PENGGUNAAN STRATEGI OPERASI KONTRA INTELIJEN DALAM RANGKA MENGHADAPI ANCAMAN SIBER NASIONAL

THE USE OF COUNTER – INTELLIGENCE OPERATION STRATEGY IN COPING WITH CYBER THREATS

Yosua Praditya Suratman[1]

Sekretariat Dewan Analis Strategis
(ypsuratman@gmail.com)

Abstrak – Peningkatan jumlah serangan siber yang terjadi saat ini menandai bahwa Indonesia adalah sasaran empuk bagi aktor kejahatan di dunia siber. Serangan siber dipilih karena jauh lebih efektif dibandingkan serangan konvensional – militer, dan aktornya tidak terlihat. Belum lagi, kapasitas penanganan siber, baik infrastruktur, dana, maupun sumberdaya manusia-nya di Indonesia berbanding terbalik dengan jenis perkembangan serangan siber yang semakin meningkat dalam satu dekade terakhir. Langkah dan strategi intelijen, utamanya kontra intelijen, menjadi salah satu jawaban untuk menangkal dan mendeteksi secara dini serangan tersebutdisampingpemerintah membenahi regulasi dan kebijakan terkait penanganan ancaman siber nasional.

Kata Kunci : siber, kontra-intelijen, keamanan

Abstract – *The increasing number of cyber attacks that occur today indicates that Indonesia is an easy target for crime actors in the cyber world. Cyber attacks are selected because they are far more effective than conventional attacks - the military, and the actors are also invisible. Not to mention, the capacity of cyber handling, both infrastructure, funds, and human resources in Indonesia is inversely proportional compared to the number of cyber attacks in the last decade. Intelligence strategies, primarily counter-intelligence, isthe answer to deter and detect the attacks,while the government fixing the regulations and policies of national cyber threats.*

Keywords: *cyber, counter intelligence, security*

[1] Penulis adalah alumnus Universitas Pertahanan Prodi Manajemen Pertahanan Cohort 4 dan saat ini bekerja sebagai Staf Sekretariat Dewan Analis Strategis sejak 2015 sampai sekarang.

Pendahuluan

Kehadiran ancaman yang semakin kompleks di Indonesia memperlihatkan bahwa dinamika ancaman nir-militer terus berkembang seiring dengan perkembangan waktu dan teknologi. Ancaman siber merupakan salah satu bentuk ancaman nir-militer yang laju pertumbuhannya mengalami peningkatan yang sangat cepat dalam satu dekade terakhir ini. Tidak dapat dipungkiri bahwa kemajuan teknologi siber dengan berbagai inovasi infrastrukturnya semakin menghilangkan batas-batas antar negara. Dunia seakan menjadi lebih sempit dan bahkan kenyamanan dan kemudahan menjadi dua kata kunci dalam suatu pekerjaan baik di organisasi pemerintah maupun swasta. Analisis dan komputerisasi data di sektor pemerintahan, transaksi keuangan di sektor perbankan, manfaat teknologi militer pada alutsista, dan berbagai pekerjaan yang umum dilakukan oleh publik seakan tidak dapat lepas dari eksistensi media *cyberspace,* termasuk internet.Pada tahun 2016, tercatat sekitar 47 persen penduduk dunia sudah menggunakan fasilitas internet, dimana angka ini naik dari 43 persen sebelumnya pada 2015.[2] Angka ini jelas diprediksi akan terus meningkat karena hubungan antara teknologi dan waktu adalah linier.

Menjadi lumrah apabila pemerintah Indonesia saat ini memberikan perhatian yang sangat tinggi terhadap ancaman siber dalam beberapa waktu terakhir. Pada 2016 lalu, tercatat Indonesia menerima sekitar 1,2 juta lebih ancaman siber, serta Indonesia diperkirakan berada di posisi ke-26 secara global yang paling rentan menerima serangan siber.[3] Serangan tersebut umumnya berupa *malware* yang semakin terus bertumbuh, modus pencurian data akun bank, rekening tabungan giro, kartu kredit, *ransomware,* dan data-data penting dari setiap lembaga/ instansi pemerintahan maupun swasta. Artinya semua sektor menjadi rawan akan ancaman siber saat ini. Beberapa fakta tersebut turut menunjukkan bahwa Indonesia merupakan sasaran empuk bagi *cyber-criminal* dunia.Pendekatan intelijen tampaknya menjadi pilihan utama dalam menangkal serangan siber yang terus mengalami perkembangan secara fenomenal dalam satu dekade terakhir. Penggunaan strategi kontra intelijen menjadi salah satu upaya yang perlu dilaksanakan untuk mencegah dan mendeteksi secara dini terhadap segala potensi ancaman siber. Oleh karena itu, dalam penulisan ini, akan dibahas tiga hal terkait tata kelola ancaman siber, yaitu *pertama,* tren peningkatan ancaman siber dalam beberapa waktu terakhir; *kedua,* jenis ancaman siber yang dihadapi Indonesia; dan *ketiga,* analisis kontra intelijen melihat perkembangan ancaman siber nasional.

[2] "47 percent of the world's population now use the Internet, study says," http://www.washingtonpost.com, 22 November 2016, diakses pada 5 Juni 2017.

[3] "Ancaman siber di Indonesia Kian Mengkhawatirkan", http://www.cnnindonesia.com, 8 September 2016, diakses pada 5 Juni 2017.

