Jurnal Kajian Stratejik Ketahanan Nasional

Volume 2
Number 1 *JKSKN Volume 2 No 1 2019*

Article 3

1-1-2019

Identifikasi Ancaman PCI (Positif Clandestine Intelligence) Berbentuk Cyber Terrorism Terhadap Keamanan Nasional

Yudha Fernando
Sekolah Tinggi Intelijen Negara, Fernandoalonzo27@gmail.com

Recommended Citation

Fernando, Yudha (2019) "Identifikasi Ancaman PCI (Positif Clandestine Intelligence) Berbentuk Cyber Terrorism Terhadap Keamanan Nasional," *Jurnal Kajian Stratejik Ketahanan Nasional*: Vol. 2: No. 1, Article 3.
DOI: 10.7454/jkskn.v2i1.10017
Available at: https://scholarhub.ui.ac.id/jkskn/vol2/iss1/3

ISSN: 2620-7419
Jurnal Kajian Stratejik Ketahanan Nasional, Vol..2, No.1, 2019

Identifikasi Ancaman PCI (Positif Clandestine Intelligence) Berbentuk *Cyber Terrorism* Terhadap Keamanan Nasional

Yudha Fernando[1]
Fernandoalonzo27@gmail.com

Abstract

This research is motivated by the vigilance towards the development of cyberspace technology that is so fast that it causes dependence on it in almost all fields. This condition poses a potential threat to our national ressiliance in various fields, especially in the national security sector. Researchers try to identify the threat of Positive Clandestin Intelligence (PCI) in the form of cyber terrorism on national security, so that it can bring stakeholders to a better level of knowledge. Some theories and concepts that researchers use are related to threats, national security, positive clandestine intelligence, terrorism and cyber terrorism (CT). The research approach used in this study is a qualitative approach and the type of research is descriptive qualitative. In primary and secondary data collection, researchers used interview techniques and document studies. Then the data is evaluated and analyzed with an interactive analysis model. Researchers also validate by measuring the degree of accuracy between the data that occurs in the object of research with data that can be reported by researchers. This research succeeded in identifying the types of Positive Clandestine Intelligence Cyber Terrorism (PCI CT) targets, forms of PCI CT attacks, psychological motivations of PCI CT perpetrators and the position of PCI CT threats in the taxonomy of Rogers M.K's cyber crime behavior.
Keywords: *Cyber Terrorism, Nasional Ressiliance, Terrorism, Positive Clandestine Intelligence (PCI)*

Penelitian ini dilatarbelakangi oleh kewaspadaan terhadap perkembangan teknologi dunia maya yang begitu cepat sehingga menyebabkan ketergantungan padanya di hampir semua bidang. Kondisi ini berpotensi menimbulkan ancaman terhadap kemeriahan nasional kita di berbagai bidang, terutama di sektor keamanan nasional. Para peneliti mencoba mengidentifikasi ancaman Positive Clandestin Intelligence (PCI) dalam bentuk terorisme cyber pada keamanan nasional, sehingga dapat membawa para pemangku kepentingan ke tingkat pengetahuan yang lebih baik. Beberapa teori dan konsep yang digunakan peneliti terkait dengan ancaman, keamanan nasional, intelijen klandestin positif, terorisme, dan terorisme cyber (CT). Pendekatan penelitian yang digunakan dalam penelitian ini adalah pendekatan kualitatif dan jenis penelitiannya adalah deskriptif kualitatif. Dalam pengumpulan data primer dan sekunder, peneliti menggunakan teknik wawancara dan studi dokumen. Kemudian data dievaluasi dan dianalisis dengan model analisis interaktif. Peneliti juga memvalidasi dengan mengukur tingkat akurasi antara data yang terjadi pada objek penelitian dengan data yang dapat dilaporkan oleh peneliti. Penelitian ini berhasil mengidentifikasi jenis-jenis target Positive Clandestine Intelligence Cyber Terrorism (PCI CT), bentuk serangan PCI CT, motivasi psikologis pelaku PCI CT dan posisi ancaman PCI CT dalam taksonomi perilaku kejahatan cyber Rogers M.K.
Kata kunci: *Cyber Terrorism, National Ressiliance, Terrorism, Positive Clandestine Intelligence (PCI)*

[1] Dosen Sekolah Tinggi Intelijen Negara

ISSN: 2620-7419
Jurnal Kajian Stratejik Ketahanan Nasional, Vol..2, No.1, 2019

1. Pendahuluan

Diskusi terhadap ancaman keamanan nasional yang tercipta diruang cyber merupakan suatu hal yang tidak dapat dihindari bagi para pihak yang berhubungan dengan isu keamanan nasonal dan ketahanan nasional. Penelitian ini mencoba memberikan gambaran dalam bentuk identifikasi terkait ancaman cyber terrorism dilihat dari kacamata intelijen keamanan nasional. Hasil dari penelitian ini diharapkan dapat memberika kewaspadaan terkait cyber terrorism selaku *positif clandestine intelijen* (PCI) bagi para pemangku kepentingan dibidang keamanan nasional, khususnya intelijen yang terkait dengan keamanan nasional.

