Strategi Operasi Kontra Intelijen *Cyber* Sebagai Upaya Peningkatan Ketahanan Negara Indonesia

Elsa Vinietta - 23215130

Abstrak

Operasi Kontra Intelijen *Cyber* menjadi hal yang penting untuk dapat diterapkan secara luas, terencana, dan terarah di Indonesia mengingat semakin maraknya pencurian informasi oleh pihak asing yang menggunakan atau memanfaatkan media komunikasi *digital*. Pada paper ini, dibahas mengenai jenis-jenis kegiatan spionase asing yang mengancam ketahanan negara, berbagai bentuk aktivitas kontra intelijen *cyber*, dan perencanaan strategi perlindungan yang efektif dan efisien untuk melindungi informasi rahasia negara.

Kata kunci: *cyber*, kontra intelijen

1. Pendahuluan

Pada era informasi seperti sekarang ini, upaya banyak negara untuk melancarkan ‘serangan’ terhadap negara lain sudah berubah menjadi memanfaatkan media komunikasi *digital*. Setidaknya ada dua alasan yang menyebabkan hal ini. Pertama, karena dengan demikian serangan dapat dilakukan dari jarak jauh dan lebih sulit untuk tertangkap. Kedua, penyimpanan dan pengiriman informasi semakin banyak menggunakan media *digital* yang menggantikan media fisik. Penyadapan yang dilakukan oleh pihak asing terhadap Indonesia sudah menjadi hal biasa bahkan semakin banyak kasus-kasus pencurian informasi oleh pihak asing melalui komunikasi *digital* terbongkar di Indonesia. Indonesia menjadi target empuk untuk kegiatan spionase asing karena Indonesia adalah negara yang kaya akan sumber daya tetapi memiliki pertahanan yang lemah khususnya di bidang teknologi informasi. Pertahanan yang dimaksud adalah dari segi teknologi, sumber daya manusia, maupun regulasi. Fakta ini perlu ditanggapi dengan serius oleh pemerintah, karena tersadapnya informasi rahasia tentu sangat merugikan dan mengancam ketahanan negara Indonesia.

Di Indonesia, dikenal istilah ‘kontra intelijen’ sebagai sebuah operasi perlawanan (kontra) terhadap aktivitas intelijen negara lain. Secara lebih spesifik, operasi kontra intelijen yang fokus pada penanggulangan spionase melalui media telekomunikasi elektronik disebut

sebagai operasi kontra intelijen *cyber*. Operasi kontra intelijen *cyber* ini mencakup pengertian yang sangat luas sehingga dibuat sistem klasifikasi untuk membagi jenis operasi sesuai dengan jenis situasi ancaman yang dihadapi. Karena itu, diperlukan pemahaman yang mendalam akan jenis-jenis situasi dan ancaman yang akan dihadapi sehingga pemilihan solusi kontra intelijen yang efektif dan efisien dapat dilakukan.

Sesuai dengan uraian di atas, paper ini dibuat dengan tujuan sebagai berikut:

1. Mempelajari bentuk-bentuk ancaman intelijen asing terhadap keamanan informasi di Indonesia
2. Mempelajari jenis-jenis serta peruntukan dari operasi kontra intelijen *cyber*
3. Menentukan solusi kontra intelijen yang tepat (efektif dan efisien) dalam melindungi informasi rahasia negara Indonesia

2. Ancaman Terhadap Keamanan Informasi Negara Indonesia

Dalam beberapa tahun belakangan ini, ada beberapa kasus mencuat terkait dengan aksi mata-mata *cyber* asing terhadap Indonesia. Tentu saja selain kasus-kasus yang telah terbukti, peluang bahwa adanya aksi-aksi lainnya yang belum disadari atau belum terbukti sangat besar. Aksi-aksi spionase *cyber* yang masih berlangsung namun belum disadari ini justru lebih berbahaya karena akan terus berlangsung dalam jangka waktu yang lama tanpa adanya penanggulangan sama sekali.

Sebelum membahas mengenai kemungkinan bahaya keamanan informasi yang belum disadari, terlebih dahulu akan dibahas mengenai kasus-kasus spionase *cyber* di Indonesia yang sudah terbongkar, sebagai bahan referensi untuk pembahasan selanjutnya. Pada tabel di bawah telah dirangkum beberapa kasus operasi intelijen yang terjadi terhadap Indonesia yang dilakukan oleh negara lain.

