Jurnal Kajian Stratejik Ketahanan Nasional

Volume 3
Number 1 *JKSKN Volume 3 No 1 2020*

Article 1

5-15-2020

Kontra Intelijen Aksi Spionase Siber Terhadap Anggota Democratic National Committee Menjelang Pemilihan Presiden AS Tahun 2016

Basuki Erwin Setiyadi
Kajian Ketahanan Nasional SKSG Universitas Indonesia, basuki.erwin@ui.ac.id

Makmur Keliat
FISIP Universitas Indonesia, makmur.keliat@gmail.com

P-ISSN: 2620-7419 E-ISSN: 2776-1827
Jurnal Kajian Stratejik Ketahanan Nasional, Vol. 3, No.1, 2020

Kontra Intelijen Aksi Spionase Siber Terhadap Anggota *Democratic National Committee* Menjelang Pemilihan Presiden AS Tahun 2016

Basuki Erwin Setiyadi[1], Makmur Keliat[2]
basuki.erwin@ui.ac.id, makmur.keliat@gmail.com

Abstract

This research is a case study of cyber espionage conducted against the member of Democratic National Committee (DNC) towards the 2016 US presidential election, caused Hillary Clinton's email leaked and published by WikiLeaks. It indicates the intelligence activities have entered into cyberspace and can disrupt the national ressilience, so it is necessary to do counterintelligence as an effort to maintain the cyber security. This research uses qualitative approach, data collected from interviews and literature study. The purposes of this research are (1) to determine the threat level of cyber espionage conducted against DNC, (2) counterintelligence methods against the threat, (3) and Indonesian Government Strategy against cyber threat. This research use counterintelligence theory, threat analysis theory, and SWOT analysis. The results of this research are (1) the threats analysis of cyber espionage indicating the threat agent has high level threat, it could harms the national interest and affect the national ressilience, (2) cyber counterintelligence are conducted by two ways i.e., defensive counterintelligence to block and detect enemy's access activity, and offensive counterintelligence to collect informations, manipulate, control, and thwart enemy's action, (3) Indonesian Government Strategies against cyber threat are strengthening legal measure, technical measure, organizational measure, capacity building, and cooperation.
Keywords *: counterintelligence; cyber espionage; democratic national committee; email; hillary clinton.*

Penelitian ini adalah studi kasus mengenai peristiwa spionase siber kepada anggota *Democratic National Committee* (DNC) menjelang pilpres AS tahun 2016, yang mengakibatkan kebocoran *email* Hillary Clinton yang dirilis oleh WikiLeaks. Hal tersebut menunjukkan bahwa aktivitas intelijen telah berkembang ke ranah siber dan dapat menganggu ketahanan nasional, sehingga perlu dilakukan upaya kontra intelijen untuk menjaga keamanan siber. Penelitian ini menggunakan pendekatan kualitatif dengan pengumpulan data melalui wawancara dan studi literatur. Penelitian ini bertujuan untuk mengetahui (1) level ancaman dari aktivitas spionase siber kepada DNC, (2) metode kontra intelijen terhadap ancaman tersebut, dan (3) strategi Indonesia untuk menghadapi ancaman siber. Teori yang digunakan adalah Teori Kontra Intelijen dan Teori Ancaman, serta analisis SWOT. Hasil dari penelitian ini adalah (1) analisis ancaman spionase siber menunjukkan bahwa pelaku merupakan sebuah ancaman dengan level tinggi sehingga membahayakan kepentingan negara dan dapat mempengaruhi ketahanan nasional, (2) kontra intelijen siber dilakukan melalui dua metode yaitu, kontra intelijen defensif yang bertujuan untuk memblokir dan mendeteksi terhadap aktivitas akses lawan dan kontra intelijen ofensif bertujuan untuk mengumpulkan informasi, memanipulasi, mengontrol, dan menggagalkan aksi lawan, (3) strategi Indonesia untuk menghadapi ancaman siber adalah dengan melakukan penguatan baik pada segi regulasi, teknik, organisasi, kemampuan, dan kerjasama.
Kata kunci : *democratic national committee; email; hillary clinton; kontra Intelijen; spionase siber*

[1] Alumni Program Studi Kajian Ketahanan Nasional Universitas Indonesia
[2] Dosen Fakultas Ilmu Sosial dan Politik Universitas Indonesia

P-ISSN: 2620-7419 E-ISSN: 2776-1827
Jurnal Kajian Stratejik Ketahanan Nasional, Vol. 3, No.1, 2020

1. Pendahuluan

Transformasi teknologi informasi dan komunikasi (TIK) yang semakin progresif telah menjadikan ancaman yang dihadapi suatu negara menjadi lebih kompleks, mengubah pemahaman terhadap kekuatan (*power*) atau kedaulatan dari suatu negara, tidak hanya dilihat dari seberapa besar kekuatan militer atau ekonomi yang dimilikinya, tetapi juga tergantung dari kekuatan sibernya. Siber (*cyber*) adalah lingkungan kompleks akibat interaksi manusia, perangkat lunak dan layanan di internet dengan menggunakan perangkat teknologi dan jaringan yang terhubung dengannya, yang tidak terdapat dalam bentuk fisik.[3]

Aktivitas intelijen telah berkembang ke ranah siber (*cyberspace*), salah satunya yaitu spionase siber (*cyber espionage*). Spionase siber adalah kegiatan yang dilakukan pemerintah asing atau kriminal jaringan (*criminal networks*) dengan mencuri informasi atau memalsukan barang (*goods*) dengan cara yang mengikis kepercayaan masyarakat terhadap layanan internet.[4]

CyberEdge Group melakukan survei mengenai tren jenis ancaman siber pada tahun 2016 kepada 10 negara di Amerika Utara, Eropa, Asia Pasifik, dan Amerika Latin. Skala terendah ditunjukkan dengan nilai 1 dan skala 5 paling tinggi, terjadi tren peningkatan pada tiap jenis ancaman siber yang menyerang organisasi pada rentang tahun 2014-2016 dengan *Malware* dan *Phising*/*spearphising* menempati posisi paling tinggi[5].

Peristiwa spionase siber menggunakan s*pearphising email* yang terjadi pada tahun 2016 adalah serangan siber yang menargetkan Komite Nasional Demokrat atau *Democratic National Committee (*DNC).[6] Pelaku menyerang sejumlah target yang berada disekitar Hillary Cinton dan berhasil memasuki akun *email* John Podesta, ketua kampanye pemenangan Hillary Clinton pada Pemilihan Presiden (pilpres) Amerika Serikat (AS). Sekitar bulan Oktober tahun 2016, WikiLeaks merilis *email* antara Hillary Clinton dengan John Podesta.

Dampak yang dialami AS sebagai negara berdaulat atas kejadian tersebut tidak hanya berpengaruh pada reputasi sebagai negara adidaya, namun juga menjatuhkan wibawa pemerintah dan negara. Stabilitas menjelang pemilu presiden terganggu, keamanan nasional dalam keadaan yang membahayakan. Muncul indikasi bahwa ada negara lain yang berusaha untuk mempengaruhi hasil pemilu.

