Jurnal Ilmu Hubungan Internasional
LIN

Volume 1, Nomor 2, Juli-Oktober 2021

E-ISSN 2797-0485

Strategi Keamanan Siber Israel dalam Menghadapi Ancaman Siber untuk Menjaga Stabilitas Keamanan Nasional

Hendrianto
PGSD Universitas Paramadina
Email: elhendrie2@gmail.com

Abstract. This research is an analysis of cybersecurity strategy policy based on document created by the Israeli government in 2017 entitled "Israel National Cyber Security in Brief". The document contains strategies, challenges and also various aspects related to the development and protection of Israel's cyber space published by the National Cyber Directorate, The State Of Israel Prime Minister's Office. This research uses quantitative analysis techniques through MAXQDA and GEPHI applications to classify various categories referring to cybersecurity concepts published by Hao Yeli in A Three – Perspective Theory of Cyber Sovereignty. *Results of this study* demonstrate Israel's ambition to lead the world in the development of cyberspace technology in an effort to strengthen its defense system and also to strengthen Israel's bargaining position in establishing cooperation relationships with other countries.

Keywords: cyber security, sovereignty, strategy, threats, israel

Abstrak. Penelitian ini merupakan analisis kebijakan strategi keamanan siber berdasarkan dokumen yang dibuat oleh pemerintah Israel pada tahun 2017 yang berjudul "Israel National Cyber Security In Brief". Dokumen tersebut berisi strategi, tantangan juga berbagai aspek yang terkait dengan pengembangan dan perlindungan ruang siber Israel yang diterbitkan oleh National Cyber Directorate, State Of Israel Prime Minister's Office. Penelitian ini menggunakan teknik analisis kuantitatif melalui aplikasi MAXQDA dan GEPHI guna mengklasifikasikan berbagai kategori yang mengacu pada teori keamanan siber yang dipublikasikan oleh Hao Yeli dalam A Three – Perspective Theory of Cyber Sovereignty. Hasil penelitian ini menunjukan ambisi Israel untuk memimpin dunia dalam pengembangan teknologi ruang siber sebagai upaya untuk memperkuat sistem pertahanannya dan juga untuk memperkuat posisi tawar Israel dalam menjalin hubungan kerjasama dengan negara-negara lain.

Kata kunci: keamanan siber, kedaulatan, strategi, ancaman, Israel

PENDAHULUAN

Kemajuan teknologi telah melahirkan warna baru dalam pergaulan internasional sekaligus merevolusi bentuk komunikasi klasik menuju era digitalisasi dengan ditandai kemunculan internet dan juga infrastruktur pendukungnya yang terus berkembang dari hari ke hari. Hal tersebut pada akhirnya semakin mengaburkan batas negara dengan konektifitas yang semakin inklusif di dunia siber. Relasi antara negara kemudian membuka keterlibatan *non state actor* secara massif membawa diskursus hubungan internasional pada tataran yang lebih terbuka. Dunia siber memungkinkan berbagai macam isu diakses oleh semua pihak dengan berbagai opininya masing masing.

Hari ini, semua orang dapat dengan mudah mendapatkan informasi di internet. Wescott memberikan contoh bagaimana kemudahan itu memberikan peluang bagi siapa pun baik itu jurnalis, pelobi, diplomat asing atau masyarakat biasa yang

ingin mengetahui pandangan pemerintah pada satu isu tertentu dapat mengakses situs web mereka secara langsung (Westcott, 2008). Kenichi Ohmae juga mengatakan bahwa informasi memainkan peran penting dalam mendorong keterlibatan publik secara global dalam hubungan internasional (Ohmae, 2002). Indrajit bahkan lebih jauh mengemukakan bahwa internet merupakan dunia tersendiri, melalui beraneka ragam peralatan teknologi informasi dan komunikasi, para individu maupun kelompok-kelompok masyarakat saling berinteraksi, bertukar pikiran, dan berkolaborasi untuk melakukan sejumlah aktivitas kehidupan (Indrajit, 2011)

Perkembangan teknologi internet secara umum memberikan keuntungan tapi juga memunculkan potensi ancaman karena kedaulatan negara telah bergeser dari yang dulunya sekedar teritori fisik kini juga harus dilihat dalam sudut pandang siber. Fakta bahwa penggunaan internet dalam berbagai pelayanan publik telah dilakukan seiring kemajuan teknologi sekaligus membuka ruang bagi pihak pihak yang tidak bertanggung jawab untuk mencuri informasi, meretas jaringan atau menyebarkan berita bohong yang menganggu kepentingan nasional. Keamanan siber kini menjadi tantangan global dan menjadi masalah besar bagi setiap negara berdaulat. Perdebatan antara kedaulatan siber dan posisi negara kini mengemuka namun pada tingkat yang lebih tinggi setiap negara memiliki hak untuk melindungi dirinya dari setiap ancaman termasuk dari serangan siber bahkan Kementerian Pertahanan RI ikut menggarisbawahi bagaimana paradigma keamanan nasional telah bergeser kepada aspek yang lebih luas termasuk jaminan keamanan pribadi warga negara dari berbagai kejahatan siber (Kemhan, 2017)

