**UNIVERSITAS PERTAHANAN**

# STRATEGI KEAMANAN SIBER KOMISI PEMILIHAN UMUM (KPU) PUSAT DALAM MENGHADAPI PEMILIHAN UMUM 2019

**M. SYADLI PRATAMA**
**NIM: 120170102018**

Tesis yang Ditulis untuk Memenuhi Sebagian Persyaratan dalam
Mendapatkan Gelar Magister Pertahanan

**FAKULTAS STRATEGI PERTAHANAN**
**PROGRAM STUDI PEPERANGAN ASIMETRIS**

**BOGOR**
**Januari 2019**

## LEMBAR PENGESAHAN

Penelitian ini diajukan oleh:

| | |
|---|---|
| Nama | : M. Syadli Pratama |
| NIM | : 120170102018 |
| Program Studi | : Peperangan Asimetris |
| Judul Proposal Tesis | : **Strategi Keamanan Siber Komisi Pemilihan Umum (KPU) Pusat dalam Menghadapi Pemilihan Umum 2019** |

Telah berhasil dipertahankan dihadapan Dewan Penguji dan diterima sebagai persyaratan yang diperlukan untuk memperoleh gelar Magister bidang Pertahanan pada Program Studi Peperangan Asimetris, Fakultas Strategi Pertahanan, Universitas Pertahanan.

DEWAN PENGUJI

Pembimbing I : Fetri Miftach, Ph.D., C.Eng., MBCS ( )

Pembimbing II: Kolonel Cba. Dr. Yusuf Ali S.E., M.M ( )

Penguji I : Laksamana Pertama TNI Dr. Suhirwan M.MT ( )

Penguji II : Brigjen TNI Dr. Moch Afifuddin, M.Si (Han) ( )

Penguji III : Letkol Inf. Dr. Triyoga Budi Prasetyo, M.Si ( )

Ditetapkan di : Bogor
Tanggal : Desember 2018

**PERNYATAAN PERSETUJUAN PUBLIKASI KARYA ILMIAH UNTUK KEPENTINGAN AKADEMIS**

Tesis ini diajukan oleh:

| | |
|---|---|
| Nama | : M. Syadli Pratama |
| NPM | : 120170102018 |
| Program Studi | : Peperangan Asimetris |
| Fakultas | : Strategi Pertahanan |
| Jenis Karya | : Tesis |

Demi pengembangan ilmu pengetahuan, menyetujui untuk memberikan kepada Universitas Pertahanan Hak Bebas Royalti Nonekskulusif (Non-exclusive Royalti-Free Right) atas karya ilmiah saya yang berjudul:

**Strategi Keamanan Siber Komisi Pemilihan Umum (KPU) Pusat dalam Menghadapi Pemilu 2019**

Beserta perangkat yang ada (jika diperlukan). Dengan Hak Bebas Royalti Noneksklusif ini Universitas Pertahanan berhak menyimpan, mengalihmedia/formatkan, mengelola dalam bentuk pangkalan data (*database*), merawat, dan mempublikasikan Tugas akhir saya selama tetap mencantumkan nama saya sebagai penulis dan sebagai pemilik Hak Cipta/Karya Intelektual dari Tesis ini.

Demikian pernyataan ini saya buat dengan kesadaran penuh tanpa paksaan dari pihak manapun.

Bogor, Desember 2018

M. Syadli Pratama

## PERNYATAAN ORISINALITAS

Dengan ini saya menyatakan bahwa dalam tesis ini tidak terdapat karya atau bagian karya yang pernah ditulis ataupun diajukan orang lain untuk memperoleh gelar kesarjanaan jenjang apapun di suatu Perguruan Tinggi; dan sepanjang pengetahuan saya juga tidak terdapat istilah, frasa, kalimat, paragraf, subbab, atau bab dari karya yang pernah ditulis atau diterbitkan; kecuali yang secara tertulis dirujuk dalam naskah ini dan disebutkan dalam daftar referensi.

Apabila di kemudian hari terbukti bahwa terdapat plagiat dalam tesis ini saya bersedia menerima sanksi sesuai ketentuan peraturan dan undang-undang yang berlaku.

Bogor, Desember 2018

M. Syadli Pratama

## KATA PENGANTAR

Puji syukur penulis Panjatkan sepenuh hati atas kehadirat Tuhan Yang Maha Esa karena berkat rahmat dan karunia-Nya, sehingga Penulis dapat menyelesaikan karya ilmiah ini sesuai dengan yang pengharapan. Adapun penulisan tesis ini ditujukan sebagai salah satu syarat dalam memperoleh gelar Magister dalam Ilmu Pertahanan pada Program Studi Peperangan Asimetris Fakultas Strategi Pertahanan Universitas Pertahanan.

Penulis sepenuhnya menyadari bahwa karya tulis ini jauh dari kata sempurna dan tentunya tidak sedikit kendala dan hambatan yang ditemui dalam penyusunannya. Sehingga Penulis ingin menyampaikan apresiasi dan ucapan terimakasih kepada:

1. Mayjen TNI Dr. Tri Legionosuko selaku Rektor Universitas Pertahanan
2. Mayjen TNI Dr. Hipdizah, S. ADM., M.Si selaku Dekan Fakultas Strategi Pertahanan
3. Laksmana Pertama TNI Dr. Suhirwan, M.MT. selaku Wakil Dekan Fakultas Strategi Pertahanan
4. Kolonel Kav. Dr. Yusuf, S.Sos, M.M. selaku Sesprodi Peperangan Asimetris Fakultas Strategi Pertahanan Universitas Pertahanan
5. Fetri Miftach, Ph.D., C.Eng., MBCS selaku Pembimbing I
6. Kolonel Cba. Dr. Yusuf Ali S.E., M.M selaku Pembimbing II
7. Bapak Aditya Haris Kemal selaku Kasubdit. Jaringan dan Komunikasi Data dari Komisi Pemilihan Umum (KPU) Pusat
8. Bapak Gunawan Suswantoro selaku Sekretariat Jendral dari Badan Pengawas Pemilu (Bawaslu)
9. Bapak Ir. Herry Abdul Azis, M.Eng selaku SAM. Bidang Teknologi Kementerian Komunikasi dan Informatika
10. Bapak Ir. Riki Arif Gunawan M.Sc selaku Direktur Jendral Aplikasi Informatika Kementerian Komunikasi dan Informatika

11. Ibu Dra. Siti Meiningsih MSc. Mewakili Direktur Jenderal Informasi dan Komunikasi Publik Kementerian Komunikasi dan Informatika
12. Bapak Sulistyo, S.Si., S.T., M.Si selaku Direktur Deteksi Ancaman Badan Siber dan Sandi Negara (BSSN)
13. Bapak Agung Nugraha, S.IP., M.Si(Han) selaku Direktur Proteksi Infrastruktur Informasi Kritikal Nasional Badan Siber dan Sandi Negara (BSSN)
14. Bapak Hadar Nafis Gumay selaku *Commissioner NetGrit*
15. Bapak Yuliardi Sutedja selaku *Founder & Chairman of Indonesia Cyber Security Forum (ICSF)*
16. Bapak Budi Rahardjo selaku Praktisi IT dan Ahli Keamanan Informasi
17. Ibunda N. Norma dan Widya dan Keluarga Tercinta yang telah mendukung penyusunan tesis ini terutama
18. Rekan-rekan teman sekelas Program Studi Peperangan Asimetris Cohort 6 Universitas Pertahanan

Semoga Tuhan Yang Maha Esa membalas kebaikan-kebaikan berbagai pihak atas segala kontribusinya.

Penulis mengerti bahwa terdapat keterbatasan dalam pembuatan tesis ini, maka dengan kerendahan hati mengharapkan kritik dan saran yang konstruktif demi menunjang penelitian ini.

Akhirnya, semoga tesis ini dapat memberikan manfaat terhadap pengembangan ilmu pertahanan dan bermanfaat bagi Mahasiswa Universitas Pertahanan. Dan Komisi Pemilihan Umum (KPU) pusat khususnya.

Bogor, Desember 2018

M. Syadli Pratama

# ABSTRAK

## STRATEGI KEAMANAN SIBER KOMISI PEMILIHAN UMUM (KPU) PUSAT DALAM MENGHADAPI PEMILU 2019

**M. SYADLI PRATAMA**

Pemilihan Umum merupakan pilar demokrasi dalam menjaga tonggak kedaulatan suatu negara. Ancaman eksistensial berdimensi non-militer merupakan jenis ancaman yang tengah dihadapi oleh penyelenggara pemilu di seluruh dunia termasuk Indonesia. Komisi Pemilihan Umum (KPU) Pusat memiliki tanggung jawab untuk mewujudkan Pemilu yang Langsung, Umum, Bebas dan Rahasia serta Jujur dan Adil (LUBER dan JURDIL) dari segala potensi ancaman termasuk dari ranah siber yang dapat muncul pada Pemilu 2019 mendatang. Sebuah strategi *Collaborative Approach* dengan konsep *Triple Helix* yang terdiri atas *Government*, *business*, dan *Intellectual* dengan peran serta tanggung jawab masing-masing. Penelitian ini mengelaborasikan strategi KPU dalam model *Ends-Ways-Means* dan menganalisa sinergitas dari para *stakeholders* serta faktor-faktor penghambat yang dihadapi. Teori dan konsep yang dipergunakan adalah strategi, keamanan siber, sinergitas dan hambatan melalui metode kualitatif dengan pendekatan fenomenologi. Hasil penelitian menunjukkan bahwa implementasi strategi kolaborasi digunakan walaupun masih terdapat beberapa hambatan berupa ketidakhadiran payung hukum yang jelas sebagai basis kerjasama diantara KPU dan instansi-instansi lainnya untuk dapat mengetahui sejauh mana keterlibatan dan tanggung jawab yang dimiliki. Walupun hal tersebut akan menimbulkan spekulasi dimasyarakat terkait intervensi Pemerintah dalam pelaksanaan tugas dan kewenangan KPU sebagai sebuah lembaga independent.

Kata Kunci: Strategi, keamanan siber, Komisi Pemilihan Umum (KPU), *collaborative approach*

## *ABSTRACT*

### *THE CYBER SECURITY STRATEGY OF GENERAL ELECTIONS COMMISSION IN FACING THE GENERAL ELECTION 2019*

**M. SYADLI PRATAMA**

*General election is a pillar of democracy in establishing the milestone of a country's sovereignty. Existential threats in non-military dimension are a type of threat currently being faced by election organizers all around the world including Indonesia. KPU has the responsibility to conduct a Direct, General, Free, in Secret, Honest and Fair Election from all potential cyber threats that might emerge in the upcoming 2019 Election. A Collaborative Approach strategy with an Ttriple Helix concept consisting of Government, business, and Intellectual with their respective roles and responsibilities. The study elaborates KPU's strategy in Ends-Ways-Means model and analyzed the synergy of the stakeholders and their obstacles. The theories and concepts used are strategy, cyber security, synergy and constrain through qualitative method with phenomenological approach. The results shows that the implementation of the collaboration strategy is used even though there are still some obstacles in the form of the absence of a clear legal umbrella as a basis for collaboration between the KPU and other agencies to be able to determine the extent of their involvement and responsibilities. Even though this may lead to speculation in the community regarding Government intervention in the implementation of the KPU's duties and authority as an independent institution.*



*Keywords: Strategy, cyber security, General election commission (KPU), collaborative approach*

## DAFTAR ISI

## DAFTAR GAMBAR

## DAFTAR TABEL

# BAB I
# PENDAHULUAN

## 1.1 LATAR BELAKANG

Perkembangan globalisasi yang dipercepat oleh teknologi informasi berdampak pada arus informasi dan komunikasi yang mengalir secara luas tanpa mengenal batas ruang dan waktu. Globalisasi membentuk satu kesatuan masyarakat dunia yang terintegrasi[1] yang terbentuk melalui dua dimensi, yaitu dimensi ruang dan waktu, dimana dimensi ruang semakin dipersempit dan waktu yang semakin dipersingkat.[2] Jan Aart Scholte mendefinisikan globalisasi sebagai suatu proses transformasi lingkungan global sebagai kontinuitas dari situasi sebelumnya yang ditandai dengan ciri kemajuan teknologi dan informasi, menimbulkan interdepedensi, pengaburan terhadap batas-batas negara (*borderless state*).[3] Sehingga, dari beberapa definsi tersebut dapat disintesakan bahwa proses globalisasi dipercepat oleh kemajuan teknologi informasi yang memberikan dampak besar dan signifikan dalam konstelasi hubungan antar negara tanpa adanya batasan ruang dan waktu. Melihat dampak yang diakibatkan oleh teknologi informasi itu sendiri, banyak negara memandangnya sebagai suatu peluang yang dapat memberikan kontribusi positif bagi kesejahteraan masyarakatnya dan global, akan tetapi tak sedikit pula memandangnya sebagai suatu bentuk ancaman asimetris terhadap eksistensi mereka.

Ruang siber (*Cyberspace*) merupakan bidang jaringan komputer (termasuk para pengguna dibaliknya) dimana informasi disimpan, dibagikan dan dikomunikasikan secara *online*.[4] Ruang siber sendiri sebagai salah satu produk dari perkembangan teknologi informasi yang kini menjadi

---

[1] Albrow, Martin and Elizabeth King (eds). *Globalization, Knowledge and Society* (*London: Sage*, 1990). hlm 8

[2] Krisna. *Pengaruh Globalisasi Terhadap Pluralisme Kebudayaan Manusia di Negara Berkembang.* (Public Journal, 2005)

[3] Scholte, J.A. *Globalization: A Critical Introduction.* (London: Palgrave McMillan, 2000)

[4] James A. Green. *Cyber Warfare A Multidisciplinary Analysis.* (Lanchester University: Routledge Studies in Conflict, Security and Technology.2015). hlm. 2

domain terbaru pada perang generasi ke-5 selain darat, laut, udara dan luar angkasa. Sebagai suatu domain baru, ruang siber menginterkoneksikan berbagai sistem terkomputerisasi melalui jaringan yang mendukung bekerjanya infrastruktur nasional yang kritis (*Critical National Infrastructure*) yang menjadi jantung kehidupan dari suatu negara.

Dengan segala efektifitas dan efisiensi yang ditawarkan dalam perkembangan dunia siber, maka terjadi konvergensi dan depedensi akan pemanfaatan dunia siber oleh banyak negara yang terus mengalami eskalasi signifikan dari tahun ke tahun dan tentunya hal ini membuka pintu ancaman yang beresiko tinggi terhadap keamanan nasional. Dengan alasan inilah mengapa ruang siber menjadi teater perang asimetris yang rentan terhadap berbagai ancaman yang tidak hanya berasal dari pihak internal atau eksternal, dan tidak hanya dilakukan oleh individu (*individuals*), kelompok (*non-state actors),* bahkan oleh suatu negara (*state actors)* dengan tujuan keuntungan pribadi atau kelompok baik moneter, militer maupun suatu kepentingan politik.[5]

Pemilihan umum sebagai pilar demokrasi dalam penyelenggaraan pemerintahan suatu negara menjadi hal fundamental dan krusial. Sehingga, adanya gangguan pada pelaksanaan pemilu dapat berimbas pada kekacauan politik hingga instabilitas keamanan dalam negeri dan mengancam pertahanan nasional. Walaupun pemilihan umum di Indonesia masih dilakukan secara konvensional, tetapi teknologi informasi telah terimplementasi secara parsial pada beberapa sistem.

Berdasarkan Undang-undang Dasar 1945 Pasal 22E ayat 1 yang menyatakan bahwa “Pemilihan Umum dilaksanakan secara langsung, umum, bebas, rahasia, jujur dan adil setiap lima tahun sekali’. Hal-hal tersebut menjadi asas pelaksanaan pemilihan umum yang selama ini diikuti oleh pemerintah Indonesia. Komisi Pemilihan Umum sebagai badan penyelenggara pemilihan umum di Indonesia seharusnya dapat menjamin

---

[5] Michael Smith. *Research Handbook on International Law and Cyberspace.* (Cheltenham UK: Edward Elgar Publishing Limited, 2015). hlm 2

pelaksanaan pemilu sesuai asas-asas tersebut bagi masyarakat Indonesia. Pada kenyataannya bahwa pelaksanaan pemilu sejak beberapa tahun terakhir mengalami disrupsi. Terjadinya berbagai macam gangguan pada pelaksanaan pemilu yang pernah dialami menjadi bukti empiris bagaimana pemilu tidak lagi sesuai dengan asas-asas yang ada. Gangguan-gangguan tersebut merupakan implikasi dari era teknologi digital yang membuka spektrum ancaman yang lebih masif pada saat pemilu seperti berbagai ancaman yang dimulai dari misinformasi untuk mempengaruhi publik hingga serangan siber yang sering dialami oleh situs-situs miliki KPU pusat dan daerah.

Komisi Pemilihan Umum (KPU) sebagai penyelenggara pemilihan umum di Indonesia seharusnya dapat belajar dari pengalaman beberapa negara dalam pengamanan pemilu. Dengan perkembangan teknologi yang pesat serta penetrasinya dalam pemilihan umum, maka membuka peluang bagi ancaman yang lebih luas dalam ranah siber. Intensitas, frekuensi dan tipe serangan yang pernah terjadi pada pemilu di beberapa negara, seharusnya dapat dipelajari oleh pihak KPU untuk dapat mengidentifikasi pola serangan siber. Sehingga, ketika suatu serangan terjadi maka dapat diketahui tujuan (*purpose*), target (target), konteks (*context), dan* skala (*scale*).

Serangan siber yang pernah dialami oleh KPU yang terus bereskalasi dalam frekuensi, dan publisitas dari tahun ke tahun menjadi tantangan tersendiri dalam membentuk keamanan siber. Dalam menghadapi spektrum ancaman siber yang luas dan dengan kemajuan teknologi pada saat ini, KPU sepantasnya memiliki infrastruktur yang menunjang kinerjanya. Tetapi pada kenyataannya hal tersebut masih menjadi permasalahan yang harus dihadapi oleh KPU pada pelaksanaan pemilihan umum 2019 mendatang. Sehingga untuk mengatasi kekurangan tersebut, KPU membangun kerjasama dengan instansi-instansi lainnya.

Dalam pelaksanaan pemilu selama ini, KPU telah bekerjasama dengan pihak akademisi seperti Universitas Indonesia dan Institut Teknologi Bandung dalam pengembangan sistem informasi (SI) dan teknologi informasi (IT). Sedangkan sepanjang tahun 2017 hingga 2018, KPU berencana akan berkolaborasi dengan institusi-insitusi lain yang *trustworthy* dan *eligible* serta memiliki *capacity* dan *capability* dalam pengamanan informasi. Institusi-institusi seperti Badan Siber dan Sandi Negara (BSSN), Kementerian Komunikasi dan Informatika (Kominfo), Badan Intelijen Negara (BIN), Kementerian Koordinator Politik, Hukum dan Keamanan serta *Cybercrime* POLRI akan turut berkontribusi dalam melakukan deteksi, proteksi serta prevensi terhadap ancaman dan serangan siber yang dapat terjadi pada Pemilu 2019.

*Global Risks Landscape Report* melalui surveinya pada tahun 2017 dan 2018 menempatkan serangan siber (*cyberattacks*) dengan prioritas tertinggi dibandingkan dengan *interstate conflict* ataupun serangan teroris. Serangan siber sendiri memiliki berbagai bentuk seperti *Cyber War, Cyber Terrorism, Cyber Espionage* dan *Cyber Crime.* Ancaman-ancaman tersebut merupakan salah satu bentuk ancaman non-tradisional dan menjadi suatu isu yang tersekuritisasi karena mengancam eksistensi dan keamanan negara sebagai referen tertinggi yang mencakup keamanan militer, lingkungan, ekonomi, sosial dan politik. Dalam menghadapi ancaman-ancaman tersebut maka perlu dibangun suatu kemampuan pertahanan nirmiliter di dunia maya (*Cyberspace*) yang disebut dengan *Cybersecurity*. Keamanan siber (*Cybersecurity*) sendiri merupakan aktivitas untuk melakukan pengamanan terhadap sumber daya telematika demi mencegah terjadinya tindakan *Cybercrime.*

Berdasarkan *Conceptual Framework Global Cybersecurity Index* oleh *International Telecommunication Union (ITU),* Indonesia berada pada peringkat ke-70 dengan *score* 0.424 yang mengindikasikan bahwa Indonesia masih memiliki kelemahan dalam implementasi pilar keamanan

siber.[6] Dalam penelitiannya *Global Cybersecurity Index* menekankan tingkat keamanan siber pada lima pilar yaitu *legal, technical, organizational, capacity building* dan *cooperation.*

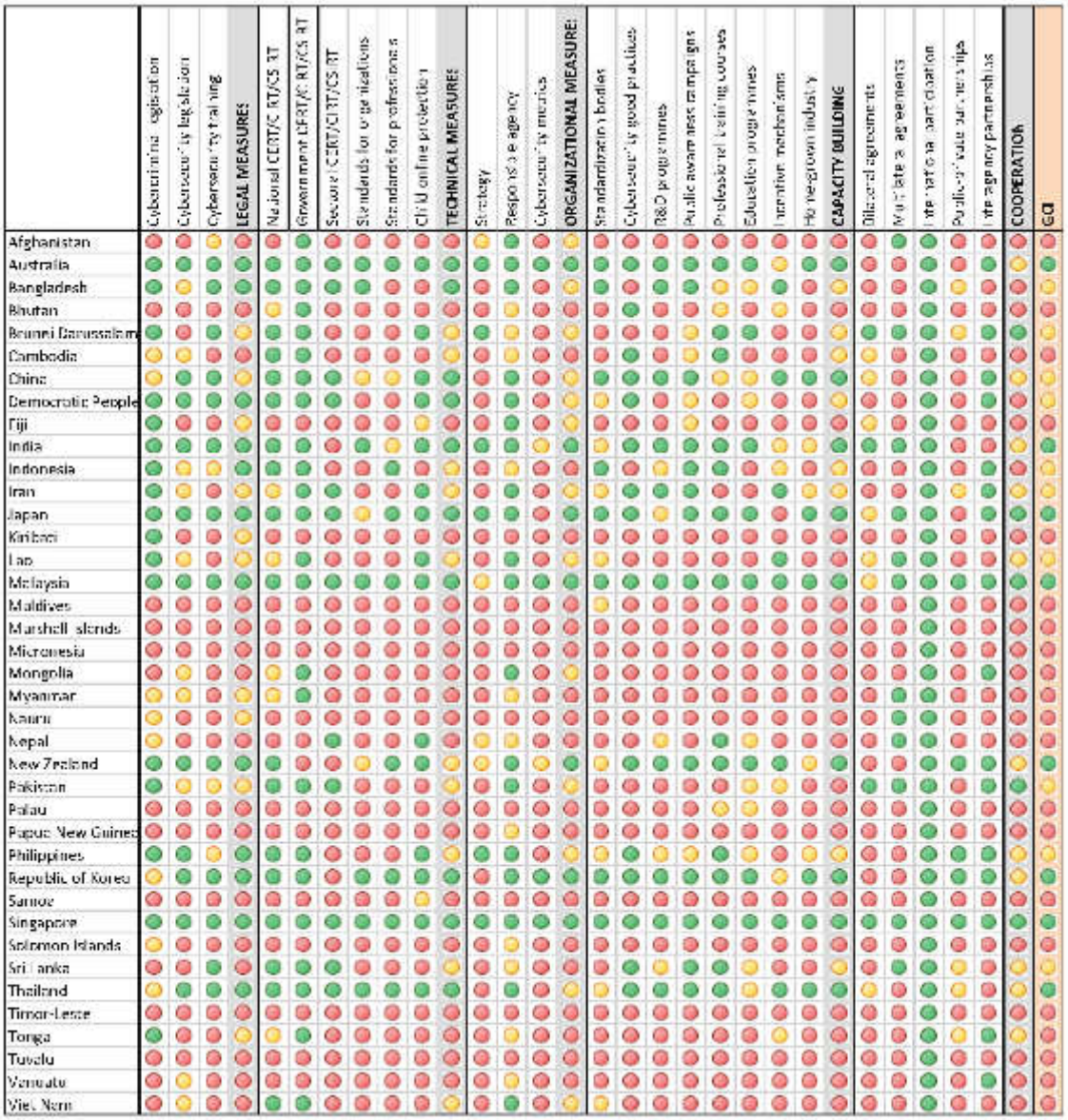
Pilar legal diukur berdasarkan keberadaan lembaga hukum dan kerangka kerja yang berhubungan dengan *cybersecurity* dan *cybercrime.* Pilar teknis diukur berdasarkan keberadaan lembaga teknis dan kerangka kerja yang berhubungan dengan keamanan siber. Pilar organisasi diukur berdasarkan keberadaan lembaga organisasi kebijakan dan strategi untuk pengembangan keamanan siber di tingkat nasional. Pilar Peningkatan Kapasitas yang diukur berdasarkan keberadaan penelitian dan pengembangan, pendidikan dan program pelatihan; profesional bersertifikat dan lembaga sektor publik yang mendukung kapasitas bangunan. Dan pilar kerjasama diukur berdasarkan keberadaan kemitraan, kerangka kerja koperasi dan jaringan berbagi informasi.[7]

Pada gambar 1.1 memperlihatkan komitmen dalam keamanan siber bahwa Indonesia masih memperoleh nilai rendah pada pilar *organizational* dan *cooperation* yang berarti masih lemahnya pemerintah dalam penerapan strategi yang terorganisir, koordinasi antar institusi serta kompilasi indikator dalam *tracking* kejahatan siber (*cybercrime*).

---

[6] *Asia and the Pacific Region Scorecard. Global Security Index* (GC) 2017 (https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf)

[7] *Ibid* hlm 4




**Gambar 1.1 *Scorecard* wilayah Asia dan Pasifik**

(Sumber: *global security index 2017*)

Perwujudan keamanan siber tidak dapat dilakukan secara sendiri, tetapi dibutuhkan kerjasama dengan instansi-instansi lainnya. Indonesia telah memasuki era keamanan siber 2.0 yang mengadopsi model kolaborasi diantara lembaga pemerintah, industri teknologi informasi dan perguruan tinggi yang cenderung menentukan arah perkembangan teknologi siber kedepan.

Dibawah ini merupakan peta ancaman yang terjadi pada pemilu baik sebelum pemilu dilaksanakan, sepanjangan pelaksanaan pemilu hingga ketika pemilu telah terlaksana.

**Tabel 1.1 Peta Ancaman Pemilu**

| **Jenis Ancaman** | |
|---|---|
| Sebelum pemilihan | Ancaman sosiokultural berupa misinformasi atau *disinformation campaign,* hoax dll untuk mempengaruhi dan menggiring opini publik |
| Sepanjang pemilihan | Peretasan terhadap sistem (server*,* transmisi) untuk mempengaruhi berjalannya proses pemilihan |
| Setelah pemilihan | Peretasan terhadap sistem untuk memanipulasi hasil perhitungan suara |

*Sumber: Diolah oleh Peneliti*

Dengan mengetahui indikator-indikator tersebut maka menjadi hal yang penting bagi publik untuk mengetahui bagaimana cara kerja sistem pemilihan umum pemerintah dan strategi tepat apa yang dapat diterapkan.

Berdasarkan permasalahan diatas, peneliti tertarik meneliti mengenai strategi Keamanan siber KPU Pusat dalam menghadapi Pemilihan Umum 2019 dalam membendung kemungkinan ancaman siber sebagai kajian dari peperangan asimetris dengan judul ***Strategi Keamanan Siber Komisi Pemilihan Umum (KPU) Pusat Dalam Menghadapi Pemilihan Umum 2019.***

## 1.2 FOKUS DAN SUB FOKUS PENELITIAN

### 1.2.1 Fokus Penelitian

Berdasarkan latar belakang penelitian, maka peneliti tertarik mengkaji strategi keamanan siber yang diterapkan oleh Komisi Pemilihan Umum (KPU) Pusat dalam menghadapi pemilihan umum 2019.