Indonesia sebagai negara besar dengan wilayah yang cukup luas dan dengan jumlah pengguna internet yang mencapai 132,7 juta pada tahun 2016 [7], tidak menutup kemungkinan memperoleh ancaman yang serupa. Terlebih lagi dengan adanya *Five Power Defence Arrangements* (FPDA) yang beberapa anggotanya adalah negara tetangga yang wilayahnya dekat dengan Indonesia seperti Malaysia, Singapura, Australia, dan Selandia Baru.[8]

Dari kasus tersebut, perlu dilakukan upaya kontra intelijen terhadap kegiatan spionase siber lawan sebagai tindakan yang membahayakan kepentingan negara. Serangan siber adalah bentuk ancaman terhadap Ketahanan Nasional suatu negara yang perlu diantisipasi. Peneliti mengkaji tentang (1) tingkat ancaman spionase siber kepada DNC

[3] ISO/IEC 27032:2012. *Information technology – Security techniques – Guidelines for cybersecurity*
[4]Klimburg, A. (2012). *National Cyber Security Framework Manual*. NATO Cooperative Cyber Defence Centre of Excellence. Hlm 16.
[5] CyberEgde Group. *2016 Cyberthreat Defense Report*.
[6] *Internet Security Threat Report*, Volume 22. (2017). Symantec. Hlm 16
[7]Asosiasi Penyelenggara Jasa Internet Indonesia. (2016). *Infografis Penetrasi & Perilaku Pengguna Internet Indonesia. Survey 2016*.
[8]https://nasional.sindonews.com/read/1154663/14/panglima-tni-beberkan-potensi-ancaman-yang-mengintai-indonesia-1478861976. Tanggal tayang 11 November 2016. Tanggal akses 3 April 2017.

https://scholarhub.ui.ac.id/jkskn/vol3/iss1/1
DOI: 10.7454/jkskn.v3i1.10032

P-ISSN: 2620-7419 E-ISSN: 2776-1827
Jurnal Kajian Stratejik Ketahanan Nasional, Vol. 3, No.1, 2020

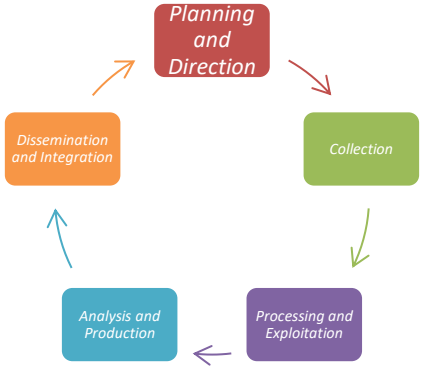
yang mengakibatkan kebocoran isi *email* Hillary Clinton, (2) kontra intelijen terhadap spionase siber terkait kasus tersebut, dan (3) strategi Indonesia dalam mengahdapi ancaman siber.

2. Tinjauan Teoritis

2.1.Intelijen

Secara universal pengertian Intelijen meliputi[9]: (1) pengetahuan, yaitu informasi yang sudah diolah sebagai bahan perumusan kebijakan dan pengambilan keputusan; (2) organisasi, yaitu suatu badan yang digunakan sebagai wadah yang diberi tugas dan kewenangan untuk menyelenggarakan fungsi dan aktivitas intelijen; dan (3) aktivitas, yaitu semua usaha, pekerjaan, kegiatan, dan tindakan penyelenggaraan fungsi penyelidikan, pengamanan, dan penggalangan.

Aktivitas intelijen akan menghasilkan produk-produk intelijen yang terdiri dari tiga jenis, yaitu : *current intelligence*, *basic intelligence*, dan *intelligence estimates*.[10] Intelijen sebagai aktivitas adalah serangkaian kegiatan/proses untuk menghasilkan pengetahuan/*knowledge.* Sebagai bagian dari aktivitas intelijen, proses intelijen meliputi serangkaian prosedur atau langkah yang membentuk suatu siklus intelijen.[11] Sebagai aktivitas, siklus intelijen dapat digambarkan sebagai berikut[12] :



Gambar 1. Siklus Intelijen

2.2.Kontra Intelijen

Kontra Intelijen adalah usaha nasional untuk mencegah badan intelijen asing dan gerakan politik yang dikendalikan kekuatan serta kelompok asing, yang sering kali didukung oleh badan intelijen lainnya agar tidak melakukan infiltrasi ke dalam lembaga negara, struktur angkatan bersenjata dan Departemen Sipil di dalam maupun luar negeri melalui kegiatan spionase, subversi dan sabotase. Apalagi targetnya dapat mencakup warga negara atau penduduk yang tidak memiliki afiliasi secara formal dengan pemerintah [13]

Kontra Intelijen dikategorikan menjadi defensif kontra intelijen yang terdiri dari (1) pencegahan, dan (2) deteksi; dan ofensif kontra intelijen yang terdiri dari (1) deteksi, (2) desepsi (muslihat), dan (3) menetralisir upaya oposisi untuk mengumpulkan informasi.[14]

2.3.Cyber Intelligence

Definisi mengenai *Cyber Intelligence* (intelijen siber) : *Intelligence, surveillance, and*

[9] Penjelasan Undang-Undang No.17 Tahun 2011 tentang Intelijen Negara
[10] Widjajanto, A. Lay, C. Keliat, M. (2006). Velox et Exatus. Universitas Indonesia. Hlm. 48.
[11] Prunckun, H. (2015). *Scientific Methods of Inquiry for Intelligence Analysis*, Rowman & Littlefield. Hlm.6.hlm.7.
[12] Vardangalos, G. (2016). *Cyber Intelligence and Cyber Counterintelligence (CCI) : General Definitions and Principles*. Center for International Strategic Analyses (KEDISA). Hlm 5.
[13]Johnson, William R. 1994. Thwarting Enemies at Home and Abroad: How to Be a Counterintelligence Officer. Bethesda, Md.: Stone Trail Press. (2) Zuehlke, Arthur A. 1980. What is Counterintelligence? In: Intelligence Requirements for the 1980s: Counterintelligence. Godson, Roy S; ed. Washing-ton D.C.: National Strategy Information Center. (3) Olson, James M. 2001. A Never-Ending Necessity. The Ten Commandments of counterintelligence. Washington D.C.: Studies in Intelligence
[14]Prunckun, H. (2012). *Counterintelligence Theory and Practice*. USA : Rowman & Littlefield. Hlm. 25.

P-ISSN: 2620-7419 E-ISSN: 2776-1827
Jurnal Kajian Stratejik Ketahanan Nasional, Vol. 3, No.1, 2020

reconnaissance (ISR) dalam ruang siber dapat didefinisikan sebagai "kemampuan untuk memberikan analisis kolaboratif, intelijen terpadu, dan kemampuan ISR PCPAD (*planning and collecting, collection, processing and exploitation, analysis and production, dissemination*) untuk memungkinkan operasi dunia maya.[15] Dalam ruang siber, Menurut Kamal Jabbour, *cyber agility* bukan hanya sekedar kecepatan analisis, namun juga antisipasi terhadap perilaku dan dampak di masa depan, dan penetapan tingkat pertahanan *real-time* yang efektif.[16]

2.4.Cyber Counterintelligence

Cyber Counterintelligence (CCI) didefinisikan sebagai semua upaya yang dilakukan oleh satu organisasi intelijen untuk mencegah musuh, organisasi intelijen musuh atau organisasi kriminal dalam mengumpulkan dan menghimpun informasi digital sensitif atau informasi intelijen tentang mereka melalui komputer, jaringan dan peralatan terkait. CCI adalah langkah-langkah untuk mengidentifikasi, menembus (*penetrate*), atau menetralisir operasi komputer yang menggunakan senjata siber sebagai sarana dan mekanisme untuk mengumpulkan informasi. Fokus tidak hanya pada intrusi, tapi juga pada maksud intrusi dan metode pengumpulan (*tradecraft*) yang digunakan.[17]

