 ISBN : 978-602-19681-6-1

PENGUATAN KERJASAMA *CYBER DEFENSE* ASEAN GUNA MENGHADAPI ANCAMAN *CYBERWAR*

oleh : Anang Setiyawan

Abstract

Technology affects the nature of the threat to the country becomes modern and complex. Cyber threats such as cyber war potentially disrupt security and national interests of a country. Cyber threat is a common threat that is increasingly dangerous and need to be addressed comprehensively. Strengthening cyber security cooperation not only on the cooperation of handling the cybercrime issues and cyber terrorists but also cyber defense cooperation to maintain peace and stability of the Asean region.

1. Pendahuluan

Perkembangan dan penguasaan teknologi masa kini tidak hanya mempengaruhi konsep-konsep sosial masyarakat namun juga mempengaruhi sifat ancaman yang lebih modern dan kompleks yang berada pada domain virtual terhadap pertahanan dan keamanan suatu negara. Ancaman *cyber* saat ini tidak terbatas pada bentuk ancaman *cyber* dengan motif ekonomi atau *cybercrime* namun ancaman dalam bentuk *cyberwar* yang lebih mengandung sifat politis dengan tujuan menggangu pertahanan, keamanan maupun kepentingan nasional suatu negara secara luas. Ancaman *cyberwar* dianggap sangat berbahaya karena mampu mengakibakan kehancuran, gangguan, kerusakan jaringan infrastruktur militer maupun sipil yang sangat dibatasi serta diprediksi dampak dan ukurannya

Ancaman *cyber* secara global akan semakin berbahaya, sistematis dan lebih canggih dari sebelumnya. Hal ini disebabkan karena ketergantungan negara terhadap teknologi informasi dan komunikasi yang semakin tinggi sehingga berbanding lurus dengan resiko potensi dan ancaman yang dihadapinya. Saat ini negara-negara maju melihat *cyber space* sebagai domain strategis yang harus

ISBN : 978-602-19681-6-1

dikelola dengan baik karena ancaman *cyber* mampu mempengaruhi keadaan ekonomi, sistem pertahanan dan keamanan nasional suatu negara.

Ancaman global *cyberwar* ini membutuhkan peningkatan perhatian negara-negara diseluruh negara dunia karena penanganan ancaman *cyber* hanya bisa efektif jika dilakukan melalui kerjasama internasional yang kuat. Di Eropa, *cyberwar* yang pernah dialami salah satu negaranya mendorong negara-negara anggota lainnya meningkatkan kesadaran dan kemampuan pertahanan *cyber* negara masing-masing sekaligus bekerja sama menyusun pertahanan *cyber* bersama yang terintegrasi di dalam NATO.

Negara-negara Asean sendiri sebenarnya telah mulai menyadari potensi bahaya ancaman *cyber*, bahkan isu ini telah menjadi bahasan khusus pada beberapa agenda *Asean Regional Forum* (ARF), bahkan ARF Tahun 2015 menghasilkan *ASEAN Regional Forum Work Plan on Security of and in The Use of Information and Communications Technologies*. Isu-isu yang dibahas pada agenda-agenda ARF cenderung terbatas pada penanganan *cybercrime* dan *cyber terrorist* serta belum menyentuh kerjasama penanganan ancaman *cyberwar*. Melalui kesepakatan penguatan pertahanan dan keamanan regional yang dibuat para Menteri Pertahanan Negara Asean melalui *Joint Declaration of the ASEAN Defence Ministers On Strengthening Defence Cooperation of ASEAN in The Global Community to Face New Challenges* seharusnya kerjasama dapat mengarah pada pembentukan *cyber defense* bersama untuk menangani ancaman *cyberwar* yang lebih serius.

Meskipun secara kesadaran normatif Negara Asean terhadap ancaman *cyber* mengalami kemajuan namun kesepakatan-kesepakatan tersebut harus sesegera mungkin diwujudkan mengingat ancaman *cyber* merupakan ancaman bersama yang semakin berbahaya dan membutuhkan penanganan komprehensif. Diperlukan penguatan kerjasama keamanan cyber yang tidak hanya terbatas pada kerjasama penanganan masalah *cybercrime* dan *cyber* terrorist namun juga kerjasama *cyber defense* guna menghadapi ancaman *cyber war* untuk menjaga perdamaian dan stabilitas kawasan Asean.