### 1.2.2 Subfokus Penelitian

Pada latar belakang telah dijelaskan ancaman siber yang sering dialami oleh KPU serta kondisi infrastruktur yang dimiliki. Komisi Pemilihan Umum telah mengalami beberapa kali penyerangan yang menyebabkan kebocoran data (*data breach)* hingga manipulasi data (*data manipulation*). Sehingga peneliti menitikberatkan bagaimana Komisi Pemilihan Umum (KPU) Pusat mewujudkan keamanan siber sebagai antisipasi dan *prevensi* terhadap ancaman siber melalui dimensi keamanan informasi sebagai bagian dari keamanan siber dengan berfokus pada dimensi organisasional. Disamping hal-hal tersebut, terdapat beberapa sub-fokus penelitian diantaranya:

1. Strategi keamanan siber yang diterapkan oleh Komisi Pemilihan Umum (KPU) Pusat dalam menghadapi Pemilu 2019
2. Sinergitas antara Komisi Pemilihan Umum (KPU) Pusat dengan institusi-institusi lainnya terkait aspek keamanan siber untuk dapat menjamin pelaksanaan Pemilu 2019
3. Faktor-faktor penghambat yang dihadapi oleh KPU dalam kerjasama tersebut pada pelaksanaan Pemilu 2019.

## 1.3 RUMUSAN MASALAH

Banyaknya jumlah, sumber dan pola serangan merupakan tantangan tersendiri yang harus dihadapi oleh KPU dalam melaksanakan tanggungjawabnya. Dengan bergerak sendiri, maka pekerjaan tersebut terkesan lebih berat, sehingga perlu dibuat suatu kebijakan dan organisasional berupa kolaborasi diantara KPU, institusi-institusi resmi pemerintah lainnya, *private sector* dan akademisi yang dapat berbagi peran dan tanggung jawab dalam mendukung keberhasilan pemilu. Dengan kerjasama *Triple Helix* ini diharapkan dapat mendeteksi dan melindungi sistem pemilihan dari ancaman *online*, serta prevensi terhadap intervensi siber dari yang tidak memiliki otoritas dan memastikan bahwa hasil pemilihan sebagai representasi suara rakyat benar-benar dilindungi pada

pelaksanaan pemilu 2019. Berdasarkan permasalahan diatas, peneliti membuat pertanyaan sebagai berikut:

1. Bagaimana strategi keamanan siber yang diterapkan oleh Komisi Pemilihan Umum (KPU) Pusat dalam menghadapi Pemilu 2019?
2. Bagaimana sinergitas antara Komisi Pemilihan Umum (KPU) Pusat dengan institusi-institusi lainnya terkait aspek keamanan siber untuk dapat menjamin pelaksanaan Pemilu 2019?
3. Faktor-faktor penghambat apa saja yang dihadapi oleh Komisi Pemilihan Umum (KPU) Pusat dalam mengimplementasikan keamanan siber pada Pemilu 2019*?*

## 1.4 TUJUAN PENELITIAN

Adapun tujuan penelitian ini adalah untuk:

1. Menganalisa strategi keamanan siber yang diterapkan oleh Komisi Pemilihan Umum (KPU) Pusat dalam menghadapi Pemilu 2019.
2. Menganalisa sinergitas Komisi Pemilihan Umum (KPU) Pusat dengan instansi-instasi terkait aspek keamanan siber*.*
3. Mengetahui faktor-faktor penghambat yang dihadapi oleh Komisi Pemilihan Umum (KPU) Pusat dalam bekerjasama dengan instansi-instansi lainnya*.*

## 1.5 MANFAAT PENELITIAN

### 1.5.1 Teoretis

Penelitian ini dapat memberikan kontribusi akademis dalam pengembangan teori-teori dan pengayaan yang terkait dengan strategi dan keamanan siber pada pegelaran pesta demokrasi di Indonesia terutama pada Pemilu 2019. Penelitian ini juga diharapkan dapat menjadi masukan bagi pihak akademisi dan komunitas lainnya untuk dapat berkontribusi lebih dalam mendukung pemerintah untuk menciptakan keamanan siber pada pemilihan umum mendatang.

### 1.5.2 Praktis

Diharapkan melalui penelitian ini dapat memberikan kontribusi bagi pemangku kepentingan, khususnya lembaga Komisi Pemilhan Umum (KPU) Pusat, Kementeriaan Pertahanan dan Kementerian Komunikasi dan Informatika dan instansi-instansi lainnya demi meningkatkan keamanan siber pemerintah. Selanjutnya hasil penelitian ini juga diharapkan dapat digunakan sebagai bahan pertimbangan dan pengambilan kebijakan bagi pemangku kepentingan dalam pengembangan aspek keamanan siber pada pegelaran Pemilihan Umum Indonesia pada tahun 2019 dan tahun-tahun mendatang.

# BAB II
# KAJIAN TEORITIK

## 2.1 Deskripsi Konseptual

Bab ini mengelaborasikan terkait kajian teoritik, penelitian terdahulu dan teori yang digunakan untuk menganalisis permasalahan dan dapat memberikan solusi bagi masalah yang diteliti. Pada suatu penelitian, kajian teoritik dipergunakan sebagai fundamen dalam merumuskan Kerangka Teori yang lalu kemudian digunakan untuk mengembangkan Kerangka Konsep penelitian. Dengan alasan tersebut, dalam rangka menganalisis dan memahami penelitian, maka peneliti menggunakan beberapa dasar teori dan konsep sebagai berikut:

### 2.1.1 Teori Ilmu Pertahanan

Pertahanan merupakan gambaran dalam mengenali kekuatan suatu negara.[16] Oleh Keliat dikutip dari Eppeler pertahanan direpresentasikan kembali sebagai suatu kenyataan yang menakrifkan kedaulatan dan keselamatan suatu bangsa dan negara. Sehingga dapat disintesakan bahwa pertahanan merupakan suatu gambaran dalam mengenali kekuatan suatu negara melalui kedaulatan dan keselamatannya. Dalam Buku Putih Pertahanan sendiri disebutkan bahwa:[17]

> *Pertahanan negara diselenggarakan untuk mempertahankan kedaulatan negara, keutuhan wilayah Negara Kesatuan Republik Indonesia, dan keselamatan segenap bangsa dari ancaman dan gangguan terhadap keutuhan bangsa dan negara*

Berdasarkan peraturan tersebut maka kebijakan-kebijakan Pemerintah terkait pertahanan negara dilakukan melalui analisis dinamika perkembangan lingkungan strategis. Demi pengkajian secara komprehensif terkait pertahanan negara maka dikembangkanlah ilmu pertahanan. Oleh Makmur Supriyanto, ilmu pertahanan didefinisikan sebagai seni dalam

[16] Erhard Eppler. *The Return of The State.*(London: Forumpress, 2009)
[17] Undang-undang Nomor 3 Tahun 2002 tentang Pertahanan Negara Pasal 1 ayat (1)

pemanfaatan segala sumber daya dan kekuatan nasional dengan tujuan untuk menghadapi ancaman internal ataupun eksternal, baik itu ancaman militer ataupun non-militer untuk mencapai tujuan nasional dan kepentingan nasional bangsa.[18]

Siber telah menjadi teater perang asimetris dan domain peperangan generasi kelima. Dengan serangan siber yang terus mengalami eskalasi dalam intensitas dan frekuensi maka dapat menjadi ancaman tersendiri yang harus dapat diantisipasi. Demi mendukung terciptanya keamanan nasional dalam rangka mendukung terwujudkan pertahanan nirmiliter yang kuat maka dengan alasan ini peneliti mengangkat topik penelitian keamanan siber.

### 2.1.2 Teori Strategi

Rich Horwart mengungkapkan bahwa strategi berasal dari keinginan seseorang untuk mengalahkan musuhnya[19]. Konsep strategi muncul dalam konteks militer dimana satu entitas berperang dengan entitas lainnya. Atas dasar intensi untuk mengalahkan, suatu entitas akan menggunakan sumber daya yang dimiliki dengan berbagai cara demi mencapai tujuannya. Hal inilah yang disebut sebagai strategi.

Nawawi mendeskripsikan strategi secara etimologis dalam manajemen organisasi sebagai kiat, cara dan taktik yang dipersiapkan secara sistematik dalam melakukan fungsi-fungsi manajemen yang terarah pada tujuan organisasi.[20]

Strategi seringkali definisinya dipertukarkan dengan taktik. Pada dasarnya kedua hal ini berbeda secara krusial. Carl Von Clausewitz melihat taktik adalah penggunaan sumber daya dalam sebuah pertempuran,

---

[18] Suriyatno, Makmur.*Tentang Ilmu Pertahanan.* (Jakarta: Yayasan Pustaka Obor Indonesia, 2014). hlm. 29.
[19] Horwart, Rich. "*The Origin of Strategy" dalam* http://www.strategyskills.com/Articles_Samples/origin_strategy.pdf. Diakses pada 12 Maret 2018
[20] Nawawi, Hadari. *Manajemen Stratejik.* (Yogyakarta: Gadjah Mada Press, 2005).

Maka taktik merupakan lingkup sempit dari sebuah strategi.[21] Dalam perang modern, pemikiran Clausewitz mengenai strategi tetap dipergunakan dan dikembangkan oleh Kolonel Arthur F. Lykke Jr kedalam suatu model yang diterjemahkan oleh suatu gambaran bahwa "*Strategy equals ends (objectives toward which one strives) plus ways (courses of action) plus means (instruments by which some end can be achieved)".* Dimana *Ends* diinterpretasikan sebagai tujuan yang hendak dicapai dari sebuah strategi yang telah direncakanan. *Means* diterjemahkan sebagai seluruh sumber daya atau instrumen yang dapat digunakan guna mendukung pencapaian tujuan dan *Ways* merupakan cara yang ditempuh atau digunakan guna mencapai tujuan.[22]. Konsep strategi Lykke diekspresikan kedalam suatu bentuk formula sebagai berikut:

"*Strategy* = *Ends* + *Ways* + *Means*"

Sedangkan strategi oleh Henry Mintzberg dikembangkan kedalam 5 (lima) definisi yang dikenal sebagai "*5Ps Strategy*" dengan penjabaran sebagai berikut:[23]

1. *Strategy as Plan* (Strategi sebagai Rencana)

   Dalam definisi ini, Mintzberg mendefinisikan strategi sebagai suatu bentuk perencanaan untuk memperjelas arah yang dituju oleh suatu organisasi dalam mewujudkan tujuan jangka panjang yang dilakukan secara sadar. Strategi dibuat dan ditindaklanjuti dengan implementasi serta pengembangan aktual dan juga bisa disebut 'strategi yang disengaja'.

2. *Strategy as Ploy* (Strategi sebagai Taktik)

   Strategi sebagai taktik atau 'siasat' yang biasanya merupakan manuver dalam suatu kompetisi atau permainan, yang dilakukan

[21] Clausewitz, C. Von, On War (Princeton University Press, eds Howard, M. and Paret, P., 1976)

[22] Baker N. & Stephens A*., Making Sense of War: Strategy for the 21st Century* (Cambridge: Cambridge University Press, 2006)

[23] Mintzberg, Henry, James Brian Quinn, dan Jhon Voyer. 1995. "*The Strategy Process*". London: Prentice Hall International, Inc.,

untuk mendapatkan yang lebih baik dari pesaing dengan memanfaatkan peluang yang muncul.

3. *Strategy as Pattern* (Strategi sebagai Pola)
   Strategi juga harus dikonsiderasikan dalam hal hasil. Strategi dapat direncanakan, tetapi hasilnya mungkin tidak sesuai dengan yang diharapkan. Dalam beberapa kasus dimungkinkan untuk melihat kembali apa yang telah terjadi, dan menggambarkan strategi ke dalam hal pola-pola yang muncul.
4. *Strategy as Position* (Strategi sebagai Posisi)
   Strategi sebagai sebuah posisi (*Position*) oleh Mintzbergi terkait visi yang terintegrasi antara organisasi dengan lingkungannya yang menjadi batas bagi aktivitasnya.
5. *Strategy as Perspective* (Strategi sebagai Perspektif)
   Pada akhirnya, strategi dapat didefinisikan dalam hal kepribadian dan budaya perusahaan yang telah diadopsi dari waktu ke waktu. Strategi adalah cara perusahaan memandang dirinya di dunia, melalui mata manajemen dan karyawannya. Ini bisa merujuk pada budaya organisasi.

Maka melalui beberapa pengertian tersebut, dapat disintesakan bahwa strategi dibuat secara sistematik guna mencapai tujuan khususnya mengatasi ancaman atau mengalahkan lawan. Dalam pencapaiannya dibutuhkan sumber daya yang siap dan digunakan dengan cara-cara tertentu sesuai dengan ancaman yang dihadapi. Adapun pada rencana peneliti menggunakan teori strategi *Ends-Means-Ways* tersebut sebagai *grand theory* dalam menganalisa penelitian yang akan dilaksanakan.

### 2.1.3 Konsep Manajemen Stratejik

Mamdu M. Hanafi menjelaskan manajemen sebagai perencanaan, organisir, mengarahkan, dan mengendalikan kegiatan untuk mencapai

tujuan organisasi dengan menggunakan sumber daya organisasi.[24] Sedangkan strategi dijabarkan sebagai penetapan tujuan jangka panjang yang dasar dari suatu organisasi dan pemilihan alternatif tindakan serta alokasi sumber daya yang diperlukan untuk mencapai tujuan tersebut.[25] Lebih lanjut dijelaskan bahwa Manajemen strategis adalah proses manajemen yang komprehensif dan berkesinambungan yang bertujuan untuk memformulasikan dan mengimplementasikan strategi yang efektif, hal ini merupakan cara untuk menanggapi peluang dan tantangan. Sedangkan menurut Siagian, manajemen strategi merupakan serangkaian pengambilan keputusan yang bersifat mendasar dan menyeluruh, disertai penetapan cara pelaksanaannya yang dibuat oleh pemimpin serta diimplementasikan oleh segenap jajaran didalam suatu organisasi untuk mencapai tujuan dari organisasi tersebut.[26]

Selain itu, peneliti juga menggunakan rumusan stratejik dimana dijabarkan sebagai sebuah proses manajemen untuk mencapai peluang dengan memobilisasi seluruh potensi sumber daya yang dimiliki (*resources*) dengan tujuan mencapai sasaran utama (*Ends)* yaitu keunggulan dan daya saing jangka panjang dengan mengantisipasi berbagai perubahan yang terjadi pada lingkungan internal dan eksternal organisasi. Manajemen stratejik merupakan suatu kesatuan rencana yang dirancang sedemikian rupa, bersifat komprehensif dan terpadu guna menjamin tercapainya sasaran-sasaran pokok organisasi atau lebih dikenal dengan istilah *Total Strategy Integration.*[27]

Dalam mencapai tujuan maka perlu dilakukan analisa pada manajemen yang terdiri atas beberapa unsur yang berpengaruh terhadap

---

[24] Mamduh M. Hanafi. *Manajemen.* (Jakarta: Unit Penerbitan dan percetakan STIM YKPN, 2011). Hlm 6.
[25] *Ibid*. hlm 134
[26] Siagian P., Sondang. *Manajemen Stratejik.* (Jakarta: PT. Bumi Aksara, 2011). Hlm. 15
[27] Matondang, M.H. *Kepemimpinan, Budaya Organisasi dan Manajemen Stratejik.* (Yogyakarta: Graha Ilmu, 2008).

pelaksanaan strategi. Beberapa unsur tersebut dijabarkan sebagai berikut:[28]

a. *Man Power* (Sumber Daya Manusia)

   Merupakan unsur fundamental dan krusial dengan alasan bahwa manusia berperan sebagai perancang dan penetap tujuan serta sekaligus berperan sebagai pelaksana dalam mencapai tujuan yang teah ditetapkan.

b. *Material* (Materi)

   Dalam mencapai tujuan dibutuhkan sarana dan prasaran yang berperan sebagai alat (*Means*) dalam mencapai tujuan.

c. *Machine* (Teknologi)

   Dengan hampir terkonvergensinya seluruh aspek kehidupan manusia dengan teknologi, maka menjadi salah satu faktor penentu dalam mencapai tujuan.

d. *Method* (Metode)

   Merupakan cara atau metode yang akan diimplementasikan guna mencapai tujuan.

e. *Money* (Uang)

   Faktor anggaran berkontribusi dalam mendukung proses pelaksanaan strategi.

f. *Market* (Pasar)

Pada manajemen stratejik ini dijabarkan juga mengenai definisi dari kekuatan, kelemahan, peluang maupun ancaman. Hal ini menjadi krusial dalam menganalisa berbagai kondisi ataupun situasi yang ada baik yang bersifat internal maupun eksternal guna mengidentifikasi berbagai hal yang dapat menjadi pendorong maupun penghambat dalam proses pencapaian tujuan yang telah ditetapkan. Adapun elaborasi dari faktor-faktor tersebut sebagai berikut:[29]

---

[28] Agustini, *Pengelolaan dan Unsur-unsur Manajemen.* (Jakarta: Citra Pustaka, 2013). Hlm. 61

[29] Siagian P., Sondang. *Op cit* hlm 172-173

a. Faktor kekuatan

   Diinterpretasikan sebagai kompetensi khusus yang terdapat dalam organisasi yang berakibat pada pemilikan keunggulan komparatif oleh unit usaha di pasaran.

b. Faktor kelemahan

   Diinterpretasikan sebagai keterbatasan atau kekurangan dalam hal sumber, keterampilan, dan kemampuan yang menjadi penghalang serius bagi kinerja organisasi

c. Faktor peluang

   Diinterpretasikan sebagai berbagai situasi lingkungan yang dapat menguntungkan bagi satuan bisnis.

d. Faktor ancaman

   Diinterpretasikan sebagai berbagai situasi lingkungan yang tidak menguntungkan bagi suatu satuan bisnis.

### 2.1.4 Konsep Hambatan

Menurut Kamus Besar Bahasa Indonesia (KBBI), hambatan berasal dari kata dasar hambat yang berarti membuat sesuatu (perjalanan, pekerjaan, dan sebagainya) menjadi lambat atau tidak lancar. Poerwandarminta menjabarkan hambatan sebagai sebuah halangan, rintangan atau suatu kondisi yang tidak diinginkan atau disukai kehadirannya, menghambat perkembangan individu, menimbulkan kesulitan bagi diri sendiri maupun orang lain dan ingin atau perlu untuk dieliminasi.[30]

Siber sebagai domain peperangan generasi terkini menjadi media untuk dapat melakukan peperangan yang dilakukan dengan cara nonlinier, tidak langsung dan bersifat proxy. Peperangan tersebut menjadi tren untuk

[30] Poerwandari, E., *Pendekatan Kualitatif dalam Penelitian Psikologi,* (Jakarta: Lembaga Pengembangan Sarana Pengukuran dan Pendidikan Psikologi (LPSP3). Fakultas Psikologi Universitas Indonesia. 1991).

menguasai suatu negara dengan menggunakan ‘senjata’ asimetris yang dibangun secara sistematis. Penciptaan kondisi menggunakan kemajuan teknologi informasi dan ruang siber menjadi keunggulan tersendiri sehingga melahirkan ancaman siber.[31]

Segala aktifitas di dunia maya yang dikategorikan sebagai ancaman dan berimplikasi terhadap kelangsungan hidup organisasi dikonsiderasikan sebagai suatu hambatan yang harus dapat diatasi dan dieleminasi guna mencapai tujuan organisasi. Pada penelitian ini, peneliti berusaha menganalisa hambatan apa saja yang menjadi kendala bagi KPU untuk dapat mewujudkan keamanan siber pada Pemilu 2019 berdasarkan konsep keamanan yang telah dipaparkan sebelumnya. Keamanan baik secara fisik ataupun virtual

### 2.1.5 Konsep Ancaman Siber

Aspek ancaman merupakan segala sesuatu yang melatarbelakangi terjadinya ancaman siber, yang meliputi berbagai aspek diantaranya ideologi, Politik, Ekonomi, Sosial, Budaya, Kebangsaan, MIliter, Ilmu Pengetahuan dan Teknologi serta aspek lainnya yang relevan dengan kehidupan berbangsa, bernegara dan bermasyarakat termasuk kepentingan pribadi.[32] Adapun bentuk ancaman siber yang sering terjadi yang dapat berupa hal-hal berikut:[33]

a. Serangan *Advanced Persistent Threats (APT), Denial of Service (DoS)* dan *Distributed Denial of Service (DDoS).* Serangan ini dilakukan dengan melakukan *overloading* kapasitas sistem dan mencegah pengguna yang sah untuk dapat mengakses dan menggunakan sistem atau sumber daya yang ditargetkan.
b. Serangan *Defacement*, dilakukan dengan cara melakukan modifikasi terhadap halaman web dari target sesuai dengan motif dari penyerang.

[31] Buku Putih Pertahanan. *Op cit.* hlm 11
[32] Peraturan Menteri Pertahanan No. 82 Tahun 2014 tentang Pertahanan Siber. *Op cit*
[33] *Ibid.*

c. Serangan *Phising*, dilakukan dengan cara memberikan alamat *website* palsu dengan tampilan serupa dengan *website* aslinya dengan tujuan untuk memperoleh informasi penting dan sensitive seperti *username, password,* dan lain-lain.
d. Serangan *Malware* yang merupakan suatu program atau kode berbahaya yang dapat dipergunakan untuk mengganggu operasi normal dari sebuah sistem komputer.
e. Penyusupan siber, yang dapat menyerang sistem melalui identifikasi pengguna yang sah dan parameter koneksi seperti *password,* melalui eksploitasi kerentanan yang ada pada sistem.
f. *Spam* merupakan penyerangan melaui pengiriman *e-mail* secara masif yang tidak dikehendaki.
g. Penyalahgunaan Protokol Komunikasi. Sebuah serangan *Spoofing Transmission Control Protocol* (*TCP*) bergantung pada kenyataan bahwa protocol *TCP* menetapkan koneksi logis antara dua ujung sistem untuk mendukung pertukaran data.

Sedangkan jenis ancaman menurut Michael D. Mcdonnell dan Terry L. Sayers dikelompokkan berdasarkan jenisnya sebagai berikut:[34]

a. Ancaman perangkat keras (*hardware threat*), ancaman yang disebabkan oleh pemasangan peralatan tertentu yang berfungsi untuk melakukan kegiatan tertentu dalam suatu sistem, sehingga peralatan tersebut mengganggu sistem jaringan dan kerja perangkat keras lainnya.
b. Ancaman Perangkat Lunak (*software threat*), merupakan ancaman yang disebabkan oleh masuknya *software* tertentu yang berfungsi untuk melakukan kegiatan seperti : Pencurian Informasi (*Information Theft*), Perusakan Informasi/Sistem (*Information/System Destruction*), Manipulasi Informasi (*Information Corruption*) dan lain sebagainya, ke dalam suatu sistem.

[34] *Ibid* hlm 12

c. Ancaman Data/Informasi (*data/information threat*), adalah ancaman yang diakibatkan oleh penyebaran data/informasi tertentu yang bertujuan untuk kepentingan tertentu, seperti yang dilakukan dalam *information warfare* termasuk kegiatan propaganda.

### 2.1.6 Konsep keamanan siber

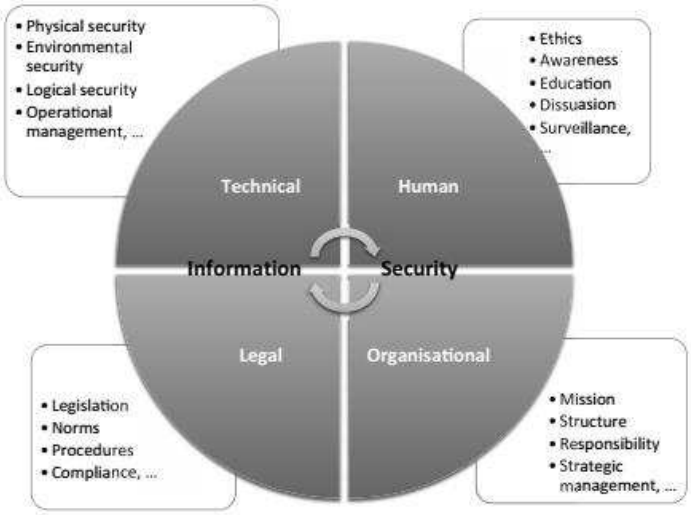
Konsep keamanan oleh Paul D. Williams yang menyatakan dapat diasosiasikan dengan pengurangan dari ancaman yang membahayakan nilai-nilai yang dimiliki, hingga jika sampai tidak direspon dengan baik akan mengancam keberlangsungan dari objek khusus yang dimaksud di masa yang akan datang[35]. Ada dua pandangan dalam mengkaji keamanan yaitu melihatnya sebagai komoditas dimana keamanan bisa didapat ketika kita bisa mengakumulasikan *power* atau memiliki hal tertentu. Pandangan kedua ialah melihat keamanan sebagai emansipasi atau bersifat pada hubungan dimana keamanan dipahami sebagai hubungan antar aktor yang berbeda. Konsep keamanan bisa diraih ketika ia berhasil mencapai kebebasan dari ancaman apapun ataupun kebebasan untuk melakukan apapun.

Keamanan siber sendiri adalah aktivitas untuk melakukan pengamanan terhadap sumber daya telematika demi mencegah terjadinya tindakan *cybercrime* seperti dijelaskan sebelumnya[36]. Konsep ini berupaya untuk mencegah serta merespon atas *vulnerability* yang dimiliki oleh organisasi tertentu, baik berada pada tatanan pemerintah, swasta bahkan individu sekalipun. Maka keamanan siber dihadapkan pada keamanan nilai-nilai tertentu khususnya berkaitan dengan TIK. Ghernaoti melihat setidaknya terdapat enam nilai yang fundamental dalam TIK yaitu aspek ketersediaan, integritas, kerahasiaan, keaslian, bisa teraudit (akuntabel), dan imputabilitas. Aspek ketersediaan berkutat pada keamanan data yang

[35] Williams, Paul D. *Security Studies: An Introduction*. (USA: Routledge, 2008)
[36] J. Falahuddin, Muhammad. *"Sekilas Tentang Cyber Crime, Cyber Security dan Cyber War* " dalam https://inet.detik.com/security/d-3005339/sekilas-tentang-cyber-crime-cyber-security-dan-cyber-war diakses pada 12 Maret 2018

disimpan sehingga bisa digunakan ketika dibutuhkan. Kerahasiaan melihat akses keamanan data hanya dimiliki yang diberi pertanggung jawaban.

Untuk mengamankan nilai-nilai itu perlu pengamanan atau *measures* tertentu. Pengamanan bisa lakukan secara teknis dan non teknis bergantung pada jenis serangan yang akan ditangkal maupun di respon. Pengamanan bisa dilakukan melalui dimensi-dimensi dari keamanan siber. Ghernaoti dalam *Cyber Power* mengklasifikasikan empat dimensi penting dalam keamanan siber yaitu teknis, sumber daya manusia, hukum, dan organisasional[37].