Langkah-langkah kontra intelijen siber dapat dilakukan dengan dua metode, yaitu [18] :

a. Defensif kontra intelijen siber, dapat diartikan sebagai tindakan yang dilakukan untuk mengidentifikasi dan mengatasi gangguan (instrusi) musuh sebelum terjadi serta upaya untuk mengidentifikasi dan meminimalkan lanskap ancaman. Contohnya yaitu mencegah akses yang tidak sah ke fasilitas dan sistem, penyusupan *malware*, penanganan terhadap gangguan dan malfungsi keamanan, investigasi dan merespon terhadap gangguan keamanan, melaksanakan asesmen terhadap celah kerawanan dan *penetration testing.*

b. Ofensif kontra intelijen siber yaitu interaksi dengan lawan untuk secara langsung mengumpulkan informasi tentang operasi pengumpulan intelijen lawan atau untuk menipu (*deceive*) mereka. Contohnya yaitu pemanfaatan *sock puppets* (atau *virtual agent*) di forum *online* untuk mengumpulkan informasi tentang operasi intelijen lawan (kemampuan, korban, taktik, dll.), membuat agen musuh menjadi agen ganda untuk melakukan penyusupan. Selain itu, *honeypot* dapat digunakan untuk menipu lawan dan menampilkan informasi palsu.

Tujuan metode defensif kontra intelijen adalah untuk memblokir akses lawan dan mengumpulkan informasi mengenai lawan. Sedangkan metode ofensif kontra intelijen bertujuan untuk memanipulasi, mengontrol, dan menggagalkan aksi lawan.[19]

2.5.Analisis Ancaman

Proses untuk mengukur tingkat ancaman yaitu dengan melakukan kodifikasi hasil wawancara dan sumber literatur, kemudian dikaitkan dengan kategori-kategori dari ancaman tersebut. Selanjutnya diukur dengan skala yang telah ditentukan sehingga akan mendapatkan angka koefisien. Apabila angka koefisien ini adalah 1 (satu) atau bernilai rendah maka dapat dikatakan bahwa tingkat

[15]Hurley, M. M. Conceptualizing Cyber Intelligence, Surveillance, and Reconnaisance. *Air & Space Journal*. USAF. 2012. Hlm. 14.
[16] Jabbour, K. *Cyber Vision and Cyber Force Development*, Strategic Studies Quarterly 4, no. 1 (Spring 2010): 65, http://www.au.af.mil/au/ssq/2010/spring/spring10.pdf.
[17] Vardangalos, G. (2016). *Cyber Intelligence and Cyber Counterintelligence (CCI) : General Definitions and Principles*. Center for International Strategic Analyses (KEDISA). hlm. 6.
[18] Ibid, hlm. 7.
[19]Beer, P. D. von Solms Basie, S. (2013). The Case for cyber counterintelligence. *Adaptive Science and Technology (ICAST)*. Pretoria.

https://scholarhub.ui.ac.id/jkskn/vol3/iss1/1
DOI: 10.7454/jkskn.v3i1.10032

P-ISSN: 2620-7419 E-ISSN: 2776-1827
Jurnal Kajian Stratejik Ketahanan Nasional, Vol. 3, No.1, 2020

ancamannya dapat diabaikan. Namun apabila nilainya medium atau tinggi, maka menjadikan keharusan untuk melakukan kontra intelijen untuk dapat menangkal ancaman tersebut ataupun mengurangi ancaman tersebut. Analisis ancaman dilakukan dengan berdasarkan tingkat ancaman dengan 4 (empat) komponen yang menyusun ancaman. Dengan persamaan, Ancaman = [Kemampuan = (Sumber Daya + Pengetahuan)] + [Niat = (Keinginan + Harapan)].[20]

3. Metode Penelitian

Penelitian ini menggunakan pendekatan yang bersifat kualitatif. Jenis penelitian yang yang digunakan adalah studi kasus terhadap peristiwa spionase siber terhadap anggota DNC sehingga mengakibatkan kebocoran isi email Hillary Clinton yang dirilis oleh WikiLeaks pada tahun 2016. Teknik pengumpulan data dilakukan dengan studi pustaka, wawancara, dan dokumentasi. Narasumber pada penelitian ini yaitu (1) Kepala Pusat Teknologi Informasi dan Komunikasi Kementerian dan Perwakilan beserta staf, Kemenlu, (2) Pejabat dan staf pada Deputi Bidang Pengamanan Persandian, Lemsaneg, (3) Anggota Biro Analis, Baintelkam Polri, (4) *Chairman* CISSReC, (5) Koordinator Fungsi Komunikasi KBRI di Washington DC. Data yang telah diperoleh selanjutnya diproses dengan teknik triangulasi data untuk melakukan pemeriksaan keabsahan/validitas data, selanjutnya dilakukan teknik analisis data dengan menggunakan reduksi data, kemudian dilakukan analisis ancaman dan analisis SWOT, dan pada tahap akhir dilakukan penarikan kesimpulan.

4. Hasil Penelitian

4.1. Spionase Siber *Democratic National Committee*

Menurut laporan *National Intelligence Council*, mengenai dugaan aktivitas dan tujuan Rusia pada pemilu tahun 2016 berdasarkan analisis proses dan insiden siber, tujuan Rusia adalah untuk meruntuhkan kepercayaan publik terhadap proses demokrasi di AS, merendahkan Hillary, dan membahayakan elektabilitas dan potensinya menjadi presiden.[21] Hillary juga dianggap sebagai ancaman sehingga Rusia berusaha meruntuhkan legitimasinya.[22]

Berdasarkan laporan bersama antara *Department of Homeland Security* (DHS) dan *Federal Bureau of Investigation* (FBI), *Russian civilian and military intelligence Services* (RIS) diduga membobol dan mengeksploitasi jaringan dan *endpoints* yang terkait dengan pilpres AS, serta berbagai entitas Pemerintah, sektor politik dan sektor swasta. Pemerintah AS menghubungkan aktivitas kejahatan siber yang dilakukan oleh RIS sebagai GRIZZLY STEPPE.[23] Operasi siber tersebut menggunakan metode *spearphishing* yang menargetkan organisasi pemerintah, entitas infrastruktur kritis, *think tank*, universitas, dan organisasi politik.

Pemerintah AS mengkonfirmasikan bahwa dua aktor RIS yang berbeda berpartisipasi melakukan intrusi ke dalam partai politik AS. Kelompok pertama, yang dikenal sebagai *Advanced Persistent Threat* (APT) 29, yang kedua dikenal sebagai APT28.[24] APT29 dikenal juga sebagai COZYBEAR atau The Dukes, terindikasi bekerja atas perintah *Federal Security Service* (FSB).[25] APT28 terindikasi

[20] Prunckun, H, (2015).*Scientific Methods of Inquiry for Intelligence Analysis*. Rowman & Littlefield. Hlm. 284-292.

[21] Intelligence Community Assesment (CIA, FBI, NSA). (2017). *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*. National Intelligence Council. USA. hlm. 1.