ISBN : 978-602-19681-6-1

2. Urgensi *Cyber Defense Asean* untuk Menghadapi Ancaman *Cyberwar*

Cyberwar meskipun dilakukan melalui komputer tetapi mampu bersifat destruktif, menyebabkan gangguan di jaringan infrastruktur sipil dan militer yang sangat sulit serta diprediksi dampak dan ukurannya. Serangan pada *Cyberwar* dikatakan berhasil tidak hanya dapat dilihat sebatas akibat kehancuran dapat ditimbulkannya namun juga pada pengaruhnya terhadap kondisi ekonomi suatu negara serta layanan dasar terhadap penduduk sipil seperti misalnya air, listrik, sistem komunikasi, sistem transportasi dll. Efektifitas *cyberwar* ini akan efektif jika ditunjang oleh dua hal, yaitu *means* yang berarti sumber daya manusia dan peralatan untuk menyerang serta *vulnerability* yaitu sejauh mana ketergantungan ekonomi dan militer sebuah negara menggunakan jaringan teknologi informasi dan komunikasi. Teknik serangan yang digunakan dalam *cyberwarfare* identik dengan teknik serangan yang digunakan dalam konteks *cybercrime* dan seringkali sulit sekali untuk dapat dibedakan.

Cybercrime cenderung dilakukan oleh orang atau sebuah kelompok dengan motif ekonomi sedangkan *cyberwar* cenderung dilakukan oleh negara secara langsung, dilakukan orang atau kelompok yang menjadi organ dari negara tersebut dan memiliki kecenderungan menjadikan infrasrukur vital sebagai sasaran serta memiliki motif politik maupun keamanan nasional suau negara. Tingkat ancaman *cyber war* menurut Deb Bodeau, Jenn Fabius-Greene, and Rich Graubart tingkat ancaman *cyberwar* dapat dibagi menjadi 5, yaitu:

ISBN : 978-602-19681-6-1

Threat Level	***Capability***	***Intent***	***Targeting***
Advanced	*The adversary is very sophisticated and Well resourced and can generate its own opportunities to support multiple successful, continuous, and coordinated attacks.*	*The adversary seeks with Great determination to undermine, impede severely, or destroy, a mission, program, or enterprise, by exploiting a presence in the organization's systems or infrastructure. The adversary is concerned about disclosure of tradecraft only to the extent that it would impede their ability to complete their goal*	*The adversary analyzes information obtained via reconnaissance and attacks to target persistently a specific organization, enterprise, program, or mission, focusing on specific high value or mission – critic al information, resources, supply flows, or functions ;specific employees or positions; and supporting infrastructure providers and suppliers and on partnering organizations*
Significant	*The adversary has a* *Sophisticated level of expertise, with Significant resources and opportunities to support multiple successful coordinated*	*The adversary seeks with determination to undermine or impede critical aspects of a mission, program, or enterprise, or place itself in a position to do so in the* *Future , by maintaining a presence in the organization's systems or infrastructure. The adversary*	*The adversary analyzes information* *obtained via reconnaissance to* *target persistently a specific* *organization, enterprise, program,* *or mission, focusing on* *specific high value or*

ISBN : 978-602-19681-6-1

	attacks.	*Is very concerned about minimizing* *Detection of their attacks or disclosure of tradecraft, particularly while preparing for future attacks.*	*mission-critical information, resources, supply flows, or functions,* *specific employees supporting those functions, and/or key positions*
Moderate	*The adversary has Moderate resources, expertise, and opportunities to support* *Multiple successful* *attack*	*The adversary seeks to obtain or modify specific, critical information and/or to usurp or disrupt the organization's cyber resources by establishing a foothold in the organization's systems or infrastructure, but is concerned about minimizing detection of their attacks or disclosure of tradecraft, particularly when carrying out attacks (e.g., ex filtration) over long time periods. The adversary is willing to knowingly impede aspects of the organization's mission to achieve these ends.*	*The adversary analyzes publicly* *available information to target persistently specific high value organizations (and key positions,* *such as Chief Information Officer), programs, or information.*

