Universitas Katolik Parahyangan

Fakultas Ilmu Sosial dan Ilmu Politik

Program Studi Ilmu Hubungan Internasional

Terakreditasi A

SK BAN-PT NO: 3095/SK/BAN-PT/Akred/S/VIII/2019

Dampak Penggunaan *Malware* oleh Tiongkok dan *Big Data Privacy* tahun 2010-2019

Skripsi

Oleh

Salman Alfarizi

2017330059

Bandung

2021

Universitas Katolik Parahyangan

Fakultas Ilmu Sosial dan Ilmu Politik

Program Studi Ilmu Hubungan Internasional

Terakreditasi A

SK BAN-PT NO: 3095/SK/BAN-PT/Akred/S/VIII/2019

Dampak Penggunaan *Malware* oleh Tiongkok dan *Big Data Privacy* tahun 2010-2019

Skripsi

Oleh

Salman Alfarizi

2017330059

Pembimbing

Giandi Kartasasmita, S.IP., M.A.

Bandung

2021

Fakultas Ilmu Sosial dan Ilmu Politik
Jurusan Hubungan Internasional
Program Studi Ilmu Hubungan Internasional

Tanda Pengesahan Skripsi

Nama : Salman Alfarizi
Nomor Pokok : 2017330059
Judul : Dampak Penggunaan *Malware* oleh Tiongkok dan *Big Data Privacy* tahun 2010-2019

Telah diuji dalam Ujian Sidang jenjang Sarjana
Pada Rabu, 14 Juli 2021
Dan dinyatakan **LULUS**

Tim Penguji
Ketua sidang merangkap anggota
Dr. Aknolt K. Pakpahan : _____

Sekretaris
Giandi Kartasasmita, S.IP., MA : _____

Anggota
Sapta Dwikardana, Ph.D. : _____

Mengesahkan,
Dekan Fakultas Ilmu Sosial dan Ilmu Politik

Dr. Pius Sugeng Prasetyo, M.Si

SURAT PERNYATAAN

Saya yang bertandatangan di bawah ini :

Nama	:	Salman Alfarizi
NPM	:	2017330059
Jurusan/Program Studi	:	Ilmu Hubungan Internasional
Judul	:	Dampak Penggunaan *Malware* oleh Tiongkok dan *Big Data Privacy* tahun 2010-2019

Dengan ini menyatakan bahwa skripsi ini merupakan hasil karya tulis ilmiah sendiri dan bukanlah merupakan karya yang pernah diajukan untuk memperoleh gelar akademik oleh pihak lain. Adapun karya atau pendapat pihak lain yang dikutip, ditulis sesuai dengan kaidah penulisan ilmiah yang berlaku.

Pernyataan ini saya buat dengan penuh tanggung jawab dan bersedia menerima konsekuensi apa pun sesuai aturan yang berlaku, apabila di kemudian hari diketahui bahwa pernyataan ini tidak benar.

Bandung, 7 Juli 2021

Salman Alfarizi

2017330059

ABSTRAK

Nama : Salman Alfarizi
NPM : 2017330059
Judul : Dampak Penggunaan *Malware* oleh Tiongkok dan *Big Data Privacy* tahun 2010-2019

Revolusi Industri 4.0 menjadi sebuah pergerakan masif dalam bidang teknologi dan informasi. Pergerakan pada sektor teknologi ini terus dikembangkan dengan terciptanya suatu konsep *Internet of Things* (IoT). Konsep IoT merupakan sebuah integrasi antara perangkat keras dengan sistem internet. Dalam mengaplikasikan konsep ini perlu didukung dengan banyak data yang terhubung antara internet dengan perangkatnya. Semakin banyaknya data yang dihimpun, ini merupakan sebuah konsep yang disebut sebagai Big Data. Penerapan Big Data merupakan tempat penyimpanan data pengguna secara besar yang diintegrasikan menggunakan IoT. Semakin banyaknya data yang dikumpulkan dalam suatu *server* dapat dijadikan keuntungan dalam pengembangan IoT dalam Revolusi Industri 4.0 yang bertujuan memudahkan kehidupan manusia. Namun, tentu saja dengan sistem yang kompleks tersebut memiliki sebuah ancaman di dalamnya, salah satunya dengan adanya sistem *malware* yang memiliki peran untuk pengambilan data tanpa adanya izin. Dalam penggunaan *malware* dalam Big Data Privacy. Tiongkok dan perusahaan *state-owned* menjadi aktor yang terduga dalam menggunakan *malware* dalam tindakannya. Berangkat dari permasalahan yang ada dalam pengembangan IoT pada Revolusi Industri 4.0, tulisan ini mengangkat pertanyaan penelitian yaitu "Bagaimana dampak *Malware* yang digunakan oleh Tiongkok dalam Big Data Privacy pada tahun 2010 - 2019?". Dalam rangka untuk menjawabnya, penulis akan menggunakan konsep Shoshana Zuboff yang mengemukakan konsep dari *surveillance capitalism* dan teori dari *cybersecurity dilemma* yang dikemukakan oleh Ben Buchanan berbasiskan kepada teori *security dilemma*. Teori dan konsep tersebut menjelaskan penggunaan *malware* untuk kepentingan Tiongkok. Tulisan ini menemukan bahwa dalam penggunaan *malware* yang dilakukan oleh Tiongkok berdasarkan teori dan konsep yang digunakan bahwa Tiongkok melakukannya untuk keuntungan dan pertahanan diri.