**Gambar 2.1 Dimensi Keamanan Informasi**

Sumber: Ghernaouti, Solange, *Cyber Power*, 2013

Dalam kajian analisis keamanan siber, keempat dimensi ini diimplementasikan pada setiap organisasi ataupun institusi pemerintahan. Sebagai instansi pemerintah, Kementerian Pertahanan sendiri menerapkan keamanan siber melalui Peraturan Menteri Pertahanan tentang Pedoman Pertahanan Siber dengan implementasi model strategi "*Ends-Ways-Means"* yang memfokuskan pada sasaran, prioritas dan aksi yang terukur melalui 5 (lima) agenda kebijakan keamanan siber. Kebijakan

[37] Ghernaouti, Solange. *Cyber Power*. (Switzerland: EPLF Press. 2013). hlm 338

tersebut meliputi *Capacity Building* (pembangunan kapasitas)*, Policy and Legal Framework* (kerangka hukum dan kebijakan)*, Organizational Structure* (struktur organisasi)*, Technical and Operational Measures* (tindakan-tindakan teknis dan operasional)*,* dan *International Cooperation* (kerjasama internasional)*.*[38]

Terkait dimensi dari keamanan siber ini, maka peneliti memfokuskan pada dimensi organisasional atau *organizational structure* dimana dimensi ini mengkaji terkait keberadaan kemitraan, kerangka kerjasama dan jaringan berbagi informasi dalam mewujudkan keamanan siber yang meliputi misi, struktur, tanggung jawab dan manajemen stratejik.

### 2.1.7 Konsep Pemilihan Umum

Bagi negara demokrasi pemilihan umum yang juga disingkat pemilu merupakan salah satu pilar utama dari kulminasi representasi keinginan rakyat dalam memilih pemimpin. Pemilihan umum merupakan suatu proses yang ditujukan untuk memilih kandidat-kandidat yang akan duduk di kursi pemerintahan berdasarkan mayoritas suara terbanyak. Mengutip Ali Moertopo yang menyatakan bahwa pemilu pada hakekatnya merupakan suatu sarana yang tersedia bagi rakyat untuk menjalankan kedaulatannya sesuai dengan azas yang termaktub dalam pembukaan Undang-Undang Dasar 1945. Pemilu itu sendiri pada dasarnya adalah suatu Lembaga Demokrasi dimana anggota-anggota perwakilan rakyatnya dipilih secara langsung yang terdiri atas MPR, DPR, DPRD yang pada gilirannya bertugas untuk bersama-sama dengan pemerintah, menetapkan politik dan jalannya pemerintahan negara. Sesuai dengan Undang-undang Nomor 7 Tahun 2017 tentang Pemilihan Umum (Pemilu) ditegaskan bahwa pelaksanaannya berdasarkan asas langsung, umum, bebas, rahasia, jujur dan adil.

[38] Peraturan Menteri Pertahanan Nomor 82 Tahun 2014. *Op cit.* hlm 3.

Di Indonesia, pelaksanaan pemilu masih dilakukan secara konvensional dimulai dari pendaftaran dan verifikasi peserta pemilih dalam pemilu hingga pencoblosan oleh pemilih dan proses perhitungan suara. Walaupun ada beberapa sistem yang telah terkomputasi. Dengan seiring perkembangan teknologi dan komunikasi, maka jenis ancaman yang dihadapi tidak hanya berupa ancaman teknis tetapi juga sosio-kultural.

### 2.1.8 Konsep Sinergitas

Harwood mengutip dari Castell, Gregory, Hindle, James dan Ragsdall yang menyatakan bahwa sinergitas diserap dari kata Yunani kuno *Synergos* yang berarti bekerja bersama-sama. Hal tersebut berperan sebagai suatu program untuk partisipasi melalui pengembangan dialog diantara disiplin dan orang yang merupakan hal yang bersifat fundamental dari sistem berfikir.[39] Sedangkan Surowiecki mengungkapkan bawah sinergitas merupakan suatu kolaborasi yang terbentuk antara beragam kelompok yang memiliki perspektif berbeda melalui kerjasama dengan tujuan meningkatkan efektifitas melalui kolaborasi pengetahuan, persepsi dan perspektif bersama. Surowiecki menyampaikan bahwa "ketika memecahkan suatu permasalahan, suatu kelompok cenderung lebih pintar dibandingkan dengan individu terpintar di kelompok tersebut".[40]

Sinergitas juga didefinisikan sebagai suatu konsep interaksi diantara dua atau lebih sumber kapital intelektual baik itu dari bisnis yang berbeda, aktifitas berbeda ataupun proses berbeda yang menciptakan suatu nilai menyeluruh yang jauh lebih baik dari dari jumlah efek individual.[41] Sinergitas dapat terbangun melalui dua acara yaitu:

---

[39] Harwood, C.J. (*Review of "Synergy matters: Working with systems in the twenty-first century* by A.M. Castell, A.J. Gregory, G.A. Hindle, M.E. James and G. Ragsdall (Eds), Kybernetes, 29(4). 2000) hlm 523-529.

[40]Surowiecki, James. *The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations*. (USA: Doubleday; Anchor. 2004).

[41] Gupta, O. & Roos, G. *Mergers and acquisitions through an intellectual capital perspective. Journal of Intellectual Capital*, 2(3). 2001. hlm. 297-309. & Krumm, J.M.M.,

1. Komunikasi

   Komunikasi dapat diartikan sebagai sebuah proses pertukaran informasi diantara individu-individu melalui suatu sistem simbolik, tanda-tanda ataupun sikap yang sama.[42]

2. Koordinasi

   Selain komunikasi, sinergitas juga memerlukan koordinasi. Hal ini dikarenakan komunikasi tidak dapat berdiri sendiri tanpa adanya koordinasi. Mungutip Moekijat, terdapat 9 (Sembilan) syarat dalam mewujudkan sebuah koordinasi yang efektif yaitu:

   1) Hubungan langsung, bahwa koordinasi dapat lebih mudah dicapai melalui hubungan pribadi langsung;
   2) Kesempatan awal, bahwa koordinasi dapat dicapai lebih mudah dalam tingkat-tingkat awal perencanaan dan pembuatan kebijaksanaan;
   3) Kontinuitas, bahwa koordinasi merupakan suatu proses yang kontinu dan harus berlangsung pada semua waktu mulai dari tahap perencanaan;
   4) Dinamisme, bahwa koordinasi harus secara terus-menerus diubah mengingat perubahan lingkungan baik internal maupun eksternal;
   5) Tujuan yang jelas, bahwa tujuan yang jelas itu penting untuk memperoleh koordinasi yang efektif;
   6) Organisasi yang sederhana, bahwa struktur organisasi yang sederhana memudahkan koordinasi yang efektif;
   7) Perumusan wewenang dan tanggung jawab yang jelas, bahwa wewenang yang jelas tidak hanya mengurangi pertentangan di antara pegawai-pegawai yang berlainan,

---

Dewulf, G. & De Jonge, H. *Managing key resources and capabilities: pinpointing the added value of corporate real estate management. Facilities*, 16(12/13). 1998. hlm. 372-379.

[42] Merriam-Webter. https://www.merriam-webster.com/dictionary/communication. Diakses pada 9 Maret 2018

tetaip juga membantu mereka dalam pekerjaan dengan kesatuan tujuan;

8) Komunikasi yang efektif, bahwa menjadi salah satu persyaratan untuk koordinasi yang baik;
9) Kepemimpinan supervisi yang efektif, bahwa menjamin koordinasi kegiatan orang-orang, baik pada tingkat perencanaan maupun pada tingkat.[43]

Deardroff dan William mengungkapkan bawah sinergitas bukanlah sesuatu yang dapat dipegang secara fisik, tetapi suatu istilah yang berarti melipatgandakan pengaruh (*multiplier effect*) yang memungkinkan energi pekerjaan atau jasa individu berlipat ganda secara eksponensial melalui usaha bersama.[44]

Sinergi kelompok dielaborasikan sebagai suatu respon yang berkembang dan mengalir dari kelompok orang yang bekerja bersama secara sinkron satu sama lain, sehingga mereka dapat bergerak dan berfikir sebagai satu kesatuan. Tindakan sinergi ini dilakukan dengan insting, positif, memberdayakan dan menggunakan sumber daya kelompok secara keseluruhan.

Merujuk dari penjelasan Surowiecki, Deardroff dan William, maka sinergitas yang dimaksud dalam konteks penelitian yang dilakukan ini adalah adanya suatu bentuk komunikasi dan koordinasi antara KPU dan pihak strategis lainnya sebagai kapital intelektual melalui kolaborasi pengetahuan, persepsi dan perspektif bersama guna memperoleh efek yang berlipat ganda dalam bentuk kerjasama. Hal ini bertujuan untuk membangun keamanan siber yang tidak dapat dilakukan secara sendiri. Badan Siber dan Sandi Negara (BSSN), Kementerian Komunikasi dan Informatika (Kemkominfo), Kementerian Koordinator Politik, Hukum dan Keamanan (Menkopolhukam), Badan Intelijen Negara (BIN), POLRI dan

[43] Moekijat, *Koordinasi (Suatu Tinjauan Teoritis),* (Bandung: Mandar Maju, 1994), hlm. 39
[44] Deardorff, D.S., & Williams, G. *Synergy Leadership in Quantum Organizations*. (Fesserdorff Consultants. 2006)

instansi-instansi lainnya diharapkan dapat berkolaborasi dan bersinergi dengan KPU dalam mewujudkan keamanan siber sesuai dengan fungsi dan tugasnya. BSSN sebagai badan yang menyelenggarakan keamanan siber memiliki peran besar dalam mendukung keberhasilan program pemerintah dalam menyelenggarakan tonggak demokrasi di Indonesia.

## 2.2 Hasil Penelitian Terdahulu

Dalam hal ini, penulis melakukan kajian terhadap penelitian-penelitan terdahulu yang relevan dengan tema yang diangkat sebagai judul tesis. Tujuannya adalah untuk melihat perbedaan dan persamaan antara penelitian sebelumnya dengan penelitian yang penulis lakukan. Disini peneliti melakukan analisa lanjutan dari 4 (empat) penelitian terdahulu, mengingat adanya beberapa kesamaan yang saling berkaitan. Adapun penelitian tersebut diantaranya:

1. Handrini Ardiyanti (2016) dalam *Cyber-security* dan Tantangan Pengembangannya di Indonesia memfokuskan pada pembangunan *Cyber-security* di Indonesia yang mengkaji faktor-faktor kelemahan dan tantangan yang dihadapi oleh Pemerintah Indonesia dalam membangun *Cyber-security*.
2. Ni Putu Arga Oktoviramitha Sari (2016) dalam Pengembangan Tata Kelola Teknologi Informasi di Komisi Pemilihan Umum Pusat yang membahas mengenai Sistem Manajemen Keamanan Informasi (SMKI) yang dimiliki oleh Komisi Pemilihan Umum (KPU) Pusat dengan Kajian kemanan informasi yang lebih bersifat teknis.
3. Erwin Kurnia N. M (2013) dalam Kebijakan Strategi Keamanan *Cyber* Nasional Dalam Menghadapi Perang *Cyber (Cyber Warfare)* yang membahas mengenai kebijakan strategi Pemerintah dibidang siber dalam mengatasi berbagai ancaman keamanan cyber nasional dalam mendukung pertahanan negara.
4. Guruh Prasetyo Putro (2014) dalam Peran Media Dalam Perang Informasi Pada Kampanye Pemilihan Presiden 2014 yang mengkaji

mengenai bagaimana media sosial dipergunakan dalam kampanye pemilihan Presiden dengan tujuan untuk memperoleh hati dan pikiran publik untuk memenangkan pemilu.

**Tabel 2.1** Penelitian Terdahulu

| Nama Peneliti (Tahun) | Judul | Teori | Metode | Hasil Penelitian | Perbedaan |
|---|---|---|---|---|---|
| Handrini Ardiyanti 2016 Tesis | *Cyber-security* dan Tantangan Pengembangannya di Indonesia | 1. Manajemen Teknologi Informasi<br>2. *Cybersecurity*<br>3. Pertahanan Negara | Kualitatif | Permasalahan terkait dengan pembangungan *cybersecurity* di Indonesia yaitu:<br>1. Lemahnya pemahaman penyelenggara negara akan *security* terkait dengan dunia *cyber* dan penggunaan *secured system*.<br>2. Belum adanya legalitas yang memadai terhadap penanganan penyerangan di dunia *cyber.*<br>3. Tata kelola kelembagaan *cyber-security* secara nasional yang masih parsial dan tersebar serta tidak adanya koordinasi yang baku dalam penanganan masalah *cyber security*.<br>4. Masih lemahnya industri di Indonesia dalam memproduksi dan mengembangkan perangkat keras atau *hardware* terkait dengan teknologi informasi. | Penulis hanya membahas keamanan siber di KPU dalam menghadapi pemilihan umum 2019. Apa saja yang dilakukan untuk dapat mendukung keberhasilan pelaksanaan pemilihan umum dalam aspek keamanan siber. |
| Ni Putu Arga Oktoviramitha Sari 2016 Tesis | Pengembangan Tata Kelola Teknologi Informasi di Komisi Pemilihan Umum Pusat | 1. Kebijakan<br>2. Tata Kelola Teknologi Informasi (*IT Governance*) | Kualitatif | Permasalahan terkait dengan Sistem Manajemen Keamanan Informasi (SMKI) dengan hasil penelitian:<br>1. KPU pada akhirnya menggunakan kombinasi antara metodologi manajemen TI menggunakan ITIL, COBIT dan ISO/IEC 27002 sehingga menjadi | Penulis berfokus pada dimensi organisasional (kerjasama) dalam mewujudkan keamanan siber. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | relevan pada indeks peniliain keamanan informasi.<br>2. Pada Indeks kesiapan manajemen keamanan informasi KPU Pusat bernilai normal yang berarti KPU pusat tidak membutuhkan usaha ekstra dalam melakukan perbaikan. Sehingga *Confidentiality, Integrity* dan *availability* dari keamanan Teknologi Informasi belum sepenuhnya diarahkan ke tujuan organisasi. | |
| Erwin Kurnia N.M<br>2013<br>Tesis | Kebijakan Strategi Keamanan *Cyber* Nasional Dalam Menghadapi Perang *Cyber (Cyber Warfare)* | 1. Kebijakan Strategi dan Ancaman *Cyber* | Kualitatif | 1. Peperangan siber (cyber warfare) bertujuan untuk menghancurkan sistem jaringan komputer suatu negara dan peralatan lain yang berhubungan dengan penggunaan sistem komputer. Adanya cyber attack, sebagai bentuk perang modern dapat mengancam dan melumpuhkan sistem keamanan dan pertahanan negara serta mengancam kehidupan masyarakat dalam suatu negara.<br>2. Kebijakan strategi di bidang cyber dan pembentukan lembaga cyber nasional diharapkan menjadi solusi dalam mengatasi berbagai ancaman keamanan cyber nasional dalam | Peneliti hanya membahas terkait ancaman siber dan strategi keamanan siber KPU dalam menghadapi ancaman siber pada Pemilu 2019 sebagai bentuk pertahanan negara dalam mewujudkan kedaulatan NKRI. |

| | | | | | |
|---|---|---|---|---|---|
| | | | | mendukung pertahanan negara di bidang cyber. | |
| Guruh Prasetyo Putro 2014 Tesis | Peran Media Dalam Perang Informasi Pada Kampanye Pemilihan Presiden 2014 | 1. Peran Media<br>2. Teori Agenda Setting<br>3. Teori Kultivasi (Terpaan Media)<br>4. Media Sosial<br>5. Perang Informasi<br>6. Kampanye Pemilihan Presiden | Kualitatif | 1. Peran media sosial pada saat kampanye Pemilihan Presiden 2014 adalah sebagai media penyebar informasi yang efektif, mudah, murah dan mampu menjangkau pengguna yang luas.<br>2. Subjek yang mendapatkan paparan informasi dari media secara terus-menerus maka akan membentuk persepsi, pemahaman, dan keyakinan dari informasi yang diterimanya tersebut.<br>3. Kegiatan kampanye di media sosial dapat dimanfaatkan untuk mendapatkan dukungan calon pemilih dan menjatuhkan *image* lawan di mata publik. | Penulis tidak berfokus pada kegiatan kampanye dan penggunaan media, tetapi akan membahas terkait kerjasama organisasional KPU dalam mewujudkan keamanan siber pada pemilu 2019. |

# BAB III
# METODE PENELITIAN

## 3.1 Desain Penelitian

Pada penelitian ini, penulis menggunakan metodologi kualitatif yang oleh Creswell dikutip dari Denzin & Lincoln diterjemahkan sebagai penempatan peneliti pada lokasi dunia global untuk melakukan aktifitas yang terdiri dari serangkaian praktik penafsiran material yang memperjelas dunia penelitian dengan tujuan mentransformasi dunia.[46] Peneliti kualitatif mempelajari segala sesuatu dilingkungan alaminya, berusaha untuk memaknai atau menafsirkan fenomena dalam suatu perspektif makna-makna yang diberikan oleh masyarakat kepada peneliti. Lebih lanjut, pendekatan yang dipilih adalah fenomenologi yang merupakan pendekatan kualitatif dimana peneliti mengidentifikasi esensi dari pengalaman-pengalaman manusia mengenai sebuah fenomena yang sebagaimana digambarkan oleh partisipan.[47] Pengalaman manusia dalam penelitian ini adalah pengalaman dari pihak-pihak yang terlibat langsung dari fenomena yang dikaji sebagai narasumber. Melalui metode kualitatif fenomenologi ini penulis akan mengkaji, mempelajari dan menganalisis secara komprehensif terkait strategi keamanan siber yang diimplementasikan Komisi Pemilihan Umum Pusat terutama pada aspek organisasional yang dianggap dapat membendung ancaman siber pada pemilu 2019. Selain itu, penulis juga ingin mengetahui sinergitas antara Komisi Pemilihan Umum Pusat dengan instansi-instansi Pemerintah lainnya dalam menghadapi ancaman tersebut.

[46] Cresswell, John W. *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. Third Edition.* (California: Sage Publication. 2009). Hlm. 13
[47] *Ibid* hlm.135-136

## 3.2 TEMPAT DAN WAKTU PENELITIAN

### 3.2.1 Tempat Penelitian

Tempat atau lokus penelitian akan dilaksanakan pada beberapa untuk mengumpulkan data terkait penelitian. Adapun lokus utama yang akan diteliti adalah:

Komisi Pemilihan Umum (KPU) Pusat
Jalan Imam Bonjol No.29, RT.8/RW.4, Menteng, Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta 10310

### 3.2.2 Waktu Penelitian

Proses penelitian akan dilakukan sepanjang tahun 2018 yang diinisiasi pada bulan Juni hingga November dengan rincian sebagai berikut.

**Tabel 3.1 Jadwal Penelitian**

| No. | KEGIATAN | 2018 | | | | | | | 2019 |
|---|---|---|---|---|---|---|---|---|---|
| | | Juni | Juli | Agus | Sep | Okt | Nov | Des | Jan |
| 1. | STUDI PENDAHULUAN | | | | | | | | |
| | a. KONSULTASI | | | | | | | | |
| | b. PENGAJUAN JUDUL | | | | | | | | |
| 2. | BIMBINGAN PROPOSAL | | | | | | | | |
| 3 | SEMINAR PROPOSAL | | | | | | | | |
| 4. | PENGUMPULAN DATA | | | | | | | | |
| 5. | ANALISIS DATA | | | | | | | | |
| 6. | PENYUSUNAN TESIS | | | | | | | | |
| 7. | KONSULTASI DAN BIMBINGAN | | | | | | | | |
| 8. | UJIAN TESIS | | | | | | | | |
| 9. | PERBAIKAN TESIS | | | | | | | | |
| 10. | PENYERAHAN TESIS | | | | | | | | |

## 3.3 SUBJEK DAN OBJEK PENELITIAN

### 3.3.1 Subjek Penelitian

Subjek dalam penelitian ini merupakan orang *(person*) yang terlibat langsung dalam pengumpulan data primer ataupun orang-orang yang menjadi narasumber pada kegiatan wawancara. Adapun narasumber yang dimaksud adalah sebagai berikut:

**Tabel 3.2 Koding Narasumber**

| No. | Jabatan/Instansi | Nama | Kode |
|---|---|---|---|
| 1. | SAM. Bidang Teknologi 6<br>Kementerian Komunikasi dan Informatika | Ir. Herry Abdul Azis, M.Eng | A-1 |
| 2. | Direktur Jendral Aplikasi Informatika<br>Kementerian Komunikasi dan Informatika | Ir. Riki Arif Gunawan M.Sc | B-1 |
| 3. | Direktorat Jendral Informasi dan Komunikasi Publik<br>Kementerian Komunikasi dan Informatika | Dra. Siti Meiningsih MSc. | B-2 |
| 4. | Direktur Deteksi Ancaman<br>Badan Siber dan Sandi Negara | Sulistyo, S.Si., S.T., M.Si | B-3 |
| 5. | Direktur Proteksi Infrastruktur Informasi Kritikal Nasional<br>Badan Siber dan Sandi Negara | Agung Nugraha, S.IP., M.Si (Han). | B-4 |
| 6. | Kepala Sub. Bagian Pengembangan Jaringan dan Komunikasi Data<br>Biro Perencanaan dan Data<br>Komisi Pemilihan Umum (KPU) Pusat | Aditya Haris Kemal Nugraha S.Komp | C-1 |
| 7. | Sekretaris Jenderal<br>Badan Pengawas Pemilu (Bawaslu) | Gunawan Suswantoro | A-2 |
| 8. | *Board Secretary and Chairman*<br>*ICT Community & Indonesia Cyber Security Forum* (ICSF) | Yuliardi Sutedja K. | C-2 |
| 9. | Praktisi IT dan Ahli Keamanan Informasi<br>Institut Teknologi Bandung | Ir. Budi Rahardjo M.Sc., Ph.D. | C-3 |

Melalui subjek penelitian, diharapkan berkontribusi penuh dalam memperoleh data yang digunakan dalam menjawab pertanyaan penelitian.

### 3.3.2 Objek Penelitian

Menurut Spradley dalam Sugiyono, pada penelitian kualitatif tidak menggunakan istilah populasi dan sampel, namun menggunakan istilah "*Social Situation",* yang berarti penelitian kualitatif meneliti suatu kasus atau fenomena sosial yang terdiri atas tiga elemen, yaitu: tempat (places), pelaku (*actors*), dan aktivitas *(activity).*[48] Hal ini berarti situasi sosial dapat diartikan sebagai objek penelitian dengan meneliti apa yang terjadi, dimana terjadinya, siapa yang terlibat dan bagaimana terjadinya. Oleh sebab itu, sampel dalam penelitian kualitatif disebut narasumber atau informan.

Penelitian kualitatif menuntut peneliti untuk memasuki situasi sosial yang akan diteliti, agar kemudian dapat melakukan observasi dan wawancara terhadap orang yang dianggap tahu permasalahan yang akan diangkat. Terdapat dua jenis teknik pengambilan sampling pada penelitian kualitatif, yaitu *probability sampling* dan *non-probability sampling*. Probability sampling dilakukan dengan anggapan bahwa setiap calon narasumber memiliki informasi yang dibutuhkan. Teknik ini meliputi *simple random sampling, proportionate stratified random sampling, disproportionate stratified randon* dan *area (cluster) sampling.*

Sedangkan nonprobability sampling merupakan teknik yang memilih anggota populasi untuk dijadikan sampel. Pada penelitian kualitatif teknik sampling yang sering digunakan yaitu *Purposive sampling* dan *snowball sampling.* Pada penelitian ini peneliti menggunakan teknik *purposive sampling,* karena seorang informan yang akan dijadikan sampel akan diobservasi terlebih dahulu oleh peneliti apakah sesuai kriteria yang ditetapkan oleh peneliti.

---

[48] Sugiyono. (2017). *Metode Penelitian Kombinasi*. Bandung: Alfabeta, 2017. hlm 297

## 3.4 Instrumen Penelitian

Instrumen penelitian pada penelitian yang akan dilakukan ini merupakan peneliti sendiri. Para peneliti kualitatif mengkolektifkan data sendiri melalui analisis berbagai dokumen, mengamati perilaku dan mewawancarai para partisipan.[49] Peneliti merupakan perencana, pelaksana pengumpulan data, penganalisis, penafsir data dan sekaligus pelapor hasil penelitian yang dilakukan.

## 3.5 Sumber Data

Pada penelitian ini sumber data terbagi atas dua jenis, yaitu sumber data primer dan sumber data sekunder yang dijabarkan sebagai berikut:

1. Sumber data primer

   Data primer merupakan data yang diperoleh dari sumber yang asli dan secara langsung serta tidak tersedia dalam bentuk file. Data ini berasal dari narasumber atau disebut responden yang merupakan orang-orang yang dijadikan objek penelitian atau dijadikan sebagai sarana untuk memperoleh informasi atau data.[50] Pada penelitian ini, peneliti mengambil data langsung dari Komisi Pemilihan Umum (KPU) Pusat dan para ahli serta praktisi IT yang kompeten pada bidang keamanan informasi dan keamanan siber diantaranya:

   a. Komisi Pemilihan Umum
   b. Badan Pengawas Pemilu
   c. Badan Siber dan Sandi Negara (BSSN)
   d. Kementerian Komunikasi dan informatika
   e. Senior Researcher ICT Watch
   f. Praktisi IT dan Ahli Keamanan Informasi

---

[49] Creswell, John W. *Penelitian Kualitatif & Desain Riset. Memilih di antara Lima Pendekatan*. (Yogyakarta: Pustaka Pelajar, 2015) hlm. 60

[50] Sarwono, Jonathan. *Metode Penelitian Kuantitatif dan Kualitatif*. Yogyakarta: Graha Ilmu, 2006).hlm. 129.

2. Sumber data sekunder

Data sekunder merupakan data yang telah tersedia sehingga peneliti hanya perlu mencari dan mengumpulkan data penelitian yang relevan.[51] Untuk memperoleh data sekunder ini, peneliti membaca berbagai referensi yang terkait dengan penelitian seperti dari buku-buku, koran, majalah dan *daring* yang membahas dan mengkaji terkait pelaksanaan pemilihan umum dan keamanan informasi dan keamanan siber.

## 3.6 Teknik Pengumpulan Data

Teknik pengumpulan data merupakan serangkaian kegiatan yang dilakukan dengan tujuan untuk mengumpulkan data baik itu sumber primer dan sekunder serta merupakan suatu langkah fundamental dan strategis dari suatu penelitian.[52] Adapun sumber primer dari penelitian yang diperoleh melalui wawancara langsung dengan pihak yang bertanggung jawab dan terlibat langsung dalam pelaksanaan pengamanan kegiatan Pemilihan Umum 2019 pada Komisi Pemilihan Umum (KPU) dan BSSN Sedangkan sumber sekundernya sendiri diperoleh dari studi dokumen untuk mendukung dan memperkuat data primer sehingga menunjang validasi data yang diberikan. Pada penelitian ini, peneliti menggunakan 4 (empat) teknik pengumpulan data diantaranya wawancara, studi pustaka dan studi dokumen yang dipaparkan sebagai berikut.

### 3.6.1 Wawancara

Wawancara merupakan percakapan dengan maksud tertentu yang dilakukan oleh dua pihak diantara *pewawancara (Interviewer*) yang mengajukan pertanyaan dan terwawancara (*interviewee*) yang memberikan

---

[51] *Ibid* hlm 124

[52] Sugiyono. *Metode Penelitian Kuantitatif Kualitatif dan R&D.* (Bandung:Alfabeta, 2012). hlm 224.

jawaban atas pertanyaan tersebut.[53] Peneliti akan melakukan wawancara untuk memperoleh informasi yang komprehensif mengenai topik yang dikaji. Wawancara dilakukan secara langsung ataupun melalui telepon. Adapun jenis wawancara dalam penelitian kualitatif yang dilakukan menurut Esterberg, yaitu:

- Wawancara Terstruktur, merupakan wawancara terhadap narasumber yang dilakukan oleh peneliti yang telah mengetahui informasi apa yang hendak diperoleh.
- Wawancara Semiterstruktur, merupakan wawancara yang lebih bersifat tidak terikat dengan tujuan untuk menemukan jawaban dari permasalahan yang lebih luas dan terbuka. Dengan alasan tersebut, narasumber dapat memberikan pendapat dan ide-ide terkait topik yang dikaji oleh peneliti.
- Wawancara Tak Terstruktur, merupakan wawancara dimana peneliti masih belum memiliki gambaran ataupun informasi yang akan diperoleh, sehingga peneliti harus dapat mendengarkan informasi dari narasumber secara seksama.[54]

Pada penelitian ini, teknik wawancara semiterstruktur dipilih oleh peneliti dengan alasan bahwa narasumber dapat memberikan lebih banyak masukan terkait topik penelitian. Banyaknya pihak yang terlibat juga menjadikan sumber informasi bervariasi. Wawancara akan dilakukan kepada narasumber-narasumber yang terlibat dan bertanggung jawab langsung terkait keamanan siber baik di KPU dan stakeholders lainnya.