Tren Peningkatan Ancaman Siber dalam Satu Dekade Terakhir

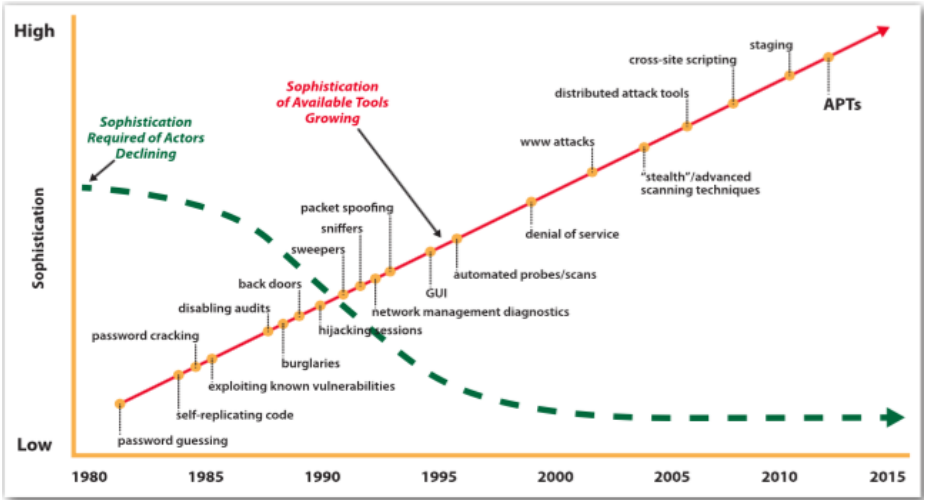
Menurut Smith, ancaman siber telah menjadi sumber dari berbagai ancaman yang tidak hanya menyerang negara/ pemerintah, namun juga meihat organisasi, perusahaan, dan individu menjadi objeknya. Hal ini dilakukan dengan tujuan untuk mendapatkan keuntungan bagi kelompoknya, baik finansial, militer, maupun kepentingan politiknya.[4] Dapat diibaratkan seperti pedang bermata dua, di satu sisi *cyberspace* menawarkan manfaat yang besar namun ketidakpastian akan keamanan turut diberikan juga, entah itu secara sengaja atau tidak. Menurut Setyawan dan Sumari, ancaman siber digunakan karena luang lingkupnya mampu mencuri informasi, penyebaran ide yang bersifat destruktif, maupun serangan terhadap sistem informasi di berbagai bidang, seperti data perbankan maupun jaringan militer dan sistem pertahanan negara. Bahkan survei yang dilakukan oleh *Ponemon Institute* pada 2015 terhadap kurang lebih 1000 pemimpin senior *Information Technology* (IT) dan IT *Security* di berbagai perusahaan dan instansi pemerintah di Amerika, Eropa, Timur Tengah, dan Afrika menyatakan terjadi peningkatan serangan terus menerus pada negara yang semakin canggih diikuti dengan ancaman siber atau terorisme *cyber* dan pembobolan data yang tinggi.[5]

Laju peningkatan ancaman siber pun turut terjadi di kawasan Asia Pasifik, termasuk Indonesia, dimana pada 2015 lalu terdapat peningkatan *host* aktif situs-situs berbahaya sebanyak 61 juta, yang naik dari 41 juta pada 2014 lalu.[6] Beberapa tahun terakhir memang metode yang dilakukan aktor serangan siber sudah berubah sangat drastis, dimana pada masa lampau serangan masih bersifat *visible* dan oportunistik yang menargetkan objek individu dan belum negara. Akan tetapi saat ini cakupan ancaman siber lebih luas dengan target yang sudah terdata dari aktor yang tersembunyi.[7] Hal ini dapat dilihat pada gambar 1.

Berdasarkan gambar 1 tersebut, serangan siber 1980 – 1990 lebih condong pada tujuan yang oportunis untuk mendapatkan keuntungan bagi kelompoknya. Sebut saja seperti *password guessing, self-replacing code,* dan *bulgaries*yang tujuan awalnya memang menyerang perusahaan dan mendapatkan dana. Namun tren ancaman semakin berubah memasuki periode 2005 – 2015, dimana karakteristik ancaman sudah bersifat sangat tersembunyi (*stealth)* dan penggunaan sistemnya pun sudah semakin canggih (*advanced)* dalam menyerang pertahanan suatu

[4] Michael Smith, *Research Handbook on International Law and Cyberspace,* (Cheltenham UK: Edward Elgar Publishing Limited, 2015), hlm. 2.
[5] David Setyawan dan Arwin Sumari, "Diplomasi Pertahanan Indonesia Dalam Pencapaian *Cybersecurity* Melalui ASEAN Regional Forum on *Cybersecurity Initiatives", Jurnal Penelitian Politik,*Vol. 13, No. 1, Juni 2016, Jakarta: Lembaga Ilmu Pengetahuan Indonesia, hlm.3.
[6] "Catatan Trend Micro Tentang Ancaman Siber di Asia Pasifik", Antara News, 17 Juni 2015, diakses pada 7 Juni 2017.
[7] Eric Cole, "Detect, Contain, and Control Cyberthreats", SANS Institute, Juni 2015, dalamhttps://www.sans.org/.../detect-control-cyberthreats-36187, diakses pada 7 Juni 2017, hlm. 4.

Gambar 1. Grafik Evolusi Ancaman Siber dari 1980 - 2015



Sumber: Eric Cole, "Detect, Contain, and Control Cyberthreats", SANS Institute, Juni 2015, dalam https://www.sans.org/.../detect-control-cyberthreats-36187, diakses pada 7 Juni 2017.

negara. Yang lebih berbahaya adalah saat ini serangan siber tidak membutuhkan perlatan yang canggih untuk menyerang, namun cukup dengan seorang SDM yang handal dibelakang layar *laptop*-nya (tools). Aktor ancaman siber saat ini lebih beragam dan banyak.[8]

Jenis-Jenis Ancaman Siber yang Berkembang Saat Ini

Konvensi Budapest pada *EU Convention on Cybercrime November 23th 2001* di Hongaria dibentuk dalam rangka mengingat karakteristik ancaman siber yang bersifar *borderless* dan menggunakan teknologi tinggi sebagai media. Oleh karena itu, kovensi ini turut melihat kebijakan kriminalisasi di bidang teknologi informasi yang harus memperhatikan perkembangan upaya penanggulangan *cybercrime* baik regional maupun internasional dalam rangka harmonisasi dan uniformitas pengaturan *cybercrime*.[9] Dari konvensi Budapest ini terdapat tiga jenis kategori ancaman siber yang dijabarkan sebagai berikut:[10]

1. *Kategori Pertama*

   Ancaman siber adalah kumpulan jenis serangan dimana teknologi informasi dan komunikasi menjadi alat atau senjata utama untuk melakukan kejahatan. Contohnya adalah komputer dan internet dipergunakan sebagai alat dan medium untuk menyebarkan aliran-aliran sesat; telepon genggam yang digunakan untuk mengirimkan

[8] *Ibid.*

[9] Amirulloh, Muhammad et al., "Laporan Kajian EU Conventional on Cybercrime Dikaitkan Dengan Upaya Regulasi Tindak Pidana Teknologi Informasi" ,(Jakarta: Laporan Puslitbang Badan Pembinaan Hukum Nasional Departemen Hukum dan Hak Asasi Manusia Republik Indonesia, 2009), hlm. 4.