Dalam Pasal 1 ayat 1, Undang-undang nomor 17 tahun 2011, disebutkan bahwa Intelijen adalah pengetahuan, organisasi, dan kegiatan yang terkait dengan perumusan kebijakan, strategi nasional, dan pengambilan keputusan berdasarkan analisis dari informasi dan fakta yang terkumpul melalui metode kerja untuk pendeteksian dan peringatan dini dalam rangka pencegahan, penangkalan, dan penanggulangan setiap ancaman terhadap keamanan nasional.

Pada era revolusi industry 4.0 sekarang ini, ancaman terhadap keamanan nasional telah menemukan bentuk baru, termasuk ancaman yang berjenis *positif clandestine intelligence* (PCI). Secara konsep, PCI mempunyai berbagai macam bentuk, salah satunya adalah teror. Metode teror telah berhasil berdialektika dengan lingkungan eksternalnya guna menciptakan ketakutan. Perkembangan teknologi yang sangat dinamis dan globalisasi yang tidak dapat dihindari menjadi faktor pendukung eksistensi ancaman teror tersebut. Ancaman teror yang dimaksud adalah ancaman teror dalam ruang maya atau *cyber terrorism*. Penelitian ini mencoba untuk mengidentifikasi bentuk, jenis dan motivasi psikologis pelaku teror, sehingga dapat menjadi masukan bagi system ketahanan nasional negara ini didalam menemukan solusinya.

2. Landasan Teori

2.1. Positif Clandestine Intelijen (PCI)

Intelijen dalam suatu negara dimaknai dalam tiga penampilannya, yaitu penampilan sebagai organisasi (*organization*), penampilan sebagai aktivitas (*activity*), dan penampilan sebagai suatu pengetahuan (*knowledge*). Intelijen sebagai aktivitas, berarti suatu aktivitas yang tertutup, baik dalam bentuk *clandestine activities* maupun *covert action*. Aktivitas itu mencakup kegiatan-kegiatan yang sifatnya rutin dan operasi-operasi intelijen yang bersifat temporer dan dibatasi waktu. Output dari aktifitas intelijen disebut Positif Clandestine Intelligence, bentuknya bisa berupa espionage, propaganda, konflik sosial maupun teror.

2.2. Terorisme

Whittaker, mengutip beberapa pengertian terorisme antara lain Walter Reich yang menyatakan bahwa terorisme adalah *a strategy of violence designed to promote desired outcomes by instilling fear in the public at large* (suatu kekerasan yang dirancang untuk meningkatkan hasil-hasil yang diinginkan, dengan cara menanamkan ketakutan di kalangan masyarakat umum). Terorisme adalah penggunaan atau ancaman penggunaan kekerasan, yang bertujuan untuk mencapai terjadinya perubahan politik.

Sementara Sederberg mengartikan terorisme merupakan suatu penggunaan atau ancaman penggunaan kekerasan untuk kepentingan-kepentingan politik, apabila aksi seperti itu ditujukan untuk mempengaruhi sikap dan perilaku dari suatu kelompok sasaran yang lebih besar, daripada sekedar, korban-korban yang berjatuhan seketika itu, dan jaringannya telah melampaui batas-batas nasional.

https://scholarhub.ui.ac.id/jkskn/vol2/iss1/3
DOI: 10.7454/jkskn.v2i1.10017

ISSN: 2620-7419
Jurnal Kajian Stratejik Ketahanan Nasional, Vol..2, No.1, 2019

Tujuan para pelaku terorisme dan motivasinya di masa lalu beragam, yaitu demi keuntungan ekonomi, memperoleh gengsi sosial (*glory*), memaksakan ideologi, penafsiran keyakinan atau eksploitasi agama, kebudayaan, hegemoni, kekuasan, dominasi kultural ataupun pemaksaan suatu konsep filsafati.

2.3. Ancaman

Undang-undang Nomor 17 Tahun 2011 tentang Intelijen Negara menyatakan bahwa ancaman adalah setiap upaya, pekerjaan, kegiatan, dan tindakan, baik dari dalam negeri maupun luar negeri, yang dinilai dan/atau dibuktikan dapat membahayakan keselamatan bangsa, keamanan, kedaulatan, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan kepentingan nasional di berbagai aspek, baik ideologi, politik, ekonomi, sosial budaya, maupun pertahanan dan keamanan.Ancaman adalah suatu hal, suatu keadaan, suatu kejadian, suatu tindakan yang bisa membahayakan, menyulitkan, mengganggu, menimbulkan rasa sakit, merugikan, dll.