Tabel 1 Beberapa Kasus Operasi Intelijen Asing Terhadap Indonesia

Tahun Kasus	Pelaku	Target	Referensi
2009	Intelijen Australia dan Selandia baru	Sambungan telepon pribadi Presiden, ibu negara, dan pejabat penting	Okezone [1]
2009	Intelijen Amerika (NSA)	Jaringan operator Telkomsel dan Indosat	Okezone [1]

Dari rangkuman pada tabel 1, terlihat bahwa kasus pencurian informasi oleh intelijen asing yang terbongkar masih sangat minim jumlahnya. Jika melihat potensi dan ancaman yang ada di Indonesia, sangat besar kemungkinan bahwa ada aksi-aksi intelijen asing yang belum terbongkar. Faktor pendukung kemudahan aksi intelijen asing di Indonesia antara lain: operator telekomunikasi yang sebagian milik asing, penggunaan satelit asing sebagi satelit komunikasi utama, dan teknologi enkripsi yang digunakan di Indonesia masih sangat standar [2].

Untuk mengetahui lebih lanjut mengenai ancaman operasi intelijen asing terhadap Indonesia, dibahas juga mengenai kasus-kasus operasi intelijen yang terjadi di luar negeri, bisa dilihat pada tabel 2 di bawah ini:

Tabel 2 Beberapa Kasus Operasi Intelijen yang Terjadi di Luar Negeri

Tahun Kasus	Pelaku	Target	Referensi
2009	Anonim, diduga bermarkas di Cina	*Server* milik kontraktor *national defense* Amerika yang berisi informasi tentang pesawat tempur F-35	Fox News [3]
2009	Mata-mata Cina dan Rusia	Sistem komputer yang mengelola kelistrikan Amerika Utara	Fox News [3]
2009	Jaringan mata-mata yang berbasis di Cina	Sistem komputer diplomatik terkait 103 negara	Fox News [3]
2009	Mata-mata Cina dan Rusia	Tim kampanye senator Amerika	Fox News [3]
2002	*Hacker* Inggris	Komputer militer Amerika dan NASA	Fox News [3]
2015	Diduga Cina	Data pribadi 18 juta penduduk Amerika	Security Affairs [4]
2015	Diduga Rusia	Perusahaan energi asal Inggris	Security Affairs [4]
2013	Intelijen Amerika (NSA)	34 kepala negara dan kepala pemerintahan dunia	Okezone [1]

Dari rangkuman pada tabel 1 dan 2, dapat disimpulkan tiga alasan utama mengapa suatu sistem komputer atau komunikasi menjadi target operasi intelijen asing:

1. Sistem tersebut mengandung informasi krusial suatu negara
2. Sistem tersebut terkait dengan pejabat penting atau orang yang berpengaruh di suatu negara
3. Sistem tersebut berpengaruh terhadap kebutuhan pokok banyak orang

3. Kontra Intelijen *Cyber*

3.1 Pengertian Kontra Intelijen *Cyber*

Pada dasarnya, hal-hal terkait intelijen negara Republik Indonesia telah diatur dalam Undang-Undang Republik Indonesia nomor 17 tahun 2011 tentang Intelijen Negara tepatnya pada pasal 6. Pasal 6 ayat 1 menyebutkan bahwa: "Intelijen Negara menyelenggarakan fungsi penyelidikan, pengamanan, dan penggalangan." Sementara itu pasal 6 ayat 3 yang mengacu pada ayat 1 menyebutkan mengenai aktivitas kontra intelijen, isinya sebagai berikut: "Pengamanan sebagaimana dimaksud pada ayat (1) terdiri atas 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." [5] Telah disebutkan bahwa kontra intelijen *cyber* adalah aktivitas kontra intelijen yang berfokus pada penanggulangan kegiatan intelijen lawan yang menggunakan media komunikasi elektronik. Dengan demikian, pengertian kegiatan kontra intelijen *cyber* yang sesuai dengan UU No. 17 tahun 2011 adalah: "Serangkaian kegiatan yang dilakukan secara terencana dan terarah untuk mencegah dan/atau melawan upaya, pekerjaan, kegiatan intelijen pihak lawan yang memanfaatkan atau menggunakan media komunikasi elektronik dan merugikan kepentingan dan keamanan nasional".

Referensi [6] menyebutkan bahwa kontra intelijen bisa didefinisikan sebagai aktivitas yang bertujuan untuk mengidentifikasi, mengeksploitasi, dan menggagalkan aksi intelijen musuh yang merugikan entitas yang yang bersangkutan.