Kata Kunci: Revolusi Industri 4.0, *Internet of Things*, *Malware*, Big Data, Tiongkok

ABSTRACT

Name : Salman Alfarizi
Student Number : 2017330059
Title : *Impact of the Use of Malware by China and Big Data Privacy in 2010-2019*

4th Industrial Revolution has become a massive movement. This movement in the technology sector continues to develop with production to the Internet of Things (IoT). IoT concepts need integration between hardware and internet systems. IoT needs to be supported by massive data to connect within the internet and the devices – known as Big Data. The implementation of Big Data is a large user data repository that – is combined into IoT. More data collected on a server can use as an advantage in the development of IoT in 4thIndustrial Revolution, which aims to facilitate human life. This complex system has a threat inside it, one of which is the presence of a malware system that has a role in data retrieval without permission. In the use of malware in Big Data Privacy, China and state-owned companies are suspected actors in using malware in their actions. From these issues that exist in the development of IoT in 4th Industrial Revolution, this paper raises a research question, which is " How is impacted from Malware that used by China in Big Data Privacy in 2010-2019?". To answer this, the author will use Shoshana Zuboff's concept as the founder of surveillance capitalism and the theory of cybersecurity dilemma by Ben Buchanan based on the security dilemma theory. These theories and concepts explain the use of malware for the benefit of China. This paper finds that China's use of malware, based on the theory and concepts used that China is doing it for profit and self-defense.

***Keywords**: 4th Industrial Revolution, Internet of Things, Malware, Big data, China*

KATA PENGANTAR

Segala puji dan syukur dipanjatkan kepada Allah SWT karena atas kuasa-Nya, penulis dapat menyelesaikan penulisan skripsi ini di waktu yang tepat. Melalui skripsi ini, penulis berusaha untuk memaparkan dan menjelaskan "Dampak Penggunaan *Malware* oleh Tiongkok dan *Big Data Privacy* tahun 2010-2019".

Penulis berharap, melalui skripsi ini pembaca dapat menjadi Sebagai referensi dan pedoman bagi penulis lain yang hendak mengangkat topik mengenai Big Data Privacy dan penggunaan *malware* sebagai utilisasi yang berdampak kepada *cyberwarfare*. Tentunya juga sebagai saran dan rekomendasi bagi pengguna dunia maya untuk selalu berhati-hati dalam Big Data yang sudah semakin pesat perkembangannya. Pada penelitian ini, poin yang perlu diperhatikan adalah Tiongkok menggunakan *malware* bersamaan dengan masuknya *trend* Revolusi Industri 4.0. Dengan demikian dengan tindakan tersebut memiliki dampak kepada produk maupun program dari Revolusi Industri 4.0 seperti *Internet of Things* (IoT) dan Big Data Privacy menjadi target Tiongkok dalam *cyberspace* sebagai *self-defense* dan *for-profit* dengan melalui *malware* sebagai utilisasi.

Melalui skripsi ini, penulis juga ingin mengucapkan terima kasih kepada Mas Giandi Kartasasmita, S.IP., M.A., selaku Dosen Pembimbing penulis sendiri karena telah memberikan arahan, pelajaran, kritik, dan saran selama dalam proses penyusunan Skripsi ini. Tanpa adanya beliau sebagai pembimbing Skripsi, penulis tidak akan mampu menyelesaikannya. Terima kasih juga penulis ucapkan kepada seluruh pihak yang telah memberi dukungan. Walau begitu, penulis sangat menyadari bahwa penulisan akademik ini masih jauh dari kata sempurna dan membutuhkan perbaikan dalam penelitian ini. Maka, penulis sangat terbuka terhadap saran, kritik, ataupun masukan yang membangun untuk mengembangkan tulisan ini. Terima kasih.

Bandung, 16 Juli 2021

Salman Alfarizi

UCAPAN TERIMA KASIH

Saya ingin menyampaikan rasa terima kasih atas dukungan, waktu, kebahagiaan, kesedihan, stres yang tak kunjung usai, hiburan serta memori di masa perkuliahaan ini. Penulis ucapkan terima kasih yang diberikan untuk:

1. **Allah SWT** – yang telah melimpahkan segala karunia dan kuasa-Nya kepada penulis untuk dapat menyusun dan menyelesaikan skripsi ini.
2. **Keluarga** – Terima kasih kepada Mamah dan Papah yang sudah memberikan support dalam menyelesaikan Skripsi ini. Tanpa adanya kalian Skripsi ini tidak mungkin akan selesai. Lalu, ucapan terima kasih diberikan kepada saudara dan tante yang telah memberikan support juga kepada saya. Terima kasih.
3. **Giandi Kartasasmita, S.IP., M. A.,** – Terima kasih kepada Mas Gi selaku dosen pembimbing penulis dalam mewujudkan hasil dari penelitian penulis selama 1 semester ini. Berkat bantuan yang diberikan oleh Mas Gi seperti masukan kritik dan saran mengenai peneltian penulis mengenai pengguanaan *malware* yang dilakukan oleh Tiongkok; berkat pemikiran-pemikaran yang diberikan Mas Gi kepada penulis, sehingga penulis dapat mewujudkan karya penulisan ini hingga sidang Skripsi ini. Sekali lagi, TERIMA KASIH MAS. Semoga dilain waktu saya dapat bertemu dengan Mas Gi dilain kesempatan. Sehat terus, Mas Gi!
4. **Dr. Aknolt Kristian Pakpahan, S.IP., M.A.** (Bang Tian) dan **Sapta Dwikardana, Ph.D.** (Mas Sapta) – Sebagai dosen penguji saat saya sidang Skripsi. Saya sangat berterima kasih kepada Mas Sapta dan Bang Tian yang telah memberikan masukan-masukan mengenai penelitian saya dalam Skripsi ini. Walaupun, saya jarang diajar oleh Mas Sapta dan Bang Tian, tetapi saya berterima kasih dengan ilmu-ilmu yang diberikan kepada saya terutama ilmu yang diberikan saat memberikan masukan terhadap Skripsi saya. Saya ingin berterima kasih kepada Mas Sapta sebagai salah satu inspirasi saya dalam melakukan penelitian ini yang berbasiskan kepada mata kuliah Kekuatan Jaringan Informasi Global (KJIG) dengan ilmu yang

diberikan sebagai landasan dalam topik saya ini. Sekali lagi, Terima kasih kepada Mas Sapta dan Bang Tian yang memberikan *input* terhadap penelitian di Skripsi saya ini.