Pada dasarnya ancaman memiliki sasaran dan kepentingan, yaitu sebagai berikut:

1) Negara: kepentingan ancamannya adalah kedaulatan dan kemerdekaan negara serta keutuhan wilayah.
2) Bangsa: kepentingan ancamannya adalah persatuan bangsa dan nilai-nilai luhur bangsa.
3) Pemerintah: kepentingan ancamannya adalah kebijaksanaan dan tindakan pemerintah serta legitimasi pemerintah.
4) Masyarakat: kepentingan ancamannya adalah kehidupan masyarakat dan kepentingan kelompok masyarakat.
5) Individu: kepentingan ancamannya adalah keamanan jiwa diri dan keluarga serta harta kekayaan.

2.4. Keamanan Nasional

Sebagai bagian dari sistem keamanan nasional, intelijen berperan sebagai sistem peringatan dini dan sistem strategis untuk mencegah terjadinya pendadakan strategis yang mengancam keamanan nasional. Keamanan nasional secara umum diartikan sebagai kebutuhan dasar untuk melindungi dan menjaga kepentingan nasional suatu bangsa yang menegara dengan menggunakan kekuatan politik, ekonomi dan militer untuk menghadapi berbagai ancaman baik yang datang dari luar maupun dari dalam negeri. Keamanan nasional juga dapat diartikan sebagai kondisi atau keadaan yang bersifat nasional dan menggambarkan terbebasnya negara, masyarakat, dan warga negara dari segala bentuk ancaman dan atau tindakan baik yang dipengaruhi oleh faktor eksternal maupun internal. Keamanan nasional dimaknai sebagai kebutuhan dasar untuk melindungi dan menjaga kepentingan nasional suatu bangsa dengan menggunakan kekuatan politik, militer dan ekonomi untuk menghadapi ancaman baik yang datang dari dalam maupun luar negeri. Pandangan ini mendukung argumentasi bahwa keamanan nasional di Negara demokrasi umumnyamencakup keamanan Negara, keamanan masyarakat, dan keamanan manusia *(state security, public security dan human security)*

2.5. Cyber terrorism

Cyber craft dapat diartikan sebagai segala jenis aktivitas intelijen yang menggunakan teknologi telematika sebagai medianya. Bentuk dari *cyber craft* mulai dari propaganda dalam bentuk pencemaran nama baik melalui media sosial, Hoax, Hatespeech sampai yang '*high tech*' seperti cyber terrorism dengan menggunakan Ddos attach, Malware maupun ransomware.

Definisi dari Cyber terrorism dapat diartikan sebagai berikut penggunaan tehnik-

ISSN: 2620-7419
Jurnal Kajian Stratejik Ketahanan Nasional, Vol..2, No.1, 2019

tehnik jaringan komputer guna membuat tidak berfungsinya suatu infrastruktur utama jaringan komputer, dengan tujuan untuk mengintimidasi atau memaksa pemerintah dan kelompok masyarakat. Sedangkan yang dimaksud dengan infrastruktur utama jaringan komputer adalah, system dan asset yang jika dihancurkan akan membawa dampak pada keamanan infrastruktur, keamanan ekonomi dan keamanan sistem kesehatan public. Termasuk didalamnya indsutri energy, pangan, transportasi, banking, komunikasi, pemerintahan dan ruang maya itu sendiri. Pelaku dari cyber terrorism bisa dari State actors (SA) maupun Non State actors (NSA). Tergantung motivasi dari user organisasi intelijen tersebut yang menggunakan PCI cyber terrorism sebagai sebuah aktifitas intelijen diruang maya.

3. Metode Penelitian

3.1 Pendekatan & Jenis Penelitian

Penelitian ini menggunakan pendekatan kualitatif. Pendekatan kualitatif peneliti pilih karena penelitian ini bertujuan untuk mengidentifikasi ancaman *PCI* cyber terrorism terhadap keamanan nasional melalui fenomena-fenomena sosial yang terjadi dari sudut pandang subjek, dimana peneliti merupakan instrumen kuncinya.

Proses penelitian kualitatif ini melibatkan upaya-upaya penting, seperti mengajukan pertanyaan-pertanyaan dan prosedur-prosedur, mengumpulkan data yang spesifik dari para informan, menganalisis data secara induktif mulai dari tema-tema yang khusus ke tema-tema umum, dan menafsirkan makna data. Pendekatan kualitatif dinilai peneliti sesuai untuk mengidentifikasi ancaman PCI cyber terrorism terhadap keamanan nasional merupakan fenomena sosial yang cenderung dapat digambarkan dengan deskripsi dalam bentuk kata-kata dibandingkan dengan angka.