[10] Prof. Richardus Eko Indrajit, "Enam Aspek Menjaga dan Melindungi Dunia Maya", ID-SIRTI (Internet and Infrastructure/Coordination Center) Indonesia, dalam http://www.idsirtii.or.id/doc/IDSIRTII-Artikel6_aspek_menjaga_dan_melindungi_dunia_maya.pdf, hlm.5, diakses pada 7 Juni 2017.

pesan-pesan atau sms untuk menipu calon korban; dan *electronic mail* dipakai sebagai sarana untuk mengirimkan gambar-gambar atau video bernuansa pornografi.

2. *Kategori Kedua*

   Ancaman siber adalah kumpulan dimana komputer atau teknologi informasi menjadi sasaran pusat serangan dari pelaku tindak kejahatan, seperti, *pertama,*Melakukan transaksi keuangan fiktif dalam sebuah sistem perbankan berbasis internet (*e-banking);kedua,* mematikan atau memacetkan kerja-kerja sebuah jejaring internet secara remote; dan *ketiga,* menyebarkan virus-virus untuk mengganggu kinerja komputer-komputer tertentu.

3. *Kategori Ketiga*

   Ancaman siber ini ditujukan bagi peristiwa yang bertujuan merusak (termasuk memodifikasi dan memfabrikasi) data atau informasi tersimpan didalam media perangkat teknologi informasi. Serangan pada kategori ini berupa:*pertama,* merubah isi sebuah situs tanpa sepengetahuan pemiliknya; *kedua,* mengambil kumpulan *password* atau informasi lengkap kartu kredit sekelompok individu untuk disalahgunakan atau diperjualbelikan; dan *ketiga*, merusak sistem basis data utama sehingga informasi di dalamnya menjadi tidak dapat terbaca atau diakses secaa normal dan lain sebagainya.

Ketiga jenis ancaman di atas menunjukan bahwa subjek ancaman siber tidak hanya ditujukan kepada pemerintah, tetapi termasuk individu, kelompok masyarakat, dan perusahaan. Dampaknya jelas besar meskipun belum ada takaran menghitung konversi kerugian yang diakibatkan oleh *cyberspace*, namun yang pasti ancaman jenis dan tren ancaman ini dipastikan akan meningkat terus seiring dengan perkembangan teknologi. Menurut Brenner & Clarke, ada tiga alasan mengapa jenis ancaman siber saat ini lebih dipilih dari pada serangan konvensional, seperti militer pada umumnya.

Pertama, mengembangkan kapasitas serangan siber memerlukan biaya yang lebih sedikit dibandingkan pengembangan kapasitas perang militer di abad ke-21. Biaya *cyberwarfare* mencakup pelatihan dan pembiayaan perangkat keras serta lunak lebih murah dibandingkan biaya perang konvensional. *Kedua,* penggunaan aktornya jauh lebih sedikit dibandingkan perang milier, serta pelaksanaanya dapat dilakukan dari jarak yang jauh. Artinya, perang siber tidak lagi melihat jarak, waktu, dan jumlah personil, namun selama sistem itu bisa diserang maka suatu negara dengan mudah dapat melakukan serangan siber. Aktornya pun tidak terbatas apakah negara atau non-negara, selama mereka mampu menyerang sistem yang dituju, entah itu milik negara atau perusahaan

atau kelompok. *Ketiga,* serangan siber sangat mudah untuk disponsori tanpa mengetahui siapa aktor sesungguhnya, entah itu negara A, negara B, organisasi A, organisasi B, atau bahkan hanya segelintir kelompok/individu.[11]

Tantangan Ancaman Siber di Indonesia dan Kebijakannya Saat ini

Tidak dapat dipungkiri bahwa kondisi mendesak akan ancaman siber di Indonesia dapat dikatakan dalam kondisi yang kritis. Dengan jumlah penduduk pengguna internet sebanyak 132 juta pada 2016, bukan tidak mungkin Indonesia menjadi sasaran empuk serangan siber dari *state* dan *non-state actor*. Penjabaran pengguna internet di Indonesia dapat dilihat sebagai berikut:[12] (1) 67,2 juta orang atau 50,7 persen mengakses melalui perangkat genggam dan komputer; (2) 63,1 juta orang atau 47,6 persen mengakses dari *smartphone;* dan *(3)* 2,2 juta orang atau 1,7 persen mengakses hanya dari komputer. Selain itu, dari survei yang dipresentasikan oleh APJII (Asosiasi Penyelenggara Jaringan Internet Indonesia), tercatat bahwa sekitar 86,3 juta orang atau 65 persen dari angkat total pengguna internet tahun ini berada di Pulau Jawa. Sedangkan sisanya adalah sebagai berikut: (1) 20,7 juta atau 15,7 persen di Sumatera; (2) 8,4 juta atau 6,3 persen di Sulawesi; (3) 7,6 juta atau 5,8 persen di Kalimantan; (4) 6,1 juta atau 4,7 persen di Bali dan NTB; dan (5) 3,3 juta atau 2,5 persen di Maluku dan Papua.

Melihat data di atas dan dibandingkan dengan kesiapan pemerintah dalam mengatur keamanan siber nasional, maka tidak heran apabila masih banyak mendapat kritik sebagian besar kelompok masyarakat. Menurut Adriyanti terdapat lima kebijakan *cyber-security* di Indonesia saat ini yang mendapat perhatian penuh, yaitu:[13]

A. Kepastian Hukum

   Legalitas penanganan kejahatan di dunia *cyber* masih lemah, karena meski telah ada peraturan perundang-undangan yang melarang bentuk penyerangan atau perusakan sistem elektronik dalam UU Informasi dan Transaksi Elektronik No.11 Tahun 2008, namun belum terdapat peraturan perundang-undangan yang mengatur secara khusus *cyber crime* dan penanganannya. Padahal di sisi lain, bentuk kejahatan dunia *cyber* semakin meningkat dan pola kejadiannya sangat cepat sehingga sulit untuk ditangani oleh aparat penegak hukum.

B. Teknis dan Tindakan Prosedural

   Penangganan kejahatan *cyber* yang masih parsial dan tersebar serta tidak adanya koordinasi yang baku

[11] Susan Brenner dan Leo Clarke, "Civilians in Cyberwarfare: Conscripts,*Vanderbilt Journal of Transnational Law,* Vol. 43, hlm. 1011, 2011, University of Dayton School of Law, 2011, hlm. 3-4.