### 3.6.2 Studi Pustaka

Studi pustaka merupakan metode pengumpulan data yang diarahkan kepada pencarian sebuah data dan informasi dari berbagai sumber seperti dokumen, foto, gambar, maupun dokumen elektronik yang

---

[53] Moleong, Lexy J. *Metodologi Penelitian Kualitatif.* (Bandung: Remaja Rosda Karya, 1991). hlm. 186
[54] Sugiono *Op Cit* hlm. 319

mendukung dalam proses penulisan[55]. Tahapan ini, penulis melakukan analisa terkait konsep keamanan siber yang akan diimplementasikan oleh KPU pada Pemilihan Umum 2019 mendatang. Pada tahap berikutnya, penulis menggunakan sumber-sumber referensi keamanan siber yang telah ada dan dikembangkan baik internal ataupun eksternal Penulis akan mendalami sejauh mana tingkat keamanan siber yang telah diimplementasikan oleh pihak KPU.

### 3.6.3 Studi Dokumen

Studi dokumen merupakan teknik pengumpulan data melalui bahan tertulis ataupun film, baik itu dokumen pribadi ataupun dokumen resmi. Dokumen pribadi merupakan catatan atau karangan seseorang secara tertulis tentang tindakan, pengalaman, dan kepercayaannya dengan maksud untuk memperoleh kejadian aktual tentang situasi sosial dan arti berbagai faktor di sekitar subjek penelitian. Sedangkan dokumen resmi yang terbagi atas dokumen internal dan dokumen eksternal. Dokumen internal berupa memo, pengumuman, instruksi, aturan suatu lembaga masyarakat tertentu yang digunakan dalam kalangan sendiri. Termasuk risalah atau laporan rapat, keputusan pemimpin kantor dan semacamnya. Sedangkan dokumen eksternal berisi bahan-bahan informasi yang dihasilkan oleh suatu lembaga sosial, misalnya majalah, buletin, pernyataan, dan berita yang disiarkan kepada media massa. Penelitian dengan studi dokumen sebagai sumber data dimanfaatkan untuk menguji, menafsirkan, dan bahkan meramalkan.

---

[55] *Ibid*

### 3.7 Pemeriksaan Keabsahan Data

Pada penelitian kualitatif, pemeriksaan keabsahan data disebut juga dengan uji validitas. Sugiyono memaparkan validitas sebagai derajat ketepatan antara data yang terjadi pada objek penelitian dengan data yang dapat dilaporkan oleh peneliti.[56] Pemeriksaan keabsahan data dilakukan dengan tujuan bahwa data yang diperoleh adalah valid dan dapat dipertanggungjawabkan kebenarannya. Uji keabsahan data dalam penelitian kualitatif dibagi atas empat (4) yaitu:

a. *Credibility* (validitas internal) berkenaan dengan tingkat atau derajat ketepatan dari desain penelitian dengan hasil yang dicapai.[57] Dilakukan dengan mengamati lebih lanjut, pengamatan secara terus menerus, triangulasi atau memeriksa keabsahan data yang telah dikolektifkan dan dijadikan pembanding, serta mengadakan *member check.*
b. *Transferability* (validitas eksternal) tujuannya adalah agar data dari penelitian yang dilakukan tersebut tepat dan dapat diimplementasikan di tempat data tersebut dikumpulkan.
c. *Dependability* (realibilitas) berarti bahwa hasil penelitian harus mengacu pada konsistensi peneliti baik itu dalam proses mengumpulkan data, membentuk, dan menguraikan konsep-konsep ketika membuat interpretasi untuk menarik kesimpulan.
d. *Confirmability* (objektivitas) berarti apakah penelitian dapat dibuktikan kebenarannya dimana hasil penelitian telah sesuai dengan data yang dikumpulkan dan dicantumkan dalam laporan lapangan.

Untuk pemeriksaan keabsahan data, maka penulis memilih menggunakan *credibility* atau validitas internal. Tahap ini diawali dengan perpanjangan pengamatan yang dilakukan dengan melakukan kembali pengamatan di lapangan dan melakukan wawancara kembali untuk

---

[56] *Ibid* hlm. 361
[57] *Ibid*

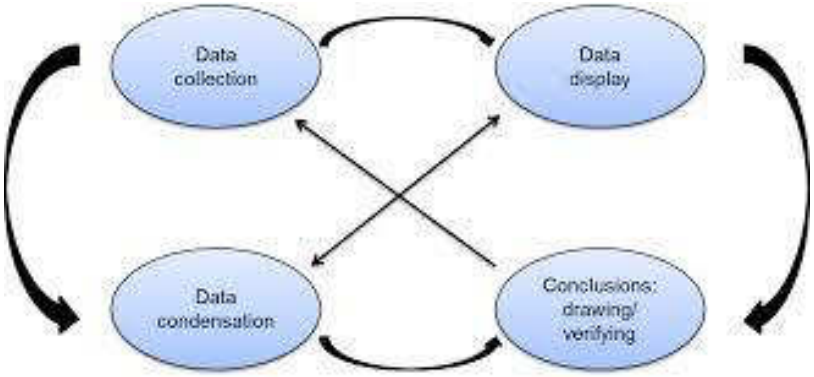
konfirmasi data yang telah diperoleh. Hal ini bertujuan untuk menjalin hubungan emosional dengan mendekatkan diri dengan narasumer, sehingga narasumber tidak lagi merasa asing dan ingin memberikan informasi detail terkait topik penelitian. Peneliti akan melakukan penelitian dengan melaksanakan pengumpulan data di Komisi Pemilihan Umum (KPU) Pusat dan Badan Siber dan Sandi Negara yang berada di Jakarta. Pendekatan awal dengan tujuan memperoleh data untuk kemudian dapat melaksanakan pengamatan dan wawancara secara komprehensif. Kemudian pada uji kredibilitas akan dilakukan pengamatan ulang dengan detail atas data-data yang telah ditemukan. Pada tahap ini peneliti dapat memberikan deskripsi data yang akurat dan sistematis tentang apa yang diamati.

Tahap selanjutnya adalah triangulasi pengumpulan data yang dilakukan dengan memeriksa data hasil wawancara, observasi, dan dokumentasi. Hal ini dilakukan untuk menyelaraskan data yang diperoleh, jikalau terdapat perbedaan maka akan dilakukan diskusi kembali dengan para narasumber utama terkait kebenaran dari data tersebut. Selanjutnya akan dilakukan triangulasi waktu dengan tujuan untuk memperoleh data yang seragam dan kredibel yang seringkali berbeda karena dipengaruhi oleh waktu pengambilan data. Data yang diperoleh saat pagi hari dapat berbeda dengan data yang dipeoleh ketika malam hari karena dapat dipengaruhi oleh kondisi fisik ataupun emosi dari narasumber. Oleh karena itu perlu dilakukan pengecekan kembali data yang diperoleh dengan narasumber pada waktu yang berbada untuk memvalidasi data yang diperoleh.

### 3.8 Teknik Analisa Data

Analisis data yang digunakan dalam penelitian ini menggunakan analisis interaktif yang merupakan kolaborasi dari proses siklus dan interaktif. Adapun siklus dari interaktif tersebut dimulai dari proses pengumpulan data, penyajian data, reduksi data, dan kesimpulan atau

verifikasi.[58] Berikut ini merupakan proses yang dilakukan dalam analisis data, mengacu pada Miles dan Huberman :




**Gambar 3.1 Gambar Analisa Data Kualitatif Miles & Huberman**

Sumber: Miles & Huberman, *Qualitative Data Analysis*

| PROSES | KEGIATAN |
|---|---|
| Kondensasi Data (*Collective*) | Perumusan rangkuman, pembuatan transkrip wawancara serta pemilihan data terkait pelaksanaan Pemilihan Umum pada 2019 dan implementasi keamanan siber yang telah dilaksanakan. |
| Penyajian Data (*Display*) | Pemilahan dan pengategorisasian informasi melalui kategori berikut; 1) Implementasi strategi keamanan siber sebelum, saat pelaksanaan, dan pasca pemilu 2) kondisi keamanan siber KPU sebelum, saat pelaksanaan, dan pasca pemilu 3) identifikasi ancaman siber sebelum, saat pelaksanaan, dan pasca pemilu |
| Reduksi Data (*Reduction*) | Teknik analisis guna memilih data yang relevan melalui penggolongan, dan pengorganisasian sehingga dapat ditarik suatu kesimpulan untuk selanjutnya dapat ditampilkan untuk selanjutnya dapat diolah. |

[58] Idrus, Muhammad. *Metode Penelitian Ilmu Sosial: Pendekatan Kualitatif dan Kuantitatif.* (Jakarta: Erlangga, 2016)

| | |
|---|---|
| Penarikan Kesimpulan (verifikasi) | Interpretasi terhadap kondisi keamanan siber KPU dan bagaimana KPU melalui kerjasama dengan para pihak strategis guna mekonsolidasikan segenap kemampuan sesuai dengan peran dan tanggung jawab masing-masing melalui deteksi, proteksi dan prevensi guna mendukung keberhasilan Pemilu 2019 yang bebas dari ancaman ataupun serangan siber pada saat sebelum, pelaksanaan dan pasca pemilu. |

# BAB IV
# HASIL DAN PEMBAHASAN

Pada Bab IV ini, peneliti akan menyajikan data hasil penelitian yang diperoleh di lapangan yang kemudian dielaborasikan menggunakan teori yang sebelumnya telah dipilih dan disesuaikan dengan maksud dan tujuan penelitian.

## 4.1. Hasil Penelitian

Pada subbab ini, peneliti menampilkan deskripsi umum mengenai objek penelitian untuk memperoleh data dan hasil penelitian dengan tujuan untuk menjawab rumusan masalah sebagai berikut:

### 4.1.1. Komisi Pemilihan Umum (KPU) Pusat

Deskripsi umum objek penelitian merupakan studi yang dilaksanakan di Komisi Pemilihan Umum (KPU) Pusat yang terletak di Jalan Imam Bonjol No. 29 RT.8/RW.4, Menteng, Kota Jakarta Pusat, Daerah Khusus Ibukota Jakarta. Komisi Pemilihan Pusat yang biasa disingkat KPU merupakan lembaga independen yang dibentuk oleh Pemerintah yang bertanggung jawab dalam penyelenggaraan Pemilihan Umum yang Mandiri, Profesional dan Berintegrasi.

Tugas dan kewenangan KPU dijabarkan dalam Pasal 10 Undang-undang Nomor 3 Tahun 1999 tentang Pemilihan Umum dan Pasal 2 Keputusan Presiden Nomor 16 Tahun 1999 tentang Pembentukan Komisi Pemilihan Umum dan Penetapan Organisasi dan Tata Kerja Sekretariat Umum Komisi Pemilihan Umum, dijelaskan bahwa untuk melaksanakan Pemilihan Umum, KPU mempunyai tugas kewenangan sebagai berikut:

1. Merencanakan dan mempersiapkan pelaksanaan Pemilihan Umum;
2. Menerima, meneliti dan menetapkan Partai-partai Politik yang berhak sebagai peserta Pemilihan Umum;
3. Membentuk Panitia Pemilihan Indonesia yang selanjutnya disebut PPI dan mengkoordinasikan kegiatan Pemilihan Umum mulai dari

tingkat pusat sampai di Tempat Pemungutan Suara yang selanjutnya disebut TPS;

4. Menetapkan jumlah kursi anggota DPR, DPRD I dan DPRD II untuk setiap daerah pemilihan;
5. Menetapkan keseluruhan hasil Pemilihan Umum di semua daerah pemilihan untuk DPR, DPRD I dan DPRD II;
6. Mengumpulkan dan mensistemasikan bahan-bahan serta data hasil Pemilihan Umum;
7. Memimpin tahapan kegiatan Pemilihan Umum.

Dalam Pasal 2 Keputusan Presiden Nomor 16 Tahun 1999 terdapat tambahan huruf:

1. Tugas dan kewenangan lainnya yang ditetapkan dalam Undang-undang Nomor 3 Tahun 1999 tentang Pemilihan Umum. Sedangkan dalam Pasal 11 Undang-undang Nomor 3 Tahun 1999 tersebut juga ditambahkan, bahwa selain tugas dan kewenangan KPU sebagai dimaksud dalam Pasal 10, selambat-lambatnya 3 (tiga) tahun setelah Pemilihan Umum dilaksanakan, KPU mengevaluasi sistem Pemilihan Umum.

Adapun susunan organisasi dari Komisi Pemilihan Umum (KPU) berdasarkan Peraturan KPU No. 6 Tahun 2008 tentang Susunan Organisasi dan tata Kerja Sekretariat Jenderal Komisi Pemilihan Umum, Sekretariat Komisi Pemilihan Umum Provinsi, dan Sekretariat Komisi Pemilihan Umum Kabupaten/Kota sebagaimana telah diubah menjadi Peraturan KPU No. 22 Tahun 2008.


**Gambar 4.1 Struktur Organisasi Sekretariat Jenderal KPU**

*Sumber: Peraturan KPU No. 22 Tahun 2008*

Penelitian ini akan berfokus pada kerjasama *Triple Helix* (*Government, Business, Intellectual*) yang dilakukan oleh KPU pada aspek keamanan siber pada Pemilu 2019 mendatang, sehingga hanya akan meneliti pada Biro Perencanaan dan Data. Adapun tugas dari biro ini adalah menyusun rencana, program, anggaran, kerjasama antar-lembaga, penelitian dan pengembangan, pengolahan data dan informasi, serta monitoring dan evaluasi. Sedangkan fungsi dari Biro Perencanaan dan Data adalah:

a. Penyusunan rencana, program, dan anggaran;
b. Pelaksanaan kerjasama antar lembaga, penelitian dan pengembangan organisasi dan sistem Pemilu;
c. Pelaksanaan pengolahan data dan informasi;
d. Pelaksanaan monitoring dan evaluasi; dan
e. Pelaksanaan urusan tata usaha biro

Peneliti menjadikan KPU sebagai objek penelitian dengan alasan bahwa Pemilihan Umum 2019 merupakan pemilihan Presiden dan pemilihan legislatif yang pertama kali diadakan secara serentak di Indonesia. Pemilihan Umum ini merupakan pesta demokrasi terbesar dalam perjalanan sejarah demokrasi Indonesia dengan besar anggaran 24.8 triliun Rupiah.[60] Mengingat urgensi diadakannya pemilihan umum bagi pemerintahan yang merupakan salah satu pilar utama dari sebuah akumulasi kehendak rakyat dan juga merupakan prosedur demokrasi untuk memilih tokoh politik yang akan memimpin Indonesia selama beberapa tahun kedepan. Maka, dengan adanya gangguan akan dapat menyebabkan instabilitas politik yang berimplikasi luas terhadap keamanan nasional hingga mengancaman pertahanan negara.

[60] Pesta sudah dimulai: Yang Perlu Anda ketahui soal Pemilu 2019. Dalam http://www.bbc.com/indonesia/indonesia-45618212. Diakses pada 15 November 2018

Sepanjang tahun 2017, Indonesia sendiri mengalami serangan siber yang cukup signifikan dalam frekuensi dan intensitas yaitu sebanyak 205.502.159 serangan.[61] Jumlah serangan termasuk usaha peretasan terhadap Komisi Pemilihan Umum (KPU) diawal bulan Februari tepat saat perhitungan suara Pemilihan Gubernur dan Wakil Gubernur DKI Jakarta putaran pertama. Sebelumnya KPU juga mengalami serangan pada tahun 2004, 2009 dan 2014. Pada tahun 2004, Dani Firmansyah seorang alias Xnuxer berhasil masuk ke situs KPU dan mengubah nama-nama partai peserta Pemilu.[62] Sedangkan pada saat pemungutan suara Pemilihan Presiden dan Wakil Presiden 2014, situs KPU kembali diretas dengan tindakan *blocking* terhadap jaringan.[63] Peristiwa-peristiwa yang telah terjadi ternyata tidak menjadi pembelajaran bagi pihak KPU untuk berbenah, mantan kepala Lembaga Sandi Negara (Lemsaneg) Djoko Setiadi berhasil meretas situs KPU untuk menguji tingkat keamanannya. (BAB 4)

Berdasarkan hasil uji kerawanan sistem informasi Pilkada 2017 oleh pihak BSSN diperoleh informasi bahwa terdapat beragam aktifitas serangan siber dimulai dari SQL-*Injection* yang dilakukan terhadap beberapa situs KPU di Indonesia termasuk kpujakarta.go.id, infopilkada.kpu.go.id, pilkada2017.kpu.go.id, ppid.kpu.id, sip.kpu.id, simonika.kpu.id dan sidalih.kpu.id. Pada tahun 2018 ini sendiri, pihak KPU mengimplementasikan kebijakan *active-down* secara sepihak dengan tujuan untuk menangkal serangan peretas terhadap perhitungan suara Pilkada Serentak 2018 yang tengah berlangsung. Hal ini menunjukkan bahwa tingkat kerentanan keamanan siber dan sistem informasi sepanjang pelaksanaan pemilu masih sangat tinggi dan masih belum dapat teratasi

[61] Laporan Tahunan *Indonesia Security Incident Response Team of Internet Infrastructure* (ID-SIRTII) 2017

[62] Anonim. "*Xnuxer,'Hacker Partai Jambu' Situs KPU",* dalam https://inet.detik.com/cyberlife/d-2643201/xnuxer-hacker-partai-jambu-situs-kpu diakses pada 10 Maret 2018

[63] Antara. "*Jaringan KPU Sempat Diretas Saat Rekapitulasi Suara Pilpres 2014",* dalam http://news.metrotvnews.com/politik/yNLAZZ6b-jaringan-kpu-sempat-diretas-saat-rekapitulasi-suara-pilpres-2014 diakses pada 10 Maret 2018

hingga saat ini. Intensitas serangan terhadap situs KPU dan data pemilu dapat saja meningkat pada tahun 2019 dikarenakan belum terwujudnya sistem keamanan yang optimal. Sehingga dibutuhkan suatu strategi keamanan siber yang dapat digunakan yang meliputi deteksi, proteksi serta prevensi dari ancaman.

### 4.1.2. Strategi Keamanan Siber Komisi Pemilihan Umum (KPU) Pusat dalam Menghadapi Pemilu 2019

Strategi dibuat untuk mencapai suatu tujuan, dimana dalam pencapaiannya dibutuhkan sumber daya (*resources*) yang siap dan digunakan dengan cara-cara tertentu sesuai dengan ancaman yang dihadapi. Sesuai dengan kajian Buku Putih Pertahanan yang menyatakan bahwa sebuah strategi meliputi elemen membentuk, merespon dan menyiapkan dengan indikator 1) *Ends; 2) Means; 3) Ways*.

Berdasarkan data yang telah dikumpulkan di lapangan melalui wawancara (*in-depth interview)*, dan didukung oleh studi pustaka serta dokumen, maka diperoleh hasil evaluasi dari setiap indikator-indikator tersebut, antara lain:

***a. Ends***

*Ends* merefleksikan tujuan yang ingin dicapai, dalam hal ini adalah visi dari Komisi Pemilihan Umum (KPU) Pusat yaitu menjadi penyelenggara pemilihan umum yang mandiri, professional dan beritintegrasi untuk terwujudnya pemilu yang benar, jujur dan adil. Manifestasi dari visi tersebuat tertuang dalam strategi *collaboration approach* yang ditelah diimplementasikan oleh KPU pusat dengan melibatkan seluruh pemangku kepentingan (*stakeholders)* dari Pemerintah, pihak swasta dan Akademisi (*Triple Helix*) dalam mencapai tujuan. Kerjasama ini meliputi seluruh aspek keamanan siber pada Pemilu 2019 yang meliputi deteksi ancaman, proteksi terhadap sistem keamanan dan mitigasi ancaman.

Berdasarkan hasil wawancara dengan pejabat terkait, diperoleh informasi bahwa kerjasama dalam pengamanan pelaksanaan pemilihan umum tidak hanya dilakukan secara fisik tetapi juga virtual (keamanan siber). Walaupun sistem pemilihan umum di Indonesia saat ini masih dilakukan secara manual (*non-electronic*), tetapi terdapat beberapa sistem elektronik yang mendukung pelaksanaannya (*partial*). Sehingga terdapat kemungkinan ancaman yang lebih luas yang meliputi ancaman sosiokultural hingga peretasan. Apapun yang terjadi di dunia maya berimplikasi terhadap dunia nyata dan juga sebaliknya. Dengan demikian untuk mengatasi berbagai jenis ancaman tersebut,[64] maka perlu dilakukan prevensi dan eleminasi baik itu pada saat sebelum pemilihan, sepanjang pemilihan dan setelah pemilihan.

***b. Means***

*Means* merepresentasikan sumber daya (*resources*) yang dimiliki oleh aktor dengan dimensi *tangible* maupun *intangible* yang mencakup seluruh sumber daya yang dimiliki oleh aktor dan dapat dipergunakan untuk pemenuhan strategi.[65] Dari 6 (enam) unsur dalam manajemen stratejik yang digusung oleh Agustini, KPU menggunakan mengoptimalkan 3 (tiga) sumber daya yang dimiliki meliputi sumber daya manusia (*Man Power*), infrastruktur (*technology*) dan regulasi (*legal*). Berikut merupakan hasil temuan peneliti di lokus penelitian yang dilakukan.[66]

Informan C-1 memaparkan bahwa dalam bidang pengamanan IT pihak KPU Pusat mengalami keterbatasan *Man Power* dimana hanya didukung oleh 3 orang organik dan 2 orang non-organik. Hal serupa juga dialami oleh KPU-KPU Daerah di Indonesia. Dengan keterbatasan *Man Power* dan dengan pola serangan yang beragam serta eskalasi serangan yang sangat tinggi pada saat pemilu, maka pihak KPU setidaknya

[64] Michael D. Mcdonnell dan Terry L mengelompokkan jenis ancaman atas 3 (tiga) jenis yaitu ancaman perangkat keras, ancaman perangkat lunak dan ancaman data/informasi.
[65] Nainggolan dalam Freddy Rangkuti, *Analisis SWOT Teknis Membedah Kasus Bisnis,* (Jakarta: Gramedia Pustaka Utama, 1998) hlm. 3-4
[66] Agustini, *Op cit*

membutuhkan bantuan personel dari institusi lain dalam pengamanan siber. KPU seharusnya didukung oleh SDM yang memiliki kapasitas dan kapabilitas di bidang keamanan siber. Diperlukan penambahan *Man Power* dan usaha yang besar untuk melakukan perekrutan, pelatihan dan me-maintenance SDM, sehingga memiliki *skill* dan *experience* yang cukup untuk dapat memonitor, menganalisis dan memberikan rekomendasi terhadap jaringan terkait insiden siber yang akan dan sedang terjadi.

Disamping itu, beliau menambahkan bahwa masih minimnya kesadaran (*awareness*) para pihak KPU yang terlibat dalam pelaksanaan pemilu menjadi sebuah celah kerentanan. *Phising* dan S*ocial-engineering* yang pernah terjadi pada Pilkada 2018 melalui peretasan terhadap akun *social media (messenger)* dari salah satu pihak KPU menjadi pembelajaran tersendiri. Sehingga diharapkan adanya edukasi dan sosialisasi keamanan siber bagi seluruh pihak strategis yang terlibat.

Pada aspek infrastruktur, KPU cukup optimis dengan teknologi yang dimiliki baik itu perangkat keras (*hardware)* maupun perangkat lunak (*software*). Teknologi milik KPU juga dikonsolidasikan dengan teknologi dari para *stakeholders* untuk menunjang kinerja dan backup sistem KPU. Meski demikian, KPU tetap melakukan konseling dan diskusi dengan stakeholders lainnya. Perspektif sama juga turut disampaikan oleh Informan C-3 yang menyatakan bahwa dimensi keamanan informasi yang dimiliki oleh Pemerintah secara teknis dianggap sudah cukup memadai. Tetapi hal ini bukan merupakan sesuatu hal yang perlu dipamerkan untuk dapat menarik perhatian publik dan mengundang ancaman baru.

Dari perspektif regulasi, sejauh ini KPU dalam bekerjasama hanya bersinergi dengan Kementerian Komunikasi dan Informatika (Kemkominfo) dan Badan Pengawas Pemilu (Bawaslu) dalam MoA pada pelaksanaan Pilkada 2018 yang juga melibatkan penyedia jasa media sosial (*social media platform*) dan Penyedia jasa internet (APJII). Sedangkan untuk Pemilu 2019, MoA tersebut akan dilanjutkan dengan penambahan beberapa poin tertentu dan sedang dalam tahap pengajuan menunggu

persetujuan dari Menteri Komunikasi dan Informatika. *Memorandum of Action* pada Pilkada 2018 memberikan kontribusi positif pada penurunan angka penyebaran *hoax* sepanjang pelaksanaan Pilkada 2018. Namun, pencapaian tersebut tidak terlepas dari peran serta *stakeholders* lain seperti *Cybercrime* POLRI dalam perannya menindaklanjuti pelanggaran Undang-Undang Informasi dan Transaksi Elektronik (ITE). Keterlibatan dan dukungan instansi-instansi pemerintah diluar Kementerian Komunikasi dan Informatika merupakan benefit bagi KPU.

***c. Ways***

*Ways* merupakan cara/taktik/strategi dalam penggunaan *resources* (*means*) yang dimiliki untuk mencapai tujuan (*ends*). Adapun cara/taktik/strategi yang diimplementasikan oleh Komisi Pemilihan Umum (KPU) Pusat dalam menghadapi Pemilu 2019 dalam konteks keamanan siber adalah sebagai berikut:

**1) Cara/taktik/strategi**

Dalam rangka pengamanan Pemilu, khususnya di bidang siber. KPU melakukan strategi kolaboratif dengan merangkul berbagai *stakeholders* dengan *expertise* dibidang keamanan siber serta yang terlibat secara langsung dalam pelaksanaan pemilu. Serangan siber yang terjadi pada saat pelaksanaan pesta demokrasi di berbagai negara dan di Indonesia sepanjang Pemilu 2009 dan 2014 menjadi fakta empiris yang menjadi pembelajaran bagi seluruh pihak yang terlibat. Berbagai serangan siber pada Pemilu di luar negeri menggunakan teknik yang beraneka ragam seperti *voting data maipulation*, *DDoS/Defacement*, *troll farms/Fake News* dan *Hack/Leak/Amplify*. Di Indonesia sendiri, teknik yang sama digunakan dalam menyerang situs-situs KPU seperti yang ditunjukkan pada gambar berikut.


**Gambar 4.2 Serangan siber pada Pemilu/Pilkada di Indonesia**
*Sumber: Dokumen Badan Siber dan Sandi Negara*

Informan B-4 menyatakan berdasarkan statistik serangan *DDoS* (*Distributed Denial of Services)* di Indonesia, pada tahun 2018 dari Januari hingga April memperlihatkan frekuensi serangan yang tidak tinggi, kemudian pada bulan Mei tidak terdapat serangan sama sekali. Hingga pada bulan Juli pada saat PILKADA berjalan, terjadi eskalasi frekuensi serangan sepanjang pemilu hingga pada Agustus tidak terdeteksi adanya ancaman sama sekali. Melalui gambaran ini, tidak menutup kemungkinan potensi model *behavior* atau *pattern* ini akan terjadi lagi pada Pemilu 2019 mendatang.