Jenis penelitian yang digunakan adalah jenis deskripsi kualitatif dengan mempelajari bentuk ancaman PCI cyber terrorism terhadap keamanan nasional. Penelitian deskriptif kualitatif berupaya untuk mendeskripsikan, mencatat, analisis dan menginterpretasikan bentuk ancaman PCI cyber terrorism terhadap keamanan nasional, dengan kata lain penelitian ini bertujuan untuk memperoleh informasi mengenai keadaan yang ada. Penelitian deskriptif ini menggunakan model studi kasus, dimana peneliti berusaha untuk mengidentifikasi bentuk ancaman PCI cyber terrorism terhadap keamanan nasional. Laporan akhir untuk penelitian ini memiliki struktur atau kerangka yang fleksibel. Siapa pun yang terlibat dalam bentuk penelitian ini harus menerapkan cara pandang penelitian yang bergaya induktif, berfokus terhadap makna individual, dan menerjemahkan kompleksitas suatu persoalan.

3.2 Validasi Data

Penelitian ini menggunakan teknik triangulasi didalam tahap validasi data. Teknik triangulasi adalah pengecekkan data dengan mencocokkan dengan sesuatu di luar data itu sebagai bahan perbandingan. Teknik triangulasi dilakukan melalui wawancara, observasi langsung dan observasi tidak langsung.

3.3 Metode Pengumpulan Data

Sumber data utama yang diperoleh peneliti dalam penelitian ini adalah kata-kata, tindakan dan data tambahan seperti dokumen lainnya. Penelitian ini menggunakan teknik pengumpulan data untuk mendapatkan sumber data utama dan tambahan. Jenis data yang didapatkan dalam pengumpulan data ini terdiri dari data primer dan data sekunder. Data primer didapatkan melalui wawancara mendalam dengan informan (Praktisi, akademisi dan peneliti). Sedangkan data

https://scholarhub.ui.ac.id/jkskn/vol2/iss1/3
DOI: 10.7454/jkskn.v2i1.10017

ISSN: 2620-7419
Jurnal Kajian Stratejik Ketahanan Nasional, Vol..2, No.1, 2019

sekunder didapatkan dari observasi dan studi dokumen-dokumen yang terkait dengan tujuan penelitian.

3.4 Evaluasi Data

Melakukan evaluasi terhadap suatu informasi adalah sebuah langkah yang bersifat integral dalam suatu proses analisis, dan pada umumnya evaluasi dilakukan pada saat informasi diperoleh. Data dievaluasi menurut tingkat kepercayaan terhadap sumber data serta keakuratan terhadap informasi aktual. Pada saat mengevaluasi informasi, analis memberikan beberapa pertanyaan seperti:

1. Bagaimana tingkat kepercayaan terhadap sumber informasi?
2. Apakah sebelumnya sumber informasi pernah memberikan informasi?
3. Bagaimana tingkat akurasi informasi tersebut?
4. Bagaimana informasi itu pada saat ini?

Proses evaluasi diperlukan karena tipuan informasi atau *deception* merupakan suatu hal yang biasa ditemui didalam dunia intelijen. Untuk membuat tingkat atau level informasi, analis dapat menggunakan *Information Accuracy Codes* dan *Information reliability Codes*

3.5 Teknik Analisis Data

Dalam penelitian ini, analisis data dilakukan oleh peneliti sejak awal penelitian dan selama proses penelitian dilakukan. Data diperoleh, kemudian dikumpulkan untuk diolah secara sistematis. Dimulai dari wawancara, observasi, mengedit, mengklasifikasi, mereduksi, selanjutnya aktivitas penyajian data serta menyimpulkan data. Teknis analisis data dalam penelitian ini menggunakan model analisis interaktif, yaitu suatu analisa yang di mulai dengan tahapan mereduksi data, lalu menyajikan data tersebut dan diakhiri dengan penarikan kesimpulan. Tahap penarikan kesimpulan mulai dari mencari arti-arti implisit dari arti benda-benda, mencatat keteraturan, pola-pola penjelasan, alur sebab akibat dan proposisi. Kesimpulan yang semula belum jelas akan meningkat menjadi kesimpulan yang terperinci. Kesimpulan-kesimpulan final akan muncul bergantung pada besarnya kumpulan-kumpulan catatan lapangan, pengkodeanya, penyimpanan, dan metode pencarian ulang yang digunakan, dan kecakapan peneliti.

