Global Political Studies Journal
Volume 6 Nomor 1 Edisi April 2022
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v6i1

Jaga Diri di Baltik

Edmondus Iswenyo Noang
Alumni Kajian Wilayah Eropa, Universitas Indonesia
Jl. Salemba Raya No. 4, Jakarta Pusat

e-mail: iswenyo@gmail.com

Abstract

Finland is geographically and politically bordered by Russia. This makes Finland as buffer zone between Russia and Europe. Politically, Finland is a member of the European Union, but not a member of NATO. This article focuses on the reasons why Finland cooperates with NATO in the Political Framework on Cyber defence which was signed on February 16, 2017. The research methodology used is qualitative with a literature study method. The problem analysis in this article uses complex interdependence theory. The article concludes that Finland and NATO need such cooperation as a precaution against future attacks such as the denial of service on websites of non-governmental organizations, companies, and the Ministry of Defense. For NATO, cooperation is a measure to anticipate threats that come from closest enemies who have the potential to steal information or secret documents of the organization.

Keywords: *Cyber defence, Finland, Geopolitics, NATO*

Abstrak

Finlandia secara geografis dan politik berbatasan langsung dengan Rusia. Hal tersebut menjadikan Finlandia sebagai *buffer zone* antara Rusia dan Eropa. Secara politik, Finlandia adalah negara anggota Uni Eropa, tetapi bukan anggota NATO. Artikel ini berfokus pada penyebab Finlandia menjalin kerjasama dengan NATO dalam *Political Framework on Cyber defence* yang ditandatangani pada 16 Februari 2017. Metodologi penelitian yang digunakan adalah kualitatif dengan metode studi pustaka. Analisis masalah pada artikel ini menggunakan teori *complex interdependence*. Kesimpulan dari artikel adalah Finlandia dan NATO memerlukan kerjasama tersebut sebagai langkah antisipasi terhadap serangan di masa depan seperti yang pernah terjadi yaitu *denial of service* pada website organisasi non pemerintah, perusahaan, dan Kementerian Pertahanan. Bagi NATO, kerjasama sebagai langkah antisipasi ancaman yang datang dari musuh-musuh terdekat yang berpotensi mencuri informasi atau dokumen rahasia organisasi tersebut.

Kata kunci: Finlandia, NATO, Pertahanan siber, Geopolitik

1. Pendahuluan

1.1 Latar Belakang

Hubungan Internasional pada masa lampau berfokus pada kajian mengenai perang dan damai. Selanjutnya, objek kajian ilmu tersebut menjadi lebih luas untuk mempelajari perkembangan, perubahan, dan kesinambungan yang berlangsung dalam hubungan antar negara atau antar bangsa dalam konteks sistem global tetapi masih menitik berat pada *high politics*. Hubungan internasional kontemporer tidak lagi memfokuskan perhatian dan kajian kepada hubungan politik yang berlangsung antar negara atau antar bangsa dengan ruang lingkupnya melintasi batas-batas wilayah negara. Peran dalam hubungan internasional juga mencakup kegiatan yang dilakukan oleh aktor-aktor non negara (Rudy,2011)

Global Political Studies Journal
Volume 6 Nomor 1 Edisi April 2022
P-ISSN 2301-749X E-ISSN 2686-2905
DOI 10.34010/gpsjournal.v6i1

Globalisasi telah mengubah tatanan hubungan internasional di abad ke-21 dimana terjadi perpindahan arus manusia, barang dan informasi terjadi sangat cepat dalam waktu yang singkat. Hal ini mendorong terjadinya pergeseran budaya masyarakat dan perubahan dalam struktur politik internasional. Tatanan global saat ini tidak lagi bergantung pada wilayah, kekuatan militer, dan sumber daya manusia. Saat ini, hubungan internasional juga bergantung pada penyebaran informasi melalui internet, pembaruan teknologi, dan institusi yang fleksibel (Wenger, 2001). Kepentingan nasional tidak hanya semata-mata pada ekonomi, tetapi juga pada isu-isu global seperti migrasi internasional, terorisme, krisis lingkungan, penyebaran senjata, hingga *cyber threat* (Brown & Studemeister, 2001).