5. **Fathya Nurul Meilianti** – Terima kasih, Sayang. Terima kasih atas segala support yang diberikan kepada saya. Sebagai *partner* hidup saya selama ini yang telah mendengar keluh kesah saya dalam menjalani Skripsi maupun permasalahan lainnya. Terima kasih telah menemani saya dari awal penulisan Skripsi ini dan yang telah mengingatkan saya untuk tetap fokus dalam mengerjakan penelitian di dalam Skripsi ini. Tanpa adanya kamu sebagai salah satu orang penting dalam hidup saya ini, mungkin Skripsi ini tidak akan selesai dengan tepat waktu. *Thank you for accompanying me until now.*
6. **Bandung United WA Version** – Dalam kesempatan ini saya ingin berterima kasih langsung kepada Rayhan (Rayy) dan juga Sembara yang mendengar keluh kesah baik mengenai persoalan Skripsi hingga persoalan non-skripsi. Terima kasih juga telah memberikan masukan-masukan mengenai *value* soal kehidupan dan pembelajaran ini. Lalu, untuk Sembara; terima kasih telah menjadikan rumah *maneh* menjadi tempat *basecamp* untuk tempat berkumpulnya *urang* sama Rayy, baik dalam mengerjakan Skripsi maupun sekedar *curhat-ceria* hingga malam hari. Makasih kalian!
7. **Cilla, Dana dan Megi** – Untuk Dana, terima kasih membantu untuk support dalam menenangkan mental *gw*. Saya tidak bisa berkata-kata lagi; *lu* adalah orang yang saat teman ada masalah akan membantu hingga masalah menjadi ringan. Untuk Megi, *lu* sama seperti Dana, kita emang sudah jarang ngobrol tetapi saat *gw* membutuhkan kalian. Kalian selalu support dalam permasalahan *gw*. Terima kasih, Kalian! Semoga kita dilain waktu dapat bertemu dan *ngopi* dengan Cilla tanpa adanya laptop dan melakukan *deep-talk*. Terima kasih! Terakhir, untuk Cilla; Terima kasihh, Cill!!!! Tanpa adanya *lu* mungkin Skripsi ini akan *stuck* disitu-situ aja dan berkat *lu* masalah-masalah Skripsi bisa terlewati. Terima kasih sudah mau diganggu dari awal seminar sampai akhir sidang, bahkan setelah sidang masih diganggu sama *gw*. Terima kasih telah menjadi teman untuk melakukan

brainstorming dalam menjalani Skripsi ini. Teman yang memberikan solusi hingga permasalahan dalam Skripsi ini terpecahkan. Semoga dilain waktu, kita bisa *ngopi* dan *sebat* sambil ngoborol sesi curhat-ceria bersama teman yang lain tanpa adanya laptop. *THANK YOU!*

8. **Pedjoeang Skripsi** – Rafi, Dika, Helmut, Adhi, Rayy, Iqbal, Sembara dan Fathur. Grup yang dibentuk pada saat setelah sidang seminar ini memiliki kenangannya tersendiri. Grup yang dibentuk untuk memberikan keluh kesah saya saat menjalani penelitian pada Skripsi ini. Grup yang memberikan semangat dengan caranya sendiri, entah dengan melakukan *distraction* seperti bermain game atau sekedar memberikan sebuah gambar atau video *meme* yang membuat *mood-booster* bagi penulis. Grup yang menjadi tempat segala informasi mengenai bagaimana penulisan Skripsi hingga bagaimana caranya untuk melalui birokrasi yang ada. Semoga kita dilain waktu dapat berkumpul secara *offline* ditempat sakral kita; kopiyor dan di Pares. Semoga juga dilain waktu kita dapat bermain *capsa* lagi, terima kasih kalian!
9. **Delegasi Russia (Tim Apresiasi)** – Rayy, Dika, Aldo, Iqbal, Sembara, Indita, Fathur, dan William. (*Alas*!) Terima kasih atas support yang diberikan kalian kepada saya. Terutama kepada Dika, Aldo, Iqbal yang sudah datang saat sidang saya dengan memberikan support secara langsung. Lalu, kepada kalian Indita, Sembara, Fathur, dan William semoga dilain waktu kita dapat bertemu kembali dan merumuskan kebijakan Russia dengan yang lainnya HAHA. Semoga delegasi ini bisa bertemu secara *offline* dan melakukan reuni bersama.
10. **Teman-teman di UNPAR** – Saya ingin memberikan ucapan terima kasih secara langsung kepada **Tasyar** sebagai teman *ngopi* saya, dan yang memberikan support secara langsung saat selesainya sidang. Terima kasih, *baturan urang*! Lalu, kepada **Audi** dan **Ranti** sebagai anak bimbingan Mas Gi yang sudah lulus tetapi masih membantu saya dalam melakukan penelitian ini dan selalu ditanya-tanya mengenai *behavior* yang bisa dilakukan sebagai anak bimbingan Mas Gi. Saya juga ingin berterima kasih kepada teman-teman bimbingan Mas Gi yaitu **Ribka** dan **Tina** yang saling

membantu dan memberikan support sesama anak bimbingan dari Mas Gi. Kepada **Farra** Jurusan Hukum 18 yang selalu saja memberikan support dengan mengirimkan makanan dan minuman kepada saya, Terima kasih ya kebaikanmu sangat berarti! Kepada teman-teman di **KSMPMI**, terima kasih telah memberikan pembelajaran bagi saya selama 1.5 Tahun, dan juga kepada divisi **ALF** sudah memberikan ilmu-ilmu mengenai bagaimana melakukan *review* yang baik dan benar. Terakhir, saya ingin berterima kasih kepada teman-teman saya yang memberikan support secara *virtual* baik melalui *Instagram* dan *chat* secara personal. Saya dengan kalian memang secara personal kurang dekat, tetapi dengan kehangatan yang diberikan kepada saya dan ucapan-ucapan dan kenangan yang diberikan saat selama 4 Tahun di HI UNPAR itu tidak terhitung kebaikannya bagi saya sendiri. Terima kasih semuanya, terutama kepada Angkatan HI 17. Sekali lagi, terima kasih semuanya!