4. Hasil & Pembahasan

4.1 Reduksi Data (Data Reduction)

Penelitian ini berhasil mengumpulkan data primer dan data sekunder guna dijadikan bahan analisa lebih lanjut. Data primer yang berhasil peneliti peroleh berasal dari hasil *indepth interview* dengan peneliti intelijen, akademisi maupun praktisi intelijen. Guna menambah kualitas hasil analisa, peneliti juga mengumpulkan data sekunder dengan tehnik observasi dan studi dokumen. Data primer dan sekunder tersebut selanjutnya dievaluasi menurut tingkat kepercayaan serta keakuratan terhadap informasi aktual. Data yang sudah terevaluasi tersebut kemudian direduksi dengan cara merangkum, memilih hal-hal pokok, memfokuskan pada hal-hal penting terkait identifikasi ancaman *PCI* (*Positive Clandestine Intelligence*) dalam bentuk cyber terrorism terhadap keamanan nasional.

Data primer yang diperoleh dari kegiatan wawancara dengan praktisi intelijen (narasumber A) menjelaskan bahwa aktifitas intelijen dalam bentuk *PCI cyber terrorism* memang sudah terjadi di Indonesia. Hal ini dapat dilihat dari kejadian virus wannaCry yang menyerang sejumlah rumah sakit pada tahun 2017. Serangan tersebut tergolong dalam cyber terrorism dengan menggunakan metode Ransomware. Selain contoh tersebut, narasumber juga menambahkan beberapa contoh serangan cyber terrorism seperti serangan cyber terrorism terhadap server Komisi Pemilihan Umum (KPU) pada tahun

ISSN: 2620-7419
Jurnal Kajian Stratejik Ketahanan Nasional, Vol..2, No.1, 2019

2004 dan 2005. Bentuk serangan cyber terrorism pada tahun 2004 berbentuk deface terhadap tampilan halaman tabulasi nasional hasil pemungutan suara milik KPU. Sedangkan bentuk serangan cyber terrorism pada tahun 2005 dalam bentuk takedown server KPU, sehingga jaringan internet di pusat tabulasi nasional KPU tidak dapat berfungsi. Menurut narasumber, tujuan serangan cyber terrorism (CT) terbagi menjadi tiga jenis serangan, yaitu confidentiallity data, integrity data dan terakhir avaibility data.

Data primer kedua, peneliti dapatkan dari hasil wawancara mendalam dengan dosen mata kuliah terorisme di Sekolah Tinggi Intelijen Negara (STIN), DR. Supriyadi, SE.,M.Si. Dalam wawancara mendalam tersebut, beliau memaparkan bahwa bentuk, bentuk serangan cyber terrorism dapat berbentuk wabah virus adalah Serangan virus yang masuk dalam komputer kita; Spammail/mailbomb adalah Serangan yang biasa terjadi pada email seseorang yang dikirimi oleh orang yang tak bertanggung jawab; Dos Attack adalah Serangan yang bisa melumpuhkan sistem computer seseorang jika mereka dikirimi serangan dos attack; Unauthorized Access adalah terjadinya penyusupan pada computer kita tanpa sepengetahuan kita dan tanpa seizin kita.

Data primer ketiga peneliti dapatkan dari hasil wawancara dengan Direktur Eksekutif Center of Intelligence and Strategic Studies, DR (Candidate) Ngasiman Djoyonegoro. Menurut beliau fenomena cyber terrorism sesuai dengan salah satu buku yang beliau tulis, yaitu Intelijen di Era Digital. Serangan terorisme bukan lagi secara konvensional, akan tetapi akan menggunakan media cyber. Hal ini terkait semakin sulitnya pergerakan teroris didalam melakukan ancaman secara konvensional.

Selain data primer, peneliti juga berhasil memperoleh data sekunder dengan tehnik studi dokumen. Peneliti mendapatkan data berupa Kontinum Taksonomis pelaku kejahatan cyber yang berkisar dari orang baru (novice) dan amatir yang berupa kenakalan biasa hingga tindakan terorisme besar. Taksonomis ini peneliti dapatkan dari buku The Psyche of Cybercriminals: A Psycho-Social Perspective karangan Roger M.K. Penjelasan Taksonomi cyber crime tersebut dapat dijelaskan sebagai berikut:

