) *Cybersecurity Information Sharing Act* (CISA) dan *Cybersecurity Act* 2015 : Undang – undang ini memberikan peraturan tentang bagaimana informasi harus dibagi antara pemerintah lokal, suku, dan federal dan entitas non-federal untuk meningkatkan keamanan dunia maya secara nasional. CISA dan *Cybersecurity Act* tersebut bertujuan untuk memberikan opsi kepada perusahaan swasta untuk berbagi informasi tentang ancaman *cyber* yang potensial. Undang-undang tersebut berfokus terutama pada dua tujuan, memberikan kerahasiaan kepada warga Amerika dan melindungi dan mendorong perusahaan untuk berbagi informasi dengan pemerintah (6) *Cybersecurity National Action Plan* (CNAP) : Presiden Obama merilis *Cybersecurity National Action Plan* pada awal Februari 2016 sebagai sebuah inisiatif untuk memperbaiki pengetahuan *cybersecurity*

warga Amerika dan infrastruktur *cyber* pemerintah AS. Undang – undang tersebut lebih menitikberatkan untuk mendidik warga AS tentang ancaman *cyber* secara personal dan tentang kenaikan anggaran *cybersecurity* menjadi $19 miliar.

Kerjasama Internasional terkait Cyber Security

Amerika serikat tahu jika hanya dengan meningkatkan keamanan nasional saja tidak bisa membendung serangan siber. Diperlukan bantuan dari negara lain untuk membentuk lingkungan siber internasional yang sehat, yang terpercaya dan transparan. Pada 2011, Amerika Serikat membuat strategi *cyber security* internasional. Strategi diplomatik A.S. untuk *cyber security* didasarkan pada kerjasama pembangunan antar negara dan mencapai kesepakatan mengenai norma dan langkah-langkah membangun kepercayaan (*confidence building measures* / CBMs).

Dengan adanya norma yang disepakati oleh sistem internasional, maka akan meningkatkan stabilitas. Budaya politik adalah salah satu konsep paling penting yang membantu kita untuk lebih memahami mekanisme masyarakat internasional. Wendt mengidentifikasi tiga periode berbeda dari budaya politik anarki: budaya Hobbes, budaya Lockean dan budaya Kantian. Dari ketiganya, budaya Kantian aktif mempromosikan kolaborasi dalam sistem internasional. Di sini keamanan satu anggota dianggap sebagai keamanan semua anggotanya. Kepentingan individu atau nasional dipandang sebagai kepentingan semua pemangku kepentingan, sehingga kerjasama dan kemitraan adalah mungkin (Wendt, 1999).

Terlepas dari itu, dengan norma yang disepakati oleh negara – negara setidaknya ada harapan kedepan dalam kemajuan aturan *cyber security*. Amerika Serikat mulai menginisiasi untuk membentuk norma *cyber security* dengan menjalin kesepakatan dengan organisasi keamanan regional di Eropa (OSCE), *ASEAN Regional Forum* (ARF), dan Organisasi Negara-Negara Amerika (OAS), forum Kerjasama Ekonomi Asia Pasifik (APEC), "*London Process*", dan PBB untuk mengembangkan langkah dan norma membangun kepercayaan.

Selain mempromosikan kebijakan *cyber security* ke dunia internasional yang bersifat mulitlateral, Amerika Serikat juga menjajaki kesepakatan mengenani *cyber security* melalui upaya perjanjian bilateral dengan negara – negara lain, seperti : China, Rusia, Kanada, Australia, Jepang, India, Singapura, Arab Saudi, United Arab Emirates, Ukraina, Argentina, Israel. Hal itu dilakukan sebagaimana apa yang tercantum dalam *International Cybersecurity Strategy* tahun 2011 yang salah satunya berisi tentang kerjasama internasional dalam menguatkan sektor pertahanan siber. Isi dari kesepakatan *cyber security* sebagian besar sama yaitu menjalin kepercayaan satu sama lain dan sharing informasi mengenai ancaman siber dan penanganannya. Hal tersebut dilakukan sebagai respon dari *cyber attack* yang didapat oleh Amerika Serikat, seperti yang tercantum dalam dokumen perjanjian bilateral Amerika Serikat dengan negara lain yang didasarkan oleh alasan untuk menghadapi ancaman *cyber.*

Kesimpulan

Cyber attack yang dialami oleh Amerika Serikat mempengaruhi kebijakan publik di Amerika Serikat dan *cyber security* dari dimensi domestik dan internasional. Dari kebijakan publik Amerika Serikat, kebijakan *cyber security* merupakan sebuah kompromi dari *cyber attack* yang akhirnya menghasilkan kebijakan *cybersecurity* dan kenaikan anggaran *cybersecurity* yang disebabkan karena pengaruh lingkungan ekonomi sebagai hasil kompromi kebijakan *cybersecurity* yang semakain kompleks. Perspektif konstruktivisme memandang interaksi yang dihasilkan individu dengan lingkungannya, menghasilkan keamanan nasional yang merupakan hasil dari kompromi aktor didalamnya.

Maka, kebijakan *cybersecurity* dihasilkan dari kompromi aktor yang melihat keadaan lingkungannya dan budaya politik masyarakat internasional menimbulkan kerjasama antar negara sangat dimungkinkan. Beberapa kebijakan *cybersecurity* seperti *Cyberspace Policy Review (2009)* yang dikeluarkan oleh *Departement of Homeland Security* untuk tingkat nasional dan undang- undang dari badan legislatif dan *International Strategy for Cyberspace* (2011) oleh Gedung Putih untuk tingkat internasional merupakan hasil dari kompromi pemerintah Amerika Serikat dengan lingkungan *cyber* Amerika Serikat.

Referensi

18 U.S. Code § 1343 - Fraud by wire, radio, or television https://www.law.cornell.edu/uscode/text/18/1343 (diakses 8 Mei 2018)

2016 Internet Crime Report. Federal Bureau of Investigation. https://pdf.ic3.gov/2016_IC3Report.pdf (diakses 2 April 2018)

Eriksson, Johan and Giampiero Giacomello, International *Relations Theory and Security in the Digital Age*, in *International Studies Association Convention,* Montreal, 2004

Lin, Herbert. *An Evolving Research Agenda in Cyber Policy and Security*. http://cisac.fsi.stanford.edu/content/evolving-research-agenda-cyber-policy-and-security (diakses 14 Maret 2018)

Passas, N., 2003, '*Cross-border crime and the interface between legal and illegal actors*' *Security Journal*, vol. 16(1), pp. 19-38.

Penanggulangan Kejahatan Lintas Negara Teroganisir. https://www.kemlu.go.id/id/kebijakan/isu-khusus/Pages/Penanggulangan Kejahatan-Lintas-Negara-Teroganisir.aspx (diakses 8 Juni 2018)

Syaltout, Mahmud, dkk .2012. Laporan Akhir Kompendium Hukum tentang Kerjasama Internasional di Bidang Penegakan Hukum. Badan Pembinaan Hukum Nasional Kementerian Hukum dan HAM.

Soeparna, Intan Innayatun. 2008. Kejahatan Telematika sebgai Kejahatan Transnasional. Seminar Nasional Hukum Telematika. Universitas Airlangga.

National Strategy for Secure Cyberspace https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (diakses 8 Mei 2018)

Wendt, Alexander, *Social Theory of International Politics*, Cambridge University Press, Cambridge, 1999.