Berdasarkan Konvensi Budapest, jenis serangan di dunia maya dapat dikategorikan menjadi tiga jenis. Kategori pertama adalah kumpulan jenis serangan dimana teknologi informasi dan komunikasi menjadi alat atau senjata utama untuk melakukan kejahatan. Kategori kedua adalah kumpulan peristiwa dimana komputer atau teknologi informasi menjadi sasaran pusat serangan dari pelaku tindak kejahatan dan kategori serangan ketiga ditujukan bagi peristiwa yang bertujuan utama untuk merusak (termasuk memodifikasi dan memfabrikasinya) data atau informasi yang tersimpan di dalam media perangkat teknologi informasi. (Indrajit, 2011)

Semakin terbukanya akses informasi dan penggunaan internet memaksa negara-negara wajib untuk memperkuat sistem pertahanannya termasuk pertahanan siber karena saat ini, perang tidak lagi dalam bentuk tradisional namun telah juga meluas ke dunia siber. Setiap negara berlomba-lomba dalam memperbarui sistem pertahanannya termasuk Israel. Negara ini merupakan negara yang unik karena secara geographis dikelilingi oleh musuh-musuh ideologisnya. Akibat agresi mereka terhadap tanah Palestina membuat Israel seperti musuh bersama bagi negara-negara Arab. Sejak awal pendirian negara Israel ditentang oleh negara-negara tetangganya dan telah terlibat dalam konflik berkepanjangan dengan negara-negara tersebut. (Fraser, 2004).

Israel menyakini musuh mereka ada dimana-mana dan karena potensi ancaman skala besar maka Israel terus memperkuat sistem pertahanannya meskipun normalisasi hubungan dengan beberapa negara Arab telah dilakukan yang mengubah konstalasi politik di Timur Tengah (Ereli, 2020). Namun normalisasi hubungan tersebut belum bisa menghapus sikap saling curiga satu sama lain. Israel menyadari bahwa agresi mereka ditanah Palestina telah melukai banyak negara-negara Islam. Hal tersebut juga dipercayai Amstrong dan dikutip Syafii Maarif bahwa sepanjang konflik Palestina-Israel belum selesai maka politik identitas akan terus ada (Syafii Maarif, 2010). Artinya, konflik Palestina-Israel menopang militansi dan radikalisme khususnya didunia Islam. Argumentasi tersebut membuat Israel berambisi untuk menjadi yang terdepan dalam mengelola ruang siber demi meredam serangan dari manapun.

Israel melakukan langkah-langkah penguatan institusi keamanan siber nasional sejak lama untuk menjaga stabilitas dalam negeri. Parlemen Israel-Knesset telah memberlakukan Undang-Undang Basis Data Biometrik yang menetapkan pengaturan untuk data biometrik dalam dokumen identifikasi resmi seperti KTP dan paspor (Deborah Housen-Couriel, 2017). Hal tersebut untuk memudahkan kontrol negara terhadap arus

keluar masuk orang ke wilayah Israel. Selain itu, Israel juga menikmati keunggulan militer kualitatif dengan penguasaan drone, rudal dan juga kemampuan sibernya. (Huggard, 2020). Keunggulan siber tersebut juga menjadi daya tarik bagi Israel dalam membuka jalur diplomatiknya ke negara Arab dan terbukti, salah satu isu dalam perjanjian damai Israel dan UEA adalah kerjasama dibidang siber. (Wicaksono, 2020).

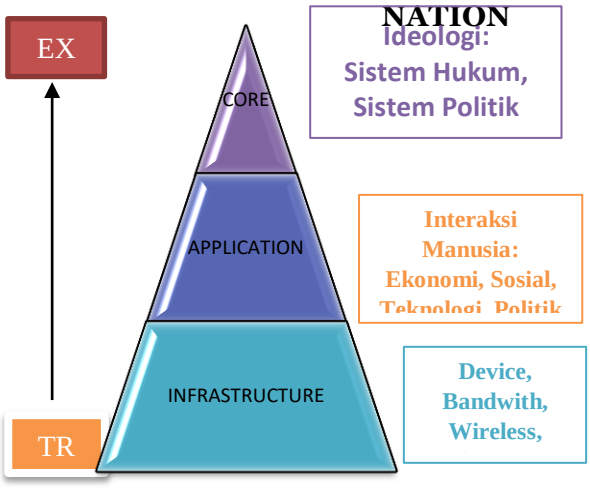
KERANGKA TEORI

Tulisan ini bertujuan untuk menganalisa *Israel National Cyber Security Strategi in Brief* yang terbit pada tahun 2017. Analisis dilakukan dengan menekankan pada tiga kategori (Code) yaitu aspek, aspek, nation dan juga kedaulatan yang didalamnya ada subkateori yang berbeda. Pada akhirnya relasi antar berbagai kategori tersebut memperlihatkan bagaimana strategi Israel dalam meredam potensi ancaman di ruang siber.

Hao Yeli dalam *A Three-Perspective Theory of Cyber Sovereignty* mengemukan bahwa ada tiga actor yang secara aktif terlibat dalam ruang siber yaitu Negara, Warga negara dan Komunitas Internasional. Tiga aktor tersebut memiliki perspektifnya masing-masing yang berujung pada benturan kepentingan antar ketiganya. (Yeli, 2017). Tiga aktor dengan tiga perspektif dan melahirkan iga kepentingan dan kontradiksi yang kemudian mengemukakan: 1) Kedaulatan siber versus kedaulatan negara; 2) Kebebasan siber versus hak asasi manusia; 3) Kedaulatan siber versus tata kelola internet.