3.2 Taksonomi Kontra Intelijen *Cyber*

Kontra intelijen *cyber* sesuai dengan pengertian pada bagian 3.1 masih mencakup pengertian yang sangat luas yaitu semua bentuk kegiatan yang bertujuan untuk melawan kegiatan intelijen pihak lawan. Karena itu dibuatlah berbagai macam klasifikasi yang dapat digunakan dalam membahas mengenai strategi kontra intelijen *cyber*.

Referensi [6] merepresentasikan konsepsi yang umum digunakan dalam membedakan mode kerja kontra intelijen sebagai sebuah matriks seperti tabel 3 di bawah ini:

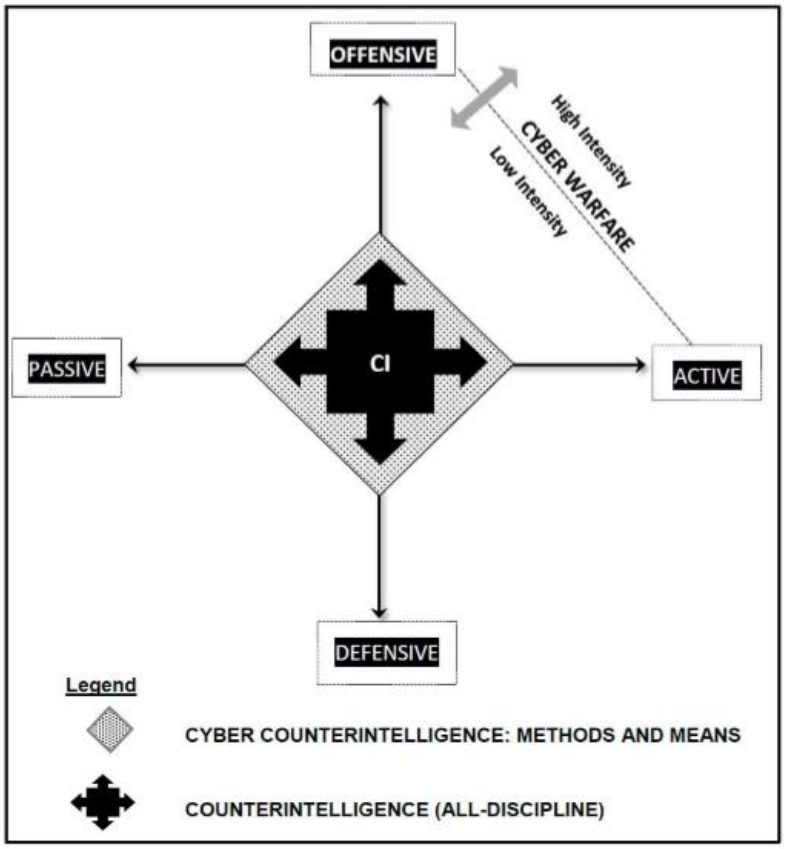
Tabel 3 Matriks Kontra Intelijen [6]

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 sebenarnya tidak ada, atau sesuatu yang salah, kamuflase).	**Ofensif Aktif** Secara langsung mengirimkan informasi yang salah melalui aksi rahasia.

Pada matriks di atas, kontra intelijen terbagi dua secara horizontal maupun vertikal. Pada pembagian secara horizontal, kontra intelijen dibedakan berdasarkan misinya: ofensif atau defensif. Perlu dipahami bahwa kedua fungsi tersebut tidak diterapkan secara terpisah. Taktik kontra intelijen defensif diperlukan untuk menyediakan informasi dan bertindak sebagai *trigger* bagi tindakan ofensif. Praktek defensif dan ofensif perlu dilaksanakan secara sinergis [6].

Sementara itu, pembagian secara vertikal membedakan operasi kontra intelijen menjadi aktif 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 respon-respon tertentu sesuai dengan situasi dan kondisi.

Lebih spesifik untuk kontra intelijen *cyber*, dikembangkan sebuah matriks oleh penulis referensi [6] seperti terlihat pada gambar 1.



Gambar 1 Matriks Kontra Intelijen *Cyber* Terintegrasi [6]

Dari gambar 1 terlihat bahwa kontra intelijen *cyber* disimbolkan menganut metode dan cara yang sejalan dengan kontra intelijen umum. Selain empat kuadran pada matriks yang serupa dengan tabel 3, operasi juga dibagi berdasarkan intensitasnya, *high intensity* atau *low intensity*.