11. **Teman-Teman Lainnya** – Terima kasih kepada teman-teman saya yang tidak disebutkan satu per satu dari teman dekat SMP hingga SMA. Terima kasih telah menjadi tempat buat cerita keluh kesah secara *random*, walaupun kita sudah jarang sekali untuk bertemu, tetapi *chemistry* itu tetap ada, terima kasih!
12. **Tempat Penulis Skripsian** – Kepada Kopi Eyang, Kaka Café, dan Kongdjie. Terima kasih kepada kalian yang memberikan waktu hingga tutup Café dan tidak dipernah diusir saat sedang menjalani skripsian. Cepat buka kalian, semoga PPKM saat ini cepat berlalu!
13. **Kepada Penulis** – *Last but not least, I wanna thank me; I wanna thank me for believing in me; I wanna thank me for doing all this hard work; I wanna thank me for having no days off; I wanna thank me for, for never quitting. I wanna thank me for just being me at all times, and I'm so proud of myself.* Selesai juga kan?

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

DAFTAR AKRONIM

AI	: Artificial Intelligence
BBC	: British Broadcasting Corporation
CCCPC	: Central Committee of the Chinese Communist Party
CDC	: Centers for Disease Control and Prevention
EICAR	: European Institute for Computer Antivirus Research
FCC	: Federal Communication Commission
GRPS	: Global Risks Perception Survey
IACS	: Industrial Automation and Control Systems
IBM	: International Business Machines
IEEE	: Institute of Electrical and Electronics Engineers
IISP	: Internet and Information Service Providers
IoBT	: Internet of Battlefield Things
IoMT	: Internet of Military Things
IoT	: Internet of Things
MNC	: Multinational Corporation
NSA	: National Security Agency
PBB	: Persatuan Bangsa-Bangsa
PDB	: Produk Domestik Bruto
PMS	: Preparation of Military Struggles

BAB I

PENDAHULUAN

1.1 Latar Belakang Masalah

Revolusi industri menjadi sebuah tolak ukur perkembangan dalam teknologi. Pada abad-21, perkembangan revolusi industri telah memasuki tahap keempat atau disebut sebagai Revolusi Industri 4.0. Perkembangan ini disebut sebagai perkembangan signifikan dalam perihal teknologi. Teknologi *Internet of Things* (IoT) dikembangkan pada revolusi industri keempat ini. Dalam IoT sendiri disebutkan sebagai menyatunya segala aktivitas baik secara fisikal dan non-fisik dalam internet dengan mengandalkan perangkat lunak (*Software*). *Software* tersebut menjadi sebuah perangkat yang digunakan untuk menyatukan seluruh perangkat. Dengan demikian, setelah fenomena ini terjadi diharuskan adanya penyimpan data yang mumpuni dikarenakan semakin banyaknya pengguna pada masa ini; penyimpanan tersebut disebut sebagai *Big Data*; Big Data mempunyai sebuah sistem yang terintegrasi.[1]

Big data sendiri sebagai bidang yang menangani cara menganalisis, mengekstrak informasi secara sistematis, atau menangani kumpulan data yang terlalu besar atau kompleks untuk ditangani oleh perangkat lunak aplikasi pemrosesan data tradisional. Data dengan banyak kasus (baris) menawarkan kekuatan statistik yang lebih besar, sementara data dengan kompleksitas yang lebih tinggi (lebih banyak atribut atau kolom) dapat menyebabkan tingkat penemuan

[1] Alasdair Gilchrist, *Industry 4.0: the Industrial Internet of Things* (New York?: Apress, 2016).

palsu yang lebih tinggi.[2] Tantangan big data meliputi pengambilan data, penyimpanan data, analisis data, pencarian, berbagi, transfer, visualisasi, kueri, pembaruan, privasi informasi, dan sumber data. Data besar awalnya dikaitkan dengan tiga konsep utama: volume, variasi, dan kecepatan. Saat kami menangani data besar, kami mungkin tidak mengambil sampel tetapi hanya mengamati dan melacak apa yang terjadi. Oleh karena itu, data besar sering kali menyertakan data dengan ukuran yang melebihi kapasitas perangkat lunak tradisional untuk memproses dalam waktu dan nilai yang dapat diterima.[3]

Terdapat pula ancaman terhadap big data sehingga dapat mengganggu *privacy* penggunanya. Salah satu ancaman yang biasanya ditemukan disebutkan sebagai *Malware*. Karakteristik malware sendiri layaknya *software* pada umumnya. Dimana memiliki tugas untuk memenuhi kepentingan penggunanya. *Malware* sendiri menjadi sebuah ancaman karena disebut sebagai perangkat lunak berbahaya, termasuk virus, *ransomware*, dan *spyware*. *Malware* biasanya terdiri dari kode yang dikembangkan oleh penyerang dunia maya, yang dirancang untuk menyebabkan kerusakan besar pada data dan sistem atau untuk mendapatkan akses tidak sah ke jaringan. *Malware* biasanya dikirim dalam bentuk link atau *file* melalui *email* dan mengharuskan pengguna untuk mengklik *link* atau membuka *file* untuk mengeksekusi *malware*.[4] *Malware* sebenarnya telah menjadi ancaman bagi individu dan organisasi sejak awal tahun 1970an ketika virus Creeper pertama kali

[2] Breur, Tom (July 2016). "Statistical Power Analysis and the contemporary "crisis" in social sciences". Journal of Marketing Analytics. 4 (2–3): 61–65. doi:10.1057/s41270-016-0001-3. ISSN 2050-3318
[3] Ibid.
[4] Archiveddocs, “Defining Malware: FAQ,” accessed September 28, 2020, https://docs.microsoft.com/en-us/previous-versions/tn archive/dd632948(v=technet.10)?redirectedfrom=MSDN.

muncul. Sejak itu, dunia telah diserang dari ratusan ribu varian *malware* yang berbeda, semuanya dengan tujuan menyebabkan gangguan dan kerusakan sebanyak mungkin.[5]