Dalam *A Three-Perspective Theory,* Nation terbagi dalam tiga kategori besar yaitu: *core, application, infrastructure* – yang kemudian mengarah pada dua sifat kedaulatan (*sovereignty)* yakni kedaulatan *exclusive* (tertutup) dan kedaulatan yang bersifat *transfer* (terbuka) seperti dalam gambar 1.

Gambar 1



Core menyangkut ideology, sistem negara termasuk ideology politik dan system hukumnya. Application menyangkut aktifitas manusia termasuk relasi sosial masyarakat yang terintegrasikan dalam berbagai sektor seperti teknologi, budaya, ekonomi, perdagangan, dan aspek-aspek lain dari kehidupan. Infrastructure menyangkut perluasan jaringan internet, bandwith, device, gadget, wireless dan sebagainya.

Sementara dalam *Three-Perspective Theory*, kedaulatan terdiri dari dua yaitu, kedaulatan yang bersifat ekslusif atau kedaulatan klasik seperti prinsip prinsip suatu negara yang tidak bisa dilanggar dan kedua adalah kedaulatan yang bersifat terbuka dan dapat ditransfer seperti pengembangan teknologi bersama, inovasi dan kerjasama secara bebas dan adil.

METODOLOGI

Tulisan ini menggunakan teknis analisis gabungan kuantitatif dan kualitatif, narasi kualitatif didasarkan pada penggunaan aplikasi Maxqda dan Gephi untuk membuka data kuantitatif dalam tiga kategori (code): aspek,-aspek, nation juga kedaulatan yang didalamnya juga ada sub-kategori berbeda. Selain itu juga penggunaan aplikasi Maxqda untuk mengkategorisasi (code) secara linguistik konsep strategi keamanan siber Israel dan menganalisa gramatika dan mendefenisikan berbagai frasa frasa

penting dalam teks. Kategorisasi aspects yang didalamnya berisi sub-kategori yang disesuakan dengan kebutuhan atau menyangkut frasa yang ditemukan dalam teks. Dalam I*srael National Cyber Security Strategi in Brief* ditemukan beberapa aspek yang sangat relevan untuk dijadikan sub-kategori, yaitu: *State Actor, Non State Actors, National Security, National Interest, World Leadership, Economic Growth, Threats, Social Welfare dan Technologi Innovasion.* Sembilan kategori ini masuk dalam kode Aspects yang akan memperlihatkan secara gramatika konsep besar Israel dalam keamanan siber. Setelah dari aplikasi Maxqda, data yang ada akan dimasukan kedalam aplikasi Gephi untuk memunculkan secara visual relasi antara kategori kategori tersebut. Dengan menggunakan aplikasi Maxqda dan Gephi dan pendekatan geopolitik dengan berbagai referensi jurnal yang tersedia karena dokumen resmi Israel National Cyber Security Strategi sangat singkat maka narasi kualitatifnya menggunakan sumber diluar data, sehingga tulisan ini dapat memberikan pemahaman tentang stretagi komprehensif strategi keamanan siber Israel.

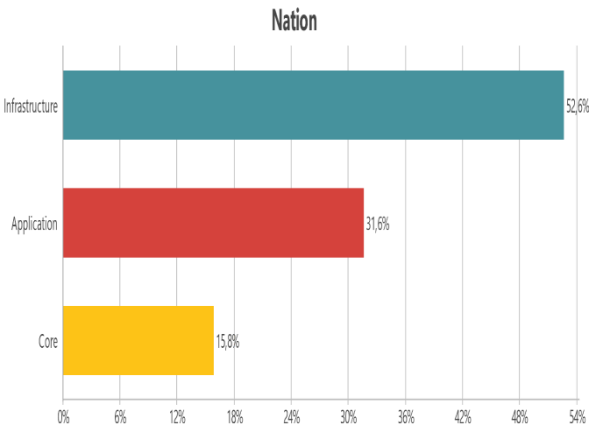
PEMBAHASAN

Strategi Keamanan Siber Israel.

Israel menitik beratkan penggunaan siber selain untuk melindungi kepentingan nasionalnya termasuk menjaga keamanan wilayahnya juga digunakan untuk meningkatkan pertumbuhan ekonomi. Pemerintah Israel meyakini bahwa revolusi internet adalah revolusi ketiga setelah revolusi pertanian juga revolusi industri dan tidak ada negara yang dapat mengharapkan pertumbuhan ekonomi yang berkelanjutan di masa depan tanpa pengembangan ruang siber. (Danino, 2017)

Nation

Dari hasil data dengan menggunakan aplikasi MAXQDA dapat dilihat presentase angka angka yang cukup signifikan. Nation yang terdiri dari tiga kategori dapat dilihat pada gambar 2 dibawah.