4. Strategi Operasi Kontra Intelijen *Cyber* di Indonesia

Strategi yang menjawab tujuan operasi kontra intelijen *cyber* di Indonesia perlu dibuat sebelum melaksanakan operasi, karena tanpa strategi besarnya usaha yang dikeluarkan bisa jadi tidak sebanding dengan hasil yang didapatkan. Strategi yang dibuat harus efektif dan efisien, dalam arti ampuh untuk menangkal aksi intelijen asing yang merugikan negara, namun fokus pada perlindungan aset-aset informasi terpenting sehingga tidak menghabiskan sumber daya pada perlindungan informasi yang tidak krusial atau tidak rahasia.

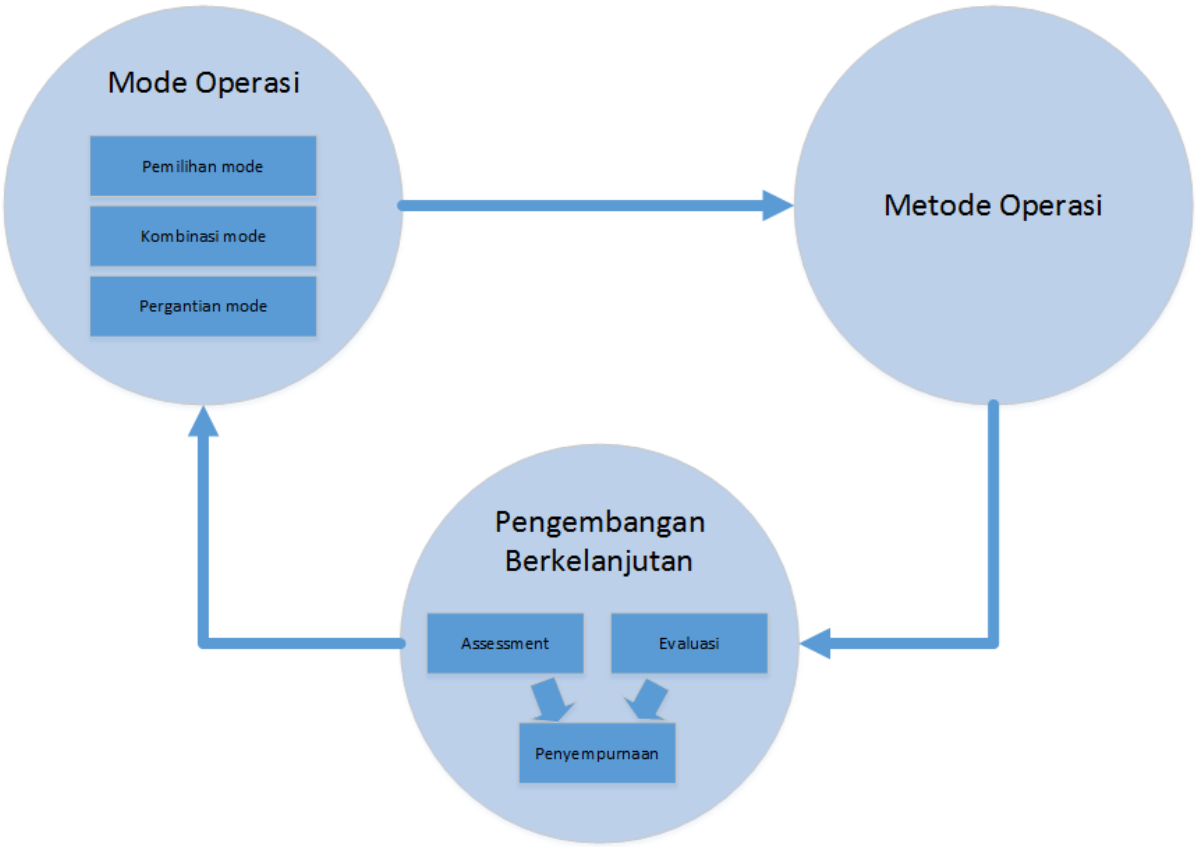
Strategi kontra intelijen harus turut memperhitungkan *cost* operasi sebagai salah satu aspek utama. Kerugian ekonomi yang ditimbulkan serangan intelijen *cyber* bisa sangat

bervarasi. Sebagai contoh ekstrim, strategi Rusia yang melancarkan serangan *cyber* yang dibarengi dengan perang fisik mengakibatkan negara targetnya mengalami kerugian properti, infrastruktur, bahkan nyawa manusia. Umumnya, biaya yang perlu dikeluarkan sebuah negara untuk bertahan dari serangan intelijen *cyber* sangat tinggi [7].