Cyber threat merupakan nama lain bagi ancamaan yang dilakukan melalui dunia maya atau *cyber space*. Istilah *cyber space* dikenalkan oleh penulis fiksi William Gibson yang mendefinisikannya sebagai ruang "halusinasi konsensual". *Cyber space* adalah sebuah arena dimana seluruh jaringan komunikasi, data, sumber dan pengguna informasi melebur dalam sebuah dimensi elektronik yang berinteraksi dengan kecepatan sangat tinggi, sangat beragam, dalam volume yang sangat besar. Pada kenyataannya *cyber space* sebenarnya tidak bersifat maya seperti yang dibayangkan, tetapi bersifat nyata dimana dalam sebuah ruangan dibangun komputer sebagai server, kabel, baik tembaga hingga *fiber-optic*, bentangan *repeaters*, dan satelit serta gadget telekomunikasi kabel dan seluler (Nugroho, 2014).

Salah satu negara pelopor perkembangan teknologi informasi dan komunikasi adalah Finlandia, yang merupakan negara asal Nokia. Dalam sejarahnya, Nokia pernah menjadi perusahaan telekomunikasi terbaik di dunia sebelum era Android dan Apple. Secara geografis, Finlandia terletak di semenanjung Skandinavia dan berbatasan dengan Swedia, Norwegia, Rusia, Laut Baltik, dan Samudera Arktik. Pasca berakhirnya Perang Dunia II, Finlandia berada dibawah bayang-bayang Uni Soviet hingga akhir Perang Dingin pada akhir tahun 1980-an. Pada 1 Januari 1995, Finlandia secara resmi bergabung dengan Uni Eropa. Negara ini menghabiskan sebagian besar anggaran dalam bidang pendidikan, kegiatan pelatihan, dan penelitian (BBC, 2016).

Di regional Eropa, Finlandia merupakan anggota Uni Eropa, dan belum menjadi anggota NATO. Seiring perkembangan teknologi, sistem pertahanan tidak hanya berfokus pada segi militer, tetapi juga nirmiliter seperti *cyber defence*. Kasus *cyber attack* terbaru yang dialami Finlandia adalah *Denial of Service* (DoS) pada situs Kementerian Pertahanan Finlandia pada 22 Maret 2016. Serangan tersebut terjadi beberapa jam sebelum pertemuan Presiden Finlandia Sauli Niinisto dan Presiden Rusia Vladimir Putin dengan agenda penguatan kerjasama perbatasan (Defense News, 2016).

Dengan posisi yang dimiliki, pemerintah Finlandia menjamin keamanan dalam negerinya terkait isu-isu *cyber crime* dengan mengeluarkan *Finland's Cyber Security Strategy* tahun 2013. Pada buku strategi tersebut dijelaskan tiga visi *Cyber Security Strategy* Finlandia adalah Menjamin keamanan dari segala *cyber threats* dalam situasi apapun; Masyarakat, pemerintah, dan pebisnis dapat memanfaatkan *cyber domain* secara baik dalam akses baik nasional maupun internasional; dan Pada tahun 2016

Finlandia akan menjadi pelopor global dalam menghadapi ancaman *cyber* dan mengatasi masalah akibat ancaman *cyber* tersebut.

Di level regional, Uni Eropa telah mengeluarkan *EU Cyber Defence Policy Framework* tahun 2014 dimana fokus dari kebijakan tersebut adalah mendukung pengembangan *cyber defence* negara anggota yang mendukung *Common Security and Defence Policy* (CSDP) dan sebagai CSDP akan bergantung pada C4 yaitu *Command, Control, Communications* dan *Computer* (C4). Kebijakan ini juga meningkatkan perlindungan jaringan komunikasi CSDP yang digunakan oleh entitas Uni Eropa.

NATO sebagai organisasi pakta pertahanan negara-negara Eropa dan Amerika Serikat juga memiliki kebijakan terkait *cyber defence*. Hal ini ditandai dengan adanya kerjasama *Cooperative Cyber Defence Centre of Exellence* (CCDCOE) yang berpusat di Tallin, Estonia. Kegiatan tersebut bukanlah sebuah pusat operasi *cyber* dan tidak berada di bawah struktur komando NATO secara langsung. Pembiayaan dan pelaksanaan dikembalikan pada negara-negara anggota CCDCOE. *Cyber Defence Centre* dibangun untuk memperkuat kapabilitas, kerjasama dan pertukaran informasi antara NATO, negara anggota CCDCOE dan partner dalam *cyber defence* dengan mengutamakan pendidikan, penelitian dan pengembangan, dan konsultasi (Atlantic Council, 2013).