Gambar 2

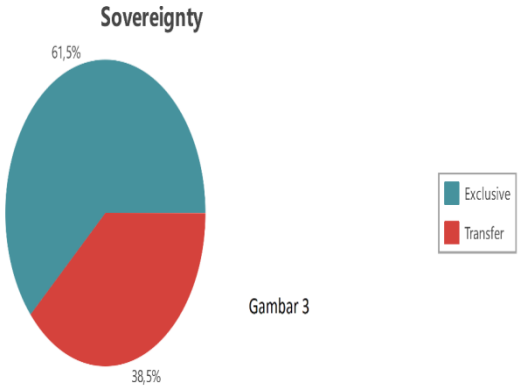
1. Infrastucture mencapai angka 52.6%
2. Application mencapai angka 31,6%
3. Core/ Ideologi mencapai angka 15,8 %

Analisis teks *Israel National Cyber Security Strategi in Brief* memperlihatkan bagaimana core/ideologi menempati urutan terendah dibanding dua kategori lainnya. Data tersebut menunjukan bahwa pemerintah Israel tidak memiliki pretensi ideologi bangsa terancam. Hal itu bukan hal yang aneh karena sudah terlihat dari struktur masyarakat Israel yang ekslusive. Yahudi merupakan etnisitas berdasarkan genetik atau dengan kata lain menjadi Yahudi artinya seseorang harus memiliki darah Yahudi. (Kaell, 2017). Mereka tidak memiliki misi menyebarkan demokrasi didunia seperti AS, atau mencoba memaksakan konsep pasar bebas seperti negara negara Uni Eropa begitu juga agama Yahudi yang dianut oleh rata rata masyarakat Israel bukan merupakan agama yang mengenal istilah syiar seperti apa yang dipraktekan Arab Saudi dan Iran. Alasan tersebut menjadikan pemerintah Israel tidak memiliki kekuatiran berlebihan pada ancaman ideologis dan sikap jumawa itu justru diperlihatkan dengan pembangunan infrastruktur, dilihat dari angka presentasi paling tinggi berdasarkan hasil olahan dari aplikasi Maxqda.

Dikenal sebagai negara *start-up*, Israel telah berinvestasi besar-besaran dalam kemampuan sibernya, terutama system keamanan siber, sejak awal diramalkan bahwa dunia maya akan

menjadi medan pertempuran penting di masa depan, Israel telah lebih dulu berbenah dan hal itu dapat dilihat dari angka 52,6% pada sub code Infrastucture. Untuk code Application yang berada ditengah memperlihatkan angka yang representatif. Application berada diatas lebih tinggi dari ideologi karena pemerintah Israel meyakini skala paling luas dalam menjaga ideologi bukan hanya tugas dunia siber tapi mengembangkan kemampuan siber dianggap jauh lebih penting untuk menjaga teritorialnya.

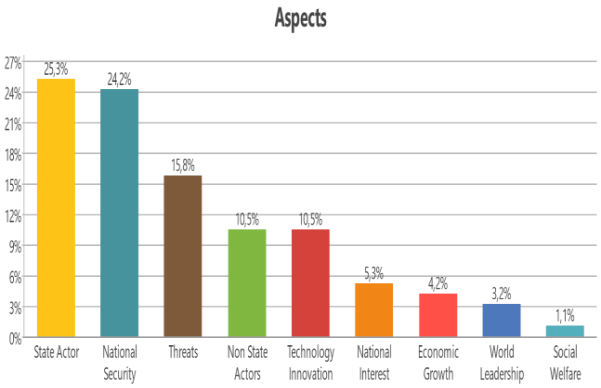
Sovereignty



Gambar 3

Pada gambar diatas, akumulasi angka untuk kedaulatan yang bersifat exclusive memiliki nilai 61,5% dan sisanya 38,5% adalah angka untuk kedaulatan yang bersifat transfer. Ruang siber adalah lanskap yang terus berubah dan pendekatan Israel terhadap keamanan siber bersifat adaptif. Kedaulatan eksklusif adalah kedaulatan alamiah menyangkut batas negara juga sistem sosial politik yang dianut oleh satu negara. Pada point ini, pemerintah Israel meski terlibat aktif dalam transfer teknologi keseluruh belahan dunia namun tetap berkomitmen dalam menjaga wilayahnya. Angka 61,5% merupakan angka yang sangat rasional bagi negara yang secara geopolitik diapit oleh negara-negara Arab. Menjadi satu-satunya negara Yahudi di Timur Tengah membuat Israel harus tetap fokus pada serangan yang bisa datang tiba tiba. Disisi lain, kedaulatan yang bersifat transfer merupakan strategi Israel untuk membangun koalisi dan dukungan dari negara negara lain.

Aspects



Gambar 4.

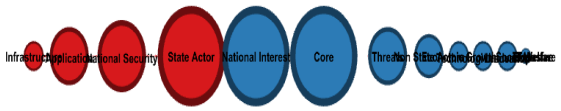
Strategi keamanan siber Israel memperlihatkan beberapa aspek penting untuk dimasukan kedalam sub-code, yaitu: State Actor, Non State Actors, National Security, National Interest, Threats, Technology Innovation, World Leadership, Social Welfare.

Dari hasil olahan data Maxqda dapat dilihat secara jelas bahwa State Actor menempati angka tertinggi dengan besaran mencapai 25,3%, disusul oleh National Security dengan angka 24,2%. Kemudian Threats senilai 15,8%, Non State Actors berjumlah 10,5%, Technology Innovation berbagi angka sama 10,5%. Selanjutnya, National Interest 5,3 % lalu Economic Growth dengan presentase 4,2 %, World Leadership 3,2 % dan Social Welfare menempati posisi terbawah dengan angka 1,1 %.