Namun, dari kompleksnya sistem yang ditawarkan oleh *big data* dan beberapa permasalahan seperti *malware*; banyaknya beberapa kepentingan menggunakan *big data* sebagai sebuah alat untuk mengetahui perilaku-perilaku pengguna. Pemerintah memiliki andil besar dalam menentukan regulasi-regulasi ini. Dimana pemerintah mengeluarkan peraturan dan regulasi untuk mengamankan penggunanya. Peran pemerintah sebagai penegak hukum dan dalam sistem ini memiliki peran sebagai regulasi untuk mengatur internet itu sendiri. Namun, dari sistem terintegrasi tersebut banyak disalahgunakan oleh para orang yang tidak bertanggung jawab untuk mengambil data yang berada di dalam sistem tersebut.[6]

Dalam beberapa tahun terakhir, Tiongkok telah terbukti dalam mengambil sebuah data-data pengguna dalam sistem big data. Salah satunya, pada bulan Agustus 2020. Perusahaan Tecno Mobile yang berbasiskan di Tiongkok terbukti memasukan sebuah malware ke dalam produknya. Pengguna di beberapa Negara Afrika melakukan klaim bahwa mereka secara otomatis melakukan pembayaran tanpa adanya persetujuan dari pengguna. Lalu, pada tahun 2019, Amerika Serikat di dalam Gedung putih ditemukan salah satu staff bahwa ponselnya terdapat malware untuk melakukan sadap. Dari beberapa kasus yang ditemukan bahwa

[5] "An Undirected Attack Against Critical Infrastructure" (PDF). United States Computer Emergency Readiness Team (Us-cert.gov).
[6] Trevor J Barnes, “Big Data, Little History,” Dialogues in Human Geography 3, no. 3 (2013): pp. 297-302, https://doi.org/10.1177/2043820613514323.

Tiongkok sendiri; dan berdasarkan artikel *Global local insight* bahwa Tiongkok belum memiliki regulasi yang kuat mengenai *data protection*.[7]

Berdasarkan apa yang telah dilakukan oleh Tiongkok bahwa menjadi sebuah permasalahan baru. Dimana Tiongkok mengambil data secara diam-diam melalui malware. Ada pun kemungkinan lainnya data tersebut dikirimkan kepada pemerintahnya. Kejadian tersebut dapat berpotensi untuk memicu *cyberwarfare* kedepannya karena Tiongkok sendiri melakukan penyerangan terhadap Amerika Serikat secara siber.

1.2 Identifikasi Masalah

1.2.1 Deskripsi Masalah

Big Data dan IoT dalam abad ke-21 ini memudahkan kinerja manusia, seperti dapat mencari informasi dan menyimpan data-data dengan mudah disebut sebagai Big Data. Big Data merupakan sebuah penyimpanan layaknya sebuah *hard drive* yang terintegrasi dengan internet, dengan demikian keamanan dari Big Data menjadi sebuah ancaman bagi para penggunanya. Negara menjadi wadah untuk merealisasikan Big Data untuk mengintegrasikan seluruh sistem yang ada untuk kemudahan masyarakatnya. Dengan adanya kemudahan yang diberikan, terdapat aktor yang memiliki kepentingan pribadi terhadap data-data tersebut, hal tersebut diharuskan membentuk sebuah badan atau organisasi untuk mengatur sistem dari Big Data tersebut dalam IoT. Organisasi dan badan tersebut memiliki fungsi sebagai melindungi kerahasiaan penggunanya. Negara sendiri sudah seharusnya

[7] Ning, Susan, and Han Wu. “International Legal Business Solutions - Global Legal Insights.” GLI - Global Legal InsightsInternational legal business solutions. Global Legal Group, 2020. https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/China.

melindungi apa yang menjadi hak bagi rakyatnya. Permasalahan ini muncul dimana terdapat beberapa negara dan *state-owned company* yang kurang menjaga keamanan pengguna dari Big Data Privacy dengan melakukan pencurian data menggunakan *malware* demi kepentingan pribadinya. *State-owned company* menjadi salah satu aktor dalam permasalahan ini, dika dilihat berdasarkan pemikiran Hart, Shleifer, dan Vishny pada tahun 1997 bahwa memang peran negara dalam suatu perusahaan bergantung kepada kontrak yang telah dibuat. Tetapi, terdapat beberapa situasi di mana pemerintah mengendalikan perusahaan dengan situasi di mana manajer swasta memegang kendali. Manajer dapat berinvestasi untuk menghasilkan inovasi yang mengurangi biaya dan meningkatkan kualitas, hingga berujung kepada pemerintah dan pengelola melakukan tawar menawar atas implementasi inovasi tersebut.[8]

Permasalahan ini sudah muncul sejak pada tahun 2010an. Dimana Tiongkok sudah melakukan aksi *cyberwarfare* terhadap Amerika Serikat. Aksi ini dilakukan dengan cara melakukan penyadapan terhadap kantor Google dan menyerang sistem *password* pada Google.[9] Spionase ini dilakukan oleh Tiongkok secara sepihak melalui kantor Google yang berada di Tiongkok. Adapun negara lainnya yang dijadikan sasaran oleh Tiongkok, seperti; Australia, Kanada, India, dan Taiwan.[10]

[8] O. Hart, A. Shleifer, and R. W. Vishny, "The Proper Scope of Government: Theory and an Application to Prisons," *The Quarterly Journal of Economics* 112, no. 4 (January 1997): pp. 1127-1161, https://doi.org/10.1162/003355300555448.
[9] Dean Cheng, *Cyber Dragon: inside China's Information Warfare and Cyber Operations* (Santa Barbara, CA, Canada: Praeger, 2017), 124.
[10] Kim Zetter, "Google Hack Attack Was Ultra Sophisticated, New Details Show," Wired (Conde Nast, January 14, 2010), https://www.wired.com/2010/01/operation-aurora/.