Pada Oktober 2016, Pemerintah Amerika Serikat menuding Rusia meretas organisasi-organisasi politik yang terlibat pada pemilihan dan membocorkan informasi yang dicuri untuk mempengaruhi hasil pemilu.[67] *Internet Research Agency* (IRA) yang berbasis di Rusia sebagai entitas yang membuat berbagai macam akun palsu di Amerika Serikat dengan menyamar sebagai aktifis melalui pencurian identitas asli orang asli AS

[67] David P. Fidler. "The U.S Election Hacks, Cybersecurity, And International Law". *Symposium on Cybersecurity and The Changing International Law of Data.* Doi:10.1017/aju.2017.5

untuk mengacau sistem politik dengan menggiring opini publik. Mereka bergerak di sejumlah social media platform seperti *Facebook, Twitter, Instagram, YouTube* dan *Tumblr*. Mereka membuat berbagai akun Facebook seperti *Secured Borders, Blacktivist*, dan *Army of Jesus*.[68]

Fakta empiris tersebut sejalan dengan pernyataan Informan A-1 dari Kementerian Komunikasi dan Informatika (Kemkominfo) yang menyatakan bahwa ancaman yang paling mengkhawatirkan adalah *framing* untuk menggiring opini publik yang intens dilakukan oleh pihak tertentu dan dalam jangka waktu serta tujuan tertentu. Pernyataan tersebut diperkuat oleh Informan C-2 dari *The Indonesia Cyber Security Forum* (ICSF) yang menegaskan bahwa telah terjadi fabrikasi informasi untuk membangun *influence building* di Indonesia menjelang Pemilu 2019 melalui sistem pemahaman publik. Pembangunan *public distrust* terhadap Pemerintah merupakan indikasi-indikasi awal bahwa negara kita sedang menghadapi masalah. Dalam pernyataannya tersebut, beliau menambahkan bahwa mempengaruhi opini publik merupakan sebuah skenario dari peperangan informasi (*information warfare*) yang merupakan doktrin militer yang dibawa ke ranah sipil, sehingga menjadi masalah besar. Pada kenyataannya bahwa masyarakat Indonesia tidak mengetahui dan tidak terlatih mengenai *psychological warfare* yang dipadukan dengan peperangan asimetris. Mereka tidak mengetahui dampak apa yang dapat ditimbulkan dari operasi intelijen dalam bentuk perang opini publik (perang informasi), *hoax, hatespeech* dan lain-lain.

Berdasarkan alasan tersebut, sejak Pilkada 2018, KPU menjalin kerjasama dengan Bawaslu dan Kemkominfo untuk mengatasi ancaman sosiokultural sebagai suatu bentuk perang asimetris yang dilakukan melalui penyebaran informasi. KPU sebagai suatu lembaga independen memiliki keterbatasan dalam melaksanakan tugas dan kewenangannya, sehingga

[68] Budi Riza. "*Ini Cara Kerja Kelompok Rusia yang Dituding Intervensi Pilpres AS*", dalam. https://fokus.tempo.co/read/1064823/ini-cara-kerja-kelompok-rusia-yang-dituding-intervensi-pilpres-as diakses pada 9 Maret 2018

membutuhkan bantuan dari pihak lain. Selama ini dalam melaksanakan fungsi dan kewenangannya, KPU cenderung bekerja bersama multi-stakeholder secara parsial. Hal ini dilakukan dengan tujuan menjaga netralitas dari KPU sendiri serta menghindari opini publik terkait intervensi pemerintah dalam pelaksanaan Pemilu.

Selain bekerjasama dengan Bawaslu dan Kemkominfo yang termanifestasi dalam *Memorandum of Action* pada Pilkada 2018 dan dengan *planning* yang sama untuk Pemilu 2019 mendatang. KPU juga melibatkan Badan Siber dan Sandi Negara (BSSN), Badan Intelijen Negara (BIN), Kementerian Politik, Hukum dan HAM (Polhukam), Bareskrim POLRI, Badan Pengkajian dan Penerapan Teknologi (BPPT), ID-SIRTII dan Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) dalam penanganan disrupsi keamanan siber dan penindakan pelanggaran Undang-Undang Informasi dan Transaksi Elektronik (ITE).

*Stakeholders business* seperti *social media platform* dan *Internet service provider* Moratelindo/Telkom Indonesia juga ikut terlibat dalam mengamankan infrastruktur dan jaringan internet sepanjang pelaksanaan pemilu 2019. Keterlibatan pihak akademisi, Universitas Indonesia (UI) dan Institut Teknologi Bandung (ITB) dalam desain dan pengembangan aplikasi merupakan refleksi kepedulian anak bangsa dalam andilnya membangun bangsa dan negara.

Setiap pihak yang terlibat merupakan *expertise* yang memiliki peran dan fungsi masing-masing dalam mendukung keberhasilan pelaksanaan pemilu pada aspek keamanan siber. Keterlibatan stakeholders dalam bingkai konsep kerjasama *Triple Helix* diterapkan oleh KPU mengingat bahwa sebagai lembaga independen terdapat keterbatasan dan kemampuan dalam melaksanakan tugasnya. Konsep keamanan siber (*Cybersecurity*) sebagai sebuah paradoks yang tidak dapat dilakukan sendiri dengan kenyataan bahwa ancaman di dunia siber tidak dapat dihilangkan sepenuhnya. Sehingga, dibutuhkan strategi kerjasama

untuk dapat mencegah dan menanggulangi segala ancaman dan insiden siber yang berpotensi terjadi sepanjang pelaksanaan Pemilu 2019.

**2) Peran *Stakeholders***

Dalam menghadapi potensi ancaman yang dapat terjadi pada sepanjang pelaksanaan pemilu, KPU tidak terlepas dari peran serta *stakeholders* yang berkontribusi dalam mendukung keamanan siber pada tiap-tiap tahap pemilu sesuai dengan peta ancaman.

**Tabel 4.1. Peta Ancaman Pemilu**

| Jenis Ancaman | |
|---|---|
| Sebelum pemilihan | Ancaman sosiokultural yaitu misinformasi berupa *negative campaign, black campaign, hoax*, *hatespeech* dll untuk mempengaruhi dan menggiring opini publik |
| Sepanjang pemilihan | Peretasan terhadap sistem (server, transmisi) untuk mempengaruhi berjalannya proses pemilihan |
| Setelah pemilihan | Peretasan terhadap sistem untuk memanipulasi hasil perhitungan suara dan *social-engineering* |

Sumber: Diolah oleh Peneliti

Berdasarkan peta ancaman pemilu tersebut, maka setiap *stakeholder* yang terlibat memiliki peran dan kontribusi tersendiri . Adapun peran para *stakeholders* dalam mendukung keamanan siber pada Pemilu 2019 pada aspek deteksi, proteksi dan prevensi yang dijabarkan pada tahap-tahap pemilu sebagai berikut:

**a) Sebelum pemilihan berlangsung**

Pada tahap ini, jenis ancaman yang dihadapi adalah ancaman data/informasi sehingga KPU berkolaborasi dengan Bawaslu bekerjasama dalam penanganan konten-konten negatif Pemilu, terkait *framing* (pembentukan opini) dan berkoordinasi dengan Kementerian Komunikasi dan Infomatika (Kemkominfo) untuk pemantauan serta tindak lanjut penanganan pada level *social media platform.* Kementerian Komunikasi

dan Infomatika memberikan masukan kepada KPU dan Bawaslu terkait akun-akun media sosial dari pasangan calon yang melakukan kampanye secara resmi agar didaftarkan sebagai *verified account*.

Kerjasama ini termanifestasi dalam *Memorandum of Action (MoA*) yang dilaksanakan sejak Pilkada 2018 yang berisi mengenai manajemen dan pengawasan konten internet dalam penyelenggaraan pemilihan Gubernur, Bupati dan Wakil Bupati Dan/Atau Walikota dan Wakil Walikota Tahun 2018.[69] MoA ini ditandatangani oleh Abhan yang mewakili Badan Pengawas Pemilihan Umum RI, Arief Budiman mewakili Komisi Pemilihan Umum RI dan Rudiantara yang mewakili Kementerian Komunikasi dan Informatika RI.

Menurut Informan B-1, MoA untuk mengatur konten internet pada Pilpres 2019 mendatang masih dalam tahap pengajuan dan pembicaraan. Adapun isi dari MoA tersebut tidak akan jauh berbeda dengan MoA yang dilakukan pada Pilkada 2018, walaupun mungkin akan terdapat sedikit penambahan terkait manajemen dan pengawasan konten internet sepanjang pelaksanaan Pemilu. Secara garis besar, MoA mengatur ruang lingkup dari para *stakeholder* dalam melaksanakan tanggung jawabnya. Dimana KPU memiliki tanggung jawab untuk memberikan aturan terkait Pemilu, Bawaslu bertanggung jawab untuk melakukan penindakan terhadap pelanggar (Partai Politik), dan Kemkominfo bertanggung jawab dalam hal teknis yaitu melakukan *take down* hingga *blocking* terhadap akun-akun yang melakukan pelanggaran. Disamping ketiga institusi tersebut, MoA turut serta melibatkan *Internet Service Provider* (ISP) dan *Social Media Platform* dalam mendukung kinerja Kemkominfo. Adapun ke-9 *social media platform* yang ikut berpartisipasi yaitu *Facebook, Google, Twitter, YouTube, BBM, Bigoo, LiveMe, MeTube* dan *Telegram.*

[69] Nota Kesepakatan Aksi antara KPU, Bawaslu dan Kementerian Komunikasi dan Informatika.

Pejabat terkait juga menambahkan bahwa selain bertanggung jawab dalam operational dan teknis, Kemkominfo juga bertugas sebagai fasilitator/penghubung diantara KPU, Bawaslu dan *Social Media Platform* serta memberikan edukasi kepada para staf KPU dan Bawaslu untuk dapat berkomunikasi dan berkordinasi secara langsung dengan para *Social Media Platform* dalam hal pelaporan dan penindakan terhadap konten-konten negatif serta akun-akun teregistrasi milik calon/partai politik yang dianggap melakukan pelanggaran. Selain hal tersebut, Kemkominfo juga memiliki kewajiban untuk melakukan pengamanan siber sebatas permintaan langsung dari KPU dan Bawaslu. Perlu diketahui bahwa kerjasama diantara KPU, Bawaslu, dan Kemkominfo yang juga melibatkan ISP dan *9 Social Media Platform* lebih bersifat repressif, sedangkan tindakan preventif dilakukan oleh pihak intelijen.

Informan B-1 dari Direktorat Jenderal Informasi dan Komunikasi Publik juga menambahkan bahwa Kemkominfo selain melakukan *filter content* terhadap informasi yang beredar di masyarakat, juga melakukan *counter* melalui narasi tunggal guna mewujudkan kondisi aman dan kondusif. Pemantauan dari sirkulasi informasi terkait Pemilu ditengah masyarakat dipantau oleh KPU bersama Bawaslu sepenuhnya dan ditindaklanjuti oleh Kemkominfo. Konten-konten yang telah melalui evaluasi oleh KPU dan Bawaslu selanjutnya ditindak lanjuti melalui aksi *take down* ataupun penutupan akun. Sedangkan untuk pelanggaran terhadap Undang-Undang ITE dilakukan oleh POLRI melalui divisi *Cybercrime* POLRI.

Kerjasama para stakeholders dalam *Memorandum of Action (MoA)* pada Pilkada 2018 dianggap cukup berhasil yang ditandai dengan deeskalasi pelanggaran dan penyebaran informasi palsu yang cukup signifikan. Sehingga diharapkan bahwa dengan perencanaan *Memorandum of Action (MoA)* untuk Pemilu 2019 dapat memberikan hasil yang positif dan diharapkan jauh lebih baik.

Dari sisi aplikasi, sejak tahun 2008 KPU telah bekerjasama dengan pihak akademisi Institut Teknologi Bandung dan beberapa tahun kemudian tepatnya pada tahun 2012 bekerjasama dengan Pusat Ilmu Komputer (Pusilkom) Universitas Indonesia untuk mengembangkan berbagai aplikasi sistem informasi Pemilu seperti Sidalih (Sistem Informasi Data Pemilih), Situng (Sistem Informasi Perhitungan Suara), Sipol (Sistem Informasi Partai Politik), Silog (Sistem Informasi Logistic), Sidapil (Sistem Informasi Daerah Pemilihan), Sitagis (Sistem Informasi Berbasis Teknologi *Geographic Information System*), Siparmas (Sistem Informasi Partisipasi Masyarakat), dan Silon (Sistem Informasi Pencalonan). Untuk sistem informasi perhitungan suara (Situng) sendiri, sebelumnya merupakan projek yang dikerjakan oleh Pusat Ilmu Komputer Universitas Indonesia pada tahun 2014. Sedangkan untuk Pemilu 2019 dialihkan ke Institut Teknologi Bandung. Seluruh aplikasi sistem informasi yang di-*develop* oleh KPU dan akademisi sebelum *go-live dan publish,* terlebih dahulu akan dikaji dan dilakukan *security testing system* yang dilakukan oleh Badan Pengkajian dan Penerapan Teknologi (BPPT). Audit aplikasi yang dilakukan oleh BPPT dengan konsiderasi bahwa insititusi tersebut sudah memiliki standar keamanan siber ISO 27001 dan memenuhi standar manajemen ISO 9001.

**b) Sepanjang dan Setelah Pemilihan**

Pada tahap ini KPU melibatkan seluruh stakeholders terkait untuk melakukan proteksi dan prevensi, walaupun tidak memiliki keterikatan secara kontrak ataupun perjanjian tertulis. Beberapa lembaga dari pemerintahan seperti Kemkominfo, BSSN, BIN, POLRI, dan Polhukam tetap proaktif mendukung keamanan siber tanpa adanya payung hukum yang membawahi hubungan kerjasama tersebut.

Menurut Informan C-1, belum terdapatnya payung hukum yang menjadi landasan bagi para instansi pemerintah untuk ikut berkontribusi secara lebih aktif dengan konsiderasi untuk menghindari polemik dan spekulasi publik terkait intervensi pemerintah terhadap hasil Pemilu. Mengingat bahwa KPU merupakan lembaga independen yang bersifat

netral, sehingga ruang gerak perlu dibatasi. Dengan ruang lingkup yang terbatas, maka kinerja dan ruang gerak dari institusi pemerintah juga terbatas.

Menurut Informan B-4, pada tanggal 2 Juli 2018, BSSN mengadakan diskusi bersama dengan beberapa *stakeholders* terkait langkah-langkah pengamanan dan peran mereka dalam pemilu berdasarkan *study case* pada PILKADA 2018. Stakeholders yang terlibat diantaranya seperti Bareskrim POLRI tindak pidana *cyber*, BIN, APJII, Kemkominfo, PT. Telkom, dan teman-teman komunitas seperti FORMASI (Forum Keamanan Informasi).

Informan B-3 menyatakan bahwa dalam mewujudkan keamanan siber saat pemilu maka BSSN melaksanakan fungsinya dalam pengamanan dimulai dari fungsi Identifikasi dan Deteksi, Proteksi, Penanggulangan dan Pemulihan, serta Pengawasan dan Pengendalian. Beliau menambahkan bahwa peran BSSN dan *stakeholders* tersebut dalam mendukung keamanan siber pada saat pelaksanaan Pemilu yaitu menerapkan strategi kemanan siber nasional (*National Cybersecurity Strategy)* yang merupakan arah kebijakan umum yang dirancang untuk meningkatkan keamanan dan ketahanan infrastruktur dan layanan dengan menetapkan berbagai tujuan dan prioritas dalam skala nasional yang harus dicapai dalam jangka waktu tertentu.

Dalam pernyataannya, beliau menambahkan bahwa dalam strategi keamanan siber nasional, beberapa poin penting di dalamnya antara lain mengenai: *Active/Dynamic Security Measures, Awareness And Training/Information Security Campaign, Critical Infrastructure Protection, Cryptographic Protection, Defence Cyber Operations/Intervention, Information Sharing/ Exchange, International Collaboration, Legislation/Legal Framework, Mandating Security Standards, National Detection Capability, Privacy Protection, Secure Protocols And Software, Strategic Cyber Security Council,* dan *Tracing Criminals And Prosecution*.

Aspek-aspek tersebut dipadukan melalui pelaksanaan fungsi identifikasi dan deteksi, proteksi, penanggulangan dan pemulihan, serta pengawasan dan pengendalian terkait keamanan siber yang saat ini telah dilakukan oleh BSSN. Dalam level operasional, BSSN memiliki unit *Security Operation Center* (SOC) yang melakukan *monitoring* anomali lalu lintas data melalui sensor-sensor yang ada.

Adapun bentuk ancaman siber yang mungkin dapat timbul pada pelaksanaan Pemilu seperti serangan *Advanced Persistent Threats (APT)*, *Denial of Service (DoS),* dan *Distributed Denial of Service (DDoS).* Selain ancaman tersebut, aksi *Defacement* hingga serangan *Phising, malware* ataupun *Trojan.* Sehingga untuk mengantisipasi ancaman tersebut maka BSSN menggunakan metode yang diimplementasikan dalam pengamanan siber yaitu pada level KPUD, dipasang 34 sensor *Honeypot*, 34 sensor Matagaruda, dan upaya identifikasi sistem informasi milik KPUD. Di KPU, dilakukan perbaikan sistem informasi KPU, pemasangan sensor Mata Garuda, *Dashboard Honeynet,* monitoring sistem KPU, dan menyiapkan insiden respon tim. Di internal BSSN, melakukan fungsi monitoring di *social media*, *media daring*, serta *instant messenger*; melakukan analisis *cyber threat intelligence.* Selain di KPU dan KPUD, juga dilakukan identifikasi sistem keamanan siber di instansi lain seperti Bawaslu, Mahkamah Konstitusi, dan Kemendagri. BSSN juga bekerja sama dengan komunitas siber dan akademisi dalam melakukan analisis dan asistensi.

Hasil rapat pada 2 Juli 2019 juga membahas mengenai *social engineering* yang pernah dialami oleh pihak KPU. Belajar dari pengalaman, maka seluruh pihak strategis bersepakat untuk menggunakan *platform social media* lokal yaitu “Pesan Kita” untuk edukasi ataupun sosialisasi terkait dengan pemilu ataupun koordinasi internal KPU sendiri. Selain mendorong penggunaan aplikasi “Pesan Kita”, diharapkan hal ini juga dapat menjadi penetrasi pada *high level management*.

Pemilihan “Pesan Kita”, dengan konsiderasi bahwa aplikasi ini dikembangkan oleh FORMASI (Forum keamanan Informasi) karya mandiri anak bangsa, dari sisi keamanan dilengkapi dengan *end-to-end encryption* dan data berada di Indonesia sehingga informasi yang bersifat *confidential* tidak tersebar secara random. Standar keamanan *comply* ke ISO 270001 dan 90001. Dikatakan bahwa pada dasarnya, *Security by design* itu seharusnya melekat pada aplikasi dengan pertimbangan dari segi keamanan baik pada saat pengembangan ataupun pada saat *go-live*.

BSSN yang dibentuk pada Januari 2018 memiliki tanggung jawab langsung dalam melaksanakan keamanan siber di Indonesia melalui pemanfaatan, pengembangan dan konsolidasi seluruh elemen yang terkait dengan keamanan siber. Dengan kehadiran BSSN diharapkan dapat membantu KPU dalam membentuk keamanan siber sepanjang pelaksanaan pemilu melalui pemberian rekomendasi keamanan siber baik itu standar dan regulasi keamanan sistem informasi serta skema audit keamanan sistem informasi. Sehingga, insiden siber yang pernah dialami didalam ataupun yang dialami oleh negara-negara lain sepanjang pemilu dapat diantisipasi dan dilakukan prevensi. Kehadiran BSSN setidaknya diharapkan dapat meminimalisir ancaman yang mungkin berpotensi muncul melalui identifikasi kerawanan (*vulnerability analysis* dan *penetration test*) dan proteksi sistem. Mengingat segala keterbatasan yang dimiliki oleh KPU, maka keterlibatan BSSN memberikan benefit tersendiri bagi KPU dalam melakasanakan tugas dan tanggung jawabnya.

### 4.1.3. Sinergitas antara Komisi Pemilihan Umum (KPU) Pusat dengan *Stakeholders* (*Triple Helix concept*)

Sinergitas merupakan suatu konsep interaksi diantara dua atau lebih sumber kapital intelektual baik itu dari bisnis yang berbeda, aktifitas berbeda ataupun proses berbeda yang menciptakan suatu nilai menyeluruh

yang jauh lebih baik dari jumlah efek individual.[70] Dalam rangka pengamanan Pemilu, khususnya di bidang siber, KPU senantiasa menjalin hubungan yang baik dengan organisasi maupun instansi yang berkaitan dengan siber. Sinergitas ini terbangun melalui komunikasi dan koordinasi yang dilakukan oleh KPU dan dijabarkan sebagai berikut:

**a. Komunikasi**

Informan C-1 menjelaskan bahwa sinergitas KPU dengan Bawaslu dan Kemkominfo sudah sangat baik. Hal ini dinilai berdasarkan tingkat kemudahan dalam berkomunikasi dengan seluruh *social media platform* serta kecepatan dalam merespon laporan yang menunjukkan sinergitas yang tinggi dalam menciptakan stabilitas politik selama pemilu. Selain itu KPU juga tetap melakukan diskusi dua arah mengenai insiden siber yang tengah dihadapi disamping melakukan *transfer of knowledge* terhadap pekerja (*Man Power*) terkait masalah teknis melalui pelatihan yang dilakukan di Kemkominfo.

Informan B-3 menyampaikan bahwa BSSN selaku Lembaga yang mengonsolidasikan fungsi siber di setiap instansi, khususnya yang berkaitan dengan penyeleggaraan Pemilu, terus berupaya membangun sinergitas setiap unsur siber yang ada di setiap instansi. Beliau menambahkan bahwa jauh sebelum pelaksanaan Pilkada serentak pada tahun 2018, BSSN telah menyelenggarakan *Forum Group Discussion* (FGD) tentang potensi ancaman siber pada Pilkada 2018, yang melibatkan banyak pihak yang memiliki fungsi siber, khususnya yang berkaitan dengan Pilkada. Kemudian, melakukan koordinasi kepada pihak-pihak terkait sebagai bentuk tindak lanjut. *Forum Group Discussion* (FDG) yang telah dilaksanakan ini dianggap sebagai titik awal membangun sinergitas dengan banyak pihak yang terlibat dengan Pilkada, tidak hanya dengan KPU. Selanjutnya beliau juga menambahkan bahwa diseminasi laporan strategis

[70] Gupta, O. & Roos, G. *Op cit.*

kepada pemangku kepentingan di masing-masing instansi juga merupakan salah satu bentuk upaya membangun sinergitas.

**b. Koordinasi**

Informan C-1 menyatakan bahwa bentuk koordinasi yang dilakukan oleh KPU, Bawaslu dan Kemkominfo dalam penanganan konten-konten negatif sejauh ini dianggap memiliki tingkat responsif tinggi. Selain itu, peran *social media platform* dalam melakukan "*turn back hoax"* juga dinilai sangat bersinergi.

Pernyataan tersebut juga dibenarkan oleh Informan A-2 yang mengatakan bahwa kordinasi dalam bersinergitas antar lembaga baik KPU dan Kemkominfo saat ini dianggap jauh lebih bagus, dimana Menkopolhukam juga bersikap lebih proaktif dalam penanganan terkait pelanggaran Pemilu. Informan B-1 juga menegaskan hal yang serupa dengan memaparkan terjadinya deeskalasi konten-konten negatif yang beredar di dunia maya merupakan salah satu bukti kerjasama yang cukup baik diantara seluruh *Stakeholders* yang terlibat.

Menurut Informan C-3, secara sejarah pihak akademisi ITB selalu ikut berkontribusi dalam membantu pelaksanaan pesta demokrasi di Indonesia sejak dulu. Beliau menambahkan bahwa permasalahannya bukan tentang *entity*, tetapi individu-individu. Sejauh ini sinergitas diantara KPU dan ITB dianggap cukup positif walaupun kurang mengetahui tingkat intensitasnya.

Selanjutnya perspektif berbeda disampaikan oleh Informan C-2 beliau menilai terdapat kesulitan dalam bekerjasama diantara para *stakeholders* Pemerintah, hal ini dikarenakan alasan adanya ego-sektoral. Menurutnya jikalau memang telah terjadi kolaborasi yang baik, maka seharusnya sudah banyak permasalahan yang dapat diselesaikan secara bersama. Mengingat bahwa KPU, Kominfo, Bawaslu adalah suatu tim.

### 4.1.4. Faktor- faktor penghambat yang Dihadapi Oleh Komisi Pemilihan Umum (Kpu) Pusat Dalam Implementasi Keamanan Siber

Dalam mencapai tujuan strategi maka terdapat hambatan yang perlu dihadapi. Hambatan yang dihadapi tentunya mempengaruhi kinerja dari Komisi Pemilihan Umum (KPU) Pusat. Adapun beberapa kendala tersebut yang diketahui melalui hasil pengumpulan data wawancara yang dilakukan dan didukung oleh observasi secara tidak langsung serta studi dokumentasi, maka diperoleh hasil evaluasi:

a. Hambatan *Budgeting*/*Money*
b. Hambatan *Man Power*
c. Hambatan *Legal*

Adapun ketiga faktor tersebut oleh KPU dianggap sebagai hambatan dalam mewujudkan keamanan siber pada Pemilihan umum 2019 dan dielaborasikan sebagai berikut:

***a. Budgeting/Money***

Permasalahan finansial merupakan salah satu faktor yang menjadi hambatan tidak hanya bagi perusahaan-perusahaan besar, tetapi juga bagi KPU demi meningkatkan keamanan siber dalam mendukung pelaksanaan Pemilu 2019 mendatang. Konsep manajemen stratejik memasukkan uang (*money*) sebagai unsur yang berpengaruh dalam pelaksanaan strategi. Kasubag. Pengembangan Jaringan dan Komunikasi data KPU, Informan C-1 menyatakan bahwa terkait anggaran sebenarnya telah ditetapkan pada awal program di tahun sebelumnya dan dengan jumlah terbatas. Sehingga, ketika terjadi *additional cost* terkait pembiayaan fasilitas jaringan ataupun perawatan maka menjadi hambatan tersendiri. Keterbatasan ini juga berimplikasi terhadap peningkatan kinerja pengamanan siber dimana kurangnya tenaga ahli dalam bidang IT khususnya pengamanan siber.

Merespon pernyataan Informan C-1, Informan B-3 mengatakan bahwa terdapat 3 (tiga) komponen inti yang perlu diperhatikan dalam konteks pengamanan siber, yaitu: *people, process* dan *technology*. Dengan keterbatasan dalam *budgeting* maka akan menjadi faktor penghambat bagi ke tiga komponen tersebut. Penyediaan sumber daya manusia dengan kapabalitas di bidang kemananan siber melalui perekrutan dan pelatihan membutuhkan biaya. Aspek *People* merupakan salah satu permasalahan dari kemajuan teknologi. Perkembangan teknologi yang tumbuh secara eksponensial tidak linear dengan ketersediaan sumber daya yang memiliki kapasitas di bidang keamanan siber sehingga memunculkan permasalahan *talent gap.* Sedangkan dari sisi teknologi, untuk membangun infrastruktur dan sarana yang mendukung maka dibutuhkan anggaran yang tidak sedikit. Suatu standar keamanan akan berjalan baik jika didukung dengan aspek manusia dan teknologi yang baik pula. Dengan adanya kerjasama maka menjadi benefit tersendiri bagi pihak KPU dalam melaksanakan fungsinya.