[12] "2016, Pengguna Internet di Indonesia Capai 132 Juta", dalam http://tekno.kompas.com/read/2016/10/24/15064727/2016.pengguna.internet.di.indonesia.capai.132.juta, 24 Oktober 2016, diakses pada 18 Juli 2017.

[13] Handrini Ardiyanti, "Cyber Security dan Tantangan Pengembangannya di Indonesia", *Jurnal Politica,* Vol. 5 No.1, Juni 2014, hlm. 99 - 101.

dalam penanganan masalah *cyber-security*. Rendahnya kesadaran akan adanya ancaman *cyber attack* yang berdampak melumpuhkan infrastruktur vital. Contohnya adalah sistem radar penerbangan di bandara internasional Soekarno Hatta yang beberapa kali mengalami gangguan.

C. Struktur Organisasi

Penanganan *cyber-security* dalam kerangka pertahanan negara hingga saat ini masih bersifat sektoral dan belum terkoodinasi serta belum terpadu. Meskipun pada akhirnya, pemerintah berhasil membentuk Badan Siber dan Sandi Negara Melalui Peraturan Presiden (Perpres) Nomor 53 Tahun 2017 tentang Badan Siber dan Sandi Negara.

D. Capacity Building

Diperlukan pembinaan SDM tentang arti pentingnya *cyber-security* guna meningkatkan pemahaman langkah-langkah preventif dalam menangkal segala tindak *cyber crime.*

E. Kerjasama Internasional

Penguatan kerjasama internasional dengan organisasi regional maupun internasional dalam rangka penanggulangan *cyber crime.* Kerjasama dalam rangka penanggulangan *cyber crime* yang telah dilakukan Indonesia pada skala regional maupun global.

Berdasarkan uraian di atas, maka dapat dilihat bagaimana kondisi saat ini dan pendekatan yang sudah dilakukan oleh Pemerintah. Berdasarkan artikel yang ditulis Handrini,[14] pendekatan yang sudah ada masih belum maksimal apabila dibandingkan dengan tingkat intensitas ancaman dan variasinya. Apalagi pengguna internet di Indonesia sangatlah banyak. Maka dari itu penguatan pendekatan kontra intelijen menjadi salah satu cakupan pembahasan yang memang harus dilakukan instansi intelijen bersama stakeholder terkait lainnya.

Pendekatan Kontra Intelijen *Cyber* dalam Menghadapi Ancamannya

Sebelumnya perlu dipahami terlebih dahulu fungsi intelijen berdasarkan UU yang berlaku di Indonesia. Mengacu pada UU No. 17 Tahun 2011 Tentang Intelijen Negara, maka penjabaran fungsi intelijen itu adalah fungsi penyelidikan, pengamanan, dan penggalangan. Dimana kegiatan kontra intelijen sendiri masuk kedalam kategori fungsi penggalangan yang didalam UU Intelijen tertulis "serangkaian kegiatan yang dilakukan secara terencana dan terarah untuk mencegah dan/atau melawan upaya, pekerjaan, kegiatan Intelijen, dan/atau Pihak Lawan yang merugikan kepentingan dan keamanan nasional."[15] Ada empat aspek kegiatan utama intelijen, yaitu kontra intelijen, spionase, propaganda, dan sabotase. Menurut Soeripto dalam

[14] *Ibid.*

[15] Lihat UU No. 17 Tahun 2011 Tentang Intelijen Negara Pasal 6 ayat 3.

Praditya, kontra intelijen sendiri adalah adalah kegiatan *preemptive* yang bersifat rahasia. Tujuannya adalah untuk mempersempit ruang gerak, menangkal, menggagalkan, dan menghancurkan operasi intelijen lawan. Penyelenggaraan kontra-intelijen terbagi menjadi dua, yaitu pasif dan aktif, sebagaimana dijelaskan dibawah:[16]

1. *Kontra-Intelijen Pasif*

   Mencakup empat hal. *Pertama*, pemeliharaan rahasia dengan membatasi jumlah orang yang mengetahui rahasia, dimana semakin sedikit jumlah orang yang mengetahui rahasia maka peluang keberhasilannya akan semakin besar. *Kedua*, pengamanan informasi dengan segala cara untuk mencegah lawan mengetahui informasi. *Ketiga*, menyaring segala jenis kegiatan dan hubungannya dalam gerakan musuh. *Keempat*, melakukan pengelabuan (kamuflase) dengan mengubah bentuk sesuatu atau memberikan info yang salah kepada musuh. *Kelima*, penyembunyian (*concealment)* gerakan intelijen supaya tidak diketahui oleh musuh.

2. *Kontra – Intelijen Aktif*

   Kontra-intelijen aktif lebih mengarah kepada *empowerment* kegiatan intelijen untuk memperoleh informasi dari pihak lawan dengan cara mengeliminasi berbagai ancaman, tantangan, hambatan, dan gangguan. Kontra-intelijen aktif berperan sebagai *counter* penetrasi, *counter* infiltrasi, *counter spionase*, *counter* pembuat sabotase, dan penggunaan kamuflase khusus di wilayah lawan, daerah musuh, atau bakal musuh. Misalnya *counter espionage* (kontra-spionase) harus betul-betul secara aktif mengamati terus-menerus setiap gejala yang muncul, sampai kasus itu terungkap. Sementara itu, kontra-pengintaian adalah usaha untuk melakukan pengintaian terhadap pihak lawan. Pengintaian dalam hal ini fokus kepada upaya mengamankan, mempertahankan, dan melindungi setiap kegiatan intelijen dari musuh. Yang menjadi pembeda utama dalam kontra-intelijen aktif adalah kegiatannya yang lebih bersifat menyerang, ketimbang bertahan. Lebih lanjut, menurut Rahardjo, pembagian kontra-intelijen di atas dapat dibagi kembali menjadi bagian vertical dan horizontal sebagaimana bagan (lihat bagan 1).