1.2.2 Pembatasan Masalah

Penulis hanya akan fokus terhadap apa yang dilakukan oleh Tiongkok dalam beberapa kasus dengan menggunakan *malware* dari tahun 2010 – 2019. Berdasarkan banyaknya kasus yang terjadi, kasus tersebut menargetkan sebuah pengguna dari negara, dari banyaknya kasus tersebut Tiongkok menargetkan Amerika Serikat dan beberapa aktor non-negara. Kasus yang dilakukan oleh Tiongkok salah satunya pada tahun 2010, Tiongkok melakukan operasi aurora dimana operasi ini menargetkan perusahaan swasta yang ada di Amerika Serikat, kasus ini disinyalir dilakukan oleh Tiongkok. Berdasarkan kasus-kasus yang melibatkan Tiongkok sebagai aktor atau *suspect* dalam melakukan spionase dari tahun 2010-2019, salah satunya tindakan operasi aurora, fokus penelitian berdasarkan kasus-kasus dalam penulisan ini akan dianalisis menggunakan *Cybersecurity Dilemma* yang diturunkan langsung berdasarkan teori *Security Dilemma* dan menggunakan konsep dari *surveillance capitalism* dengan melihat beberapa kebijakan Tiongkok dalam meningkatkan teknologi dalam agenda militer dan menggunakan kekuasaannya dalam Big Data dan sistem IoT-nya.

1.2.3 Perumusan Masalah

Melihat permasalahan yang terjadi dalam kasus *cyberwarfare* pada tahun 2010-2019, sudah seharusnya Tiongkok memberikan pengamanan terhadap privacy pengguna dari Big Data. Namun, dari beberapa kasus yang ditemukan sudah seringkali melakukan pencurian data dan spionase. Oleh karena itu, penulis merumuskan pertanyaan penelitian yaitu “Bagaimana Dampak Malware yang digunakan oleh Tiongkok dalam Big Data privacy pada tahun 2010 - 2019?”

1.3 Tujuan dan Kegunaan Penelitian

1.3.1 Tujuan Penelitian

Penulis akan memaparkan tindakan pemerintah Tiongkok dan beberapa perusahaan *state-owned* dalam menggunakan *malware* dalam Big Data Privacy. Hal tersebut dilakukan agar melihat korelasi antara aksi yang dilakukan oleh Tiongkok di berbagai negara yang terikat pada tahun 2010-2019. Kemudian, penulis akan mengaitkan hubungan penggunaan *malware* yang dilakukan oleh Tiongkok. Tindakan penggunaan *malware* ini bertujuan sebagai perlindungan domestik negaranya terhadap negara lain dan sebagai alat untuk meningkatkan keuntungan pribadi yang berpengaruh terhadap *data privacy*. Hal tersebut dilakukan agar penulis dapat menganalisis upaya Tiongkok dalam penggunaan *malware* di dalam *Big Data privacy* dan beberapa anomali yang dilakukan oleh Tiongkok.

1.3.2 Kegunaan Penelitian

1. Sebagai referensi dan pedoman bagi penulis lain yang hendak mengangkat topik mengenai *Big Data Privacy* dan penggunaan *malware* sebagai utilisasi yang berdampak kepada *cyberwarfare*.
2. Sebagai saran dan rekomendasi bagi pengguna dunia maya untuk selalu berhati-hati dalam Big Data yang sudah semakin pesat perkembangannya.

1.4 Kajian Literatur

Pemerintah dan perusahaan memiliki kepentingan dalam sistem *big data* ini. Berdasarkan jurnal yang berjudul *Big-Data Applications in the Government Sector* bahwa disebutkan perbedaan antara keduanya adalah bahwa pemerintah itu pada

dasarnya untuk mendapatkan keuntungan dengan menyediakan barang dan jasa, mengembangkan atau mempertahankan keunggulan kompetitif, dan memuaskan pelanggan dan pemangku kepentingan lainnya dengan memberikan nilai; sedangkan perusahaan tujuan utamanya adalah memelihara ketentraman rumah tangga, mencapai pembangunan berkelanjutan, mengamankan hak-hak dasar warga negara, dan meningkatkan kesejahteraan umum dan pertumbuhan ekonomi. Pada dasarnya pemerintah memiliki permasalahan dalam mengumpulkan *big data*.[11] Permasalahan yang biasa ditemukan berdasarkan dari banyaknya sumber dan format yang berbeda. Data tersebut dikumpulkan berdasarkan banyaknya *channel* (seperti; sosial media dan web) dan sumber yang berbeda (seperti negara, institusi, agensi, dan departemen). Berbagi data dan informasi antar negara merupakan sebuah tantangan khusus. Hal tersebut memiliki permasalahan dengan perusahaan, dimana kendala dalam mengumpulkan data-data yang diperlukan. Disebutkan bahwa dari kedua aktor tersebut memiliki sebuah kepentingan dalam menggunakan *big data* untuk mencari informasi yang aktor tersebut butuhkan.[12]

Berdasarkan jurnal yang berjudul *China's Cyber Warfare Capabilities* memberikan sebuah gambaran bagaimana potensi Tiongkok dalam melakukan aksinya dalam melakukan *cyberwarfare*. Peretas Tiongkok telah mampu dengan mudah mengatur 'ping' simultan yang cukup untuk merusak server Web yang dipilih (yaitu, serangan Denial-of-Service). Mereka telah mampu menembus situs Web dan merusaknya, menghapus data darinya, dan memposting informasi yang

[11] Kim, Gang-Hoon, Silvana Trimi, and Ji-Hyong Chung. "Big-Data Applications in the Government Sector." Communications of the ACM 57, no. 3 (2014): 78–85. https://doi.org/10.1145/2500873.
[12] Ibid.