***b. Man Power***

Dalam pernyataannya, Informan C-1 memyampaikan hambatan yang dihadapi saat oleh KPU adalah masalah *Man Power*. KPU Pusat memiliki suatu sistem IT yang kompleks dengan ancaman siber yang terus dialami sepanjang tahun, apalagi ketika menjelang pemilu dimana terjadi eskalasi serangan siber yang beraneka ragam dan mencapai kulminasi pada saat perhitungan suara. Menurutnya, tahap paling rentan dari Pemilu 2019 adalah pada saat perhitungan suara. Gangguan pada Sistem Perhitungan Suara (Situng) dengan alasan bahwa akan terjadi gangguan paling masif yang dilakukan mulai dari *newbie* hingga *organized hacker* dengan berbagai modus. Dengan jumlah serangan dan dengan hanya didukung oleh 5 orang staff IT, maka diperlukan usaha keras untuk dapat mewujudkan keamanan siber secara mandiri. Selanjutnya terkait *awareness* dari para staf KPU yang terlibat yang dinilai masih minim. Diperlukan adanya edukasi dan sosialisasi mengenai keamanan siber yang diimplementasikan keseluruh jajaran *top-to-down management* agar

terhindar dari ancaman *social-engineering* yang pernah dialami pada Pilkada 2018.

Beliau menambahkan bahwa kendala dalam bekerjasama dengan stakeholder lain seperti akademisi adalah permasalahan profesionalitas. Pelayanan yang tidak 24/7 dari pihak akademisi menyebabkan lambatnya respon yang diterima dalam mengatasi insiden siber yang muncul. Hal ini disebabkan karena akademisi bekerja *off-site (remote)*, sehingga terkadang permintaan yang dilakukan tidak terakomodir sama sekali. Hal tersebut diperburuk dengan *Man Power* dari akademisi yang terbatas dan tanpa ada *resource* pengganti. KPU juga mengharapkan agar instansi tersebut memiliki *"sense of awareness"* dan koordinasi yang lebih baik, tanpa harus diminta oleh KPU. Dengan konsiderasi tersebut, KPU mengakhiri kontrak kerjasama terkait aplikasi dengan Universitas Indonesia. Walaupun masih terikat dalam perjanjian terkait infrastruktur.

Informan C-3 juga menambahkan bahwa dengan *Man Power* yang terus berganti, maka memunculkan permasalahan baru dimana kita seharusnya tidak bersandar pada dokumentasi yang selalu tidak tersedia. Menyikapi hal tersebut, seharusnya terdapat kontinuitas melalui dokumentasi untuk mengetahui apa dan sejauh mana yang dikerjakan serta mengetahui apa yang seharusnya dilakukan kedepannya untuk mengembangkan sistem yang telah dibuat.

*Leadership* merupakan hambatan paling utama yang kini dihadapi oleh KPU. Belum terdapatnya leadership yang dianggap mampu dan menjadi panutan untuk menyuarakan kerjasama. Berbagai pihak akan memiliki *interest* untuk ikut berkontribusi membantu KPU jikalau terdapat seorang leader yang memberikan misi sehingga pihak-pihak tersebut tergerak untuk membantu. Di Indonesia terdapat banyak pihak yang cukup *compatible* untuk membantu dan tidak termotivasi dengan profit semata. Menurutnya publik tidak melihat visi dari KPU untuk menganggap bahwa pemilihan umum adalah sesuatu hal yang penting.

***c. Legal***

Informan C-1 menyebutkan bahwa sejak KPU Pusat tidak memiliki standar keamanan siber dalam bentuk sertifikasi ISO/IEC 27001:2009 dan manajemen 9001, maka dibutuhkan peran serta dari *expertise* yang berasal dari institusi lainnya. Dengan anggaran terbatas dan kemajuan teknologi yang terus berkembang pesat, KPU mengalami kesulitan dalam meningkatkan pelayanan keamanan. Sehingga dibutuhkan suatu bentuk kerjasama yang mengikat diantara KPU dan instansi-instansi tersebut. Kebutuhan akan dukungan *expertise* dan teknologi terkendala dengan belum tersedianya payung hukum yang menjadi kerangka dasar kerjasama yang mengikat. Sebagai suatu lembaga independen, regulasi yang mengatur kerjasama dengan institusi pemerintah lainnya menjadi suatu polemik di tengah masyarakat. Munculnya beragama spekulasi mempertanyakan netralitas lembaga KPU dalam menjalankan fungsinya.

Pernyataan tersebut dipertegas kembali oleh Informan B-3 yang menyatakan bahwa salah satu faktor kendala yang dihadapi dalam bersinergi dengan KPU maupun instansi terkait dengan pelaksanaan Pemilu dalam menciptakan keamanan siber adalah aspek kepercayaan masyarakat. Bagaimana memperoleh kepercayaan masyarakat guna membuat regulasi yang dapat mengikat seluruh entitas yang melaksanakan fungsi siber. Di lain pihak dengan kemajuan industri teknologi 4.0, dimana teknologi canggih sebagian besar didominasi oleh sektor swasta, sementara saat ini belum terdapat suatu aturan yang bersifat represif yang memaksa mereka untuk dapat membantu KPU dalam meningkatkan kinerjanya. Mengutip pernyataan dari Informan B-4 yang menyatakan:

> *Terdapat kendala bagi BSSN untuk dapat ikut secara aktif terjun dalam mewujudkan keamanan siber pada Pemilu 2019. Permasalahnnya adalah payung hukum untuk dasar legalitas dengan tujuan keterikatan secara organisasi dan peran aktif agar semua pihak dapat terlibat dan bergerak. Sejauh ini belum terdapat legalitas baik MoU ataupun perjanjian kerjasama lainnya dengan KPU, berbeda dengan institusi lainnya seperti APJI, Tim Cyber POLRI dll*

## 4.2. Pembahasan

Pada penelitian kualitatif, penjelasan atau pembahasan lebih banyak dibutuhkan,[71] sehingga peneliti berupaya mengkonstruksi empati dari sebuah kesadaran subjektif dan signifikansi dari pembaca terhadap fakta empiris, faktual serta melalui interpretasi analisa. Tujuan dari pembahasan ini adalah untuk memperoleh pemahaman yang komprehensif mengenai hasil penelitian yang dilakukan. Pada pembahasan ini, peneliti akan mengorelasikan ringkasan hasil temuan yang diperoleh di lapangan dengan teori/konsep relevan yang telah terlebih dahulu dielaborasikan dalam kajian teoritik yang terdiri atas strategi keamanan siber yang diimplementasikan oleh KPU, sinergitas yang terjalin diantara KPU dan para pihak strategis serta faktor-faktor hambatan apa saja yang dihadapi dalam mewujudkan keamanan siber pada Pemilu 2019.

### 4.2.1. Strategi Keamanan Siber Komisi Pemilihan Umum (KPU) Pusat dalam Menghadapi Pemilu 2019.

Berdasarkan penelitian terdahulu yang dilakukan oleh Handrini Ardiyanti, diperoleh informasi terkait dengan pembangunan keamanan siber di Indonesia bahwa masih lemahnya pemahaman pemerintah akan keamanan di dunia siber dan masih belum adanya koordinasi yang baku dalam penanganan masalah keamanan siber. Sehingga peneliti mencoba mengkaji strategi keamanan siber yang diterapkan oleh KPU dan sejauh mana koordinasi yang dilakukan dalam menghadapi ancaman siber pada Pemilu 2019 mendatang.

Menurut teori strategi yang dipergunakan, maka terdapat tiga indikator strategi Komisi Pemilihan Umum (KPU) Pusat dalam menghadapi pemilu 2019 pada aspek keamanan siber yaitu *Ends*, *Means*, dan *Ways* sesuai *grand theory* yang digunakan dan rumusan pedoman pertahanan siber Pemerintah dalam membangun *Secure Cyber Environment*. Adapun

[71] Neuman Dalan dalam Djam'an Satori dan Aan Komariah. Hlm. 218-220

pada indikator *Ways*, peneliti mengkorelasikan dengan teori/konsep *Cybersecurity* dari *Ghernaouti* sebagai berikut:

**a. *Ends***

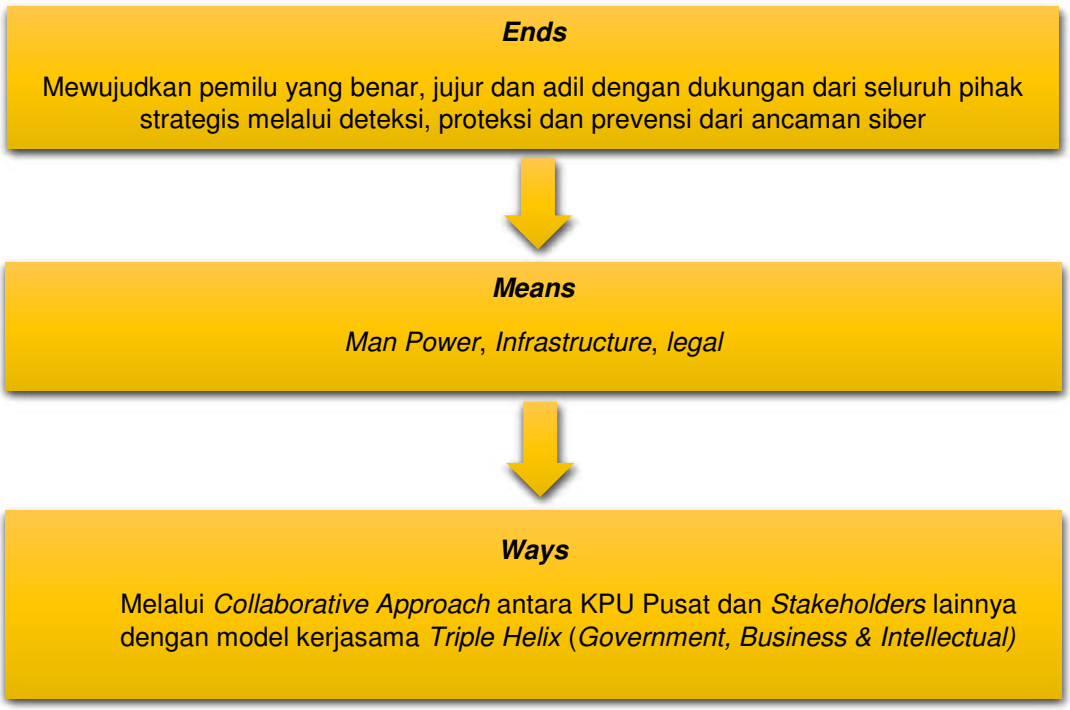
Berdasarkan hasil keterangan wawancara yang dilakukan dengan para pejabat terkait, baik dari KPU Pusat sendiri maupun dari para *stakeholders* yang terlibat seperti pihak pemerintah, swasta maupun akademisi maka yang menjadi tujuan utama adalah mewujudkan pemilu yang benar, jujur dan adil dengan dukungan dari seluruh aspek termasuk keamanan siber.

Pemilihan umum 2019 telah mengalami pergeseran dari pilkada dan pemilu 1.0 menuju pilkada dan pemilu 2.0. Pilkada dan Pemilu mengalami *upgrade* ditandai dengan semakin intensifnya peran sosial media sebagai medium opini publik. Kehadiran sosial media telah metransformasi medan politik dimana kejayaan diperoleh oleh tokoh dan partai yang memaksimalkan sosial media.[72] Sehingga membuat spektrum ancaman lebih luas dimulai dari sosiokultural (*psychological warfare*) hingga peretasan

Dari permasalahan tersebut, KPU berupaya melakukan prevensi dan mengeleminasi segala bentuk potensi ancaman dari tiap-tiap tahapan pemilu. Seluruh upaya tersebut tentunya sangat relevan karena tugas pokok dan kewenangan KPU sebagaimana termaktub pada Pasal 10 Undang-Undang Nomor 3 Tahun 1999 tentang Pemilihan Umum dan Pasal 2 Keputusan Presiden Nomor 16 Tahun 1999 tentang Pembentukan Komisi Pemilihan Umum dan Penetapan Organisasi dan Tata Kerja Sekretariat Umum Komisi Pemilihan Umum. Salah satunya menyebutkan bahwa tugas kewenangan KPU adalah merencanakan dan mempersiapkan Pemilihan Umum. Tentunya perencanaan dan persiapan Pemilihan umum dilaksanakan secara komprehensif yang meliputi aspek fisik dan juga aspek

[72] Anonim. Era Pilkada 2.0, ini langkah Kominfo dan KPU. Dalam https://www.indotelko.com/kanal?c=rm&it=era-pilkada-kpu diakses pada 20 November 2018

virtual. Sehingga tujuan yang ingin dicapai oleh KPU Pusat adalah untuk menyukseskan penyelenggaraan Pemilu 2019 dan Pemilu-pemilu yang akan mendatang.




**Gambar 4.3 Teori Strategi**

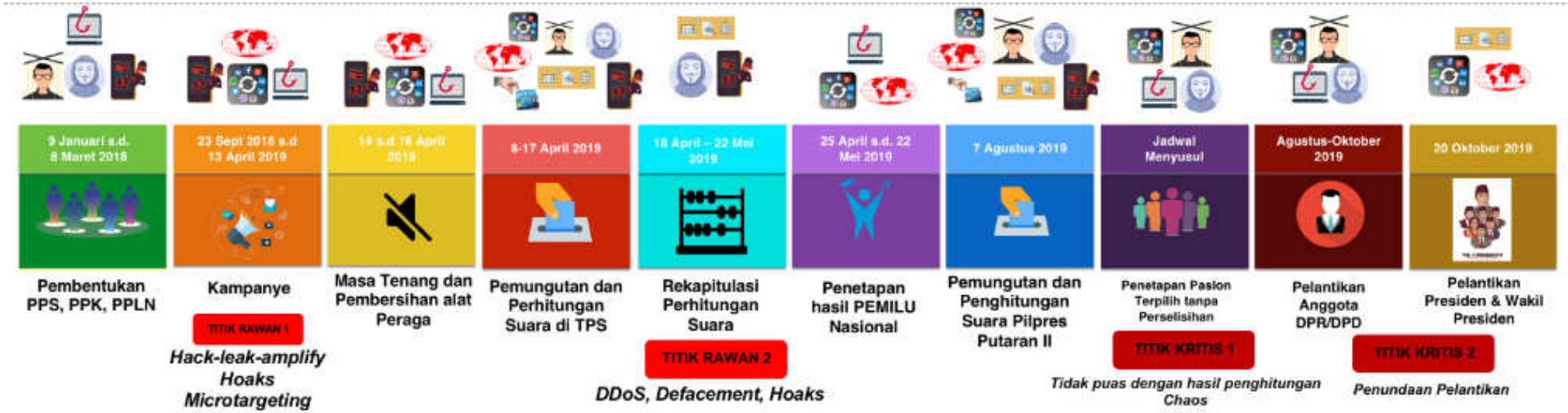
*Sumber: Diolah oleh Peneliti*

Berdasarkan gambar diatas, terlihat bahwa urgensi dibentuknya skala prioritas ancaman melalui analisa ancaman yang muncul dari setiap tahap Pemilu sangatlah diperlukan. Hal ini diimplementasi oleh KPU Pusat untuk menghadapi pemilihan umum 2019. Dengan menganalisa *behavior* dan *pattern* serangan dan besarnya potensi ancaman yang dapat muncul pada titik-titik rawan, diharapkan dapat menjadi panduan dalam peningkatan keamanan siber pada pelaksanaan Pemilu kedepannya.

Implementasi strategi ini sesuai dengan konsep keamanan yang digusung oleh Paul D. Williams yang mengasosiasikannya dengan pengurangan ancaman yang membahayakan nilai-nilai yang dimiliki, hingga jika sampai tidak direspon dengan baik akan mengancam keberlangsungan dari objek khusus yang dimaksud di masa yang akan

datang.[73] Dikarenakan peran KPU yang krusial dan dengan keterbatasan kemampuan dalam hal keamanan siber. Maka KPU merangkul BSSN untuk melakukan komunikasi dan koordinasi dalam bentuk diskusi dan *Forum Group Discussion (FGD)* dengan membuat *timeline* kerawanan dan peta ancaman siber pada Pemilu 2019 untuk dapat melakukan deteksi ancaman yang dapat terjadi, melakukan proteksi terhadap sistem keamanan baik dari sisi perangkat ataupun manusianya hingga melakukan prevensi terhadap potensi ancaman siber yang muncul. Adapun potensi ancaman yang mungkin hadir pada pemilihan umum 2019 yang diperlihatkan pada titik rawan I dan titik rawan II pada gambar berikut:

[73] Paul D. Williams, *Op cit*




**Gambar 4.4 Timeline Kerawanan dan Peta Ancaman Siber Pada Pemilu 2019**

*Sumber: Dokumen Badan Siber dan Sandi Negara*

**b. *Means***

Serangkaian upaya untuk memastikan pencapaian dan pemeliharaan sifat keamanan organisasi dan asset pengguna terhadap risiko keamaan yang relevan dalam lingkungan siber merupakan manifestasi dari keamanan siber yang meliputi alat, kebijakan, konsep keamanan, pedoman, pendekatan manajemen resiko, tindakan, pelatihan, praktik terbaik, jaminan dan teknologi yang dapat digunakan untuk menlindungi lingkungan siber dan organsisi serta asset pengguna. Organisasi dan asset pengguna dalam keamanan siber termasuk perangkat yang terhubung komputasi, personil, infrastruktur, aplikasi, layanan, sistem telekomunikasi dan totalitas informasi yang dikirimkan dan/atau disimpan dalam lingkungan maya.[74] Dalam mencapai tujuannya (*Ends),* KPU Pusat menggunakan seluruh sumber daya (*resources*) dalam mengamankan Pemilu yang akan digelar dengan membangun kekuatan solid melalui kesiapan infrastruktur teknologi baik perangkat keras (*hardware),* perangkat lunak (*software*) ataupun pekerja (*Brainware)* yang dikonsolidasikan dari *stakeholders* yang terlibat.

Adapun pengamanan dilakukan pada 4 (empat dimensi) yang diimplentasikan pada setiap organisasi termasuk KPU diantaranya aspek teknis terkait keamanan fisik, logis, lingkungan dan manajemen operasional, aspek manusia meliputi kesadaran, edukasi dan pengawasan, aspek legal terkait prosedur dan aturan atau legalitas, serta organisasional menyangkut misi, struktur, tanggung jawab dan manajemen stratejik.

Dalam hasil penelitian berbeda di KPU dengan judul "Pengembangan Tata Kelola Teknologi Informasi di Komisi Pemilihan Umum Pusat" diperoleh informasi bahwa dalam segi infrastruktur dan penerapan keamanan informasi, KPU telah memenuhi indeks kesiapan manajemen keamanan informasi. Hal tersebut mengindikasikan bahwa KPU sebenarnya telah memenuhi standar keamanan informasi, walaupun

[74] Handrini Ardiyanti, *Cyber-Security Dan Tantangan Pengembangannya di Indonesia*, Politica Vol.5 *No*. 1 Juni 2014

tidak memiliki lisensi standar keamanan internasional seperti ISO 27001. Dan indeks keamanan tersebut tidak dapat digunakan sebagai proteksi terhadap ancaman sosio-kultural melalui penggunaan media sosial seperti saat sekarang ini.

Pada masa lalu, para Politisi menggunakan cara konvensional untuk dapat menarik perhatian publik, baik itu melalui selembaran pamflet, mengadakan pertemuan ataupun berkunjung langsung untuk bertegur sapa dengan masyarakat. Tetapi seiring dengan perkembangan dalam teknologi online, telah memberikan benefit kepada politisi dan supporter sebuah cara baru untuk menyampaikan pesan mereka dengan jauh lebih mudah dan dengan jangkauan yang luas. Penggunaan media informasi seperti radio dan televisi memberikan dampak yang lebih besar, namun dengan kehadiran sosial media maka peran dalam penyampaian informasi hadir lebih signifikan dan lebih komprehensif terhadap lintas generasi.

Media sosial (*Social Media*) saat ini menjadi senjata utama dalam memperebutkan perhatian publik dan memenangkan pikiran dan hati masyarakat yang dilakukan melalui perang informasi diantara partai politik dan para politisinya seperti yang terjadi di Pemilihan umum 2016 Amerika Serikat. Kemenangan Donald Trumph dalam Pemilu 2016 dianggap tidak lepas dari interferensi Rusia dalam keberhasilannya melakukan *social engineering* untuk memanipulasi pikiran dan tingkah laku pilihan jutaan orang Amerika guna mendukung Donald Trumph dan merusak pencalonan Hillary Clinton.

Tanpa disadari ancaman eksistensial berupa sosio kultural dilakukan tidak dalam waktu yang singkat, tetapi dalam rentan waktu yang cukup lama melalui sosial media dan iklan. Terdapat suatu pola sistematis dimana perusahaan-perusahaan Rusia membeli iklan *Facebook* untuk menebarkan perpecahan di sepanjang garis rasial dan politik di Amerika Serikat. Rusia melakukan hal tersebut untuk mengobarkan kebencian

rasial, *xenophobia* dan agama.[75] Walupun memiliki sosial budaya yang sangat berbeda dengan Amerika Serikat, Indonesia juga merupakan suatu negara majemuk dengan jumlah penduduk yang besar, agama, kepercayaan dan suku yang beraneka ragam. Sehingga, besar kemungkinan teknik tersebut juga dapat berhasil untuk diimplementasikan dinegara-negara demokrasi besar seperti Indonesia.

Tugas negara demokrasi yang pertama adalah melindungi dan mempertahankan pemilihannya dari subversi. Pengalaman tersebut yang menjadi perhatian dari KPU dan Bawaslu serta Kemkominfo untuk dapat mengantisipasi ancaman sosio kultural yang dianggap sedang terjadi saat ini di Indonesia menjelang Pemilihan umum. Selama ini Kemkominfo bertindak berdasarkan permintaan dari KPU dan Bawaslu dalam memonitor dan menganalisa konten-konten yang dianggap melanggar peraturan kampanye baik itu *negative campaign, black campaign* ataupun tergolong *hoax/hatespeech.* Dalam membantu KPU, Kemkominfo menggunakan teknologi *CyberDrone* untuk memantau isu-isu tertentu yang telah dihimbau oleh KPU dan Bawaslu. Selain itu, Kemkominfo juga dibantu oleh masyarakat melalui laporan langsung ke *website* milik Kominfo. Walaupun terdapat kendala dalam hal merespon, dikarenakan pelaporan hanya dilakukan dengan menggunakan *screen-capture* dari status/akun pelanggar yang terkadang telah dihapus ataupun memiliki alamat web (*url)* yang tidak lengkap. Dengan adanya aturan kampanye yang telah ditentukan oleh KPU dan Bawaslu serta dengan didukung oleh Undang-Undang Informasi dan Transaksi Elektronik, KPU berharap dapat mewujudkan Pemilihan Umum yang yang benar, jujur dan adil sesuai dengan etika dan peraturan yang ada dengan tetap mengakomodir pemanfaatan ruang publik di media internet terutama media sosial.

[75] Anup Ghosh, *How elections are hacked via social media profiling.* Dalam https://www.csoonline.com/article/3277953/social-engineering/how-elections-are-hacked-via-social-media-profiling.html diakses pada 28 September 2018.

Sedangkan untuk pengamanan dalam menghadapi ancaman dan serangan siber seperti *Advanced Persistent Threats (APT), Denial of Service (DoS), Distributed Denial of Service (DDoS), Defacement, Phising, Malware, Trojan Horse* hingga *social engineering* dilakukan bersama dengan Badan Siber dan Sandi Negara (BSSN) didukung oleh Asosiasi Penyelenggara Jasa Internet Indonesia (APJII), Komunitas-komunitas lain (FORMASI). Peran komunitas sejauh dianggap tidak terlalu signifikan dalam mewujudkan keamanan siber di KPU pada pemilihan umum 2019.

**c. *Ways***

Peraturan Menteri Pertahanan tentang Pedoman Pertahanan Siber menyebutkan salah satu agenda kebijakan keamanan siber adalah *organizational structure* (struktur organisasi) yang mengkaji terkait keberadaan kemitraan, kerangka kerjasama dan jaringan berbagi informasi dalam mewujudkan keamanan siber.[76] Sesuai dengan teori pertahanan siber Kementerian Pertahanan dan keamanan siber yang digunakan oleh peneliti dari Ghernaouti.

Indonesia memasuki era keamanan siber 2.0 dimana keamanan siber dibentuk dengan mengadopsi model kolaborasi diantara lembaga pemerintah, industri teknologi informasi dan perguruan tinggi yang cenderung menentukan arah perkembangan teknologi siber kedepan. Secara *de facto*, negara tidak dapat menguasai seluruh aspek teknologi digital, sebaliknya perkembangan teknologi digital lebih didominasi perkembangannya oleh kalangan industri dengan dukungan investasi riset yang terus berkembang.[77]

Berdasarkan kenyataan tersebut maka KPU mengadopsi strategi *collaborative approach* dengan konsep *Triple Helix* meliputi komunikasi dan koordinasi dengan *stakeholders* dari pemerintah K/L, swasta dan akademisi. Kerjasama tersebut dilakukan guna membangun sistem

[76] Peraturan Menteri Pertahanan. *Op cit*
[77] Andi Widjajanto. Keamanan siber 2.0. Dalam https://kompas.id/baca/opini/2018/01/10/keamanan-siber-2-0/ diakses pada 20 November 2018

penangkalan, penindakan dan pemulihan terhadap serangan siber yang dilakukan bersama *Stakeholders* dengan bidang masing-masing. Dengan perancangan dan pengembangan aplikasi KPU bersama Akademisi, pembuatan dan penetapan aturan kampanye bersama Bawaslu, kegiatan pengamanan infrastruktur IT Pemilu yang dilakukan bersama Kemkominfo dan BSSN, kolaborasi pembuatan kebijakan terkait keamanan siber dengan K/L lain serta *collaboration action in Cyber threat intelligence* yang dilakukan oleh KPU dan K/L yang bersangkutan.

Salah satu kajian dalam peperangan asimetris adalah perang informasi yang marak terjadi di media sosial pada saat pelaksanaan kampanye pemilihan umum. Merujuk ke penelitian sebelumnya dengan judul "Peran Media dalam Perang Informasi pada Kampanye Pemilihan Presiden 2014" dikatakan bahwa peran media sosial saat kampanye sebagai media penyebar informasi yang efektif, mudah, murah dan mampu menjangkau pengguna yang luas. Selain itu, dikatakan juga bahwa subjek yang mendapatkan paparan informasi dari media secara intensif maka cenderung membentuk persepsi, pemahaman dan keyakinan dari informasi yang diterimanya tersebut.

Hasil penelitian tersebut sejalan dengan data yang diperoleh oleh Peneliti saat ini yaitu penggunaan media sosial sebagai media yang bertujuan untuk memenangkan hati dan pikiran masyarakat, yang dikenal dengan istilah "*winning hearts and minds".* Indonesia sebagai negara dengan jumlah pengguna sosial media terbesar di dunia dan dengan kecepatan dan dampak luas dari penggunaannya maka menjadi alasan utama penggunaan media sosial sebagai suatu trend dalam mendukung strategi berkampanye. Penggunaan sosial media untuk kampanye ternyata tidak selalu bersifat positif, hal ini dikarenakan adanya perang informasi diantara calon terpilih yang bukan hanya membangun pencitraan tetapi juga melalui cara-cara negatif yang melanggar peraturan kampanye yang dibuat dan diatur oleh KPU dan Bawaslu seperti *negative campaign* ataupun *black campaign.*

Kampanye-kampanye jenis tersebut dan pelanggaran etika kampanye lainnya yang kemudian ditindaklanjuti oleh KPU dan Bawaslu bekerjasama sama dengan Kemkominfo, *social media platform* dan APJII. Kolaborasi tersebut tidak hanya sebatas mengatur para politikus yang beradu dalam Pemilu, tetapi juga mencakup *media literasi* dengan cara memberikan edukasi dan sosialisasi terkait Pemilu dan pelaksanaannya bagi masyarakat Indonesia.