ISBN : 978-602-19681-6-1

Limited	*The adversary has Limited resources, expertise, and opportunities to support a successful attack*	*The adversary Actively seeks to obtain critical information and/or to usurp or disrupt the organization's cyber resource, and does so without concern about detection of their attacks or disclosure of tradecraft*	*The adversary uses publicly available information to target a class of high value organizations and/or information, and seeks targets of opportunity within that class*
Unsophisticated	*The adversary has very limited resources, expertise, and opportunities to support a successful attack*	*The adversary seeks to usurp, disrupt, or deface the organization's cyber resources, and does so without concern about detection of their attacks or disclosure of tradecraft*	*The adversary may or may not target any specific organization or class of organization.*

Tabel 1. Tingkatan Ancaman C*yber* dalam Konteks C*yberwar*

 ISBN : 978-602-19681-6-1

Selama ini banyak sekali serangan *cyber* yang terjad, antara lain Serangan *cyber* Rusia terhadap Estonia Tahun 2007 selama 3 minggu nyaris melumpuhkan sektor ekonomi karena tingginya ketergantungan penggunaan negara ini terhadap infrastruktur teknologi informasi pada semua bidang termasuk bidang komunikasi, perbankan dimana mayoritas transaksi perbankan di negara ini dilakukan secara elektronik.

Tahun 1998 serangan *cyber* AS dan NATO berhasil melumpuhkan dan mengecoh pertahanan udara serta pengatur lalu lintas udara Serbia (*Serbia Air Traffic Controller*) sebelum dilakukannya serangan bom terhadap target Serbia di Kosovo. Selain itu juga memblokade jaringan komunikasi Yugoslovakia selama konflik berlangsung. Strategi serupa digunakan angkatan udara Israel ketika melintas dengn tujuan menyerang fasilitas nuklir di Syria pada September 2007 tanpa dapat dideteksi oleh sistem radar pertahanan udara Syria. Teknik serangan *cyber* tersebut membuat radar tidak dapat mendeteksi aktifitas lalu lintas udara ketika malam terjadinya serangan, namun teknik serangan yang digunakan Israel tersebut masih belum bisa diketahui.

Pada tahun 2009, China diduga melakukan serangan *cyber* sistematis dan berskala besar yang dikenal dengan *GhostNet* dan *Operation Aurora*. *GhostNet* adalah serangan *cyber* dengan menggunakan virus terhadap beberapa kedutaan antara lain India, Korea Selatan, Indonesia, Taiwan, Thailand, Pakistan dan Jerman. Serangan ini juga menyerang Kementerian Luar Negeri Indonesia, Iran, Bhutan, Bangladesh, Brunei. Virus tersebut memiliki kemampuan mengaktifkan dan mengkontrol *webcam*, mikrofon dikomputer yang terinfeksi. Sedangkan *Operation Aurora* digunakan untuk mengakses program komputer, *source code* dari sektor teknologi informasi, perusahaan keamanan dan pertahanan. Bahkan China juga diduga kuat melakukan serangan *cyber* skala besar yang dikenal sebagai *Operation Night Dragon* dan *Operation Shady Rat* terhadap perusahaan bidang minyak, energy dan petrokimia serta 72 organisasi di dunia selama 6 Tahun sejak Juli 2006.

Pada tahun 2010 AS dan Israel diduga melakukan serangan cyber terhadap program fasilitas pengayaan Uranium milik Iran melalui virus *Stunext* dan kemudian pada tahun 2012 menggunakan virus *Flame* untuk menyerang kantor

ISBN : 978-602-19681-6-1

pemerintahan Iran dan negara di Timur Tengah yang mampu mengaktifkan peralatan yang terhubung dengan jaringan komputer dan komunikasi dengan tujuan memata-matai.

Kasus-kasus diatas menunjukkan bagaimana serangan *cyber* dapatdigunakan secara sistematis untuk melemahkan, mengganggu sistem pertahanan, sistem ekonomi, sistem infrastruktur publik, dan jaringan infrastruktur vital lainnya yang terkait dengan keselamatan dan keamanan suatu negara. Oleh karena itu penting bagi negara-negara didunia terutama negara-negara di Asean untuk memperkuat kerjasama dalam bidang keamanan *cyber* serta menyusun langkah bersama secara nyata untuk menangani ancaman *cyberwar* yang dapat mengganggu stabilitas ekonomi dan keamanan kawasan.