[22]http://tekno.kompas.com/read/2016/12/13/10220067/peretas.rusia.di.balik.kemenangan.trump. Tanggal tayang 13 Desember 2016. Tanggal akses 15 Desember 2017.

[23]Departement of Homeland Security and Federal Bureau of Investigation. (2016*). Joint Analysis Report : GRIZZLY STEPPE – Russian Malicious Cyber Activity*. Reference Number: JAR-16-20296A. Hlm. 1

[24] Ibid, hlm. 2.

[25]https://www.nytimes.com/interactive/2016/07/27/us/politics/trail-of-dnc-emails-russia-hacking.html. Tanggal tayang 6 Januari 2017. Tanggal akses 12 Desember 2017.

P-ISSN: 2620-7419 E-ISSN: 2776-1827
Jurnal Kajian Stratejik Ketahanan Nasional, Vol. 3, No.1, 2020

bekerja untuk Badan Intelijen Militer Rusia yaitu GRU.[26]

Pada musim panas tahun 2015, sebuah *spearphishing* APT29 mengarahkan *email* yang berisi tautan berbahaya ke lebih dari 1.000 penerima, termasuk beberapa korban dari Pemerintah AS. APT29 menggunakan domain yang sah yang terkait dengan organisasi dan institusi pendidikan AS, menanam *malware* dan mengirim *spearphishing email*. APT29 berhasil membobol salah satu partai politik AS. Setidaknya satu target individu mengaktifkan tautan dengan membuka lampiran yang berisi *malware*.

Pada musim semi tahun 2016, APT28 membobol partai politik yang sama, lagi-lagi melalui *spearphishing* kepada target. *Spearphishing email* mengelabuhi penerima untuk mengubah *password* mereka melalui domain *webmail* palsu yang berjalan pada infrastruktur operasional APT28. Dengan menggunakan data rahasia yang didapat, APT28 dapat memperoleh akses dan mencuri konten, yang kemungkinan mengarah pada pengambilan informasi dari beberapa anggota senior partai. Pemerintah AS menilai bahwa informasi tersebut telah bocor ke pers dan diungkapkan kepada publik.[27] Nama alias kelompok peretas tersebut yang terkait dengan RIS yaitu COZYBEAR, Crouching Yeti, Fancy Bear, dan Sofacy.[28] APT28 dikenal juga dengan sebutan Fancy Bear atau Sofacy. APT28 disebut sebagai kelompok besar yang memiliki tim pengembang perangkat lunak (*software development teams*), dapat beroperasi dalam skala yang luas, melakukan beberapa operasi berbeda secara serentak, dan memiliki tingkatan persiapan serangan (*levels of preparation before attack*) yang lebih tinggi dibanding dengan *state-sponsored hackers* Tiongkok[29]. APT28 alias Fancy Bear juga menjadikan lembaga militer dan politik di Ukraina dan Georgia, serta instalasi NATO sebagai target serangan siber.[30]

4.2.Teknik Spionase Siber

Berdasarkan sumber dari laporan dinas intelijen dan media AS, teknik serangan yang dilakukan kepada DNC adalah menggunakan teknik *spearphising email*, salah satu jenis teknik *social engineering*. *Spearphising email* adalah penipuan *email* atau komunikasi elektronik yang ditujukan kepada individu, organisasi atau bisnis tertentu. Meski sering bermaksud mencuri data untuk tujuan jahat, kriminal siber mungkin juga berniat memasang *malware* di komputer pengguna yang ditargetkan.[31]

APT29 melakukan *spearphishing* memanfaatkan tautan *web* yang mengandung *malicious dropper* (semacam program jahat yang sulit dideteksi oleh *antivirus*), setelah dieksekusi, kode tersebut mengirimkan *Remote Access Tools* (RAT) dan menghindari sistem deteksi menggunakan berbagai teknik dan jalur koneksi terenkripsi. APT28 dikenal dapat memanfaatkan *domain* yang sangat mirip dengan domain yang sah dan menipu calon korban untuk memasukkan data kredensial (*username*, *password*) yang sah. Aktor APT28 menggunakan URL yang dipersingkat untuk serangan *email spearphishing*. Begitu APT28 dan APT29 memiliki akses terhadap korban, kedua kelompok tersebut melakukan pengambilan data dan menganalisis informasi untuk mendapatkan nilai intelijen. Aktor-aktor ini menyiapkan infrastruktur operasional untuk mengaburkan infrastruktur sumber, *domain*

[26]http://www.chicagotribune.com/news/nationworld/ct-russian-hack-grizzly-steppe-20161230-story.html. Tanggal tayang 30 Desember 2016. Tangggal akses 12 Desember 2017.

[27] Departement of Homeland Security and Federal Bureau of Investigation. (2016*). Joint Analysis Report : GRIZZLY STEPPE – Russian Malicious Cyber Activity*. Reference Number: JAR-16-20296A. Hlm. 1

[28] Ibid. Hlm. 4.

[29]http://www.wired.co.uk/article/how-russian-hackers-work. Tanggal tayang 11 Januari 2017. Tanggal akses 12 Desember 2017.

[30]https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html. Tanggal tayang 13 Desember 2016. Tanggal akses 12 Desember 2017.

[31] https://www.kaspersky.com/resource-center/definitions/spear-phishing. Tanggal akses 20 Desember 2017.

https://scholarhub.ui.ac.id/jkskn/vol3/iss1/1
DOI: 10.7454/jkskn.v3i1.10032

P-ISSN: 2620-7419 E-ISSN: 2776-1827
Jurnal Kajian Stratejik Ketahanan Nasional, Vol. 3, No.1, 2020

host dan *malware* untuk organisasi yang ditargetkan, menetapkan *node command and control*, dan mendapatkan data kredensial dan informasi berharga lainnya dari target mereka.

Metode *spearphising* yang dilakukan oleh APT28 yaitu membangun operasional infrastruktur, dengan membuat kiriman yang seolah-olah sah dan dikenali oleh target. Kemudian mengirimkan *email* dengan tautan berbahaya (*malicious link*) kepada target. Serangan berhasil jika target tertipu dengan melakukan klik pada tautan yang telah dikirim melalui *email*. APT28 menipu target dengan membuat tampilan *website* yang terlihat sah (*legitimate*). Kemudian, APT28 mengumpulkan informasi kredensial dari target. Informasi kredensial tersebut kemudian digunakan untuk mengakses sistem target dan melakukan instalasi file berbahaya. Setelah itu, APT28 melakukan penjelajahan di sistem dan melakukan pengambilan data-data penting untuk kemudian dikirim kembali ke sistem atau infrastruktur operasional milik APT28.

Dalam kasus ini, APT28 mengirimkan pemberitahuan yang seolah-olah merupakan kiriman dari pihak yang sah kepada para target melalui *email*–bahwa ada yang telah berhasil *login* ke akun *email* target dan meminta target untuk mengganti *password* dengan mengirimkan tautannya. Setelah APT28 memeperoleh *username* dan *password* milik target, kemudian melakukan *login* ke *email* target. Setelah berhasil masuk ke akun *email* target, APT28 dapat mengakses isi *email* tersebut.