Cyber defence menjadi salah satu unsur *collective security* NATO dan sekutunya. NATO juga menegaskan dukungan terhadap penerapan hukum internasional dalam *cyber space*. Secara umum, pandangan NATO terhadap adanya *cyber defence* adalah untuk mengimbangi ancaman yang bergerak semakin luas dan membangun pertahanan *cyber* yang kuat, yang dipertegas dengan adanya adopsi kebijakan *cyber defence* dan telah disepakati pada KTT Wales bulan September 2014.

Pada KTT Warsawa 2016, NATO dan aliansinya setuju untuk memperkuat dan meningkatkan pertahanan *cyber* dan pembaharuan infrastruktur nasional. NATO juga menegaskan kembali mandat pertahanan NATO dan mengakui dunia maya sebagai wilayah operasi di mana NATO harus mempertahankan dirinya secara efektif seperti di udara, di darat dan di laut. Krisis dan konflik saat ini kebanyakan terjadi di ranah *cyber*, memperlakukan dunia maya sebagai wilayah operasi akan memungkinkan NATO untuk melindungi dan menjalankan misinya dengan lebih baik (NATO, 2016).

1.2 Pertanyaan Penelitian

Mengapa Finlandia dan NATO menjalin kerjasama dalam *Political Framework on Cyber defence?*

2. Kajian Pustaka dan Kerangka Pemikiran

Dalam kontribusi terhadap ilmu pengetahuan, penulisan artikel ini memberikan pandangan baru dalam melihat isu-isu terkait *cyber defence* menggunakan teori *complex interdepence*. Kerjasama ini merupakan program baru dari Finlandia dan NATO, dan belum ada penulisan tentang program kerjasama ini di Indonesia.

Penulisan artikel ini menarik karena isu-isu keamanan siber menjadi keresahan bersama yang dihadapi negara-negara di dunia, termasuk Eropa. Pola kehidupan yang serba digital bagai dua mata pisau dengan memberikan dampak positif sekaligus negatif. Dampak positif digital memberikan kemudahan akses informasi, administrasi dan komunikasi bagi setiap orang. Aspek negatifnya adalah privasi para pengguna layanan internet atau online dapat disadap, dibajak, oleh pihak-pihak yang tidak bertanggung jawab untuk mendapatkan keuntungan tertentu.

Melihat sisi baik dan buruk di atas, penulisan artikel ini bisa menjadi

pembelajaran bagi Indonesia, dimana negara-negara maju dalam hal teknologi seperti Finlandia dan organisasi sekaliber NATO bisa mendapat *cyber threat* yang mengganggu privasi dan rawan pencurian dokumen penting negara. Sistem digital yang makin marak di Indonesia, seharusnya diimbangi dengan tingkat keamanan akses informasi. Contoh kasus *cyber threat* di Indonesia antara peretasan situs perusahaan telekomunikasi negara, Telkomsel. Serangan lain yaitu virus *ransomware wannacry* pada website RS Dharmais, Jakarta. Dengan adanya kejadian seperti ini, Indonesia wajib meningkatkan level keamanan *cyber* dan menjalin kerjasama dengan aktor-aktor yang memiliki kemampuan dalam bidang tersebut.

Teori yang dipakai dalam menganalisis masalah dalam artikel ini adalah *Complex Interdependence*. Teori ini dikembangkan oleh Robert O. Keohane dan Joseph S. Nye pada akhir 1970-an. Hal ini membantah realisme tradisional dan struktural yang berfokus pada kemampuan militer untuk menjelaskan perilaku negara. *Complex Interdependence* sebaliknya menyoroti munculnya aktor transnasional dan berfokus pada bangkitnya rezim dan institusi internasional. Dalam kebijakan luar negerinya, teori ini lebih menekankan aspek ekonomi daripada militer. *Complex Interdependence* menjadi komponen utama perspektif neoliberal dan telah banyak digunakan dalam analisis pembuatan politik internasional. Sebuah upaya memahami suatu negara untuk masuk ke dalam aliansi kerja sama satu sama lain dalam kondisi anarki dan ketergantungan.