Posisi State Actor dalam strategi keamanan siber Israel menempati urutan teratas dan menjelaskan bagaimana peran penguatan negara dalam strategi siber Israel. Dominasi negara memperlihatkan komitmen Israel dalam penanganan ancaman. Dari data teks yang ada juga memperlihatkan adanya code *World Leadership* yang secara eksplisit tertuang dalam Strategi Kemanan Siber Israel .*"in accordance with the country's national interests. In addition, the strategy aims to ensure Israel's continuing role in the international arena, as a leader in technological innovation and as an active partner in the global processes of shaping cyberspace "* (Minister, 2017)

Statemen tersebut jelas memperlihatkan ambisi Israel untuk memimpin dunia dalam inovasi teknologi

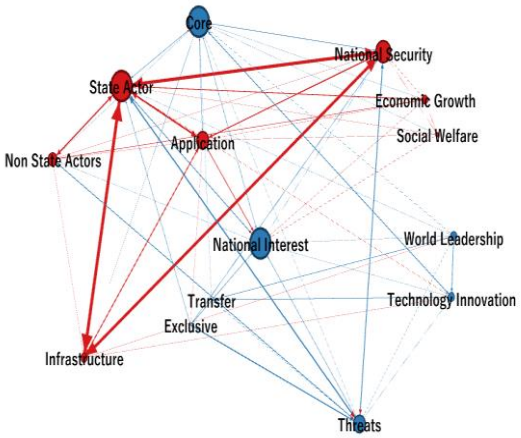
khususnya dalam bidang siber. Selanjutnya untuk aspek aspek lain akan dijelaskan dalam gambar Gephi dari hasil excel aplikasi Maxqda yang akan diproses kedalam aplikasi Gephi. Selain dipergunakan untuk melakukan analisis kualitatif, data Maxqda juga akan memberikan gambar matrix yang kemudian dikonversi menjadi data gephi.



Gambar 5.

Hasil pengolahan data Gephi menghasilkan dua kelompok besar yang disimbolkan oleh warna merah dan biru. Pada posisi merah terdapat Infrastructure, Application, National Security, State Actor dan untuk warna biru memuat National Interest, Core, Threats, Non State Actor, Economic Growth, Technology Innovation, World Leadership dan Social Welfare.

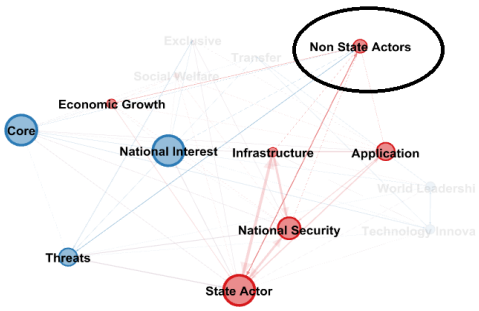
Apa yang menarik dari data diatas adalah posisi Core yang terlihat cukup signifikan, jika dibandingkan graphis dari Maxqda. Dalam Gephi, Core berelasi cukup besar hampir dengan semua kategori. Artinya Core meski angka presentasi dari Maxqda lebih kecil dari dua kategori lainnya namun setelah diproses dalam aplikasi Gephi, Core justru berperan sangat signifkan karena terkait dengan semua kategori.



Gambar 6

Pada gambar 6 terlihat dengan jelas relasi data antara code, semua kategori berelasi satu sama lain, karena ancaman yang terus berkembang maka pendekatan Israel terhadap keamanan siber juga bersifat holistik dan fleksibel. Aspek aspek yang sudah dimasukan dalam code akan dianalisis dan dibahas dibawah ini.

State Actor



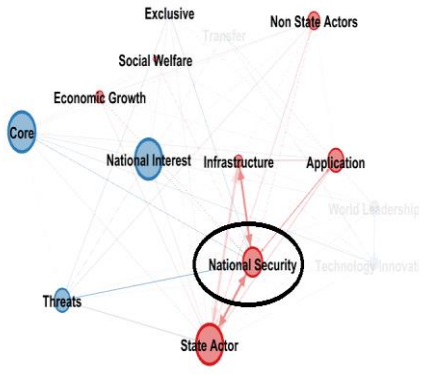
Gambar 7.

Pada aspek ini, state actor dengan angka 25, 3% memainkan peran penting dalam strategi keamanan siber Israel, penguatan peran negara menjadi kunci penting bagi Israel dalam mencegah potensi ancaman. Terlihat pada gambar diatas bagaimana state actor terhubung

dengan hampir semua code. Israel pada dasarnya menolak pembagian biner antara *attacks* dan *defense*, negara ini melihat keduanya sebagai bagian dari satu kontinum. Ini bukan hal yang aneh bagi Israel, karena dalam hal keamanan, Israel juga menolak pembatasan sipil dan militer. Sebaliknya, negara melihat kedua bidang tersebut saling terkait dan mendorong kerja sama yang luas antara badan-badan sipil dan militer. Peran state actor menjadi sentral dalam pertahanan siber Israel diaman pemerintah mendanai dan memberikan kebijakan pajak khusus bagi perusahaan siber.