4.3.Dampak Spionase Siber

Sebanyak 50.547 dokumen *email* dirilis oleh WikiLeaks yang dikirim dari–dan kepada *server email* pribadi Hillary ketika menjabat sebagai Menteri Luar Negeri. Data e*mail* tersebut dalam rentang waktu antara 30 Juni 2010 hingga 12 Agustus 2014. Sejumlah 7.570 dokumen dikirimkan oleh Hillary kepada staff ahli, para dubes dan pejabat penting AS.[32] *Email* tersebut didapatkan dari akun Ketua Kampanye Tim Sukses (Timses) Hillary Clinton, yaitu John Podesta. *Email* dari akun Podesta, yang juga mantan Kepala Staf Gedung Putih, membocorkan sejumlah informasi, mulai dari isi seminar berbayar yang disampaikan Hillary ke bankir di Wall Street hingga strategi tim kampanye Hillary menghadapi skandal *email* yang tidak henti mendera Hillary.

Juru Bicara Hillary, Glen Caplin, menuduh Rusia berkomplot dengan Wikileaks dan pendirinya Julian Assange untuk memengaruhi hasil Pemilu Presiden AS.[33] Hillary juga berpendapat perpaduan WikiLeaks dan operasi Rusia telah menyebabkan kerugian baginya dalam persaingan ketat di pilpres. Hillary memberikan contoh bagaimana publikasi WikiLeaks dilakukan untuk memberikan dampak maksimum atau mengalihkan perhatian dari skandal kampanye Trump. Misalnya, pada tanggal 7 Oktober pukul 16.00, surat kabar Washington Post menerbitkan rekaman *Hollywood Access* 2005 berisi komentar Donald Trump yang dianggap tidak sopan tentang pelecehan seksual terhadap wanita. Kurang dari satu jam kemudian, WikiLeaks merilis lebih dari 2.000 *email* John Podesta. Hillary mengatakan dibukanya *email* ini telah menepiskan dampak rekaman tersebut.[34] Selain itu, kasus skandal penggunaan *email server* pribadi (non dinas) saat menjabat sebagai Menteri Luar Negeri, dan pernyataan dari Direktur FBI James Comey (menjabat hingga Mei 2017) mengenai bagaimana Hillary menangani informasi rahasia juga merupakan

[32]https://wikileaks.org/clinton-emails/?q=iraq%7Cbaghdad%7Cbasra%7Cmosoul. Tanggal akses 1 Maret 2017.
[33]http://internasional.kompas.com/read/2016/10/08/13321811/wikileaks.bocorkan.ribuan.e-mail.ketua.kampanye.hillary.clinton. Tanggal tayang 8 Oktober 2016. Tanggal akses 22 Desember 2017.
[34]http://internasional.republika.co.id/berita/internasional/global/17/08/24/internasional/abc-australia-network/17/10/16/oxwbns366-hillary-tuding-wikileaks-dan-rusia-bantu-kemenangan-trump. Tanggal tayang 16 Oktober 2017. Tanggal akses 22 Desember 2017.

P-ISSN: 2620-7419 E-ISSN: 2776-1827
Jurnal Kajian Stratejik Ketahanan Nasional, Vol. 3, No.1, 2020

sesuatu yang berdampak pada hasil pilpres.[35]

Terkait dengan serangan siber kepada DNC, Presiden Amerika Serikat saat itu, Barack Obama resmi menyampaikan serangkaian sanksi untuk Rusia atas dugaan intervensi atau serangan yang dilakukan terhadap pilpres AS. Sanksi yang diberikan merupakan respons yang penting dan tepat menyusul tindakan membahayakan kepentingan negara serta melanggar norma-norma internasional. Sanksi tersebut diantara adalah :[36]

a. AS mengusir 35 diplomat Rusia dan menutup dua kompleks Rusia di New York dan Maryland.
b. Sanksi ekonomi dengan membekukan aset dan menghentikan sistem finansial terhadap *Main Intelligence Directorate* (GRU) dan *Federal Security Service*, *Special Technology Center* di St. Peterseburg, Zorsecurity atau Esage Lab, serta *Professional Association of Designers of Data Processing Systems*.
c. Sanksi individu diberikan pada sejumlah pihak, antara lain pada pimpinan GRU Igor Valentinovich Korobov, Deputi GRU Sergey Aleksandrovich Gizunov, Deputi satu GRU Igor Olegovich Kostyukov dan Vladimir Stepanovich Alexseyev.

Di lain pihak, Presiden Vladimir Putin akan memangkas jumlah staf diplomatik Amerika Serikat di Rusia menjadi 455 orang setelah Senat AS menyetujui penjatuhan sanksi baru terhadap Moskow. Rumah kedutaan AS dan fasilitasnya di Moskow juga disita sebagai pembalasan dari Rusia.[37]

[35]https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html. Tanggal tayang 13 Desember 2016. Tanggal akses 12 Desember 2017.
[36]https://www.cnnindonesia.com/internasional/20161230035205-134-183018/sanksi-untuk-rusia-pemerintah-as-usir-35-diplomat/. Tanggal tayang 30 Desember 2016. Tanggal akses 22 Desember 2017.
[37]https://international.sindonews.com/read/1225065/41/balas-sanksi-moskow-pangkas-staf-diplomatik-as-di-rusia-1501262019. Tanggal tayang 29 Juli 2017. Tanggal akses 22 Desember 2017.

5. Pembahasan

5.1.Analisis Ancaman

Berikut adalah hasil penelitian dari sumber literatur dan hasil wawancara yang dikelompokkan sesuai dengan masing-masing elemen ancaman.

a.Keinginan (*Desire*)

Keinginan adalah antusiasme pelaku untuk menyebabkan kerusakan demi mencapai tujuannya. Dalam kasus serangan siber yang dilakukan APT28 dan APT29, pelaku menargetkan Hillary dan beberapa koleganya, termasuk *Clinton Foundation*, *Center for America Progress*, penyedia teknologi NGP VAN, perusahaan strategi kampanye 270 Strategies, dan media berita partisan Shareblue Media.

Operasi spionase siber dimulai antara tahun 2015 sampai dengan 2016 menggunakan *spearphising*. Salah satu serangan berhasil masuk ke akun *email* John Podesta, kemudian mengambil informasi *email* dari akun tersebut. Guccifer 2.0 dan situs DCLeaks yang baru diluncurkan, bersama dengan WikiLeaks kemudian menerbitkan lebih dari 150.000 *email* yang dicuri dari anggota DNC.

b. Harapan (*Expectation*)

Harapan adalah keyakinan yang dimiliki pelaku bahwa tujuannya akan tercapai jika rencananya terlaksana. Tujuan Pelaku adalah untuk meruntuhkan kepercayaan publik terhadap proses demokrasi di AS, merendahkan Hillary, dan membahayakan elektabilitas dan potensinya menjadi presiden.

Amerika adalah negara yang strategis, hal ini menjadi motivasi pelaku untuk memainkan konstelasi politik di AS dengan melakukan serangan siber pada masa pilpres, melakukan intervensi terhadap proses

https://scholarhub.ui.ac.id/jkskn/vol3/iss1/1
DOI: 10.7454/jkskn.v3i1.10032

P-ISSN: 2620-7419 E-ISSN: 2776-1827
Jurnal Kajian Stratejik Ketahanan Nasional, Vol. 3, No.1, 2020

pilpres dan berusaha mengkondisikan hasil sesuai dengan harapan pelaku.