1) Script Kiddies (SK), adalah individu dengan kemampuan teknis yang terbatas, tanpa benar-benar memahami apa dampak dari perilakunya.
2) Cyber-punks (CP), yaitu kelompok yang "memperluas" mentalitas punk ke dunia maya. Kelompok ini tidak memiliki rasa hormat dan tidak perduli pada wewenang, simbol-simbol dan norma-norma sosial.
3) Hacktivist (H), yaitu istilah yang digunakan untuk individu ataupun kelompok yang melakukan perilaku menyimpang, tetapi dengan kamuflase semantik untuk menyamarkan tindakannya.
4) Thieves (T) termasuk kategori penjahat pada umumnya. Motivasi utamanya adalah perolehan finansial dan keserakahan.
5) Virus Writers (VW), dimulai dari masa remja dan berkembang hingga menjadi kategori mantan pembuat (ex-writer) sejalan dengan perkembangan dan kedewasaan kognitif dan kronologisnya. Terdapat sensasi pada tantangan mental dan latihan akademik (belajar) pada proses pembuatan virus.
6) Profressional (P) merupakan kelompok kategori yang paling elit dalam kelompok penjahat cyber, yang memiliki inteligensi kompetitif dan aktivitas yang abu-abu. Individu P ini dapat terlibat dalam penipuan tingkat tinggi hingga spionase korporat.
7) Cyber-terrorist (CT) dapat berupa bagian dari militer atau paramiliter sebuah negara dan diposisikan sebagai

https://scholarhub.ui.ac.id/jkskn/vol2/iss1/3
DOI: 10.7454/jkskn.v2i1.10017

ISSN: 2620-7419
Jurnal Kajian Stratejik Ketahanan Nasional, Vol..2, No.1, 2019

tentara maupun sebaliknya sebagai pejuang pembebasan dalam medan perang dunia maya. Tujuan mereka sama seperti militer tradisional, yaitu untuk memenangkan pertempuran atau peperangan. CT menjalankan dua fungsi yaitu menyerang sistem pertahanan dan masyarakat musuh dan melindungi sistemnya sendiri dari serangan serupa dari pihak lawan.

Dari buku yang sama, peneliti juga mendapatkan data terkait motivasi pelaku cyber crime, yaitu:

1) Social Learning Theory. Proses belajar sosial bekerja dalam konteks struktur sosial, interaksi dan situasi. Perilaku kriminal merupakan sebuah fungsi dari variabel proses belajar sosial, khususnya penguatan/reinforcement. Mekanisme utama dalam belajar sosial adalah termasuk oenguatan diferensial dan peniruan (imitation). Definisi-definisi dalam lingkungan sosial seseorang dicapai dari belajar melalui imitasi dan observasional. Reinforcement capat berbentuk tangible dan intangible rewards berupa aktivitas itu sendiri, uang, atau reward sosial termasuk naiknya status dalam pergaulan sosialnya. Sejalan dengan waktu, imitasi tidak lagi penting karena yang menentukan perilaku selanjutnya adalah reinforcement atau konsekuensinya.
2) Moral Disengagement – moral justification. Para pelaku cybercrime secara umum digambarkan sebagai modern Robin Hood, yang membawa fungsi bernilai dalam masyarakat.
3) Anonymity dan Social Control Theory. Penelitian pada perilaku online menemukan bahwa orang-orang berperilaku secara berbeda dalam cyberspace daripada di dunia riil. Individu cenderung untuk lebih agresif, kurang toleran, lebih sembarangan, dan opininya cenderung lebih terpolarisasi ke titik ekstrim dalam kontinum. Secara sederhana dapat kita pahami bahwa perilaku online merefleksikan diri individu yang sebenarnya dalam kondisi tanpa kontrol diri dan tanpa norma atau tekanan sosial.

Dari data sekunder hasil studi dokumen, terlihat bahwa cyber terrorism merupakan tingkat paling berbahaya dalam taksonomi cybercrime. Hal tersebut dapat terlihat dari pelaku, metode dan sasarannya yang dapat dikategorkan menjadi ancaman terhadap keamanan nasional suatu bangsa. Sedangkan dari sisi motivasi psikology, tindakan cyber terrorism termotivasi oleh variabel Moral Disengagement – moral justification dan Anonymity dan Social Control Theory. Hal ini dapat dilihat dari prilaku pelaku teror yang secara umum digambarkan sebagai sosok modern Robin Hood, yang membawa fungsi bernilai dalam masyarakat sehingga menghasilkan suatu tindakan justifikasi moral. Para pemikir radikal cenderung untuk lebih agresif, kurang toleran, lebih sembarangan. Tindakan maupun opininya cenderung lebih terpolarisasi ke titik ekstrim dalam kontinum. Secara sederhana dapat kita pahami bahwa perilaku online merefleksikan diri individu yang sebenarnya dalam kondisi tanpa kontrol diri dan tanpa norma atau tekanan sosial.

4.1 Evaluasi Data

Setelah data primer dan sekunder telah terkumpul, maka tahap selanjutnya peneliti melakukan evaluasi terhadap tingkat akurasi dan tingkat kepercayaan terhadap sumber data. Hasil dari evaluasi tersebut dapat dilihat pada tabel 1 berikut.