National Security

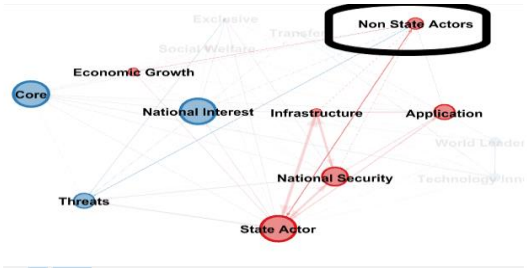
Dalam strategi keamanan siber Israel, aspek National Security mencapai angka 24,2% menandakan bagaimana kategori ini menjadi perhatian serius pemerintah. Letak Israel yang diapit oleh negara negara Arab membuat negara ini sangat *concern* terhadap isu keamanan nasional. Sejak aneksasi Palestina ditahun 1948, negara ini berkali-kali diserang hacker. National security berelasi dengan hampir semua code aspek dan secara khusus dalam konteks kedaulatan, national security berada pada cakupan kedaulatan exclusive. Bisa diliat pada gambar dibawah.



Gambar 8.

Non State Actors

Israel menghadapi ratusan serangan dunia maya setiap hari dari seluruh dunia. Banyak dari serangan ini difokuskan pada jaringan komputer Israel. Musuh-musuhnya menyadari bahwa dengan merusak jaringan mereka dapat mempengaruhi seluruh sistem, termasuk melemahkan reputasi Israel dalam dunia siber. Dengan kata lain, sisi negatif dari menjadi negara start-up adalah negara itu sangat rentan terhadap serangan dan pembobolan dunia maya. Maka dari itu negara mendorong bahkan memberi ruang bagi *actor non state* untuk terlibat dalam pertahanan dan juga pengembangan inovasi siber. Bisa diliat pada gambar 9 bagaimana *Non State Actors* terhubungan dengan beberapa subcode. Hal tersebut memperlihatkan pemerintah Israel menyadari keterlibatan sipil penting bagi kemandirian Israel didunia maya. Sebagaimana yang diyakini para pemimpin Israel bahwa untuk menjadi yang paling kuat dalam hal cyber maka negara harus bertumpu pada dua pilar: (1) militer yang kuat dan pro-aktif dan dinas intelijen yang kuat serta (2) sektor sipil inovatif. (Frei, 2020)

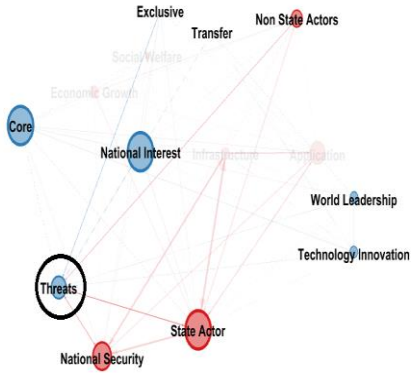


Gambar 9.

Threats

Pada tahun 2013, Israel menuduh Iran, Hamas, dan Hizbullah melakukan serangkaian serangan skala besar terhadap sistem nasional yang vital termasuk situs air, listrik, dan perbankan. Serangan Iran melampaui semua serangan sebelumnya, baik dalam lingkup dan luasnya target yang dipilih. Serangan Iran terutama menargetkan infrastruktur sipil, termasuk jaringan keuangan bahkan menargetkan sistem keamanan pemerintah, termasuk upaya untuk merebut kendali drone Israel (Matthew S Cohen, 2015). Setelah

bertahun-tahun kebijakan keamanan siber nasional Israel saat ini telah melakukan pendekatan yang berbeda terhadap keamanan siber dengan berevolusi menjadi strategi keamanan siber yang proaktif, komprehensif, dan berjangka panjang, tidak berfokus pada penyerang potensial tetapi pada potensi ancaman dan aset yang membutuhkan perlindungan. Ancaman siber yang dihadapi Israel saaat ini bukan saja meliputi hacktivist, cybercrime syndicates, trojans dan virus-virus lainnya namun juga serangan langsung ke pusat informasi Israel. Jika dilihat dari relasi datanya, threats yang mencapai angka 15,8% berkoneksi langsung dengan national interest. Bahwa serangan yang datang pada Israel sangat mengancam kepentingan nasional dan harus dicegah apapun harganya. Liat gambar dibawah.

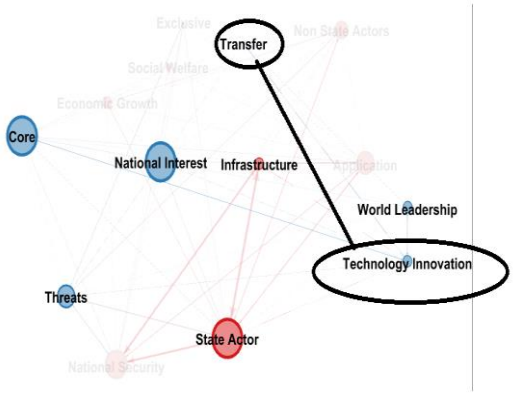


Gambar 10

Technologi Innovation

Israel percaya bahwa *human resourches* yang mereka miliki memiliki keunggulan dibanding bangsa lain dan sejarah juga mencatat pemikir pemikir dunia rata rata berkoneksi langsung dengan Israel. Maka dalam strategi keamanan sibernya, inovasi teknologi dituangkan secara eskplisit. Bahwa negara akan berdedikasi untuk menjadi yang terdepan dalam pengembangan teknologi. Kemampuan Israel dalam menangani ancaman keamanan siber pada semua level diikuti oleh pencapaian teknologi terkini seperti penggunaan drone dalam pengawasan perbatasan, penggunaan teknologi *bloc chain* untuk sistem komunikasi dan juga *big data* untuk memprediksi aksi teroris. (Ouwendijk, 2018)