Di dunia kontemporer, istilah *interdependence* sering digunakan untuk menjelaskan ketergantungan antara aktor negara dan aktor non-negara. Ketergantungan tersebut akan menciptakan kompetisi atau kerjasama dan adanya timbal balik dari ketergantungan tersebut. Kebijakan dan tindakan satu aktor memiliki dampak besar pada kebijakan dan tindakan aktor lainnya dan sebaliknya (Rana, 2015).

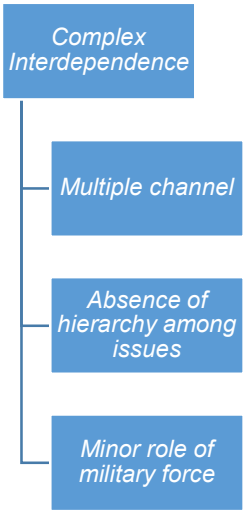
Ketika derajat interdependensi yang tinggi, negara-negara akan sering membentuk institusi-institusi internasional untuk menghadapi masalah-masalah bersama. Institusi-institusi memajukan kerjasama lintas batas internasional dengan menyediakan informasi dan dengan mengurangi biaya. Institusi tersebut dapat berupa organisasi formal seperti *World Trade Organization* atau Uni Eropa atau *Organization for Economic Cooperation and Development* atau dapat berupa serangkaian persetujuan yang agak formal atau kerjasama dalam menghadapi isu-isu bersama seperti perjanjian tentang navigasi, penerbangan, komunikasi dan lingkungan (Jackson & Sorensen, 2013).

Ada tiga variabel yang menjadi model analisis dalam teori ini antara lain, *multiple channels*, *absence of hierarchy among issues* dan *minor role of military force*. Pertama, *Multiple channels*, menjelaskan bahwa dalam politik internasional siapapun bisa berinteraksi, termasuk hubungan antar aktor negara, aktor non-negara seperti organisasi internasional, rezim internasional, *multinational corporation*, organisasi internasional non-pemerintahan. Interaksi yang terjalin tidak hanya bersifat formal dan informal antar pemerintah, tetapi hubungan informal antara pemerintah dan aktor non-negara juga menjadi semakin penting. Kedua, *Absence of hierarchy among issues*, bahwa dalam hubungan interdependence, tidak ada hierarki atau struktur terkait isu-isu apa yang paling penting dan menjadi prioritas. Tidak seperti realis, yang menekankan militer adalah komponen utama dalam hubungan internasional, variabel ini menekankan pada setiap isu yang diangkat oleh para aktor-aktor adalah sama dan dapat memberikan keuntungan dalam ketergantungan tersebut. Ketiga, *Minor role of military force*, menjelaskan bahwa dalam hubungan ketergantungan antar aktor yang semakin kompleks, isu-isu terkait militer mulai berkurang (tetapi

masih dianggap penting) sebab hubungan politik saat ini juga bergantung pada hal-hal terkait ekonomi, lingkungan, komunikasi dan lain-lain.

Model analisis akan digambarkan dalam pola di bawah ini:

Gambar 1. Model Analisis Complex Interdependence



Dalam artikel ini penulis menganalisis bahwa *Complex Interdependence* adalah hubungan kerjasama antara Finlandia dan NATO, dimana Finlandia sebagai *state actor* dan NATO sebagai *non-state actor* (organisasi internasional). Pada variabel pertama, *multiple channels* penulis merumuskan mengenai Finlandia sebagai sebuah negara menjalin kerjasama dengan NATO yang merupakan organisasi internasional. Variabel kedua, *absence of hierarchy among issues* bahwa dalam kerjasama ini tidak ada isu-isu tertentu yang dijadikan prioritas. Isu yang dijalankan dalam kerjasama, dalam hal ini terkait *cyber defence* merupakan hal penting bagi kedua pihak yang bekerjasama. Ketiga, *minor role of military force,* disini penulis menjelaskan bahwa *cyber defence* merupakan sebuah isu nirmiliter seperti disebutkan pada latar belakang, karena tidak menggunakan operasi militer khusus, tetapi lebih pada hal-hal yang bersifat kegiatan pembelajaran dan pertukaran informasi terkait *cyber crime* atau *cyberthreat*.