Di sisi sebaliknya, bagi negara penyerang, biaya intelijen *cyber* jauh lebih rendah. Selain itu ada keuntungan-keuntungan lainnya yang didapat dari cara ini, di antaranya serangan intelijen *cyber* bisa dilakukan secara anonim dan negara korban sulit membuktikan identitas pelaku, yang artinya serangan ini bisa dilakukan juga ketika situasi damai tanpa perlu takut ketahuan. Dalam dunia *cyber* menyerang lebih mudah daripada bertahan, karena pihak yang bertahan harus bertahan terhadap segala kemungkinan, sementara penyerang cukup menemukan satu celah pertahanan. Bagi sebuah negara, berinvestasi untuk operasi ofensif secara umum lebih murah dibandingkan untuk operasi defensif [7].

Pengamanan informasi negara merupakan suatu hal yang kompleks dan memerlukan penanganan yang terintegrasi. Hal pertama yang perlu dilakukan adalah menyiapkan jalur informasi yang tersandi, dan fungsi ini telah dilakukan melalui Lembaga Sandi Negara. Tanpa adanya jalur komunikasi tersandi tersebut, usaha kontra intelijen akan sia-sia saja sebab pertukaran informasi sangat mudah untuk dicuri dan dibaca pada setiap titik yang dilaluinya.

Pada paper ini, strategi operasi kontra intelijen yang direkomendasikan mengandung elemen-elemen utama yaitu: mode operasi, metode operasi, dan pengembangan berkelanjutan. Hubungan elemen-elemen tersebut diilustrasikan dengan gambar 2 berikut ini:



Gambar 2 Kerangka Strategi Kontra Intelijen *Cyber*

4.1 Mode Operasi

Jenis-jenis mode operasi kontra intelijen *cyber* mengacu pada tabel 3 dan gambar 1 yang telah dibahas pada bagian 3. Terkait dengan mode operasi yang digunakan, ada tiga aktivitas yang dilakukan yaitu memilih mode, mengombinasikan mode, dan mengganti mode operasi.

4.1.1 Pemilihan Mode

Pemilihan mode operasi kontra intelijen *cyber* adalah hal yang sangat penting dilakukan untuk dapat melindungi informasi secara efektif dan efisien. Untuk memilih mode secara tepat, tim operasi harus terlebih dahulu mempelajari kondisi dan keadaan antara lain:

1. Informasi yang dilindungi

Dengan mengetahui klasifikasi informasi yang dilindungi, operasi kontra intelijen *cyber* yang dilakukan bisa tepat sasaran. Operasi kontra intelijen memerlukan sumber daya yang cukup mahal, seperti dana untuk perangkat maupun tenaga ahli. Ada juga kemungkinan

efek samping seperti performa sistem yang menurun. Tidak perlu dilakukan operasi dengan intensitas tinggi untuk melindungi informasi yang tidak terlalu krusial atau rahasia.

2. Keamanan eksisting

Selain klasifikasi informasi, keamanan tempat informasi tersebut berada pra-operasi juga perlu dipelajari untuk mengetahui celah-celah yang rawan untuk dimasuki oleh intelijen lawan. Celah-celah tersebut bisa saja harus diperkuat, atau bisa juga dimanfaatkan sebagai pancingan untuk menipu lawan, tergantung dari strategi yang dipilih oleh tim operasi.