Berdasarkan bagan di atas, baik kontra intelijen pasif dan aktif, idealnya tidak dapat terpisahkan karena pelaksanaannya harus dilakukan secara sinergis. Yang membuat perbedaan adalah masing-masing misi, baik ofensif maupun defensif, yang menunjukan masing-masing tindakan untuk menangkal musuh. Sementara itu, pembagian secara vertikal membedakan operasi kontra intelijen menjadi aktif

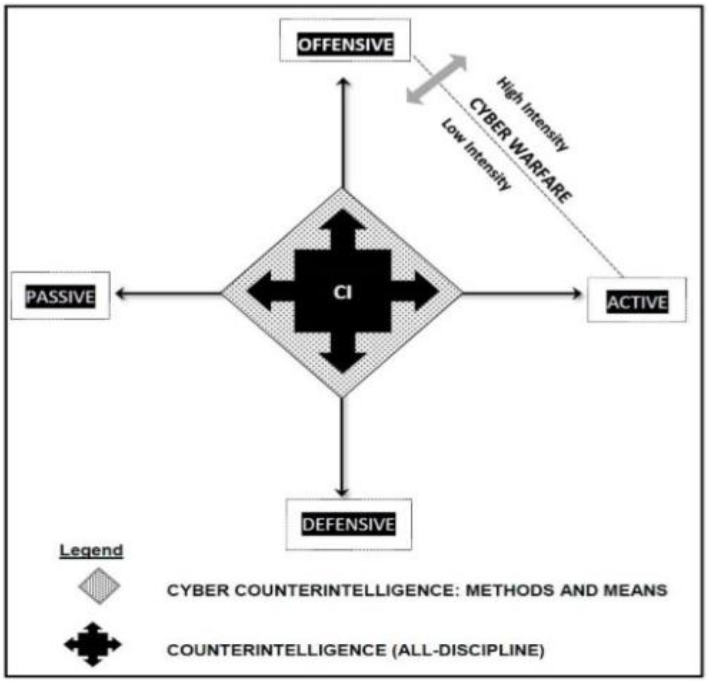
[16] Yosua Praditya, *Keamanan di Indonesia*, (Jakarta: Nadi Pustaka, 2016), hlm. 246–247.

Bagan 1. Matriks Kontra Intelijen

Mode Defensif Memblokir akses lawan dan mengumpulkan informasi mengenai lawan	
Defensif Pasif Memblokir Akses Lawan Terhadap Informasi	**Defensif Aktif** Menyelidiki aksi lawan menggunakan pengawasan, umpan, agen ganda, mata-mata, atau *electronic tapping*
Mode Ofensif Bertujuan untuk memanipulasi, mengontrol, dan menggagalkan aksi Lawan	
Ofensif Pasif Membiarkan lawan melihat informasi palsu (melihat sesuatu yang tidak ada, atau sesuatu yang sala, kamuflase)	**Ofensif Aktif** Secara langsung mengirimkan informasi yang salah melalui aksi rahasia

Sumber: Beer dan Basie dalam Elsa Vinietta, http://budi.rahardjo.id/files/courses/2016/EL6115-2016-23215130-Report.pdf, diakses pada 7 Juni 2017, hlm. 5.

Gambar 2. Kontra Intelijen Cyber Terintegrasi



Sumber: Beer dan Basie dalam Elsa Vinietta, http://budi.rahardjo.id/files/courses/2016/EL6115-2016-23215130-Report.pdf, diakses pada 7 Juni 2017.

atau pasif berdasarkan intensitas respon yang diberikan. Tindakan pasif dilakukan dengan melindungi sambil menunggu atau membiarkan operasi lawan tetapi dengan respon minim, sementara tindakan aktif dilakukan dengan melakukan respons-respons tertentu sesuai dengan situasi dan kondisi.[17]Lebih lanjut, apabila dalam melihat keterkaitan ancaman siber dengan kontra intelijen *cyber* maka dapat dilihat pada gambar (lihat gambar 2).

[17] Elsa Vinietta, "Strategi Operasi Kontra Inteijen Cyber Sebagai Upaya Peningkatan Ketahanan Negara Indonesia", dalam http://budi.rahardjo.id/files/courses/2016/EL6115-2016-23215130-Report.pdf, diakses pada 7 Juni 2017, hlm. 6.

Tabel 1. Penjelasan Kontra Intelijen Cyber Terintegrasi

No	Metode	Alur Mekanisme Operasi
1	Strategi Satu - Kontra Intelijen *Active Offensive High Intensity*	Tujuan Operasi -> menyerang; Musuh -> sudah diketahui; Prioritas -> diutamakan;
2	Strategi Dua - Kontra Intelijen *Passive Offensive High Intensity*	Tujuan Operasi -> menyerang; Musuh -> sudah diketahui; Prioritas -> tidak diutamakan;
3	Strategi Tiga - Kontra Intelijen *Active*Offensive *Low* Intensity	Tujuan Operasi -> menyerang; Musuh -> tidak diketahui; Strategi -> ofensif
4	Strategi Empat - Kontra Intelijen *Passive Offensive Low Intensity*	Tujuan Operasi -> menyerang; Musuh -> sudah diketahui; Strategi -> pasif
5	Strategi Lima - Kontra Intelijen *Active Defensive High Intenstity*	Tujuan Operasi -> bertahan; Informasi -> Sangat krusial; Resiko ancaman -> ada (tinggi).
6	Strategi Enam - Kontra Intelijen *Active Defensive Low Intensity*	Tujuan Operasi -> bertahan; Informasi -> Sangat krusial; Resiko ancaman -> rendah
7	Strategi Tujuh - Kontra Intelijen *Passive Defensive High Intensity*	Tujuan Operasi -> bertahan; Informasi -> Tidak krusial; Resiko ancaman -> ada (tinggi)
8	Strategi Delapan - Kontra Intelijen *Passive Defensive Low Intensity*	Tujuan Operasi -> bertahan; Informasi -> Tidak krusial; Resiko ancaman -> rendah

Sumber: Diolah oleh penulis dari Elsa Vinietta, "Strategi Operasi Kontra Inteijen Cyber Sebagai Upaya Peningkatan Ketahanan Negara Indonesia", dalam http://budi.rahardjo.id/files/courses/2016/EL6115-2016-23215130-Report.pdf, diakses pada 7 Juni 2017.