Kedekatan Rusia dengan Trump, akan memberikan manfaat kepada Rusia jika terpilih menjadi Presiden. Manfaat yang diterima berkaitan dengan kebijakan ekonomi, pengaruh di kawasan Eropa, dan pengaruh geopolitik di kawasan Timur Tengah yang memiliki kekayaan minyak.[38] Pencapaian tujuan ini memiliki risiko sanksi yang diberikan dari Amerika kepada Rusia.

c. Pengetahuan (*Knowledge*)

Pengetahuan adalah kepemilikan informasi yang dapat digunakan oleh pelaku untuk mencapai tujuannya. Daftar target yang menjadi serangan *spearphising* disekitar Hillary telah diketahui oleh pelaku serangan siber. Hal ini sangat membantu pelaku dalam melancarkan operasi spionase sibernya.

Setelah berhasil mendapatkan *email* di lingkaran Hillary, maka akan diketahui banyak informasi mengenai Hillary. Langkah-langkah politik yang akan diambil Hillary dan strategi-strateginya akan dapat diprediksi. Informasi tersebut juga dapat digunakan sebagai kampanye negatif untuk menjatuhkan Hillary atau digunakan untuk menguntungkan kandidat lainnya.

d. Sumber daya (*Resources*)

Sumber daya adalah kemampuan atau pengalaman serta bahan yang diperlukan untuk melaksakan rencana pelaku. Menurut laporan *National Intelligence Council* dua aktor yang berbeda berpartisipasi dalam intrusi ke dalam partai politik AS. Kelompok pertama, yang dikenal sebagai APT29, yang kedua dikenal sebagai APT28. Kasus serangan APT memerlukan *resources* yang sangat besar.

APT28 disebut sebagai kelompok besar yang memiliki tim pengembang perangkat lunak (*software development teams*), dapat beroperasi dalam skala yang luas, melakukan beberapa operasi berbeda secara serentak, dan memiliki tingkatan persiapan serangan (*levels of preparation before attack*) yang lebih tinggi dibanding dengan *state-sponsored hackers* Tiongkok.

Rusia juga memiliki manajemen yang baik (*well-managed*) terhadap kemampuan dan SDM siber internalnya. Dapat mengumpulkan SDM yang baik untuk disatukan dan memiliki visi yang telah diarahkan oleh negara. Bahkan peretas yang tidak diwadahi oleh negara bersedia tunduk terhadap pemerintahnya. Salah satu perusahaan *antivirus* ternama yang menguasai pasar ada di Rusia.[39]

Poin-poin tersebut kemudian dikonversi kedalam bentuk angka dan dimasukkan kedalam tabel sehingga menghasilkan data seperti pada tabel berikut.

Komponen			Skala	Skor
Ancaman (*Threat*)	Niat (*Intent*)	Keinginan (*Desire*)	Kritis	5
		Harapan (*Expectation*)	Tinggi	4
	Kemampuan (*Capability*)	Pengetahuan (*Knowlegde*)	Tinggi	4
		Sumber daya (*Reosurces*)	Kritis	5
Koefisien Ancaman				18

Tabel 1. Hasil penilaian ancaman

Koefisien ancaman pada Tabel tersebut yaitu 18 dengan kategori ancaman tinggi. Dari hasil tersebut, terlihat bagaimana pelaku memiliki keinginan, harapan, pengetahuan, dan sumber daya dengan koefisien yang tinggi dan

[38]Plt. Kepala Direktorat Analisis Sinyal, Lemsaneg. (2017, 6 Desember) Wawancara Pribadi.

[39]Staf Kapustikkp kemlu dan Plt. Kepala Direktorat Lemsaneg. (Desember 2017). Wawancara Pribadi

P-ISSN: 2620-7419 E-ISSN: 2776-1827
Jurnal Kajian Stratejik Ketahanan Nasional, Vol. 3, No.1, 2020

kritis. Kondisi tersebut dapat berubah sesuai dengan kebijakan diplomasi dan hubungan masing-masing negara. Dari hasil tersebut, diperlukan upaya kontra intelijen sebagai bentuk antisipasi ancaman di masa yang akan datang.

5.2.Analisis Kontra Intelijen

Dalam kasus serangan siber terhadap anggota DNC, upaya kontra intelijen siber yang dapat dilakukan yaitu :

1) Defensif kontra intelijen siber
   (a) Meningkatkan *security awareness* pada level personil, menyadari adanya ancaman siber, tidak melakukan klik sembarangan terhadap *attachment*, memperhatikan URL *website*, *website* palsu meskipun identik dengan *website* yang sah tapi memiliki perbedaan URL, memberikan pemahaman mengenai ciri-ciri serangan *spearphising*, menggunakan kombinasi *password* yang kuat; tidak menuliskan *password* pada sembarang tempat; tidak menyimpan *password* pada *browser*; tidak memberikan informasi rahasia kepada pihak yang tidak sah; tidak mengakses jaringan internet di fasilitas publik; tidak sembarangan menerima barang dari pihak yang tidak dikenal karena berpotensi dipasang alat sadap; dan melakukan *back up* data secara berkala. (b) Melakukan pemutakhiran (*update*) *patch*, sistem operasi, dan *software* secara berkala. (c) Melakukan pengamanan fisik, dengan menggunakan falisitas akses kontrol untuk pembatasan akses. (d) Menggunakan *email* dengan fitur enkripsi seperti *Pretty Good Privacy* (PGP), menggunakan *Ipsec*, *Secure Sockets Layer (SSL)*, dan *Kerberos*, untuk menjamin otentikasi pengguna dan kerahasiaan data. (e) Memanfaatkan fitur *two-factor authentication (2FA)*, yang terhubung dengan perangkat telepon sebagai media untuk otentikasi selain *password*. (f) Melakukan *security clearence* terhadap personil. (g) Melakukan IT *security assessment* atau audit keamanan sistem informasi, misalnya dengan *penetration testing*.(h) Memasang *monitoring center* untuk mengawasi jaringan dan sistem. (i) Untuk melakukan deteksi (*detection*) ancaman, dapat menggunakan *tools* untuk mengamankan komunikasi seperti UTM (*Unified Threat Management*), penyaringan konten dan pencegahan kebocoran (*leak prevention*), *remote routing*, *network address translation* (NAT), dan *virtual private network* (VPN); *anti-DDoS*; *anti-Bot*; *web application firewall*, dan *sandboxing*. (j) Memasang *toolbars* pada *web browser* yang berfungsi untuk mengidentifikasi situs *phising* dengan memeriksa *database* yang memiliki data *Fully Qualifed Domain Name* (FQDN) dan alamat IP yang telah terlapor sebagai situs *phising*.
2) Ofensif Kontra Intelijen Siber
   (a) Pemanfaatan *sock puppets* (*virtual agent*) di forum *online* untuk mengumpulkan informasi tentang operasi intelijen lawan (kemampuan, korban, taktik, dll). (b) Membuat agen musuh menjadi agen ganda untuk melakukan penyusupan. (c) Memasang *honeypot* yang bekerja sebagai sistem yang berfungsi untuk mengelabuhi (*deception*) peretas. (d) Lakukan cipta kondisi (*conditioning*) sesuai yang diinginkan, membanjiri informasi di media massa dan di internet sesuai dengan yang diinginkan. (e) Melakukan perang siber. Berusaha mendapatkan informasi milik lawan. Melakukan *intercept*, *open source* intelijen, *crawling* data di internet, penetrasi, dan penyerangan dengan *cyber weapon.*