Dalam keterkaitan dengan penindaklanjutan atas serangan siber yang dilakukan, maka kerjasama dengan Menkopolhukam dan *cybercrime* POLRI dibutuhkan, dengan landasan hukum Undang-Undang Informasi dan Transaksi Elektronik (ITE). Mengutip perkataan Sekretariat Jenderal Bawaslu yang menyatakan bahwa peran serta POLRI dalam pengamanan konten-konten negatif dianggap berhasil dikarenakan adanya *detterent-effect* bagi para pelanggar. Adanya sanksi dan tindak lanjut yang cepat dari POLRI sebagai *Law Inforcement* membuat masyarakat untuk dapat lebih bersikap bijak dalam menggunakan media sosial untuk penyebaran informasi. Walaupun tidak dapat menghilangkan isu tersebut sepenuhnya, kerjasama dengan POLRI merupakan salah satu wujud dalam mendukung keberhasilan Pemilu dengan menekan peredaran konten negatif, *hoax* ataupun *hatespeech*. Solusi keamanan dapat melindungi lingkungan tertentu dalam konteks tertentu, tetapi tidak dapat mencegah perilaku kriminal sama sekali. Hukum dan lembaga hukum harus ada untuk menghalangi perilaku kriminal dan untuk mengadili orang-orang yang melakukan tindakan ilegal.[78]

Menurut Ghernaouti, Keamanan siber tidak dapat diabstraksikan jauh dari lingkungan aplikasi dan sosio-kultural. Keamanan siber harus didekati dalam konteks interdisipliner dan multi-*stakeholders*, menempatkan individu pada pusat pertanyaan keamanan TIK untuk

[78] Ghernaouti. *Op cit.* hlm. 332

mendorong pengembangan kesadaran dan inklusifitas informasi publik. Mengutip dari Ghernouti yang menyatakan:

> *In order to make their collaboration as effective and efficient as possible, the security manager should be able to supply the elements that will help the investigator in his work*.[79]

IT KPU dalam hal ini selaku pemegang kepentingan bertindak sebagai *security manager* yang harus dapat memberikan elemen-elemen yang akan membantu investigator dalam melaksanakan tugasnya. Elemen-elemen yang dimaksud merupakan hal-hal yang didefinisikan ketika dilakukan desain dan implementasi dari sistem informasi.

Berdasarkan penelitian Erwin Kurnia dalam "Kebijakan Strategi Keamanan *Cyber* Nasional dalam Menghadapi Perang *Cyber (Cyberwarfare*)" dikatakan bahwa kebijakan strategi di bidang *Cyber* dan pembentukan lembaga *Cyber* nasional diharapkan menjadi solusi dalam mengatasi berbagai ancaman keamanan *Cyber* nasional dalam mendukung pertahanan negara.

Penelitian tersebut diatas sesuai dengan Peraturan Kementerian Pertahanan RI tentang Pertahanan Siber dikatakan bahwa dalam rangka memastikan pertahanan siber dapat dijalankan dengan baik, maka diperlukan kelembagaan yang kuat, professional dan andal untuk memastikan tujuan dari pertahanan siber yang dapat tercapai. Pertahanan siber ini salah satunya dilakukan dengan mendorong partisipasi aktif melalui kerjasama kemitraan nasional dan internasional.[80]

Berdasarkan penelitian yang telah dilakukan, maka peneliti menganggap bahwa KPU telah melaksanakan fungsi pertahanan siber sesuai dengan Peraturan Menteri Pertahanan melalui:

1. Menjamin tercapainya sinergi kebijakan pertahanan siber
2. Membangun organisasi dan tata kelola sistem penangan keamanan siber.

---

[79] Ghernaouti, *Op cit.* hlm. 321
[80] Peraturan Menteri Pertahanan. *Op cit.* hlm 20

3. Membangun sistem yang menjamin ketersediaan informasi dalam konteks pertahanan siber.
4. Membangun sistem penangkalan, penindakan dan pemulihan terhadap serangan siber.
5. Mewujudkan kesadaran keamanan siber
6. Menyelenggarakan kerjasama nasional dalam mendukung pelaksanaan strategi.

Sehingga strategi yang diimplementasikan oleh KPU yang meliputi deteksi ancaman, proteksi serta prevensi oleh Peneliti disederhanakan kedalam bentuk tabel sebagai berikut:

**Tabel 4.2 Tabel Implementasi Strategi Kerjasama**

| No. | Strategi | Kesimpulan |
|---|---|---|
| 1. | *Ends* | Mewujudkan pemilu yang benar, jujur dan adil dengan dukungan dari seluruh pihak strategis melalui pembangunan kemampuan keamanan siber yaitu deteksi, proteksi dan prevensi dari ancaman siber. |
| 2. | *Means* | Seluruh sumber daya termasuk infrastruktur (*hardware* dan *software*) serta human resources (*brainware*) yang meliputi 4 (empat) dimensi yaitu teknis, manusia, legal dan organisasional. |
| 3. | *Ways* | Kerjasama *Collaborative approach* dengan konsep *Triple Helix* meliputi komunikasi dan koordinasi dengan *stakeholders* dari pemerintah K/L, swasta dan akademisi. |

Sumber: diolah oleh Peneliti

### 4.2.2. Sinergitas antara Komisi Pemilihan Umum (KPU) Pusat dengan *Stakeholders* (*Triple Helix*)

Pada subbab ini, Peneliti akan membahas terkait sinergitas yang terlaksana antara pihak KPU dan *Stakeholders* lainnya. Sinergitas tersebut diukur berdasark indikator komunikasi dan koordinasi yang terbangun.

Sebagaimana manajemen dan teknologi tidak memungkinkan untuk menghindari insiden sepenuhnya dan tidak terdapatnya konsep "*zero risk*", maka masalah tanggung jawab menjadi sentral yang berhubungan dengan keamanan informasi. Sehingga untuk mewujudkan keamanan siber perlu ditekankan tentang perlunya koordinasi antar lembaga. Keamanan siber

tidak dapat diwujudkan seorang diri, tetapi dibutuhkan kerjasama dengan instansi-instansi lainnya.

Surowiecki mengungkapkan bawah sinergitas merupakan suatu kolaborasi yang terbentuk antara beragam kelompok yang memiliki perspektif berbeda melalui kerjasama dengan tujuan meningkatkan efektifitas melalui kolaborasi pengetahuan, persepsi dan perspektif bersama.[81] Dengan demikian untuk mengetahui tingkat sinergitas yang dilakukan oleh KPU Pusat dengan *stakeholders* dalam mencapai *Ends,* maka peneliti mengorelasikannya dengan teori O. Gupta & G. Ross yang menyatakan bahwa terbangunnya sinergitas melalui dua cara yaitu komunikasi dan koordinasi.

**a. Komunikasi**

Komunikasi dapat diartikan sebagai sebuah proses pertukaran informasi diantara individu-individu melalui suatu sistem simbolik, tanda-tanda ataupun sikap yang sama.[82] Sebagai pihak yang bertanggung jawab langsung terhadap pelaksanaan Pemilu, maka KPU dalam upaya membangun keamanan siber berusaha untuk membangun komunikasi yang aktif dengan para *stakeholder* lainnya. Model komunikasi dilakukan melalui *sharing information* dimulai dari bentuk konsultasi, diskusi hingga *Forum Groups Discussion (FGD)* yang melibatkan seluruh pemangku kepentingan yang kemudian dtindaklanjuti sebagai bentuk koordinasi dengan para *Stakeholders.*

**b. Koordinasi**

Komunikasi tidak dapat berdiri sendiri tanpa adanya koordinasi yang ditandai dengan 9 (sembilan) syarat dalam mewujudkan koordinasi yang efektif.[83] Kesembilan syarat tersebut sepenuhnya telah dipenuhi oleh KPU dalam rangka mewujudkan koordinasi yang efektif diantaranya melakukan hubungan pribadi langsung dengan para stakeholders yang

[81] Surowiecki, James. *Op cit*
[82] Merriam-Webster. *Op cit*
[83] Moekijat. *Op cit*

terlibat, melakukan perencanaan dan pembuatan kebijakan pada awal kerjasama, mempertahankan koordinasi secara berkesinambungan pada seluruh aspek perencanaan dan dilakukan secara dinamis dengan tujuan yang telah ditetapkan, implementasi struktur organisasi yang sederhana, pembagian peran dan tanggung jawab yang jelas antar stakeholders yang didukung dengan komunikasi yang aktif dan efektif serta kepemimpinan yang supervisi.

Bentuk koordinasi yang terjalin antara KPU dan institusi-institusi lainnya yaitu dimulai dari pengembangan dan pengetesan aplikasi Pemilu dengan pihak Akademisi dan BPPT, identifikasi, pelaporan dan tindak lanjut atas pelaporan tersebut yang dilakukan oleh KPU, Bawaslu, Kominfo, Menkopolhukam dan *Cybercrime* POLRI. Selain itu, pengamanan dari sisi infrastruktur dilakukan bersama sama dengan BSSN, ID-SIRTII, BIN dan APJII.

Mengkaji dari 2 (dua) cara terbangunnya suatu sinergitas yang baik melalui komunikasi dan koordinasi, maka berdasarkan hasil temuan dan teori yang digunakan maka dapat dikatakan bahwa Komisi Pemilihan Umum (KPU) Pusat telah membangun sinergitas dengan para *stakeholders* dengan baik, hanya saja sinergitas tersebut belum terkonvergensi sepenuhnya dan belum mengikat dikarenakan belum adanya payung hukum yang melindungi serta mengatur peran dan tanggung jawab dari para *stakeholders*. Sinergitas antara KPU dan para pihak strategis tersebut ditunjukkan dari table berikut:

**Tabel 4.3 Sinergitas KPU dan *Stakeholders***

| No. | Institusi | Sinergitas | Kesimpulan |
|---|---|---|---|
| 1. | Badan Pengawas Pemilu (Bawaslu) | Komunikasi dan koordinasi terlaksana dengan baik. | Berdasarkan hasil data penelitian serta pengkajian melalui konsep sinergitas maka dapat disimpulkan bahwa sinergitas yang terjalin diantara KPU dan stakeholders lainnya dapat dikatakan berjalan dengan baik, hal ini ditandai dengan adanya sikap saling |
| 2. | Kementerian Komunikasi dan Informatika (Kemkominfo) | Komunikasi dan koordinasi berjalan dengan baik. | |
| 3. | Badan Sandi dan Siber Negara (BSSN) | Komunikasi melalui diskusi dan FGD yang berjalan baik. | |

| | | | |
|---|---|---|---|
| 4. | Badan Pengkajian dan Penerapan Teknologi (BPPT) | Ketersediaan dan respon yang cepat serta koordinasi yang baik. | percaya, komunikasi dan koordinasi dalam pelaksanaan tugas dan tanggung jawab dari masing-masing stakeholders dalam perannya untuk mewujudkan keamanan siber sepanjang pemilu baik itu melalui deteksi ancaman, proteksi infrastruktur serta prevensi atas pontensi ancaman siber yang mungkin dapat terjadi. hanya saja sinergitas tersebut belum terkonvergensi sepenuhnya dan belum mengikat dikarenakan belum adanya payung hukum yang melindungi serta mengatur peran dan tanggung jawab dari para *stakeholders* |
| 5. | Asosiasi Penyelenggara Jasa Internet Indonesia (APJII) | Komunikasi dan koordinasi terlaksana dengan baik. | |
| 6. | *Cybercrime* POLRI | Respon yang cepat dalam hal *law enforcement*. | |
| 7 | Badan Intelijen Negara (BIN) | Komunikasi dan koordinasi terlaksana dengan baik. | |
| 8. | Kementerian Koordinator Bidang Politik Hukum dan Keamanan (Menkopolhukam) | Komunikasi dan koordinasi terlaksana dengan baik. | |
| 9 | *Social Media Platform (Facebook, Google, Twitter, YouTube, BBM, Bigoo, LiveMe, MeTube* dan *Telegram*) | Komunikasi yang lancar, tanpa adanya kendala dan respon yang cepat. | |
| 10. | Universitas Indonesia (UI) | Terdapat kendala terkait respon yang lambat dan ketersediaan dari tenaga pekerja yang tidak tersedia 24/7. | |
| 11. | Institut Teknologi Bandung (ITB) | Komunikasi dan koordinasi dalam pengembangan aplikasi dapat dikatakan baik. | |

Sumber: Diolah oleh Peneliti

### 4.2.3. Faktor-faktor Penghambat yang dihadapi oleh Komisi Pemilihan Umum (KPU) Pusat dalam implementasi keamanan siber

Pada sub-bab ini peneliti mengelaborasikan hasil penelitian terhadap rumusan masalah salah satunya mengenai faktor-faktor penghambat yang dihadapi oleh Komisi Pemilihan Umum (KPU) Pusat dalam mewujudkan keamanan siber pada pelaksanaan Pemilu 2019 yang dikaitkan dengan teori hambatan. Adapun hambatan-hambatan tersebut terdiri atas *budgeting, Human Power* dan *legal* yang akan dijelaskan sebagai berikut:

***a. Budgeting***

Faktor penghambat yang pertama dalam mewujudkan keamanan siber selama ini adalah adalah masalah anggaran yang dimiliki oleh KPU terutama pada Biro Perencanaan dan Data. Terjadinya ketidaksesuaian antara anggaran yang telah ditetapkan pada awal program dengan kebutuhan di lapangan pada saat pelaksanaan menjadi kendala dalam menghadapi ancaman keamanan siber terutama pada aspek infrastruktur dan sumber daya manusia.

Seiring dengan perkembangan teknologi yang eksponensial, maka jenis dan serangan siber juga mengalami peningkatan dan semakin *sophisticated*. Peretas menjadi lebih terampil dalam menemukan lubang dan kerentanan pada sistem keamanan yang menjadi ancaman keamanan siber. Sehingga dibutuhkan kesiapan dari segi infrastruktur teknologi dan juga peningkatan kemampuan dari sumber daya manusia. Dalam peningkatan kemampuan teknologi maka dibutuhkan anggaran yang tidak sedikit, apalagi dengan trend teknologi kini yang telah mengalami transformasi terus menerus, maka dibutuhkan perhatian pada anggaran infrastruktur.

***b. Man Power***

Faktor penghambat yang kedua dalam mewujudkan keamanan siber pada pemilu selama ini adalah *Man Power* (sumber daya manusia) yang dimiliki. KPU selama ini memiliki jumlah personil yang terbatas yang berjumlah 5 orang dengan rincian 3 orang organik KPU dan 2 orang Non-organik. Berdasarkan fungsi operasional manajemen sumber daya manusia yaitu pada pengadaan sumber daya manusia merupakan penentuan sumber daya yang dibutuhkan disesuaikan dengan tugas, perekrutan dan penempatan sumber daya.

Kemajuan teknologi yang pesat tidak diimbangi dengan sumber daya manusia yang professional yang memiliki *skill* dibidang IT, sehingga membentuk permasalahan *Cybersecurity Skill Crisis.* Hal ini tentunya membuat para professional IT terutama di bidang *cybersecurity* memiliki

*demand* yang tinggi dengan upah yang tidak sedikit. Dengan *budget* terbatas yang dimiliki oleh KPU maka sulit untuk memperoleh pekerja professional di bidang IT terutama keamanan siber.

Disamping hal tersebut, diperlukan juga adanya edukasi dan sosialisasi dalam bentuk training atau pelatihan terhadap para pekerja dengan tujuan meningkatkan kesadaran akan keamanan informasi dan keamanan siber. Mengingat manusia adalah mata rantai yang lemah dalam rantai keamanan dank arena manusia adalah konsumen terakhir dari layanan dan infrastruktur TIK, solusi keamanan apapun juga harus mempertimbangkan kebutuhan sosial.[84]

Selanjutnya, kurangnya dokumentasi yang merupakan artefak yang seharusnya dipelihara sebagai dasar dan standar untuk pengembangan sistem keamanan dikarenakan pekerja yang terus berganti. Permasalahan ini kemudian memunculkan *lack of transfer knowledge* dari generasi sebelumnya ke generasi berikutnya untuk dapat mengetahui alasan dari setiap *design decision* yang dilakukan.

***c. Legal***

Faktor penghambat berikutnya dalam mengaktualkan keamanan siber pada Pemilu 2019 mendatang adalah permasalahan regulasi (*legal*). Selama ini KPU hanya terikat kerjasama dengan Bawaslu dan Kementerian Komunikasi dan Informatika yang juga melibatkan *social media platform* dan juga penyedia jasa internet (APJII) yang terikat dalam *Memorandum of Action* (MoA) yang dilakukan pada Pilkada 2018. Sedangkan menjelang kampanye Pemilihan umum Presiden, rancangan kerjasama tersebut masih dalam tahap perencanaan dan pengkajian untuk dapat disetujui oleh Rudiyantara selaku Menteri Komunikasi dan Informatika.

Sejalan dengan permasalahan tersebut, Badan Siber dan Sandi Negara (BSSN) sebagai lembaga yang bertanggung jawab dalam keamanan siber di Indonesia belum terikat dalam suatu kerjasama yang

[84] Ghernaouti. *Op cit.* hlm. 331

formal sebagai payung hukum yang mendasari kontribusinya dalam pengamanan siber pada Pemilu 2019. Tanpa adanya dasar legalitas maka BSSN tidak memiliki *legal standing,* sehingga tidak memiliki kewenangan dan tanggung jawab yang dapat dilaksanakan yang berada pada koridor hukum yang telah ditentukan. Legalitas tersebut berperan sebagai landasan kerja bagi BSSN untuk dapat berperan aktif dan memberikan kontribusi bagi KPU dalam menciptakan keamanan siber pada tiap-tiap tahapan Pemilu.

Dengan adanya payung hukum tersebut, BSSN dapat diikutsertakan dalam pengamanan siber. Baik itu dalam tahap desain, pengujian aplikasi hingga pengamanan infrastruktur pada saat pelaksanaan Pemilu. Pernyataan tersebut dipertegas oleh Informan C-3 yang mengatakan seharusnya terdapat suatu regulasi yang mengatur sejauh mana keterlibatan para *stakeholders*. Selain itu seharusnya juga terdapat regulasi di KPU sendiri yang mengatur kontrak para pekerja di bidang IT, sehingga tidak terjadi pergantian staf yang akan menyulitkan dokumentasi guna pengembangan sistem keamanan siber KPU.

Sehingga faktor-faktor penghambat yang dihadapi oleh KPU dalam mewujudkan keamanan siber pada Pemilu 2019 dapat disederhanakan ke dalam table sebagai berikut:

**Tabel 4.4 Faktor-faktor Penghambat dalam mewujudkan kemanan siber pada pelaksanaan Pemilu**

| No. | Hambatan | Kesimpulan |
|---|---|---|
| 1. | *Budgeting* | Anggaran dana yang terbatas dalam pengembangan teknologi serta perekturan personel tambahan untuk IT KPU |
| 2. | *Human Power* | Sumber daya manusia yang terbatas dan rendahnya tingkat kesadaran akan keamanan siber oleh pihak KPU yang terlibat. |
| 3. | *Legal* | Belum adanya keterikatan dalam bentuk kerjasama yang legal antara KPU dan pihak strategis lainnya. |

Sumber: diolah oleh Peneliti

# BAB 5
# KESIMPULAN DAN REKOMENDASI

## 5.1 KESIMPULAN

Sebagai kesimpulan dari penelitian yang telah dilaksanakan, maka diperoleh hasil sebagai berikut:

1. Strategi keamanan siber yang diimplementasikan oleh Komisi Pemilihan Umum (KPU) Pusat pada pelaksanaan Pemilihan Umum 2019 adalah *Collaborative Approach* dengan konsep kerjasama *Triple Helix* yang melibatkan Pemerintah, Swasta dan Akademisi. Strategi tersebut meliputi deteksi, proteksi dan prevensi dari ancaman pada titik-titik kritis dan rawan pada saat sebelum, pelaksanaan dan pasca pemilu yang diharapkan dapat mendukung keberhasilan pelaksanaan Pemilu 2019 mendatang.
2. Sinergitas yang terbangun antara KPU dan *stakeholders* lainnya dapat dikatakan cukup baik dibandingkan dengan tahun-tahun sebelumnya. hal ini ditunjukkan dengan pemenuhan dari syarat sinergitas yaitu komunikasi dan koordinasi. Selain itu, terefleksi melalui deeskalasi peredaran konten-konten negatif di sosial media baik isu *hoax, hate-speech* ataupun *disinformation campaign.* Respon cepat dari *Social Media Platform* dalam menanggapi permintaan KPU dan Bawaslu serta peran aktif POLRI sebagai *law enforcement* terhadap tindaklanjut laporan dari KPU dan Bawaslu. Selain itu, sinergitas yang terjalin tidak hanya sebatas diskusi ataupun FGD, tetapi juga telah mengalami peningkatan ke level teknis melalui *transfer of knowledge* dalam bentuk pelatihan, ataupun pelaporan yang dilakukan oleh pihak strategis lainnya. Sinergitas ini terkendala dalam legalitas dimana tidak terdapatnya dasar hukum sebagai dasar kerjasama.

3. Terdapat beberapa hambatan dalam implementasi keamanan siber pada Pemilu 2019 diantaranya:

   ***a. Budgeting/Money***

   Permasalahan anggaran merupakan faktor pertama yang menghambat IT KPU dalam mengembangkan keamanan siber dari segi infrastruktur dan sumber daya manusia. Dengan anggaran yang terbatas maka sulit bagi KPU untuk dapat mengimbangi cepatnya perkembangan teknologi yang diikuti oleh transformasi ancaman yang semakin luas dan beragam.

   ***b. Human Power***

   Aspek sumber daya manusia menjadi faktor penghambat kedua bagi IT KPU dalam mewujudkan keamanan siber. Dengan jumlah personil terbatas dianggap masih kurang optimal untuk mendukung kinerja pihak IT. Permasalahan ini diperburuk dengan rendahnya tingkat *awareness* dari personel KPU yang terlibat langsung dalam Pemilu dikarenakan kurangnya edukasi dan sosialisasi mengenai keamanan informasi dan keamanan siber.

   ***c. Legal***

   Belum terdapatnya payung hukum sebagai dasar legalitas untuk dapat bekerjasama dengan para *stakeholders* lainnya, terutama dari instansi Pemerintah seperti Badan Siber dan Sandi Negara yang memiliki tanggung jawab dalam keamanan siber di Indonesia. Hambatan ini memberikan keterbatasan bagi BSSN dan *stakeholders* lainnya untuk dapat ikut terjun secara langsung dalam pengamanan siber pada pelaksanaan Pemilu 2019.

## 5.2 REKOMENDASI

Berdasarkan hasil temuan penelitian yang telah dielaborasikan melalui kesimpulan tersebut, maka dalam hal ini dibuat beberapa masukan sebagai berikut:

1. Dengan kemajuan teknologi yang pesat, seharusnya infrastruktur IT KPU juga harus dapat mengimbangi perkembangan melalui penetapan anggaran yang disesuaikan dengan kebutuhan. Penetapan anggaran harus berdasarkan pengalaman pelaksanaan pemilu pada tahun-tahun sebelumnya untuk mengetahui pola anggaran, sehingga dengan adanya pola tersebut maka akurasi anggaran dapat ditentukan. Selain itu, KPU seharusnya membangun sistem yang integrasi dari seluruh sistem informasi yang dimiliki oleh KPU agar lebih efektif dan efisien untuk mendukung kinerja serta mengimplementasikan standar keamanan siber ISO 27001 sebagai proteksi dan prevensi terhadap saranan dan prasarana yang dimiliki serta dilakukan dokumentasi sebagai dasar/standar untuk pengembangan sistem keamanan untuk mengatasi *lack of transfer knowledge* serta mengetahui sejauh mana tingkat keamanan yang dimiliki oleh KPU.
2. Diperlukan perhatian lebih terhadap perekrutan jumlah personil untuk mendukung kinerja IT KPU dan diharapkan dengan kekurangan personel tersebut, dapat bersinergi dengan personel dari *stakeholders* lainnya dan diberi payung hukum untuk melaksanakan tugasnya. Dengan adanya payung hukum sebagai *legal standing* bagi para *Stakeholders,* maka mereka dapat proaktif dalam membantu, mengetahui kewenangan dan tanggung jawab serta jauh mana mereka dapat terlibat pada pelaksanaan Pemilihan Umum 2019. Diharapkan adanya suatu bentuk kerjasama yang dapat diupayakan baik itu *Memorandum of Action* seperti yang

dilakukan bersama Bawaslu dan Kemkominfo ataupun bentuk kerjasama lainnya.

3. Diperlukan adanya sosialisasi ke publik terkait keterlibatan BSSN dalam pengamanan siber pada Pemilu 2019. Sehingga, kehadiran opini negatif masyarakat terkait pelaksanaan Pemilu yang LUBER dan JURDIL dapat ditekan. Sedangkan bagi KPU sendiri, diperlukan adanya penyelenggaraan edukasi serta sosialisasi intensif mengenai keamanan informasi dan siber pada semua tingkatan level. Dengan membingkai dan edukasi para pekerja KPU mengenai keamanan siber tentunya berdampak dasar terhadap keamanan siber pelaksanaan Pemilu. Tindakan ini merupakan bagian dari pengamanan pada aspek manusia. Disamping hal tersebut, masih diperlukan adanya *leadership* yang kuat dari KPU untuk dapat menarik *interest* pihak-pihak lain untuk dapat berkontribusi membantu KPU dalam mewujudkan Pemilu 2019 yang bebas dari ancaman ataupun serangan siber.

# DAFTAR PUSTAKA

## BUKU


Agustini. (2013). *Pengelolaan dan Unsur-unsur Manajemen.* Jakarta: Citra Pustaka.

Albrow, Martin and Elizabeth King (eds). (1990). *Globalization, Knowledge, and Society.* London:Sage Publication

Baker N. & Stephens A. (2006) *, Making Sense of War: Strategy for the 21st Century* Cambridge: Cambridge University Press

Clausewitz, C. Von. (1976). *On War*. Princeton University Press, eds Howard, M. and Paret, P.

Cresswell, John W. (2009). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. Third Edition*. California: Sage Publication

_____. (2015). *Penelitian & Desain Riset: Memilih diantara Lima Pendekatan.* Jogyakarta: Pustaka Pelajar

Erhard, Eppler. (2009). *The Return of The State.* London: Forumpress.

Ghernaouti, Solange. (2013). *Cyber Power*. Switzerland: EPLF Press

James A. Green. (2015). *Cyber Warfare A Multidiciplinary Analysis.* Lanchester University: Routledge Studies in Conflict, Security and Technology.

Krisna. (2005). *Pengaruh Globalisasi Terhadap Pluralisme Kebudayaan Manusia di Negara Berkembang.* Public Journal

Mamduh M. Hanafi.(2011). *Manajemen.* Jakarta: Unit Penerbitan dan percetakan STIM YKPN.

Matondang, M.H. (2008). *Kepemimpinan, Budaya Organisasi dan Manajemen Stratejik.* Yogyakarta: Graha Ilmu.

Michael Smith. (2015). *Research Handbook on International Law and Cyberspace.* (Cheltenham UK: Edward Elgar Publishing Limited)

Mintzberg, Henry, James Brian Quinn, dan Jhon Voyer. (1995). "*The Strategy Process*". London: Prentice Hall International, Inc.

Moekijat. (1994). *Koordinasi (Suatu Tinjauan Teoritis).* Bandung: Mandar Maju.

Moleong, Lexy J. (1991). *Metodologi Penelitian Kualitatif.* Bandung: Remaja Rosda Karya.

Nainggolan dalam Freddy Rangkuti, (1998). *Analisis SWOT Teknis Membedah Kasus Bisnis,* Jakarta: Gramedia Pustaka Utama.