Pada gambar di atas, intensitas serangan siber dikategorikan *low and high intensity*. Dengan mengacu pada metode kontra intelijen yang terintegrasi maka penjabarannya dapat dilihat pada tabel (lihat tabel 1)[18]

Berdasarkan tabel di atas, maka akan terlihat bagaimana masing-masing pendekatan kontra intelijen *cyber* terintegrasi terhadap ancaman siber. Dengan menggunakan tabel ini maka kita dapat menganalisis sumber daya, termasuk manusia, finansial, dan alat (*tools*) dapat digunakan secara efektif dan efisien. Perlu diketahui dalam menangani ancaman siber, sumber daya yang dimiliki perlu disesuaikan dengan bentuk dan tingkat intensitas ancamannya, sehingga pemerintah tidak mengeluarkan biaya yang berlebih dibandingkan realita. Dapat juga biaya menangani ancaman siber tidak perlu menggunakan dana yang berlimpah asalkan SDM yang digunakan diberikan *tools* yang tepat.

[18] *Ibid,* hlm. 10.

Analisis Kontra Intelijen *Cyber* dalam Menghadapi Ancaman Siber Nasional

Dari penjabaran tabel di atas, maka penulis memiliki pisau analisis untuk melihat bagaimana ancaman siber dihadapi sesuai dengan metodenya. Berikut adalah penjabarannya:

1. Kontra Intelijen *Active Offensive High Intensity*

   Pendekatan yang dilakukan dapat dilakukan dengan dua hal, yaitu perang siber dan penggunaan agen virtual. Indonesia sendiri dianggap masih tertinggal dari perang siber antar negara, karena Indonesia justru menjadi pasar atau "sasaran empuk" negara lain. Biasanya negara-negara lain melakukannya dengan menawarkan jasa gratis kepada masyarakat Indonesia agar dengan sukarela dan senang hati memberikan informasi pribadi melalui sosial medial. Padahal cara-cara seperti ini dikategorikan sebagai perang siber (aktif ofensif) yang dilakukan suatu negara kepada Indonesia. Baik pegawai negeri sipil (PNS), aparat militer-keamanan, termasuk warga sipil pasti memberikan informasinya secara detail kepada email dan sosial media.[19] Sementara untuk ketersediaan agen-agen virtual di Indonesia, penyebarannya masih tersebar dan justru malah terkadang menyerang instansi-instansi milik pemerintah, Polri, dan perusahaan BUMN. Padahal para *hacker* seperti ini dapat digunakan oleh aparat untuk diberdayakan membantu ketahanan siber nasional dari ancaman para peretas. Sementara di negara-negara besar, seperti AS dan Rusia, menjadi hal yang lumrah apabila para *hacker* diberdayakan untuk menyerang sistem keamanan-pertahanan negara lain. Pada intinya strategi kontra-intelijen ini bersifat menyerang, objeknya sudah diketahui (biasanya sistem IT negara lain), dan menjadi sesuatu yang diprioritaskan.

2. Kontra Intelijen *Passive Offensive High Intensity*

   Strategi ini pasif (tidak menyerang) karena tujuan utamanya adalah untuk mengumpulkan informasi dalam mendeteksi ancaman/ musuh siber. Di Indonesia sendiri pada akhirnya mensahkan Badan Siber dan Sandi Negara (BSSN) berdasarkan Perpres No. 53 Tahun 2017 oleh Presiden Joko Widodo. Tugas dari BSSN adalah melaksanakan keamanan siber secara efektif dan efisien dengan memanfaatkan, mengembangkan, dan mengonsolidasikan semua unsur yang terkait dengan keamanan siber. Dalam melaksanakan tugas tersebut, BSSN menyelenggarakan fungsi antara lain: penyusunan, pelaksanaan, pemantauan dan

[19] Pernyataan Ketua Lembaga Riset Cyber dan Komunikasi (Communication and Information System Security Research Centre/CISSReC) Pratama D Persada, "Perang Siber Sudah Menjadi Ancaman Serius", dalam http://www.republika.co.id, 17 september 2016, diakses pada 8 Juni 2017.

evaluasi kebijakan teknis di bidang identifikasi, deteksi, proteksi, penanggulangan, pemulihan, pemantauan, evaluasi, pengendalian protek *e-commerce*, persandian, penapisan, diplomasi siber, sentra informasi, dukungan mitigasi, pemulihan penanggulangan, kerentanan, insiden dan/atau serangan siber.[20] Kehadiran BSSN akan sangat membantu pemerintah untuk mengumpulkan segala bentuk informasi penting dan rahasia, serta diharapkan dapat membantu aparat hankam-intelijen dalam melakukan kontra-spionase di dunia siber.

3. Kontra Intelijen *Active Offensive High Intensity*

   Strategi ini dilakukan dengan sistem menyerang meskipun musuh (objek) belum diketahui karena intensitas ancaman sangat tinggi. Misalnys, ancaman-ancaman *ransomware* yang menyerang fasilitas publik umumnya tidak diketahui siapa aktornya, akan tetapi hal ini tidak membuat pemerintah bersikap pasif. Baru-baru ini Indonesia dikejutkan dengan serangan *ransomware wannacry,* dimana menurut Ketua *Indonesia Security Incident Response Team on Internet Infrastructure* (Id-SIRTII) M. Salahuddin mengungkapkan potensi penyebaran *ransomwarewannacry* masih akan terbuka di Indonesia karena Indonesia adalah pasar yang sangat rawan. *Ransomeware* jenis ini nantinya akan meminta tebusan sebesar Rp 4 juta dalam bentuk mata uang virtual (*cryptocurrency*) Bitcoin yang dikirimkan ke alamat dompet digital sang penjahat cyber.[21] Virus *ransomeware* ini ditengarai memanfaatkan *tool* senjata siber milik dinas intel Amerika Serikat, NSA, yang pada April lalu dicuri dan dibocorkan oleh kelompok *hacker* bernama Shadow Broker. Tool yang bernama "EnternalBlue" tersebut memanfaatkan celah keamanan di sistem operasi Windows lewat eksekusi remote code SMBv1.[22] Meskipun pemerintah sulit mengetahui informasi secara detail akan *Broken Shadow* yang menyebarkan virus tersebut, tetapi pemerintah telah mengetahui bahwa virus tersebut bocor dari NSA. Oleh karena itu, strategi pemerintah adalah bagaimana nanti menghadapi virus atau tool senjata yang berpotensi bocor dari NSA dan disalahgunakan oleh kelompok-kelompok *hacker.*

4. Kontra Intelijen *Passive Offensive Low Intensity*

   Strategi menyerang dilakukan secara pasif mengingat target/objek sudah diketahui dan tujuan masih tetap fokus untuk mengumpulkan informasi. Yang membuat perbedaan

[20] Lihat PP No. 53 Tahun 2017 Tentang BSSN pada pasal 1 ayat (3).