Tabel 1. Akurasi & Kepercayaan Data

ISSN: 2620-7419
Jurnal Kajian Stratejik Ketahanan Nasional, Vol..2, No.1, 2019

No	Jenis Data	Sumber	Kepercayaan	Ketepatan
1	Buku	Perpustakaan	A	1
2	Wawancara	Praktisi	B	2
		Peneliti	B	2
		Akademisi	A	2

4.2 Penyajian Data (Data Display)

Hasil reduksi data yang dihasilkan, kemudian peneliti sajian dalam beberapa tabel seperti tabel tujuan cyber terrorism, bentuk serangan cyber terrorism, posisi serangan cyber terrorism dalam taksologi cyber crime serta motivasi psikologis pelaku cyber terrorism. Berikut adalah tampilannya.

1) Ancaman Positive Clandestine Intelligence (PCI) dalam bentuk Cyber Terrorism (CT) terhadap keamanan nasional mempunyai tiga jenis sasaran, yaitu:

a. Confidentiallity: membuka kerahasian data suatu sasaran sehingga menimbulkan ketakutan terhadap sasaran tindak terorisme. Contohnya terlihat pada kasus snowden dan beberapa kelompok aktifis demokrasi di negara barat yang membuka data-data rahasia pemerintah dan perusahaan ke publik dikarenakan perbedaaan sikap politik.

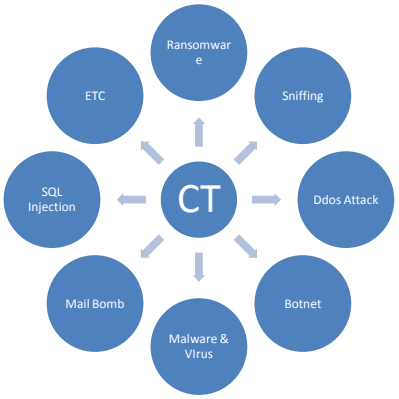
b. Integrity: Merubah integritas suatu aplikasi/sistem jaringan sehingga tidak dapat bekerja secara normal. Contohnya yang terjadi pada aplikasi tabulasi milik KPU yang dirubah tampilannya oleh pelaku cyber terrorism pada tahun 2004 dan 2005.

c. Availability: Menutup akses resmi pengguna jaringan komputer sehingga aplikasi tidak dapat digunakan. Hal ini terjadi pada tahun 2017 di beberapa rumah sakit di Indonesia yang terkena virus wannaCry sehingga jaringan pada rumah sakit terkait tidak dapat digunakan.

Table 2 Jenis Sasaran Cyber Terrorism

2) Hal berikutnya yang dapat ditampilkan dalam penelitian ancaman PCI Cyber Terrorism terhadap keamanan nasional adalah bentuk-bentuk serangan yang dipakai dalam PCI Cyber Terrorism (CT) adalah sebagai berikut:

Table 3 Bentuk Serangan Cyber Terrorism



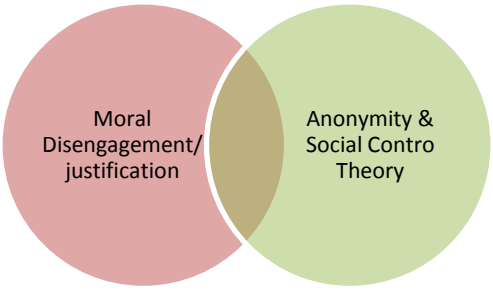
3) Pada tabel keempat ini, peneliti menampilkan hasil penelitian yang berupa motivasi pelaku cyber terrorism (CT) didalam melakukan aksi teror. Didalam daftar jenis motivasi pelaku cybercrime, pelaku cyber terrorism (CT) tergolong kedalam kelompok Moral Disengagement atau moral

https://scholarhub.ui.ac.id/jkskn/vol2/iss1/3
DOI: 10.7454/jkskn.v2i1.10017

ISSN: 2620-7419
Jurnal Kajian Stratejik Ketahanan Nasional, Vol..2, No.1, 2019

justification dan Anonymity & Social Control Theory. Motivasi bisa timbul karena salah satu dari jenis tersebut atau gabungan dari keduanya.