3. Metode Penelitian

Metode yang dipilih dalam melakukan penelitian ini adalah kualitatif. Metode kualitatif umumnya dipakai oleh peneliti hubungan internasional dalam menganalisis masalah penelitian. Metode tersebut menjadi landasan artikel ini untuk memaparkan penyebab Finlandia menjalin kerjasama *cyber defence* dengan NATO. Studi pustaka adalah teknik yang dipakai dalam proses pengumpulan data. Studi pustaka merupakan teknik pengumpulan data dari bahan-bahan berupa tulisan, buku, jurnal, majalah ilmiah, dokumen terkait alur penulisan artikel ini. Proses pengumpulan data juga dilakukan melalui penelusuran *online* dengan mengakses situs-situs terkait Finlandia dan NATO.

4. Hasil dan Pembahasan

4.1 *Minor role of military force*: *Cyber defence* sebagai isu minor militer

Cyber space adalah sebuah jaringan dimana manusia dan manusia dihubungkan melalui mesin komputer dan jaringan telekomunikasi, biasanya bekerja atas perintah manusia, atau melalui mesin-mesin yang sudah deprogram oleh manusia. *Cyber space* merupakan tempat interaksi baik bersifat menguntungkan maupun merugikan (Nugroho, 2014).

Adanya interaksi-interaksi tersebut tidak lepas dari adanya *Internet Freedom* yang pertama kali dicetuskan oleh Hillary Clinton. Kandidat Presiden AS pada tahun 2016 tersebut mengatakan bahwa kebebasan internet mencerminkan kekuatan teknologi yang mampu mempercepat perubahan politik, sosial dan ekonomi, sehingga setiap negara harus memberikan kebebasan internet kepada warga negaranya sebagai bentuk kebebasan sipil dan hak asasi manusia. Namun

kebebasan internet tidak sepenuhnya absolut. Dalam upaya melindungi dan melanjutkan kebebasan internet, pemerintah negara-negara harus mengambil peran dalam menjamin hak dan kepentingan komunitas masyarakatnya. Sejak tahun 2011 tercatat 2 milyar orang terhubung melalui koneksi internet dengan pengguna tertinggi berada di Amerika Utara dan Eropa (Putri, 2015).

Karena adanya kebebasan internet bagi setiap orang, maka potensi untuk melakukan tindak kejahatan bisa dilakukan oleh siapapun. Ancaman dalam dunia *cyber* tidak selalu berasal korps militer suatu negara, tetapi dari suatu individu atau suatu organisasi dengan kepentingan-kepentingan tertentu.

Ada beberapa ancaman *cyber* seperti *Intrusion*, yaitu masuknya penyerobot ke dalam sistem dan aplikasi komputer tanpa seizing dan sepengetahuan pengguna dan berusaha mengubah sistem pengguna. *Fraud*, yaitu bentuk penipuan yang menggunakan satu atau lebih komponen internet dan telekomunikasi termasuk ruangan chat, email, website untuk mendapatkan keuntungan nominal tertentu. *Harrasment*, berisi pengiriman gambar porno atau kekerasan, baik untuk sekadar mengganggu hingga untuk ancaman. *Hack Threat*, yaitu berupa serangan ke dalam sistem dan aplikasi komputer target yang menjadi sasarannya. *Denial of Service*, yaitu serangan ke dalam sistem atau aplikasi komputer yang menyebabkan gagalnya pengguna untuk menggunakan sistem komputer miliknya (Nugroho, 2014).

Ada tiga tingkat ancaman cyber, seperti di bawah ini.

Gambar 2. Piramida Tingkat Ancaman *Cyber*

Pada ancaman individu, penanggung jawab adalah individu. Dalam level kasus tertentu dibantu dapat dibantu oleh organisasi. Serangan *cyber* kepada individu biasanya dilakukan untuk memperoleh keuntungan. Kejadian tersebut dapat mengarah pada individu sebagai bentuk persaingan antar organisasi. Di level negara dan organisasi internasional, penanggung jawab adalah negara khususnya perlindungan terhadap website dan dokumen-dokumen rahasia kenegaraan yang disimpan secara online. Di level global, merupakan tanggung jawab semua negara terhadap upaya ancaman, seperti pada kasus penyadapan terhadap beberapa kepala negara pada tahun 2009.