[21] "Intel AS di Balik 'Ransomware' yang menyerang rumah sakit Indonesia," 13 Mei 2015, http://www.kompas.com, diakses pada 8 Juni 2017.

[22] "Begini Cara Menangkal 'ransomware' wannacray", http//www.kompas.com, 13 mei 2017, diakses pada 8 Juni 2017.

adalah intensitasnya yang rendah. Pemerintah, dalam hal ini koordinasi antara Kementerian Informatika bersama BSSN dan aparat hankam-intelijen perlu memetakan potensi-potensi ancaman yang tidak terlalu tinggi. Tujuannya adalah supaya di masa mendatang pemerintah tidak direpotkan dengan ancaman yang sudah bertransformasi menjadi ancaman yang memiliki dampak besar. Sebagai contoh, 10 tahun lalu, pemerintah belum menyadari dampak sosial yang begitu besar dari penggunaan sosial media dan internet oleh publik, dimana saat ini setiap orang dapat menyuarakan pendapat politiknya selama tidak menyalahi peraturan yang berlaku. Akan tetapi faktanya, penyebaran *hatespeech,* pesan provokatif, dan berita *hoax* seakan sulit dibendung, dan faktanya hal ini tendensi menjadi perang *proxy* negara lain untuk menjatuhkan Indonesia. Taksonomi konflik yang terjadi sangat erat kaitannya dengan perang *proxy* dan penyebarannya sangat terbantu oleh dunia internet/ sosial. Artinya, pemerintah 10 tahun lalu gagal melakukan kontra intelijen *passive offensive* untuk ancaman yang intensitas rendah (sosial media/internet), namun faktanya, sekarang ancaman tersebut sudah bertansformatif dan memiliki daya destruktif yang sangat luar biasa untuk lingkungan sosial Indonesia.

5. Kontra Intelijen *Active Defensive High Intensity*

   Pada strategi ini mengombinasikan dua hal, yaitu *hardware* dan *software*. Pada sisi *hardware*, jelas Indonesia perlu didukung kehadiran infrastruktur siber yang memadai. Saat ini, Indonesia ditengarai rugi triliunan rupiah setiap tahun, salah satunyakarenatidakmemperhatikan keamanan sistem komunikasi, termasuk infrastrukturnya. Contohnya dalam perihal *illegal logging* dan *illegal fishing* yang selalu terjadi karena sistem komunikasi yang terkoordinasi dengan baik dan rendahnya infrastruktur tekonologi. Selain itu, minimnya infrastruktur dapat berpengaruh kepada rentannya pembobolan data masyarakat Indonesia yang menggunakan e-KTP (diestimasi sebanyak 180 juta penduduk).[23] Sementara pada *software,* pemerintah melalui kehadiran BSSN mampu meng-*upgrade* sistem keamanan IT pada masing-masing lembaga/ instansi yang ada. Penerapan sistem pemerintahan yang berbasis elektronik (E-Government) menjadi objek yang perlu diperbaiki, karena Indonesia tetap dikhawatirkan menjadi sasaran empuk bagi para aktor kejahatan siber.

[23] Wawancara koran Republika dengan Ketua Lembaga Riset Keamanan Cyber dan Komunikasi (CISSReC), dengan tema "Indonesia Butuh Lembaga Pertahanan Siber", dalam http://www.republika.co.id, diakses pada 8 Juni 2017.

6. Kontra Intelijen *Active Defensive Low Intensity*

   Pada strategi ini sebenarnya sama dengan strategi sebelumnya, yaitu mengombinasikan dua hal, yaitu *hardware* dan *software.* Namun pelaksanaannya ditujukan kepada ancaman yang tingkat intensitasnya rendah. Dalam hal ini pemerintah tidak boleh lagi memandang remeh dampak kecil dari ancaman siber, karena jenis ancaman ini dipastikan bertransformasi dalam waktu yang relatif singkat. Resiko tingkat ancaman yang rendah tidak membuat Pemerintah tidak memikirkan strategi instalasi *hardware* dan *software* yang dibutuhkan sebagai langkah preventif di masa mendatang. Dapat diambil contoh, ketika lembaga CISSReC *(Communication and Information System Security Research)* menyarankan kepada pemerintah untuk membangun sistem database paspor terintegrasi, sehingga dapat melakukan pengecekan paspor online terlebih terhadap paspor ganda di Indonesia ataupun di negara lain.[24] Memang jenis ancaman terhadap kepemilikan paspor ganda saat ini intensitasnya belum begitu banyak dibanding KTP ganda, tetapi tidak berarti pemerintah tidak melakukan apa-apa.

7. Kontra Intelijen *Passive Defensive High Intensity*

   Dalam strategi ini yang dikedepankan adalah pertahanan fisik, baik itu untuk sistem keamanan IT aparat hankam dan intelijen, serta fasilitas Kementerian lainnya. Tujuannya untuk mempertahankan fasilitas sistem dari ancaman pencurian data, baik *hardware* dan *software,* atau pun serangan *malware* yang dapat mematikan piranti keras IT milik pemerintah. Selain itu, strategi ini fokus dengan rutinitas pemeriksaan personel IT, dalam hal penggunaan dan pengukuran personil, serta tidak meninggalkan vitalnya *chain management* dalam sektor IT itu sendiri. Tujuan akhirnya adalah untuk mendapatkan keamanan yang diharapkan. Dapat mengambil contoh pada sisi pertahanan udara misalnya, dimana untuk memperkuat ADIZ (*Air Defense Identification Zone)* TNI AU membutuhkan penambahan 12 radar udara.[25] Dimana penambahan radar tersebut tentu diikuti dengan penambahan jumlah personel dan pelatihannya. Radar merupakan peralatan yang merupakan infrastruktur fisik yang dibutuhkan ADIZ yang tidak lagi hanya bersifat parsial berupa lingkaran kecil perkepulauan (Jawa, Sumatera, Kalimantan, dan lain-lain), tetapi sudah berbentuk lingkaran besar

[24] "Indonesia diusulkan Segera Bangun Sistem Paspor Terintegrasi," dalam https://www.cissrec.org/, 14 September 2016, diakses pada 9 Juni 2017.

[25] "TNI AU Perkuat Zona Identifikasi Pertahanan Udara," dalam http://nasional.kompas.com/, 7 April 2017, diakses pada 9 Juni 2017.

mencakup ruang udara dari Sabang sampai Merauke.