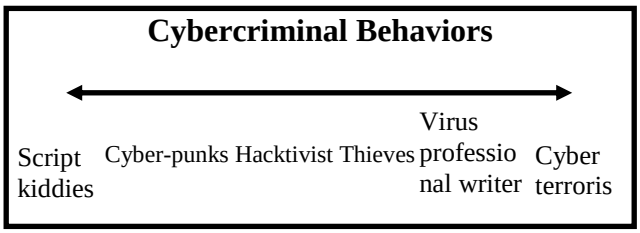
Table 4 Motivasi Pelaku Cyber Terrorism (CT)



4) Penelitian ini juga berhasil menemukan tingkat ancaman cyber terrorism (CT) dalam Kontinum Taksonomi prilaku cyber crime yang berkisar dari orang baru (novice) hingga tindakan terorisme besar. Berikut adalah tampilannya yang diambil dari buku The Psyche of Cybercriminals: A Psycho-Social Perspective karangan Roger M.K.

Pada Taksonomi prilaku cyber crime milik rogers tersebut, tampak posisi cyber terrorism (CT) berada diposisi paling kanan. Hal ini menunjukkan tingkat ancaman cyber terrorism merupakan yang paling tinggi dibandingkan bentuk cyber crime lainnya. Hal ini dikarenakan dampak yang dihasilkan oleh ancaman cyber terrorism sangat besar dan dapat mengganggu Ketahanan nasional di bidang keamanan.

Table 5 Taksonomi Prilaku Cyber Crime Rogers (2010)



5. Kesimpulan & Saran

Positive Clandestine Intelligence (PCI) telah mengalami proses dialektika seiring dengan berubahnya lingkungan tempat PCI digunakan. Terorisme, sebagai salah satu bentuk dari PCI ikut mengalami proses dialektika tersebut. Teror bukan lagi hanya benbentuk *bomb and bullets*, tapi sudah bermetamorfosis kedalam bentuk *bits and bytes*. Pelaku aksi teror sudah tidak perlu lagi keluar dari tempat persembunyian mereka, sebab mereka bisa untuk melakukan aksi teror hanya dengan sebuah komputer. Ancaman PCI dalam bentuk cyber terrorism terhadap keamanan nasional perlu mendapat perhatian khusus bagi para pemangku kepentingan dibidang keamanan nasional, sehingga ketahanan nasional tidak menjadi terganggu.

Dalam penelitian ini, peneliti telah berhasil menghasilkan pengetahuan guna identifikasi ancaman PCI cyber terrorism terhadap keamanan nasional. Pengetahuan yang peneliti hasilkan berupa jenis sasaran Positive Clandestine Intelligence Cyber Terrorism (PCI CT), bentuk serangan PCI CT, motivasi psykologis pelaku aksi PCI CT serta posisi ancaman PCI CT dalam taksonomi prilaku cyber crime milik Rogers M.K.

Daftar Pustaka

Benjamin Cole, "*Conflict, Terrorism and the Media in Asia*", Routledge, 2006

David J Whittaker, "Terrorist and Terrorism in the Contemporary World", Routledge, 2004

Barry Buzan, People, *States and Fear: an Agenda for International Security Studies in the Post-Cold War.* (Boulder: Lynne Rienner Publisher, 1991).

David Mutimer, *Beyond Strategy: Critical Thinking and the New Security Studies, dalam Contemporary Security and*

ISSN: 2620-7419
Jurnal Kajian Stratejik Ketahanan Nasional, Vol..2, No.1, 2019

Strategy, Craig A Snyder (ed), (London: Macmillan Press Ltd, 1999).

Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif dan R&D,* Alfabeta, Bandung, 2009.

Undang-Undang Nomor 17 Tahun 2011

Brian, Jenkins, *International Terrorism: A New Kind of Warfare*, Santa Monica: CA: Rand Corporation, 1974

Peter C.Sederberg, *Terrorist uths: Illusions, Rhetoric, and Reality Change*, Harpercollins College Div, 1993

Irawan Sukarno, "*Ilmu Intelijen," Puslitbang BIN & STIN*. STIN PRESS. 2014.

Wahyono S.K. *"Pengertian dan Lingkup Keamanan Nasional,"* Program Pasca Sarjana UI, Kajian Stratejik Ketahanan Nasional. 2003.

Yohanes Wahyu Saronto, (2004), "*Intelijen Teori, Aplikasi dan Modernisasi",* PT Ekalaya Saputra

Andi Widjajanto &Artanti Wardhani, *"Hubungan Intelijen-Negara,"* Jakarta. 2010.

Bambang Darmono, *"Keamanan Nasional: Sebuah Konsep dan Sistem Keamanan bagi Bangsa Indonesia,"* Sekretariat Dewan Ketahanan Nasional. 2010.

Dr.Uhar Suharsaputra, M.pd, *Metode Penelitian*, Pt.Refika Aditama, Bandung, 2014

https://scholarhub.ui.ac.id/jkskn/vol2/iss1/3
DOI: 10.7454/jkskn.v2i1.10017