berbeda tentang mereka (seperti slogan propaganda). Dan mereka telah mengembangkan berbagai virus yang cukup sederhana untuk disebarkan melalui email untuk menonaktifkan sistem komputer yang ditargetkan, serta program Trojan Horse yang dapat disembunyikan oleh email untuk mencuri informasi dari mereka. Namun, mereka hanya menunjukkan sedikit kemahiran dengan teknik peretasan yang lebih canggih. Virus dan *Trojan Horses* yang mereka gunakan cukup mudah untuk dideteksi dan dihapus sebelum terjadi kerusakan atau data dicuri. Tidak ada bukti bahwa pejuang dunia maya Tiongkok dapat menembus jaringan yang sangat aman atau secara diam-diam mencuri atau memalsukan data penting. Mereka tidak akan dapat secara sistematis melumpuhkan komando dan kendali yang dipilih, pertahanan udara dan jaringan intelijen dan basis data musuh tingkat lanjut, atau melakukan operasi penipuan dengan secara diam-diam memanipulasi data dalam jaringan ini.[13] Unit perang dunia maya Tiongkok telah sangat aktif, meskipun seringkali sangat sulit untuk menghubungkan aktivitas yang berasal dari Tiongkok dengan lembaga resmi atau swasta. Badan intelijen dan militer Tiongkok dapat dengan mudah memanfaatkan sektor korporat, termasuk tidak hanya operator telekomunikasi milik negara seperti Tiongkok Telecom Corporation tetapi juga apa yang disebut perusahaan 'swasta' yang menyediakan teknologi dan layanan telekomunikasi dan informasi.[14]

Tiongkok memiliki permasalahan mengenai *privacy*; dalam jurnal yang berjudul *China's personal information protection in a data-driven economy: A privacy policy study of Alibaba, Baidu and Tencent* memberikan sebuah analisis

[13] Ball, Desmond. "China's Cyber Warfare Capabilities." Security Challenges 7, no. 2 (2011): 81-103. Accessed October 12, 2020. https://www.jstor.org/stable/26461991.
[14] Ibid.

dimana *policy* yang ada di Tiongkok. Jurnal ini berusaha meneliti kebijakan privasi *Internet and Information Service Providers* (IISP) di Tiongkok, dalam studi ini menemukan bahwa kebijakan privasi mereka secara umum sesuai dengan ketentuan perlindungan informasi pribadi Tiongkok. IISP ini menggunakan mekanisme yang tepat yang menunjukkan komitmen, tindakan, dan penegakan mereka terhadap keamanan data, tetapi Praktik Informasi yang Adil mereka perlu ditingkatkan. Perlindungan informasi pribadi di Tiongkok sangat ketat. Kebijakan privasi menawarkan lebih banyak 'pemberitahuan' daripada 'pilihan'. IISP Tiongkok mengumpulkan dan menggunakan informasi secara ekstensif dengan kedok memberikan nilai kepada pengguna, tetapi tidak memberikan pertimbangan yang memadai untuk aliran data lintas batas dan perubahan kepemilikan. Mekanisme sosial dan teknologi belum banyak dicari.[15]

Jurnal ini membahas komparasi antara Tiongkok dan India, dimana kedua negara tersebut telah meluncurkan proyek besar yang bertujuan untuk mengumpulkan informasi pribadi penting mengenai lebih dari satu miliar populasi mereka dan dalam prosesnya membangun kumpulan data terbesar di dunia. Namun, baik Aadhaar di India dan Sistem Kredit Sosial di Tiongkok menimbulkan banyak masalah politik dan etika. Pemerintah mengklaim bahwa partisipasi dalam proyek-proyek ini bersifat sukarela, bahkan ketika mereka menghubungkan layanan penting dengan warga yang mendaftar pada proyek-proyek ini.[16]

---

[15] Fu, Tao. "China's Personal Information Protection in a Data-Driven Economy: A Privacy Policy Study of Alibaba, Baidu and Tencent." Global Media and Communication 15, no. 2 (2019): 195–213. https://doi.org/10.1177/1742766519846644.

[16] Shahin, Saif, and Pei Zheng. "Big Data and the Illusion of Choice: Comparing the Evolution of India's Aadhaar and China's Social Credit System as Technosocial Discourses." Social Science Computer Review 38, no. 1 (2018): 25–41. https://doi.org/10.1177/0894439318789343.

Membahas bagaimana media berita di India dan Tiongkok menjadi perantara data penting yang membentuk persepsi publik tentang data dan praktik teknologi melalui membingkai proyek-proyek ini sejak awal. Pemodelan topik menunjukkan bahwa liputan berita di kedua negara mengabaikan kepentingan publik dan sebagian besar berfokus pada bagaimana bisnis dapat memperoleh keuntungan darinya. Media, yang secara institusional dan ideologis terkait dengan pemerintah dan perusahaan, menunjukkan sedikit perhatian terhadap pelanggaran privasi dan pengawasan massal yang dapat ditimbulkan oleh proyek-proyek ini. Dalam jurnal ini berargumen bahwa hal tersebut dapat membuat warga secara struktural tidak mampu membuat "pilihan" yang berarti tentang apakah akan berpartisipasi atau tidak dalam proyek tersebut; implikasi untuk berbagai pemangku kepentingan dibahas.[17]

Dalam jurnal ini, penulis hanya mengambil data-data yang berkaitan dengan Tiongkok sebagai basis dalam melakukan penulisan ini. Data-data tersebut relevan dengan kasus dan permasalahan yang akan dianalisis oleh penulis. Dengan demikian, dapat disimpulkan bahwa hal yang terjadi dengan Tiongkok memiliki banyak relevansi dengan jurnal yang bersangkutan. Berdasarkan jurnal-jurnal tersebut; Tiongkok memiliki banyak kekeliruan dalam penerapan *big data* dan *privacy*. Hal tersebut akan menjadi argumen dan basis dari penulis untuk melakukan penelitian ini.

[17] Ibid.