Pada data Maxqda, angka *Technology Innovation* mencapai 10,5% yang memberikan gambaran bahwa pengembangan teknologi menjadi kategori yang krusial dalam keamanan siber karena pengembangan teknologi terhubung ke berbagai sub aspek lain. Pengembangan teknologi menjadi focus utama Israel selain untuk revolusi system pertahanan sibernya juga sebagai alat tukar dalam melakukan kerjasama dengan negara lain. Lihat gambar dibawah ini bagaimana inovasi teknologi berhubungan lurus dengan kedaulatan yang bersifat transfer.

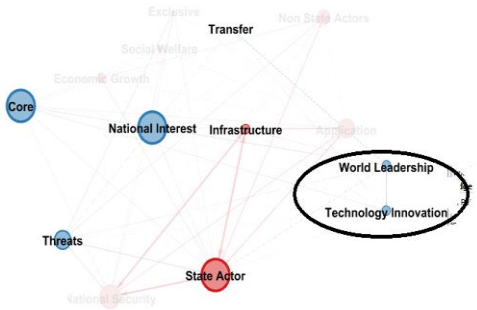


Gambar 11

World Leadership.

Israel adalah pusat inovasi terkemuka dengan kemajuan yang terus berkembang menisbatkan Israel sebagai yang kedua di dunia setelah Silicon Valley. Israel menampung salah satu ekosistem inovasi dengan performa tertinggi di dunia sekaligus sumber teknologi terkemuka. Seiring dengan pertumbuhan industri teknologi Israel yang semakin pesat. Negara ini berusaha menjadi yang terdepan dalam penguasaan teknologi

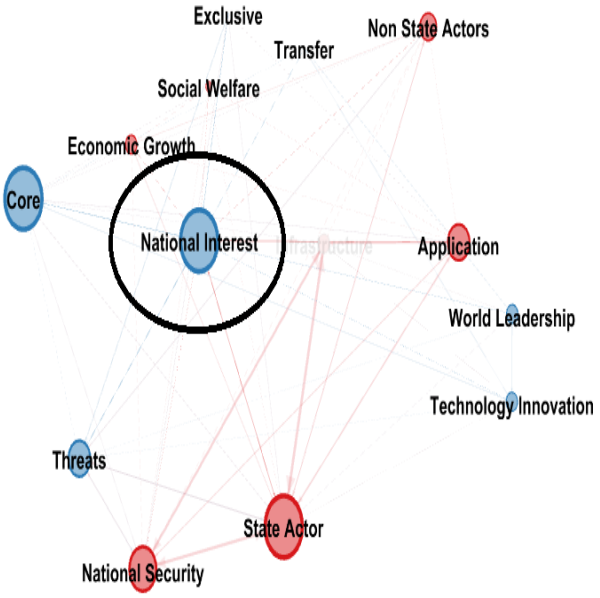
sebagai cara Israel dalam menjadi pemimpin dunia. Dalam dokumen siber sekuritinya yang dikonversi Gephi terlihat bagaimana inovasi teknologi berjalan seiring dengan sub code *world leadership* yang mencapai angka 3,2%.



Gambar 11.

National Interest.

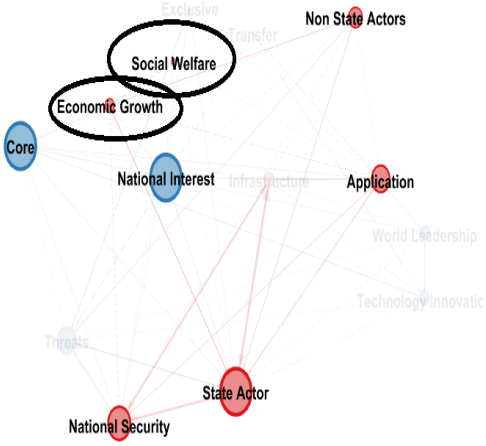
Strategi pertahanan siber Israel merupakan dokumen resmi yang digunakan sebagai konsep besar dalam mencegah ancaman bagi kepentingan nasional. Kepentingan nasional yang dalam data Maxqda bernilai 5,3% tapi terhubung dengan semua code dan sub code. Kepentingan nasional merupakan tujuan utama semua kebijakan luar negeri. Meski cuma 5,3% dalam Maxqda namun dalam Gephi, jika tombol biru national interest kita tekan maka semua code dan sub code tetap menyala dan terhubung, perhatikan gambar dibawah



Gambar 12.

Economic Growth dan Social Welfare.