5.3.Strategi Indonesia Menghadapi Ancaman Siber

https://scholarhub.ui.ac.id/jkskn/vol3/iss1/1
DOI: 10.7454/jkskn.v3i1.10032

P-ISSN: 2620-7419 E-ISSN: 2776-1827
Jurnal Kajian Stratejik Ketahanan Nasional, Vol. 3, No.1, 2020

a. Faktor internal kekuatan (*strengths*) : (1) Terdapat Badan yang bertanggung jawab terhadap keamanan siber seperti Badan Siber dan Sandi Negara, Deputi Bidang Intelijen Siber BIN, Direktorat Tindak Pidana Siber Bareskrim Polri, *Cyber Defence* Kementerian Pertahanan dan TNI, dan Kementerian Komunikasi dan Informatika. (2) Terdapat regulasi yang mengatur informasi dan transaksi elektronik, yaitu Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik (UU ITE. (3) Indeks KAMI. (4) Dukungan Pemerintah melalui RPJMN.
b. Faktor internal kelemahan (*weaknesses*) : (1) Indonesia berada pada peringkat 70 dunia berdasarkan laporan *Global Cyber Security Index* tahun 2017. (2) Belum memiliki strategi keamanan siber nasional. (3) Pemerintah belum sepenuhnya menerapkan sistem keamanan siber yang baik. (4) *User* cenderung kurang memperhatikan aspek keamanan. (5) Minimnya jumlah SDM siber.
c. Faktor eksternal peluang (*opportunities*) : (1) Kerjasama dengan komunitas siber dan akademik. (2) Kemajuan di bidang TIK. (3) Kerjasama nasional dan internasional.
d. Faktor eksternal ancaman (*threats*) : (1) Aktivitas serangan siber yang cukup tinggi. (2) *Five Power Defence Arrangements* (FPDA).

Strategi indonesia berdasarkan kombinasi dari hasil identifikasi faktor internal dan eksternal sesuai dengan matrik SWOT adalah sebagai berikut :

a. Strategi S+O
(1) Melakukan kerjasama antara instansi pemerintah dengan komunitas siber untuk memperkuat kapasitas secara teknis. (2) Berpartisipasi aktif dalam forum siber internasional untuk menjalin kerjasama, menambah penyebaran informasi di bidang keamanan siber, dan meningkatkan kompetensi di bidang siber. (3) Dengan kemajuan TIK, negara diharapkan dapat meningkatkan kemandirian dalam penyedian perangkat keamanan siber. (4) Negara memprioritaskan program untuk penerapan sistem keamanan siber pada infrastruktur kritis nasional sehingga dapat mengurangi dampak dari serangan siber.
b. Strategi W+O
(1) Pemenuhan jumlah SDM siber dapat dilakukan dengan melakukan rekrutmen SDM yang ada pada komunitas siber dan sektor akademik. (2) Pengetahuan yang diperoleh dari forum internasional, dapat diterapkan menjadi kebijakan atau regulasi yang dapat memperkuat keamanan siber. Salah satu manfaat yang diperoleh yaitu, hasil *benchmarking* dengan negara lain diharapkan dapat mensahkan kebijakan terkait keamanan siber yang komprehensif dan sesuai dengan kondisi Indonesia, seperti Strategi Keamanan Siber Nasional dan regulasi terkait keamanan siber sebagai standard/*best practice* dan manajemen sistem contohnya yaitu regulasi tentang keamanan dan perlindungan data pribadi. Kerjasama nasional juga dapat memperkuat siber secara teknis. (3) Penguatan budaya keamanan siber kepada masyarakat luas melalui kampanye dan kerjasama dengan komunitas siber.
c. Strategi S+T
(1) Memaksimalkan fungsi yang ada pada institusi seperti pemantauan dan pengendalian, deteksi dan identifikasi, proteksi, serta penanggulangan dan pemulihan sehingga dapat meminimalkan ancaman siber. dengan ruang lingkup pengamanan meliputi sektor pemerintah, infrastruktur kritis nasional, dan masyarakat (publik). (2)

P-ISSN: 2620-7419 E-ISSN: 2776-1827
Jurnal Kajian Stratejik Ketahanan Nasional, Vol. 3, No.1, 2020

Dengan penerapan regulasi yang ada, seperti UU ITE, diharapkan dapat membuat efek jera kepada pelaku kejahatan siber dan meminimalkan jumlah serangan siber. (3) Penerapan standar keamanan oleh institusi ataupun organisasi, diharapkan dapat meningkatkan infrastruktur, kesadaran dan kepatuhan personil pada prosedur/tata kelola, sehingga memeperkuat keamanan siber dan dapat meminimalkan peretas untuk melakukan penetrasi kepada sistem.

d. Strategi W+T
(1) Memperkuat keamanan sistem sehingga serangan dari peretas dapat dideteksi, diidentifikasi, dan dilindungi. (2) Meningkatkan jumlah dan kompetensi SDM siber sehingga dapat merespon dan memulihkan serangan dengan cepat. (3) Memberikan literasi kepada penyelenggara negara dan masyarakat luas tentang keamanan informasi dan ancamannya.

6. Kesimpulan

Hasil analisis ancaman serangan siber tersebut menunjukkan bahwa level ancaman pelaku spionase siber berada pada kategori tinggi, sehingga membahayakan kepentingan negara dan dapat mempengaruhi ketahanan nasional. Pelaku memenuhi elemen keinginan, harapan, pengetahuan, dan sumber daya dengan koefisien yang tinggi. Oleh karena itu, ancaman dengan level demikian perlu diantisipasi dengan kontra intelijen.

Secara umum, operasi kontra intelijen siber dibagi menjadi dua yaitu: defensif kontra intelijen siber dan ofensif kontra intelijen siber. Metode defensif bertujuan untuk memblokir dan deteksi terhadap aktivitas akses lawan, sedangkan metode ofensif bertujuan untuk mengumpulkan informasi, memanipulasi, mengontrol, dan menggagalkan aksi lawan. Pada kasus serangan siber terhadap anggota DNC, upaya defensif kontra intelijen yang dilakukan adalah dengan meningkatkan *security awareness* pada level personil, memahami akan ciri-ciri *spearphising* sehingga dapat mengantisipasi serangan pelaku. Kemudian, memanfaatkan fitur *two-factor authentication*. Langkah ofensif kontra intelijen yang mungkin dilakukan adalah melakukan cipta kondisi (*conditioning*) dengan upaya netralisasi terhadap berita yang beredar, membanjiri dengan berita baru atau berita yang sebaliknya melalui berbagai jenis media pemberitaan.

Strategi Indonesia dalam menghadapi ancaman siber antara lain dengan penguatan pada segi (1) regulasi : dengan membuat peraturan terkait keamanan siber, misalnya peraturan keamanan dan perlindungan data pribadi, (2) teknik : mengamankan sektor pemerintahan; infrastruktur kritis nasional; dan masyarakat, memberdayakan komunitas siber yang ada, (3) organisasi : menyusun strategi keamanan siber nasional, (4) *capacity building* : melakukan kampanye mengenai keamanan siber dan ancamannya kepada masyarakat, (5) kerjasama : aktif bekerjasama dalam skala nasional dan internasional.