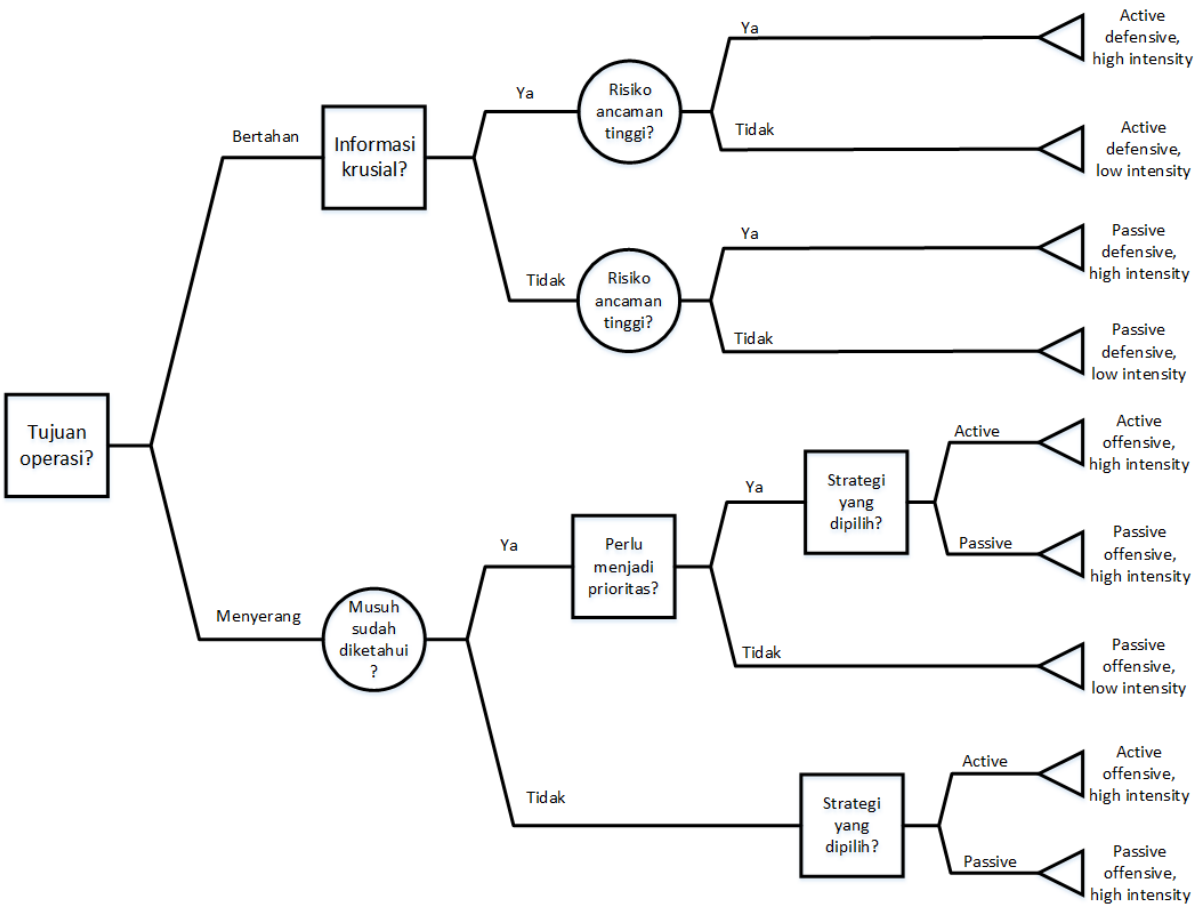
3. Risiko dan ancaman

Setelah mengetahui klasifikasi informasi dan keamanan eksisting, perlu dipelajari juga risiko dan ancaman terhadap informasi yang dilindungi. Misalnya saja, siapa pihak-pihak yang paling diuntungkan dengan mengetahui informasi tersebut. Dengan membuat hipotesis tersebut, metode penyerangan oleh lawan bisa diperkirakan dan mode operasi yang kontra terhadap metode tersebut dapat diprioritaskan.

4. Perhitungan ekonomi

Telah dibahas sebelumnya, bahwa seringkali biaya untuk melakukan operasi kontra intelijen terutama strategi defensif sangat besar. Karena itu, perlu disandingkan apakah biaya untuk melakukan operasi sebanding dengan kerugian yang ditimbulkan bila operasi tidak dilakukan. Sebagai contoh, negara seperti Amerika mengalami kerugian ekonomi sebesar 25 hingga 100 milyar dolar akibat serangan *cyber* internasional. Cina dianggap sebagai pencuri data yang mengakibatkan kerugian ini, sehingga Amerika mengucurkan investasi yang cukup besar untuk mencegah hilangnya kekuatan ekonomi negaranya [7]. Berdasarkan hal tersebut, Indonesia perlu menyelaraskan strategi operasi kontra intelijen *cyber* dengan strategi pertahanan dan ekonomi negara, terutama berkaitan dengan dunia internasional. Dengan demikian informasi apa yang dilindungi dan musuh mana yang perlu diwaspadai bisa dikerucutkan sehingga investasi untuk operasi bisa efektif dan efisien.

Secara sederhana, pemilihan mode operasi dapat dilakukan oleh tim operasi kontra intelijen *cyber* dengan memanfaatkan *decision tree* berikut yang merangkum pembahasan-pembahasan di atas:



Gambar 3 *Decision Tree* Pemilihan Mode Operasi

4.1.2 Pergantian Mode

Dalam keberjalanan operasi, keadaan bisa berubah setiap saat. Tim operasi kontra intelijen harus dapat merespon cepat setiap perubahan yang ada. Sangat mungkin perlu dilakukan pergantian mode operasi kontra intelijen *cyber*, dimana proses pemilihan mode operasi yang telah dibahas pada bagian 4.1.1 diulang lagi dari awal sebagai respon terhadap keadaan yang baru.