Salah satu komoditas paling berharga di era digital adalah informasi pribadi, tanpa solusi keamanan maka dunia usaha akan menghadapi risiko yang menghambat produktivitas. Israel meyakini keamanan siber sejalan dengan pertumbuhan ekonomi. Dalam data Maxqda, pengcodingan Economic Growth berada pada angka 4,2% dan dalam data Gephi, terhubung dengan subcode national interest, state actor, non state actors, application, dan juga core. Pertumbuhan ekonomi juga terhubung langsung dengan social welfare. Meski nilai presentase hanya 1,1 % namun konektivitas keamanan siber dan social welfare tidak bisa diabaikan. Jika data Gephi di highlight maka akan terlihat bagaimana Social welfare dan Economic Growth berada pada relasi data yang sama dan juga terhubung dengan subcode-subcode yang sama. Lihat gambar dibawah.



Gambar 13

KESIMPULAN

Israel adalah negara yang telah menghadapi berbagai ancaman terhadap keamanan nasionalnya sejak awal pembentukannya dan dalam beberapa

dekade terakhir, negara ini telah memprioritaskan keamanan siber sebagai fokus utama untuk melindungi kedaulatannya. Aparat pertahanan siber Israel terkenal di dunia dan dianggap sebagai salah satu yang terbaik dengan mencatatkan sekitar 1000 serangan siber setiap menit namun mampu mengatasinya bahkan kini Israel mengekspor miliaran dollar produk dan layanan terkait teknologi siber. (Benolie, 2015)

Israel memiliki lebih dari 400 perusahaan yang didanai di bidang keamanan siber. Perusahaan teknologi yang dikelola oleh mantan peretas militer. Pasukan pertahanan Israel berfungsi sebagai inkubator bagi bakat dunia maya, dan para veterannya memimpin perusahaan keamanan di Israel dan bahkan di AS. Israel merupakan rumah bagi perusahaan *spyware* kontroversial seperti NSO Group. Inovasi teknologi yang mereka kembangkan merupakan wujud ambisi Israel untuk menjadi pemimpin dunia dalam pencapaian teknologi mutakhir. Ambisi tersebut didukung oleh regulasi pemerintah dan juga *human resourches* memadai.

Beberapa catatan penting dalam penelitian ini memperlihatkan bagaimana prinsip prinsip kedaulatan tetap terjaga dengan tetap membuka diri dalam menjalin kerjasama dengan negara negara lain. Israel memperlihatkan cara mengelola ruang siber nya sekaligus menjaga kedaulatannya. Transfer teknologi siber ke luar negeri meningkatkan ekonomi nasional dan menjadi *bargaining* Israel untuk mencairkan sikap permusuhan negara negara lain akibat aneksasi mereka di tanah Palesina. Pemerintah Israel percaya bahwa keunggulan teknologi mereka membuat banyak negara didunia tertarik untuk datang dan membeli. Hanya dengan kemampuan tersebut maka eksitensi negara Israel akan terus terjaga.

DAFTAR PUSTAKA

Benolie, D. (2015). Toward a Cybersecurity Policy Model: Israel National Cyber Bureau Case Study. *North Carolina Journal of Law and Technology*.

Danino, O. (2017). Cybersecurity economics in Israel. *Cybersecurity and cyberdefense chair*.

Deborah Housen-Couriel. (2017). National Cyber Security Organisation: Israel. *CCDCOE*.

Ereli, H. M. (2020). The UEA and Israel Normalization: Political and Social Implication. *Orsam*.

Fraser, T. (2004). The Arab Israeli Conflict, Second Edition. *Palgrave Macmillan*.

Frei, J. (2020). Israel's National Cybersecurity and Cyberdefense Posture. *Cyber Defense Project (CDP)*.

Huggard, N. S. (2020). Israel In The Middle East for Next Two Decades. *The New Geopolits Middle East*.

Idntimes.com. (n.d.). *5 Fakta Seputar Yahudi*.

Indrajit, R. E. (2011). *Peranan Teknologi Informasi dan Internet*. Yogyakarta,: Offest.

Kaell, S. I. (2017). Lineage Matters: DNA, Race, and Gene Talk in Judaism. *Religion and American Culture: A Journal of Interpretation*.

Kemhan, K. P. (2017). Pedoman Pertahanan Siber.

Matthew S Cohen, C. D. (2015). Israel and Cyberspace: Unique Threat and Response. *International Studies Perspectives*, 4.

Minister, S. o. (2017). Israel National Cyber Security In Brief.

Ohmae, K. (2002). *Hancurnya Negara Bangsa: Bangkitnya Negara Kawasan dan Geliat Ekonomi Regional didunia tak Terbatas*. Yogyakarta: Qalam.

Ouwendijk, H. (2018). Cybersecurity & homeland security in Israel. *Rijksdienst Voor Ondernemed Nederland*.

Syafii Maarif. (2010). Politik Identitas dan Masa Depan Pluralisme Kita. *PUSAD*.

Westcott, N. (2008). Digital Diplomacy: The Impact of the Internet on International Relations. *Oxford Internet Institute*, 14.

Wicaksono, R. M. (2020). Analisis Kebijakan Uni Emirat Arab dalam Normalisasi Hubungannya dengan Israel. *Jurnal Middle East and Islamic Studies,*.

Yeli, H. (2017). A Three-Perspective Theory of Cyber Sovereignty. *PRISM*.