Penguatan kerjasama pertahanan negara-negara Asean sebenarnya telah berjalan melalui beberapa forum antara lain *the ASEAN Chiefs of Army Multilateral Meeting* (ACAMM), *ASEAN Chiefs of Defense Forces Informal Meeting* (ACDFIM), *ASEAN Defense Minister's Meeting* (ADMM), termasuk ADMM *Plus*, dan *ASEAN Regional Forum* (ARF). Selain itu terdapat dialog pertahanan *the Shangri-La Dialogue* yang diselenggarakan setiap tahun oleh *International Institute for Strategic Studies* (IISS). Namun penguatan kerjasama pertahanan masih terbatas membahas pada penanganan *cybercrime* dan *cyberterorist* dan belum mengakomodir masalah *cyberwar*.

Melihat dampak *cyberwar* terhadap keadaan ekonomi, keamanan dan kepentingan nasional suatu negara maka mutlak bagi Asean untuk segera membentuk *Cyber Defense Asean* dalam menjaga stabilitas kawasan. Hal ini sejalan tujuan *ASEAN Political-Security Community* (APSC) untuk membentuk perdamaian bagi negara-negara di kawasan ASEAN dan dunia dalam lingkungan yang demorkatis dan harmonis. Bahkan Malaysia dalam forum *The Shangri-La Dialogue* tahun 2012 menyatakan bahwa penting untuk segera membangun *cyber defense* yang lebih komprehensif dalam upaya menangani serangan yang terus meningkat.

Membangun *cyber defense* yang komprehensif artinya tidak hanya memperkuat infrastruktur keamanan *cyber* namun juga meliputi strategi, kebijakan, , riset dan kerjasama dengan berbagai pihak terkait dengan keamanan

ISBN : 978-602-19681-6-1

cyber yang tidak terbatas pada entitas negara seperti misalnya organisasi internasional, perusahaan keamanan *cyber*. Termasuk pula pembentukan organisasi *cyber defense Asean* yang mengkordinir penanganan masalah keamanan *cyber* yang mempengaruhi keamanan dan stabilitas kawasan Asean. Selain itu juga mendorong peningkatan kesadaran keamanan *cyber* dari semua pengguna teknologi informasi dan komunikasi di kawasan Asean melalui pendidikan dan pelatihan yang terpadu.

ISBN : 978-602-19681-6-1

Daftar Pustaka

Clarke, Richard A and Robert K. Knake. Cyber war: the next threat to national security and what do about it. New York: Ecco, 2010.

Lior Tabansky. Basic Concept in Cyberwarfare. Military and Strategic Affairs. Vol 3. No 1. May 2011. Pg 75-92.

Fred Scherer, Cyber warfare, DCAF Horizon 2015 Working Paper No. 7

Deb Bodeau, Jenn Fabius-Greene, and Rich Graubart, How Do You Assess Your Organization's Cyber Threat Level?, The Mitre Corporation, https://www.mitre.org/sites/default/files/pdf/10_2914.pdf

Muhammad Saleem & Jawad Hassan, "cyber warfare" the truth the real case, Project Report for Information Security Course, Linköping Universitetet, Sweden

Jason Porterfield, 2011. Careers as a Cyberterrorism Expert. The Rosen Publishing Group,

Jon Schiller, 2010. Cyber Attacks & Protection: Civilization Depends on Internet & Email, CreateSpace.

Prof. Dr. Dr. K. Saalbach, Cyber War ; Methods and Practice. Version 6.0-2 January 2013;1-54.

Oona A. Hathaway, Rebecca, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue & Julia Spiegel. The Law of Cyber-Attack.California Law Review [Vol. 100:817-2012]

http://www.inquiriesjournal.com/articles/1343/stuxnet-the-worlds-first-cyber-boomerang

http://id.berita.yahoo.com/flame-serang-komputer-di-iran-dan-timur-tengah-051143829.html,

ISBN : 978-602-19681-6-1

http://www.pelitaonline.com/read/iptek/internasional/28/17447/virus-flame-serang-ribuan-komputer-di-iran/

http://www.beritasatu.com/iptek/50900-virus-flame-diciptakan-untuk-serang-iran.html

http://www.antaranews.com/berita/313053/virus-the-flame-serang-iran.

http://www.fkpmaritim.org/diplomasi-pertahanan-asean-dalam-rangka-stabilitas-kawasan/

https://www.iiss.org/en/events/shangri%20la%20dialogue/archive/sld12-43d9/fourth-plenary-session-1353/dato-seri-dr-ahmad-zahid-hamidi-b13b

http://www.theguardian.com/technology/2007/nov/29/hacking.news

http://rt.com/news/mini-flame-malware-kaspersky-519/