4.1.3 Kombinasi Mode

Selain kemungkinan pemilihan satu mode sesuai dengan medan operasi, pada beberapa kasus perlu juga diterapkan lebih dari satu mode secara bersama-sama. Tim operasi kontra intelijen *cyber* dapat juga memilih strategi kombinasi mode bila diperlukan.

4.2 Metode Operasi

Untuk setiap mode operasi, ada satu atau lebih kemungkinan metode operasi. Pada bagian ini telah dirangkum beberapa pilihan metode operasi untuk setiap mode, sesuai dengan referensi [6]:

1. Defensif pasif
    a. Pertahanan secara fisik, melakukan perlindungan terhadap:
        - Sembarang akses terhadap fasilitas dan sistem
        - Pencurian data atau *hardware* di lokasi
        - *Malware* yang dimasukkan dari akses fisik
        - Pengrusakan fisik
        - Informasi terbaca dengan sembarangan
    b. Mengelola *supply-chain management*
    c. Pemeriksaan personil IT dan pengguna, mengadakan *confidentiality agreement*
    d. Pengukuran keamanan personil, penentuan aturan BYOD
2. Defensif aktif
    a. Mengombinasikan *hardware* dan *software*, contohnya membuat:
        - Network perimeter-based security (filter, firewall, dan lain-lain)
        - Malware scanner
        - Integrated automated system/tools
        - Intrusion Detection System (IDS) dan Intrusion Prevention System (IPS)
        - Honeynet (penggunaan defensif)
3. Ofensif pasif
    a. Mengumpulkan informasi untuk mendeteksi musuh *cyber*

b. Menggunakan IDS/IPS, aplikasi honey-client
c. Menggunakan agen virtual
d. Memata-matai lawan secara *cyber* (*cybersepionage*)

4. Ofensif aktif
    a. Honeynet yang dikonfigurasi secara ofensif untuk menipu lawan, menampilkan informasi palsu, network scanner, listener, yang bertujuan untuk mengarahkan lawan ke arah yang diinginkan
    b. Menggunakan agen virtual
    c. Perang *cyber*

4.3 Pengembangan Berkelanjutan

Sebagaimana perencanaan strategi pada umumnya, selalu diperlukan sebuah pengembangan yang berkelanjutan. Bisa jadi ada operasi yang gagal atau tidak memberi hasil sesuai harapan, atau ada kesempatan untuk perbaikan yang sebelumnya tidak disadari.

Terkait dengan pengembangan berkelanjutan, ada tiga aktivitas yang akan dibahas yaitu: *assessment*, evaluasi, dan penyempurnaan.

4.3.1 *Assessment*

Assessment adalah penilaian terhadap kinerja operasi yang dilakukan secara berkala, dan bisa dilakukan pada keseluruhan tahapan dari operasi. *Assessment* sangat penting untuk mengetahui apakah strategi yang dipilih efektif dan efisien dalam melindungi informasi, dan sejauh mana ketepatan pelaksanaan operasi dengan rencana semula. *Assessment* dapat dilakukan sekalipun operasi belum ditutup atau selesai, sehingga perbaikan dapat segera dilakukan bila memungkinkan.

Secara khusus, dunia *cyber* atau teknologi *digital* memiliki ritme perkembangan yang sangat cepat. Standar penilaian dalam aktivitas *assessment* harus juga disesuaikan dengan perkembangan teknologi terkini. Karena itu, aktivitas *assessment* juga mencakup pengumpulan informasi terkait perkembangan teknologi informasi terkini, seperti cara penyadapan, teknologi keamanan informasi dan jaringan, dan standar-standar yang dikembangkan untuk keamanan informasi maupun aktivitas kontra intelijen *cyber*.

4.3.2 Evaluasi

Evaluasi adalah kegiatan penilaian operasi yang dilakukan setelah operasi selesai. Seperti halnya *assessment*, evaluasi menilai keseluruhan operasi kontra intelijen *cyber*, apakah efektif dan efisien, dan apakah pelaksanaannya cukup baik dan memenuhi standar.