Terkait *cyber defence* bahwa dalam memberikan perlindungan di dunia maya, peran militer dikurangi, tetapi lebih pada pihak-pihak yang mampu menguasai sistem jaringan komunikasi seperti teknisi atau perusahaan komunikasi. Dengan adanya kebebasan internet, siapapun bisa berpotensi memberikan ancaman maupun mendapatkan ancaman, bahkan individu-individu tersebut telah membangun komunitas-komunitas seperti *Anonymous*.

4.2 *Multiple channels*: Kerjasama Finlandia dan NATO

Pada 16 Februari 2017 Finlandia dan NATO menandatangani perjanjian kerjasama *Political Agreement on Cyberdefence*. Inti dari kerjasama tersebut adalah melindungi dan memperkuat jaringan komunikasinya. Rancangan kerjasama ini dimulai sejak tahun 2011. Kerjasama tersebut akan meliputi pelatihan, simulasi, dan lain-lain. Ancaman *cyber* saat ini mengalami perkembangan yang cukup pesat sehingga kedua aktor hubungan internasional tersebut secara kolektif mengembangkan kemampuan *cyber defence* dan berkontribusi pada pertahanan nasional dan kawasan.

Finlandia telah bekerjasama dengan NATO di bidang *cyber* seperti dalam CCDCOE, tetapi dalam perjanjian yang benar-benar mengikat secara bilateral adalah kerjasama ini. Dengan adanya kerjasama ini, kedua pihak akan lebih leluasa dalam memperkuat *cyber defence* masing-masing, seperti responsif terhadap adanya ancaman dengan pertukaran informasi, pengembangan kemampuan *cyber*, kegiatan pembelajaran, dan pendeteksian apabila terjadi insiden-insiden dalam dunia *cyber*. Finlandia merupakan negara pertama yang menjalin kerjasama *cyber defence* dengan NATO (Valtioneuvosto, 2017).

4.3 *Absence of hierarchy among issues*: Isu *Cyber defence* bagi Finlandia dan NATO

Finlandia telah mengeluarkan proposal pendanaan lembaga legislatif dan intelijen yang dimaksudkan untuk memperkuat keamanan nasional dan infrastruktur pertahanan *cyber*. Salah satu upaya penting Finlandia yaitu pembentukan *NATO-supported European Centre of Excellence for Countering Hybrid Threats* (ECE-CHT). Selain Finlandia, ada 8 negara lain turut bergabung yaitu Prancis, Jerman, Latvia, Lithuania, Polandia, Swedia dan Inggris. Negara bagian lain diperkirakan akan bergabung dengan ECE-CHT, yang akan dibuka pada paruh kedua tahun 2017 (Fifth Domain, 2017).

Pada Februari 2017, NATO mengeluarkan pernyataan bahwa ancaman *cyber* saat ini menjadi nyata bagi anggotanya. Menurut NATO ancaman tersebut dapat mengarah kepada siapa saja baik aktor-aktor negara maupun aktor non negara. NATO menginginkan *collective security* antar anggotanya. Kegiatan yang dilakukan NATO antara lain memperkuat kemampuan dalam pelatihan, pendidikan dan simulasi, Penandatanganan kerjasama dengan Uni Eropa dalam *Technical Arrangement on cyber defence cooperation* pada Februari 2016, mengingat tantangan bersama NATO dan Uni Eropa dalam memperkuat kerja sama mereka di bidang *cyber defence* terutama di bidang pertukaran informasi, pelatihan, penelitian dan latihan. NATO terlihat semakin intens dalam bidang *cyber defence* melalui NATO *Industry Cyber Partnership* (NATO,2017).

5. Kesimpulan

Penggunaan teori *complex interdepence* pada artikel ini, mendukung analisis kerjasama antar aktor negara dan aktor non negara. Variabel dalam teori dipakai dalam menganalisis masalah ini.