8. Kontra Intelijen *Passive Defensive High Intensity*

   Strategi ini sama dengan yang sebelumnya (no. 7), yaitu penekanan kepada pembangunan sarana fisik beserta SDM dan pemeliharaannya. Namun yang membedakannya adalah strategi ini ditujukan kepada jenis-jenis ancaman yang intensitasnya masih rendah. Pada satu dekade yang lalu, masih banyak negara yang belum terpikir untuk membangun database penyimpanan informasi di awan (*cloud),* dimana AS merupakan satu-satunya negara yang sudah memikirkan hal itu. Mereka berpikir data lebih aman disimpan di awan (*cloud)* dengan bantuan teknologi satelit dibandingkan disimpan di piranti keras yang rawan dicuri, terutama untuk keperluan militer dan intelijen mereka.

Kesimpulan

Tren laju peningkatan ancaman siber sudah meningkat sangat pesat, dimana aktornya pun bisa dilakukan oleh siapa saja. Sementara itu, Indonesia dikategorikan sebagai negara yang paling rawan dan merupakan sasaran paling empuk di lingkungan Asia. Penetrasi ancaman siber yang begitu dahsyat telah terjadi, baik itu pencurian data atau pun pengrusakan sistem informasi milik pemerintah dan swasta. Ancaman siber menjadi pilihan bagi aktornya karena tidak berbiaya tinggi, tidak membutuhkan banyak personel, tidak terlihat, dan ia mampu dikendalikan dari jarak yang sangat jauh, bahkan lintas negara dan benua. Oleh karena itu, pemerintah, dalam hal ini aparat keamanan-intelijen perlu melakukan strategi operasi kontra intelijen yang tepat dalam menangani ancaman siber yang terus berkembang. Strategi kontra intelijen menjadi salah satu pilihan utama karena ia bersifat rahasia serta mampu mempersempit ruang gerak ancaman siber dari berbagai lini. Langkah dan strategi intelijen menjadi garda terdepan dalam menghadapi serangan siber yang diprediksi akan terus meningkat di masa mendatang.

Daftar Pustaka

Buku

Praditya, Yosua. 2016. Keamanan di Indonesia. Jakarta: Nadi Pustaka.

Smith, Michael. 2015. *Research Handbook on International Law and Cyberspace.* Cheltenham UK :Edward Elgar Publishing Limited.

Jurnal

Ardiyanti, Handrini. 2014. "Cyber Security dan Tantangan Pengembangannya di Indonesia". *Jurnal Politica.* Vol. 5. No.1. Juni.

Brenner, Susan dan Clarke Leo. 2011. "Civilians in Cyberwarfare: Conscripts,*Vanderbilt Journal of Transnational Law.* Vol. 43. University of Dayton School of Law.

Setyawan, David dan Sumari, Arwin. 2016. "Diplomasi Pertahanan Indonesia Dalam Pencapaian *Cybersecurity* Melalui ASEAN Regional Forum on *Cybersecurity Initiatives". Jurnal Penelitian Politik.* Vol. 13. No. 1. Juni. Jakarta: Lembaga Ilmu Pengetahuan Indonesia.

Laporan

Amirulloh, Muhammad et al. 2009."Laporan Kajian EU Conventional on Cybercrime Dikaitkan Dengan Upaya Regulasi Tindak Pidana Teknologi Informasi". Jakarta: Laporan Puslitbang Badan Pembinaan Hukum Nasional Departemen Hukum dan Hak Asasi Manusia Republik Indonesia.

Undang-Undang dan Peraturan Pemerintah

UU No. 17 Tahun 2011 Tentang Intelijen Negara Pasal 6 ayat 3.

PP No. 53 Tahun 2017 Tentang BSSN pada pasal 1 ayat (3).

Website

"Ancaman siber di Indonesia Kian Mengkhawatirkan", http://www.cnnindonesia.com, 8 September 2016, diakses pada 5 Juni 2017.

"Begini Cara Menangkal 'ransomware' wannacray", http//www.kompas.com, 13 mei 2017, diakses pada 8 Juni 2017.

Cole, Eric, "Detect, Contain, and Control Cyberthreats", SANS Institute, Juni 2015, dalam https://www.sans.org/.../detect-control-cyberthreats-36187, diakses pada 7 Juni 2017.

"Catatan Trend Micro Tentang Ancaman Siber di Asia Pasifik", http://www.antaranews.com, 17 Juni 2015, diakses pada 7 Juni 2017.

Indrajit, Richardus Eko, "Enam Aspek Menjaga dan Melindungi Dunia Maya", dari ID-SIRTI (Internet and Infrastructure/ Coordination Center) Indonesia, http://www.idsirtii.or.id/doc/IDSIRTII-Artikel6_aspek_menjaga_dan_melindungi_dunia_maya.pdf, diakses pada 7 Juni 2017.

"Intel AS di Balik 'Ransomware' yang menyerang rumah sakit Indonesia," 13 Mei 2015,http://www.kompas.com, diakses pada 8 Juni 2017.

"Indonesia Butuh Lembaga Pertahanan Siber", dalam http://www.republika.co.id, diakses pada 8 Juni 2017.

"Indonesia diusulkan Segera Bangun Sistem Paspor Terintegrasi," dalam https://www.cissrec.org/, 14 September 2016, diakses pada 9 Juni 2017.

Persada, Pratama D, "Perang Siber Sudah Menjadi Ancaman Serius", dalam http://www.republika.co.id, 17 september 2016, diakses pada 8 Juni 2017.

"TNI AU Perkuat Zona Identifikasi Pertahanan Udara," dalam http://nasional.kompas.com/, 7 April 2017, diakses pada 9 Juni 2017.

Vinietta, Elsa, "Strategi Operasi Kontra Inteijen Cyber Sebagai Upaya Peningkatan Ketahanan Negara Indonesia", dalam http://budi.rahardjo.

id/files/courses/2016/EL6115-2016-23215130-Report.pdf, diakses pada 7 Juni 2017.

"47 percent of the world's population now use the Internet, study says," http://www.washingtonpost.com, 22 November 2016, diakses pada 5 Juni 2017.

"2016, Pengguna Internet di Indonesia Capai 132 Juta", dalam http://tekno.kompas.com/read/2016/10/24/15064727/2016.pengguna.internet.di.indonesia.capai.132.juta, 24 Oktober 2016, diakses pada 18 Juli 2017.