4.3.3 Penyempurnaan

Assessment dan evaluasi yang telah dilakukan digunakan sebagai bahan penyempurnaan operasi. Karena itu, *assessment* dan evaluasi haruslah terdokumentasi dengan baik supaya dapat dipelajari oleh tim operasi kontra intelijen *cyber* pada masa-masa selanjutnya.

5. Penutup

5.1 Kesimpulan

Kesimpulan dari paper yang berjudul "Strategi Operasi Kontra Intelijen *Cyber* Sebagai Upaya Peningkatan Ketahanan Negara Indonesia" ini adalah sebagai berikut:

1. Operasi intelijen *cyber* saat ini sudah umum dilakukan oleh negara-negara di dunia pada era teknologi informasi ini. Operasi intelijen *cyber* asing di Indonesia sudah dan sangat mungkin sedang berlangsung, dan didominasi oleh negara-negara tetangga yang memiliki kepentingan ekonomi sebagai motif operasinya terhadap Indonesia.
2. Secara umum, operasi kontra intelijen *cyber* dibagi menjadi empat kategori yaitu: defensif pasif, defensif aktif, ofensif pasif, dan ofensif aktif. Strategi mode ofensif bertujuan untuk memblokir akses lawan dan mengumpulkan informasi mengenai lawan, sedangkan strategi mode ofensif bertujuan untuk memanipulasi, mengontrol, dan menggagalkan aksi lawan.
3. Secara garis besar, strategi kontra intelijen *cyber* yang direkomendasikan terdiri dari tiga aktivitas yaitu: mengelola mode operasi, menentukan dan menjalankan metode operasi, dan melakukan pengembangan yang berkelanjutan. Pemilihan mode operasi harus mempertimbangkan beberapa hal yaitu: informasi yang dilindungi, keamanan eksisting, risiko dan ancaman, serta perhitungan ekonomi. Pergantian maupun kombinasi mode operasi juga perlu dilakukan sebagai bentuk strategi. Metode operasi

yang digunakan untuk kontra intelijen *cyber* sangat beragam, dan keberhasilan setiap metode ditentukan oleh dua faktor utama: manusia dan teknologi. Pengembangan yang berkelanjutan harus terus dilakukan karena perkembangan operasi intelijen pun akan terus berlangsung, dan untuk melakukannya perlu dilaksanakan tiga aktivitas yaitu: *assessment* atau penilaian, evaluasi, dan penyempurnaan.

5.2 Saran

Saran terhadap topik strategi operasi kontra intelijen *cyber* di Indonesia adalah sebagai berikut:

1. Kerangka strategi yang telah dibuat perlu dijabarkan menjadi kebijakan dan prosedur kontra intelijen *cyber* di Indonesia. Saat ini belum ada regulasi yang memadai terkait dengan kontra intelijen khusunya pada bidang *cyber*.
2. Para pemangku kepentingan khususnya instansi intelijen maupun persandian negara perlu memberi perhatian lebih terhadap operasi kontra intelijen *cyber*. Terungkapnya kasus-kasus pencurian informasi negara di Indonesia dan dunia menyiratkan bahwa besar kemungkinan bahwa saat ini pencurian tersebut masih berlangsung dan belum disadari.
3. Operasi kontra intelijen *cyber* perlu dilakukan secara terencana dan terarah dengan memastikan terciptanya sinergi yang baik antara regulasi, tenaga ahli manusia, dan teknologi.

References

[1] D. Listiyani, "Okezone," 9 Maret 2015. [Online]. Available: http://techno.okezone.com/read/2015/03/09/54/1115836/kasus-penyadapan-menghebohkan-di-indonesia. [Diakses 21 April 2016].

[2] P. Persada, Interviewee, *Mengapa Indonesia Rentan Disadap?*. [Wawancara]. 23 Maret 2015.

[3] “Fox News,” [Online]. Available: http://www.foxnews.com/story/2009/04/22/five-serious-cases-cyberespionage.html. [Diakses 21 April 2016].

[4] P. Paganini, “Security Affairs,” 30 June 2015. [Online]. Available: http://securityaffairs.co/wordpress/38191/cyber-crime/russia-china-cyber-espionage.html. [Diakses 21 April 2016].

[5] Undang-Undang Republik Indonesia Nomor 17 Tahun 2011.

[6] P. D. Beer dan S. v. S. Basie, “The Case for cyber counterintelligence,” dalam *Adaptive Science and Technology (ICAST)*, Pretoria, 2013.

[7] Dana Rubenstein, “Nation State Cyber Espionage and its Impacts,” Dept. of Computer Science and Engineering WUSTL, Saint Louis, 2014.