7. Saran

7.1.Saran Teoritis

Penelitian ini hanya menggunakan pendekatan tingkat ancaman terhadap aksi spionase siber yang menyerang organisasi politik negara sebagai tolok ukur untuk melakukan antisipasi dengan kontra intelijen. Untuk penelitian dengan topik yang serupa, perlu dilakukan penelitian dengan menggunakan pendekatan analisis kerawanan (*vulnerability analysis*), analisis risiko (*risk analysis*), dan bagaimana menganalisis rencana pencegahan (*prevention*), persiapan (*preparation*), tanggapan (*response*), dan pemulihan (*recovery*). Sehingga dapat memberikan gambaran yang menyeluruh dan memberikan rekomendasi intelijen yang lebih komprehensif.

https://scholarhub.ui.ac.id/jkskn/vol3/iss1/1
DOI: 10.7454/jkskn.v3i1.10032

P-ISSN: 2620-7419 E-ISSN: 2776-1827
Jurnal Kajian Stratejik Ketahanan Nasional, Vol. 3, No.1, 2020

7.2.Saran Praktis

Berdasarkan hasil penelitian, ada beberapa saran yang dapat diimplementasikan oleh *stakeholder* intelijen berkaitan dengan fenomena operasi intelijen yang dilakukan melalui serangan siber, antara lain yaitu : (a) Melakukan koordinasi secara intens antar pihak yang memiliki fungsi siber sehingga dapat mengoptimalkan fungsi pemantauan dan pengendalian, deteksi dan identifikasi, proteksi, serta penanggulangan dan pemulihan. (b) Menumbuhkan dan meningkatkan *security awareness* pada level personil, karena banyak kasus serangan siber berhasil dilakukan disebabkan oleh kelalaian personilnya. (c) Upayakan dapat menyediakan perangkat keamanan TI secara mandiri, sehingga memperkecil potensi ancaman kebocoran informasi dari pihak luar.

Daftar Pustaka

Buku :

Johnson, William R. 1994. Thwarting Enemies at Home and Abroad: How to Be a Counterintelligence Officer. Bethesda, Md.: Stone Trail Press.

Zuehlke, Arthur A. 1980. What is Counterintelligence? In: Intelligence Requirements for the 1980s: Counterintelligence. Godson, Roy S; ed. Washing-ton D.C.: National Strategy Information Center.

Olson, James M. 2001. A Never-Ending Necessity. The Ten Commandments of counterintelligence. Washington D.C.: Studies in Intelligence.

Widjajanto, A. Lay, C. Keliat, M. (2006). Velox et Exatus. Universitas Indonesia.

Prunckun, H. (2012). *Counterintelligence Theory and Practice*. USA : Rowman & Littlefield.

Prunckun, H. (2015). *Scientific Methods of Inquiry for Intelligence Analysis*, Rowman & Littlefield.

Online document:

Asosiasi Penyelenggara Jasa Internet Indonesia. (2016). *Infografis Penetrasi & Perilaku Pengguna Internet Indonesia. Survey 2016*.

CyberEgde Group. *2016 Cyberthreat Defense Report*.

Departement of Homeland Security and Federal Bureau of Investigation. (2016*). Joint Analysis Report : GRIZZLY STEPPE – Russian Malicious Cyber Activity*. Reference Number: JAR-16-20296A.

Intelligence Community Assesment (CIA, FBI, NSA). (2017). *Background to "Assessing Russian Activities and Intentions in Recent US Elections": The Analytic Process and Cyber Incident Attribution*. National Intelligence Council. USA.

Internet Security Threat Report, Volume 22. (2017). Symantec.

ISO/IEC 27032:2012. *Information technology – Security techniques – Guidelines for cybersecurity*

Jurnal Online :

Beer, P. D. von Solms Basie, S. (2013). The Case for cyber counterintelligence. *Adaptive Science and Technology (ICAST)*. Pretoria.

Hurley, M. M. Conceptualizing Cyber Intelligence, Surveillance, and Reconnaisance. *Air & Space Journal*. USAF. 2012.

Jabbour, K. *Cyber Vision and Cyber Force Development*, Strategic Studies Quarterly 4, no. 1 (Spring 2010): 65, http://www.au.af.mil/au/ssq/2010/spring/spring10.pdf.

Klimburg, A. (2012). *National Cyber Security Framework Manual*. NATO Cooperative Cyber Defence Centre of Excellence.

Rubenstein, D. (2014). *Nation State Cyber Espionage and its Impacts*.

Vardangalos, G. (2016). *Cyber Intelligence and Cyber Counterintelligence (CCI) :*

P-ISSN: 2620-7419 E-ISSN: 2776-1827
Jurnal Kajian Stratejik Ketahanan Nasional, Vol. 3, No.1, 2020

General Definitions and Principles. Center for International Strategic Analyses (KEDISA).

Legislasi:

Penjelasan Undang-Undang No.17 Tahun 2011 tentang Intelijen Negara

Website:

https://nasional.sindonews.com/read/1154663/14/panglima-tni-beberkan-potensi-ancaman-yang-mengintai-indonesia-1478861976. Tanggal tayang 11 November 2016. Tanggal akses 3 April 2017.

http://tekno.kompas.com/read/2016/12/13/10220067/peretas.rusia.di.balik.kemenangan.trump. Tanggal tayang 13 Desember 2016. Tanggal akses 15 Desember 2017.

https://www.nytimes.com/interactive/2016/07/27/us/politics/trail-of-dnc-emails-russia-hacking.html. Tanggal tayang 6 Januari 2017. Tanggal akses 12 Desember 2017.

http://www.chicagotribune.com/news/nationworld/ct-russian-hack-grizzly-steppe-20161230-story.html. Tanggal tayang 30 Desember 2016. Tangggal akses 12 Desember 2017.

http://www.wired.co.uk/article/how-russian-hackers-work. Tanggal tayang 11 Januari 2017. Tanggal akses 12 Desember 2017.

https://www.kaspersky.com/resource-center/definitions/spear-phishing. Tanggal akses 20 Desember 2017.

https://wikileaks.org/clinton-emails/?q=iraq%7Cbaghdad%7Cbasra%7Cmosoul. Tanggal akses 1 Maret 2017.

http://internasional.kompas.com/read/2016/10/08/13321811/wikileaks.bocorkan.ribuan.e-mail.ketua.kampanye.hillary.clinton. Tanggal tayang 8 Oktober 2016. Tanggal akses 22 Desember 2017.

http://internasional.republika.co.id/berita/internasional/global/17/08/24/internasional/abc-australia-network/17/10/16/oxwbns366-hillary-tuding-wikileaks-dan-rusia-bantu-kemenangan-trump. Tanggal tayang 16 Oktober 2017. Tanggal akses 22 Desember 2017.

https://www.nytimes.com/2016/12/13/us/politics/russia-hack-election-dnc.html. Tanggal tayang 13 Desember 2016. Tanggal akses 12 Desember 2017.

https://www.cnnindonesia.com/internasional/20161230035205-134-183018/sanksi-untuk-rusia-pemerintah-as-usir-35-diplomat/. Tanggal tayang 30 Desember 2016. Tanggal akses 22 Desember 2017.

https://international.sindonews.com/read/1225065/41/balas-sanksi-moskow-pangkas-staf-diplomatik-as-di-rusia-1501262019. Tanggal tayang 29 Juli 2017. Tanggal akses 22 Desember 2017.

https://scholarhub.ui.ac.id/jkskn/vol3/iss1/1
DOI: 10.7454/jkskn.v3i1.10032