Nawawi, Hadari. (2005). *Manajemen Stratejik.* Yogyakarta: Gadjah Mada Press.

Poerwandari, E. (1991). *Pendekatan Kualitatif dalam Penelitian Psikologi,* Jakarta: Lembaga Pengembangan Sarana Pengukuran dan Pendidikan Psikologi. LPSP3. Fakultas Psikologi Universitas Indonesia.

Sarwono, Jonathan. (2006). *Metode Penelitian Kuantitatif dan Kualitatif*. Yogyakarta: Graha Ilmu.

Scholte, J.A. (2000). *Globalization: A Critical Introduction.* London: Palgrave.

Siagian P., Sondang. (2011). *Manajemen Stratejik.* Jakarta: PT. Bumi Aksara

Suriyatno, Makmur. (2014). *Tentang Ilmu Pertahanan.* Jakarta: Yayasan Pustaka Obor Indonesia.

Surowiecki, James. (2004). *The Wisdom of Crowds: Why the Many Are Smarter Than the Few and How Collective Wisdom Shapes Business, Economies, Societies and Nations*. USA: Doubleday; Anchor.

Sugiyono. (2012). *Metode Penelitian Kuantitatif Kualitatif dan R&D.* Bandung: Alfabeta

_____. (2017). *Metode Penelitian Kombinasi*. Bandung: Alfabeta.

Williams, Paul D. (2008). *Security Studies: An Introduction*. USA: Routledge. hlm. 56

**JURNAL**

Deardorff, D.S., & Williams, G. (2006). Synergy Leadership in Quantum Organizations. *Fesserdorff Consultants*.

Gupta, O. & Roos, G. (1998). *Mergers and acquisitions through an intellectual capital perspective. Journal of Intellectual Capital*, 2(3). 2001. hlm. 297-309. & Krumm, J.M.M., Dewulf, G. & De Jonge, H. *Managing key resources and capabilities: pinpointing the added value of corporate real estate management. Facilities*, 16(12/13).

Handrini Ardiyanti, *Cyber-Security Dan Tantangan Pengembangannya di Indonesia*, Politica Vol.5 *No*. 1 Juni 2014

Harwood, C.J. (2000). *Review of "Synergy matters: Working with systems in the twenty-first century* by A.M. Castell, A.J. Gregory, G.A. Hindle, M.E. James and G. Ragsdall (Eds), Kybernetes, 29(4).

Krisna. (2005). Pengaruh Globalisasi Terhadap Pluralisme Kebudayaan Manusia di Negara Berkembang. *Public Journal*

**UNDANG-UNDANG DAN PERATURAN PEMERINTAH**

Kementerian Pertahanan Republik Indonesia. 2015. Buku Putih Pertahanan. Kementerian Pertahanan; Jakarta

Nota Kesepakatan Aksi antara KPU, Bawaslu dan Kementerian Komunikasi dan Informatika. Tentang Manajemen dan Pengawasan Gubernur dan Wakil Gubernur, Bupati dan Wakil Bupati Dan/Atau Walikota dan Wakil Walikota Tahun 2018

Peraturan Menteri Pertahanan Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber.

Undang-Undang Nomor 3 Tahun 2002 tentang Pertahanan Negara

**LAPORAN**

*Asia and the Pacific Region Scorecard*. *Global Security Index* (GC) 2017 (https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf)

David P. Fidler. "The U.S Election Hacks, Cybersecurity, And International Law". *Symposium on Cybersecurity and The Changing International Law of Data.* Doi:10.1017/aju.2017.5

Laporan Tahunan *Indonesia Security Incident Response Team of Internet Infrastructure* (ID-SIRTII) 2017

**INTERNET:**

Andi Widjajanto. (2018, 10 Januari). Keamanan siber 2.0. Dalam https://kompas.id/baca/opini/2018/01/10/keamanan-siber-2-0/ [diakses pada 20 November 2018]

Anonim. (2018, 10 Januari). Era Pilkada 2.0, ini langkah Kominfo dan KPU. Dalam https://www.indotelko.com/kanal?c=rm&it=era-pilkada-kpu [diakses pada 20 November 2018]

Anonim. (2014, Juli 2001). *Xnuxer,'Hacker Partai Jambu' Situs KPU* https://inet.detik.com/cyberlife/d-2643201/xnuxer-hacker-partai-jambu-situs-kpu [diakses pada 10 Maret 2018]

Anonim. (2018, September 24) Pesta sudah dimulai: Yang Perlu Anda ketahui soal Pemilu 2019. Dalam http://www.bbc.com/indonesia/indonesia-45618212. [Diakses pada 15 November 2018]

Anup Ghosh. (2018, Mei 31). *How elections are hacked via social media profiling.* Dalam https://www.csoonline.com/article/3277953/social-engineering/how-elections-are-hacked-via-social-media-profiling.html [Diakses pada 28 September 2018]

Antara. (2015, 7 April). *Jaringan KPU Sempat Diretas Saat Rekapitulasi Suara Pilpres 2014* http://news.metrotvnews.com/politik/yNLAZZ6b-jaringan-kpu-sempat-diretas-saat-rekapitulasi-suara-pilpres-2014 [diakses pada 10 Maret 2018]

Merriam-Webter. (https://www.merriam-webster.com/dictionary/communication) [diakses pada 9 Maret 2018]

J. Falahuddin, Muhammad.(2015, 31 Agustus). *"Sekilas Tentang Cyber Crime, Cyber Security dan Cyber War* " dalam https://inet.detik.com/security/d-3005339/sekilas-tentang-cyber-crime-cyber-security-dan-cyber-war [diakses pada 12 Maret 2018]

Horwart, Rich.(2006) "*The Origin of Strategy" dalam* (http://www.strategyskills.com/Articles_Samples/origin_strategy.pdf) [Diakses pada 12 Maret 2018]

Riza, Budi. (2018, Februari 27). *"Ini Cara Kerja Kelompok Rusia yang Dituding Intervensi Pilpres AS*", dalam. (https://fokus.tempo.co/read/1064823/ini-cara-kerja-kelompok-rusia-yang-dituding-intervensi-pilpres-as) [diakses pada 9 Maret 2018]

LAMPIRAN 1

# SURAT PENELITIAN

**KEMENTERIAN PERTAHANAN RI**
**UNIVERSITAS PERTAHANAN**

Nomor : B / 245 / VIII/2018
Klasifikasi : Biasa
Lampiran : -
Hal : Permohonan Izin Penelitian

Bogor, 21 Agustus 2018

Kepada
Yth. Pejabat Terlampir
di
Tempat

1. Dasar:
   a. Peraturan Presiden RI Nomor 5 Tahun 2011 tentang Universitas Pertahanan sebagai Perguruan Tinggi yang diselenggarakan oleh Pemerintah.
   b. Kalender Pendidikan Program Studi Peperangan Asimetris Fakultas Strategi Pertahanan Unhan TA 2017/2018.
2. Sehubungan dasar tersebut di atas, mohon dapatnya Pejabat dalam lampiran berkenan mengizinkan mahasiswa Prodi Studi Peperangan Asimetris Fakultas Strategi Pertahanan Unhan atas nama M. Syadli Pratama, Nomor Induk Mahasiswa 12017012018, untuk melaksanakan wawancara dan atau memberikan kuesioner guna mengumpulkan data-data penelitian yang diperlukan dalam penyusunan Tesis dengan judul "Perbandingan Strategi Sistem Pemilihan Umum Amerika Serikat dan Komisi Pemilihan Umum (KPU) Pusat Dalam Mewujudkan *Cybersecurity* Pada Pemilihan Umum 2019"
3. Mohon konfirmasi waktu serta tempat pelaksanaan wawancara dan pemberian kuesioner kepada M.Syadli Pratama, NIM: 12017012018, e-mail: syadli.pratama@idu.ac.id, livelife.syah@live.com.
4. Demikian untuk menjadikan periksa.

a.n. Rektor Unhan
Warek I Bidang Akademik dan
Kemahasiswaan,

Prof. Dr. Ir. Dadang Gunawan, M.Eng
Pembina Utama IV/e

Tembusan:
1. Rektor Unhan
2. Dekan FSP Unhan
3. Karo Akademik & Kemahasiswaan Unhan.

Kawasan IPSC Sentul Bogor Telp. 021-29818758

LAMPIRAN 2

# MEMORANDUM OF ACTION

NOTA KESEPAKATAN AKSI

ANTARA

BADAN PENGAWAS PEMILIHAN UMUM REPUBLIK INDONESIA,
KOMISI PEMILIHAN UMUM REPUBLIK INDONESIA,
DAN
KEMENTERIAN KOMUNIKASI DAN INFORMATIKA REPUBLIK INDONESIA

TENTANG

MANAJEMEN DAN PENGAWASAN KONTEN INTERNET DALAM PENYELENGGARAAN PEMILIHAN GUBERNUR DAN WAKIL GUBERNUR, BUPATI DAN WAKIL BUPATI DAN/ATAU WALIKOTA DAN WAKIL WALIKOTA TAHUN 2018

Nomor : 0101/K.BAWASLU/HM.02.00/I/2018
Nomor : 13 /PL.03.4-NK/01/KPU/2018
Nomor : 142 /MOU/M.KOMINFO/HK.03.02/01/2018

Pada hari ini Rabu, tanggal tiga puluh satu bulan Januari tahun dua ribu delapan belas, bertempat di Jakarta, yang bertanda tangan di bawah ini:

1. **ABHAN**, Ketua Badan Pengawas Pemilihan Umum RI, dalam hal ini bertindak untuk dan atas nama Badan Pengawas Pemilihan Umum RI yang berkedudukan di Jalan MH. Thamrin Nomor 14, Jakarta 10350, selanjutnya disebut sebagai PIHAK KESATU;
2. **ARIEF BUDIMAN**, Ketua Komisi Pemilihan Umum RI, dalam hal ini bertindak untuk dan atas nama Komisi Pemilihan Umum RI berkedudukan di Jalan Imam Bonjol Nomor 29, Jakarta Pusat 10310, selanjutnya disebut sebagai PIHAK KEDUA;
3. **RUDIANTARA**, Menteri Komunikasi dan Informatika RI, dalam hal ini bertindak untuk dan atas nama Kementerian Komunikasi dan Informatika RI berkedudukan di Jalan Medan Merdeka Barat Nomor 9 Jakarta 10110, selanjutnya disebut sebagai PIHAK KETIGA;

PIHAK KESATU, PIHAK KEDUA, dan PIHAK KETIGA untuk selanjutnya secara bersama-sama disebut sebagai PARA PIHAK dan secara masing-masing disebut sebagai PIHAK, terlebih dahulu menerangkan hal-hal sebagai berikut:

1. PIHAK KESATU merupakan lembaga penyelenggara pemilihan umum yang mengawasi penyelenggaraan pemilihan umum di seluruh wilayah Negara Kesatuan Republik Indonesia.
2. PIHAK KEDUA merupakan lembaga penyelenggara pemilihan umum yang bersifat nasional, tetap, dan mandiri dalam melaksanakan pemilihan umum.
3. PIHAK KETIGA merupakan Kementerian yang menyelenggarakan urusan pemerintahan bidang komunikasi dan informatika.

PARA PIHAK selanjutnya menjelaskan :

bahwa dengan adanya kegiatan kampanye melalui media internet dimana dapat terjadi potensi kampanye yang diduga melawan hukum dan/atau bertentangan dengan ketentuan peraturan perundang-undangan sehingga mengakibatkan kerugian bagi masyarakat maupun peserta Pemilihan Gubernur dan Wakil Gubernur, Bupati dan Wakil Bupati, dan/atau Walikota dan Wakil Walikota Tahun 2018, maka dibutuhkan koordinasi dan komitmen PARA PIHAK untuk melakukan manajemen dan pengawasan konten internet.

Dengan memperhatikan ketentuan peraturan perundang-undangan sebagai berikut:

1. Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan Atas Undang-Undang Nomor 11 Tahun 2008 Tentang Informasi dan Transaksi Elektronik;
2. Undang-Undang Nomor 1 Tahun 2015 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2014 tentang Pemilihan Gubernur dan Wakil Gubernur, Bupati dan Wakil Bupati, serta Walikota dan Wakil Walikota Menjadi Undang-Undang sebagaimana telah beberapa kali diubah, terakhir dengan Undang-Undang Nomor 10 Tahun 2016 tentang Perubahan Kedua Atas Undang-Undang Nomor 1 Tahun 2015 tentang Penetapan Peraturan Pemerintah Pengganti Undang-Undang Nomor 1 Tahun 2014 tentang Pemilihan Gubernur, Bupati, dan Walikota Menjadi Undang-Undang;
3. Undang-Undang Nomor 7 Tahun 2017 tentang Pemilihan Umum;
4. Peraturan Pemerintah Nomor 82 Tahun 2012 tentang Penyelenggaraan Sistem dan Transaksi Elektronik;
5. Peraturan Menteri Komunikasi dan Informatika Nomor 19 Tahun 2014 tentang Penanganan Konten Internet Bermuatan Negatif;

6. Peraturan Badan Pengawas Pemilihan Umum Nomor 12 Tahun 2017 tentang Pengawasan Kampanye Pemilihan Gubernur dan Wakil Gubernur, Bupati dan Wakil Bupati, serta Wali Kota dan Wakil Wali Kota; dan
7. Peraturan Komisi Pemilihan Umum Nomor 4 Tahun 2017 tentang Kampanye Pemilihan Gubernur dan Wakil Gubernur, Bupati dan Wakil Bupati dan/atau Walikota dan Wakil Walikota Tahun 2018.

Berdasarkan pertimbangan tersebut di atas, dengan iktikad baik, saling percaya, dan tetap berpedoman pada peraturan perundang-undangan, PARA PIHAK sepakat untuk mengadakan kerja sama manajemen dan pengawasan konten internet dalam Pemilihan Gubernur dan Wakil Gubernur, Bupati dan Wakil Bupati dan/atau Walikota dan Wakil Walikota Tahun 2018 dengan ketentuan dan syarat-syarat yang diatur dalam pasal-pasal sebagai berikut:

Pasal 1
MAKSUD DAN TUJUAN

(1) Nota Kesepakatan Aksi ini dimaksudkan untuk melakukan penguatan koordinasi PARA PIHAK guna mempercepat manajemen dan pengawasan konten internet dalam Pemilihan Gubernur dan Wakil Gubernur, Bupati dan Wakil Bupati dan/atau Walikota dan Wakil Walikota Tahun 2018 sesuai dengan tugas dan kewenangan masing-masing.
(2) Nota Kesepakatan Aksi ini bertujuan untuk meningkatkan komitmen dan koordinasi PARA PIHAK dalam rangka manajemen dan pengawasan konten internet dalam Pemilihan Gubernur dan Wakil Gubernur, Bupati dan Wakil Bupati dan/atau Walikota dan Wakil Walikota Tahun 2018.

Pasal 2
RUANG LINGKUP

Ruang lingkup Nota Kesepakatan Aksi ini meliputi:
a. Koordinasi manajemen dan pengawasan konten internet dalam pelaksanaan Pemilihan Gubernur dan Wakil Gubernur, Bupati dan Wakil Bupati, dan/atau Walikota dan Wakil Walikota Tahun 2018 sesuai dengan tugas dan fungsi PARA PIHAK;
b. Pertukaran data dan informasi konten internet;
c. Peningkatan kapasitas sumber daya manusia untuk penanganan dan pengawasan konten internet;

d. Pemantauan pada konten internet yang terindikasi bertentangan dengan peraturan perundang-undangan sesuai dengan kewenangan PARA PIHAK;
e. Peningkatan sosialisasi dan edukasi dalam manajemen dan pengawasan penggunaan internet terkait materi kampanye sesuai dengan kewenangan PARA PIHAK;
f. Penguatan partisipasi publik dalam penggunaan internet dan manajemen konten internet; dan
g. Kegiatan lain yang disepakati PARA PIHAK.

Pasal 3
PELAKSANAAN

(1) PIHAK KESATU melaksanakan tugas:
   a. Menyediakan hasil pengawasan terkait konten internet yang melanggar peraturan perundangan-undangan tentang pemilihan.
   b. Menyediakan data laporan masyarakat terkait konten internet yang melanggar peraturan perundangan-undangan tentang pemilihan;
   c. Menyediakan analisis hasil pengawasan terkait media sosial dalam kampanye pemilihan; dan
   d. Memfasilitasi kegiatan koordinasi antar Lembaga dalam menunjang manajemen dan pengawasan konten internet dalam pelaksanaan Pemilihan Gubernur dan Wakil Gubernur, Bupati dan Wakil Bupati, dan/atau Walikota dan Wakil Walikota Tahun 2018.

(2) PIHAK KEDUA melaksanakan tugas:
   a. Menyediakan informasi terkait data Tim Kampanye, Pelaksana Kampanye, Petugas Kampanye, dan Juru Kampanye; dan
   b. Menyediakan informasi akun media sosial peserta Pemilihan yang telah didaftarkan kepada PIHAK KEDUA.

(3) PIHAK KETIGA melaksanakan tugas :
   a. Menindaklanjuti rekomendasi laporan hasil pengawasan terkait konten internet dalam pelaksanaan Pemilihan Gubernur dan Wakil Gubernur, Bupati dan Wakil Bupati, dan/atau Walikota dan Wakil Walikota Tahun 2018; dan
   b. Melakukan penanganan konten internet yang melanggar ketentuan peraturan perundang-undangan dalam pelaksanaan Pemilihan Gubernur dan Wakil Gubernur, Bupati dan Wakil Bupati, dan/atau Walikota dan Wakil Walikota Tahun 2018.

Pasal 4
PEMBIAYAAN

Biaya yang timbul sebagai akibat dari pelaksanaan Nota Kesepakatan Aksi ini dibebankan pada anggaran masing-masing pihak, dan sumber-sumber lain yang tidak mengikat sesuai ketentuan peraturan perundang-undangan.

Pasal 5
MONITORING DAN EVALUASI

Monitoring dan evaluasi pelaksanaan Nota Kesepakatan Aksi ini dilakukan oleh PARA PIHAK secara bersama-sama.

Pasal 6
JANGKA WAKTU

(1) Nota Kesepakatan Aksi ini berlaku untuk jangka waktu 1 (satu) tahun sejak ditandatangani oleh PARA PIHAK dan dapat diperpanjang sesuai kesepakatan PARA PIHAK.
(2) Dalam hal salah satu pihak berkeinginan untuk memperpanjang dan/atau mengakhiri Nota Kesepakatan Aksi ini maka pihak yang bersangkutan wajib memberitahukan maksud tersebut secara tertulis kepada pihak lainnya, paling lama 1 (satu) bulan sebelum berakhirnya Nota Kesepakatan Aksi ini.
(3) Apabila Nota Kesepakatan Aksi ini tidak diperpanjang lagi dan/atau diakhiri sebelum jangka waktunya habis, sebagaimana dimaksud pada ayat (2), maka pengakhiran Nota Kesepakatan Aksi ini tidak mempengaruhi hak dan kewajiban PARA PIHAK yang harus diselesaikan terlebih dahulu sebagai akibat pelaksanaan sebelum berakhirnya Nota Kesepakatan Aksi ini.

Pasal 7
PERUBAHAN

Hal-hal yang belum diatur dalam Nota Kesepakatan Aksi ini akan diatur dan disepakati oleh PARA PIHAK sebagai Perubahan/Adendum yang merupakan dokumen tidak terpisahkan dari Nota Kesepakatan Aksi ini.

Pasal 8
PENYELESAIAN PERSELISIHAN

Apabila terjadi perbedaan penafsiran dalam pelaksanaan Nota Kesepakatan Aksi ini, maka penyelesaian dilakukan dengan cara musyawarah untuk mufakat.

Pasal 9
PENUTUP

Nota Kesepakatan Aksi ini dibuat rangkap 3 (tiga) naskah asli serta bermeterai cukup, yang masing-masing mempunyai kekuatan hukum yang sama.

| PIHAK KEDUA | PIHAK KESATU |
|---|---|
| **ARIEF BUDIMAN** | **ABHAN** |

PIHAK KETIGA

**RUDIANTARA**

LAMPIRAN 3

# PEDOMAN WAWANCARA

Peneliti hanya mengemukakan rencana pertanyaan secara garis besar. Rencana pertanyaan wawancara dibuat berdasarkan teori yang dipergunakan oleh peneliti sebagai acuan umum, untuk kemudian dikembangkan secara lebih komprehensif pada saat wawancara dilaksanakan terhadap para narasumber. Sehingga dapat diperoleh informasi yang relevan dan dibutuhkan oleh Peneliti.

Adapun pedoman wawancara yang digunakan ditunjukkan pada tabel berikut.

| No. | Topik | Garis Besar Pertanyaan | Informan |
|---|---|---|---|
| 1. | Strategi dan Keamanan Siber | 1. Strategi apa dan bagaimana yang diimplementasikan oleh institusi Anda dalam mewujudkan keamanan siber dalam pelaksanaan Pemilihan Umum 2019?<br>2. Bagaimana kesiapan institusi Anda dalam imlementasi strategi tersebut dari perspektif keamanan siber?<br>3. Apakah institusi Anda memiliki standar keamanan siber? Apa dan bagaimana standar keamanan siber tersebut?<br>4. Bagaimana institusi Anda membentuk, merespon dan menyiapkan diri dalam menghadapi ancaman siber yang mungkin muncul pada pelaksanaan Pemilu 2019? | 1. Aditya Haris Kemal Nugraha S.Komp<br>2. Gunawan Suswantoro<br>3. Ir. Herry Abdul Azis, M.Eng<br>4. Ir. Riki Arif Gunawan M.Sc<br>5. Dra. Siti Meiningsih MSc.<br>6. Sulistyo, S.Si., S.T., M.Si<br>7. Agung Nugraha, S.IP., M.Si (Han).<br>8. Yuliardi Sutedja K.<br>9. Ir. Budi Rahardjo M.Sc., Ph.D |
| 2. | Sinergitas | 1. Sejauh mana keterlibatan instansi Bapak/Ibu/Saudara/i dalam implementasi keamanan siber pada persiapan pemilu 2019?<br>2. Bagaimana kerjasama institusi Anda dalam membentuk, merespon dan menyiapkan diri terhadap ancaman siber pada pemilihan umum 2019 mendatang pada saat sebelum, sepanjang dan setelah Pemilu berlangsung?<br>3. Bagaimana tingkat sinergitas Institusi Anda dengan instansi yang terlibat) dalam pengamanan siber pada pemilu Presiden 2019 mendatang? | 1. Aditya Haris Kemal Nugraha S.Komp<br>2. Gunawan Suswantoro<br>3. Ir. Herry Abdul Azis, M.Eng<br>4. Ir. Riki Arif Gunawan M.Sc<br>5. Dra. Siti Meiningsih MSc.<br>6. Sulistyo, S.Si., S.T., M.Si<br>7. Agung Nugraha, S.IP., M.Si (Han).<br>8. Yuliardi Sutedja K.<br>9. Ir. Budi Rahardjo M.Sc., Ph.D |

| | | | |
|---|---|---|---|
| 3. | Hambatan | 1. Menurut Bapak/Ibu/Saudara/i kendala-kendala apa saja yang dihadapi dalam kerjasama yang dapat menjadi kerentanan ataupun penghambat dalam konteks keamanan siber?<br>2. Bagaimana saran Bapak/Ibu/Saudara/I terkait upaya yang dapat dilakukan untuk meningkatkan sinergitas antar lembaga guna meningkatkan kesiapan keamanan siber? | 1. Aditya Haris Kemal Nugraha S.Komp<br>2. Gunawan Suswantoro<br>3. Ir. Herry Abdul Azis, M.Eng<br>4. Ir. Riki Arif Gunawan M.Sc<br>5. Dra. Siti Meiningsih MSc.<br>6. Sulistyo, S.Si., S.T., M.Si<br>7. Agung Nugraha, S.IP., M.Si (Han).<br>8. Yuliardi Sutedja K.<br>9. Ir. Budi Rahardjo M.Sc., Ph.D |

LAMPIRAN 4

# DOKUMENTASI

*Interviewee* : Aditya Haris Kemal Nugraha S.Komp
Jabatan : Kepala Sub. Bagian Pengembangan Jaringan & Komunikasi Data, Biro Perencanaan dan Data
Instansi : Komisi Pemilihan Umum (KPU) Pusat
Tanggal & Waktu : Jumat, 21 September 2018, Pukul 09.34 WIB

*Interviewee* : Gunawan Siswantoro
Jabatan : Sekretaris Jenderal
Instansi : Badan Pengawas Pemilu (Bawaslu)
Tanggal & Waktu : Jumat, 21 September 2018, Pukul 15.15 WIB

*Interviewee* : Ir. Herry Abdul Azis, M.Eng
Jabatan : SAM. Bidang Teknologi
Instansi : Kementerian Komunikasi dan Informatika
Tanggal & Waktu : Kamis, 6 September 2018, Pukul 14.33 WIB

*Interviewee* : Ir. Riki Arif Gunawan M.Sc
Jabatan : Direktur Jenderal Aplikasi dan Informatika (APTIKA)
Instansi : Kementerian Komunikasi dan Informatika
Tanggal & Waktu : Senin, 10 September 2018, Pukul 14.02 WIB

*Interviewee* : Sulistyo, S.Si., S.T., M.Si
Jabatan : Direktur Deteksi Ancaman
Instansi : Badan Siber dan Sandi Negara
Tanggal & Waktu : Jumat, 26 Oktober 2018, Pukul 15.12 WIB

*Interviewee* : Adi Nugroho Mewakili Agung Nugraha, S.IP., M.Si (Han)
Jabatan : Direktur Proteksi Infrastruktur Informasi Kritikal Nasional
Instansi : Badan Siber dan Sandi Negara
Tanggal & Waktu : Kamis, 18 Oktober 2018, Pukul 11.46 WIB

*Interviewee* : Ir. Budi Rahardjo M.Sc., Ph.D
Jabatan : Praktisi IT dan Ahli Keamanan Informasi
Instansi : Institut Teknologi Bandung (ITB)
Tanggal & Waktu : Kamis, 28 Oktober 2018, Pukul 09.43 WIB

.


*Interviewee* : **Yuliardi K. Sutedja**
Jabatan : *Board Secretary and Chairman*
Instansi : *ICT Community & Indonesia Cyber Security Forum* (ICSF)
Tanggal & Waktu : Kamis, 29 November 2018, Pukul 20.17 WIB

| | |
|---|---|
| *Interviewee* | : **Hadar Nafis Gumay** |
| Jabatan | : *Former Commissioner NetGrit* (Ex *Commissioner* KPU 2012-2017) |
| Instansi | : NetGrit (*Network for Democracy and Electoral Integrity*) |
| Tanggal & Waktu | : Kamis, 29 November 2018, Pukul 20.17 WIB |

LAMPIRAN 4

## RIWAYAT HIDUP PENULIS

M. Syadli Pratama S, lahir di Makassar pada 17 April 1986. Anak ke-5 dari pasangan bapak Drs. Syahruddin dan Ibu Nurmiati Norma. Menyelesaikan pendidikan SD Mangkura lulus tahun 1998, SMP Negeri 2 Makassar lulus tahun 2001, SMA Negeri I Makassar lulus tahun 2004, Sarjana (S-1) Universitas Komputer Indonesia lulus tahun 2015 dan pada tahun 2017 melanjutkan program Magister (S-2) di Universitas Pertahanan.

Peneliti pernah bekerja sebagai Personal Asisstant di PT. Titian Bahtera Segara, Jakarta pada September 2008 hingga Agustus 2010. Selanjutnya bekerja sebagai Associate Department Manager di PT. Askap Future, Jakarta pada Agustus 2010 hingga Januari 2011 dan terakhir bekerja sebagai Marketing Representative and Membership Consultant di Sunset Fitness, Bali pada April hingga Oktober 2011.