Kesimpulan dari penulisan artikel ini adalah bahwa isu-isu terkait dunia *cyber* telah menjadi salah satu masalah global saat ini. Adanya kebebasan akses internet yang umumnya diberikan oleh pemerintah kepada warga negaranya, tidak sepenuhnya berdampak positif. Hal ini karena beberapa individu maupun kelompok menggunakan jaringan internet untuk tindak kejahatan, seperti perdagangan manusia, senjata, *harassment, hacking or cracking,* hingga *denial of service*.

Langkah kerjasama *cyber defence* yang diambil Finlandia dan NATO bisa dibilang tepat, karena Finlandia telah mengalami beberapa serangan *denial of service* yang melanda website organisasi non pemerintah, perusahaan hingga

Kementerian Pertahanan. Sedangkan NATO, ini sebagai langkah antisipasi ancaman yang datang dari musuh-musuh terdekat yang berpotensi mencuri informasi atau dokumen rahasia organisasi tersebut.

Pada masa yang serba digital ini, dimana semua akses informasi dan data-data bersifat rahasia entah bagi individu, kelompok, organisasi, negara, hingga global, sangat dibutuhkan perlindungan yang baik dan kokoh agar tidak mudah disusupi atau dibajak oleh pihak yang tidak bertanggung jawab. Penulis menilai bahwa langkah kerjasama *cyber defence* ini bisa menjadi contoh bagi negara-negara dan organisasi internasional lain untuk memperhatikan masalah ini, menjalin kerjasama dengan pihak-pihak yang dianggap mumpuni dalam ilmu pengetahuan dan teknologi. Lebih lanjut, actor penyebab kejahatan di ranah maya masih bersifat abstrak atau sulit untuk diidentifikasi secara pasti.

Daftar Pustaka

Acuan dari buku:

Couloumbis, Theodore A. & James H. Wolfe. (1999). Pengantar Hubungan Internasional: Keadilan dan Power. Bandung: CV Putra A. Bardin.

Jackson, Robert & Georg Sorensen. 2013. Introduction to International Relations fifth edition. New York: Oxford University Press Inc.

Nugroho, Riant. 2014. *National Security Policy: Sebuah Pengantar*. Yogyakarta: Pustaka Pelajar.

Putri, Sylvia Octa. 2015. *Hubungan Internasional dan Information and Communication Technology (ICT)*. Dalam Andrias Darmayadi, dkk. *Mengenal Studi Hubungan Internasional*. (h. 129-147). Bandung: Zavara.

Rudy, T. May. 2011. *Hubungan Internasional Kontemporer dan Masalah-Masalah Global*. Bandung: PT Refika Aditama.

***Acuan artikel dalam jurnal*:**

Brown, Sheryl J. & Margarita S. Studemeister. (2001). Virtual Diplomacy: Rethinking Foreign Policy Practice in the Information Age. Information & Security, Vol. 7, 28-44

Rana, Waheeda. (2015). Theory of Complex Interdependence: A Comparative Analysis of Realist and Neoliberal Thoughts. International Journal of Business and Social Science, Vol. 6 No. 2, 290-297

Wenger, Andreas. (2001). The Internet and The Changing Face of International Relations and Security. Information & Security, Vol. 7, 5-11

Acuan artikel dalam website:

Atlantic Council. 2013. "Finland to Join NATO's Cyber Defense Center." dalam *http://www.atlanticcouncil.org/blogs/natosource/finland-to-join-nato-s-cyber-defense-center* diakses Februari 2022

Defense News. 2016. "Finnish Defense Ministry Hit by DDoS Cyber Attack" dalam *http://www.defensenews.com/story/defense/international/2016/04/04/finnish-defense-ministry-hit-ddos-cyberattack/82608438/* diakses Februari 2022

Fifth Domain. 2017. "Finland takes lead defending EU, NATO from hybrid, cyber threats" dalam *http://fifthdomain.com/2017/04/28/finland-takes-lead-defending-*

eu-nato-from-hybrid-cyber-threats/ diakses Februari 2022

NATO.2017. "*Cyber defence"* dalam http://www.nato.int/cps/en/natohq/topics_78170.htm diakses Februari 2022

Valtioneuvosto. 2017. "A political framework agreement on cyber defence signed between Finland and Nato" dalam *http://valtioneuvosto.fi/en/article/-/asset_publisher/kyberpuolustusta-koskeva-poliittinen-puitejarjestely-suomen-ja-naton-valilla* diakses Januari 2022