1.5 Kerangka Pemikiran

Dalam pembahasan Dampak Penggunaan Malware oleh di Tiongkok dalam Big Data Privacy tahun 2010-2019, penulis menggunakan beberapa teori untuk menganalisa permasalahan ini. Dalam melihat dari tindakan yang dilakukan oleh Tiongkok dengan menggunakan malware di dalam pada kasus ini dengan menggunakan konsep dari *Security Dilemma*. Pemikiran *Security Dilemma* merupakan sebuah konsep yang terbentuk berdasarkan pemikiran Anarki (*Anarchy*). Thucydides menyebutkan bahwa Tidak ada batasan tentang apa yang bisa mereka lakukan, asalkan mereka cukup kuat. Dalam krisis yang sebenarnya, setiap entitas harus berjuang sendiri. Oleh karena itu, kekuatan dan kemandirian sangat penting, biasanya jauh lebih penting daripada moralitas atau keadilan. Kepercayaan dan kerjasama sulit didapat. Akibatnya, kehidupan di bawah anarki, dalam kutipan kata-kata yang dibentuk oleh ahli teori politik Inggris Thomas Hobbes berdasarkan pemikiran Thucydides bahwa anarki didasari dari "*solitary, poor, nasty, brutish, and short*."[18]

Dalam pendapat yang disampaikan oleh Thucydides bahwa yang terjadi di antara pemerintah menemukan adalah masalah lainnya. Negara modern sendiri ada dalam sistem anarkis yang masih belum memiliki otoritas eksternal. Dalam keadaan seperti itu, setiap negara harus menyediakan keamanannya sendiri. Tidak ada batasan nyata tentang apa yang dapat dilakukan untuk mencapai tujuan itu. Bahkan jika negara tidak memiliki tujuan untuk menaklukkan orang lain dan negara lain, negara harus selalu waspada terhadap apa yang mungkin dilakukan orang lain dan

[18] Ben Buchanan, *The Cybersecurity Dilemma Hacking, Trust and Fear Between Nations* (Oxford, United Kingdom: Oxford University Press, 2017).

negara lain. Bahwa pada dasarnya Anarki ini memfasilitasi *Security Dilemma*, dengan landasan ini Di dalamnya, Jervis dalam bukunya berjudul Cooperation under the *Security Dilemma* mengembangkan dua argumen penting. Pertama, ia menjelaskan bahwa *Security Dilemma* adalah kunci untuk memahami bagaimana dalam sistem internasional yang anarkis, negara-negara dengan tujuan yang secara fundamental kompatibel masih berakhir dalam persaingan dan perang. *Security Dilemma* muncul ketika banyaknya cara yang digunakan suatu negara untuk meningkatkan keamanannya menurunkan keamanan negara lain yang dapat memicu persaingan dan meregangkan hubungan politik. Kedua, dalam bukunya menjelaskan bahwa besarnya dan sifat *security dilemma* bergantung pada dua variabel: keseimbangan serangan-pertahanan dan diferensiasi pelanggaran-pertahanan. Akibatnya, *security dilemma* dapat berbeda antar ruang dan waktu. Meskipun negara-negara berada dalam kondisi anarki internasional yang tidak bervariasi, mungkin ada variasi yang signifikan dalam daya tarik sarana kooperatif atau kompetitif, prospek untuk mencapai tingkat keamanan yang tinggi, dan kemungkinan perang.[19]

John Herz sebagai seorang ilmuwan politik, pertama kali menciptakan istilah tersebut pada tahun 1950, dan Herbert Butterfield sebagai seorang sejarawan independen mengajukan konsep serupa tidak lama kemudian setelah apa yang dikemukakan John Herz. Negara dituntut harus menyediakan keamanan mereka sendiri dan akan berusaha untuk memperoleh banyak hal, dan menciptakan kekuasaan untuk meminimalkan risiko yang ditimbulkan oleh negara lain. Namun, ketika sebuah negara memperkuat dirinya sendiri dan meningkatkan kemampuan

[19] Ibid.

suatu negara untuk tumbuh secara tidak sengaja akan mengancam negara lain. Negara-negara lain itu akan mengenali kelemahan relatif dan serangan ketakutan mereka sendiri. Biasanya tidak dapat beralih ke arbiter eksternal, mereka perlu mengembangkan kekuatan mereka sendiri dan menyediakan keamanan mereka sendiri, memulai rangkaian peristiwa yang berpotensi berbahaya.[20]

Seiring berjalannya waktu, dengan perkembangan teknologi dalam Revolusi Industri 4.0 dalam pemahaman mengenai *Security Dilemma* mengalami perubahan. Pemahaman tersebut mengalami perubahan dari yang didasari penguatan dasar negara dalam bentuk militer secara umum, tetapi dalam Revolusi Industri 4.0 ini memiliki hal penting lainnya untuk dimiliki oleh negara; yaitu dalam penguatan dalam ranah *cyberspace*. Ben Buchanan dalam bukunya menyebutkan beberapa faktor negara untuk melakukan penguatan ini, berawal dari adanya "pengacau" dari segi keamanan konvensional. Pada 2010, terjadinya penyerangan terhadap sistem komputer di Iran. Saat dilakukan penelitian lebih lanjut bahwa ditemukan sebuah kode berbahaya dan menemukan tanda yang tidak biasa. Kode tersebut menyebar ke komputer lainnya dengan metode yang tidak diketahui sebelumnya. Sistem yang terprogram menargetkan sistem kontrol industri dengan cara yang sangat tepat. Penyelidik akhirnya akan menyimpulkan bahwa tujuannya adalah sabotase rahasia program nuklir Iran. Penyidik menyebut kode berbahaya Stuxnet, nama yang berasal dari kombinasi beberapa filenya. Pemeriksaan forensik dan kebocoran pers akhirnya mengungkapkan bahwa kode tersebut kemungkinan merupakan bagian dari operasi Amerika-Israel. Serangan digital terhadap fasilitas nuklir Iran Natanz secara diam-diam menghancurkan sekitar seribu sentrifugal yang

[20] Ibid.

memproses bahan nuklir, hampir seperlima dari semua perangkat pengayaan uranium Iran.[21]

Dengan semakin berkembangnya terhadap penyerangan dalam jaringan publik maupun jaringan privasi. Dikembangan jaringan pengaman dalam menghindari penyerangan yang dilakukan oleh beberapa sektor pengamanan. Salah satunya, di Amerika Serikat membentuk suatu program dinamakan sebagai Byzantine Candor oleh *National Security Agency* (NSA). Program ini dijalankan untuk mengantisipasi dalam penggunaan dan serangan dari *malware*.[22] Program ini semakin jelas bahwa *security dilemma* secara konvensional sudah menjadi kurang relevan dalam Revolusi Industri 4.0, dikarenakan negara-negara mulai menguatkan jaringan dan sistem teknologinya agar tidak mudah diretas oleh orang yang tidak bertanggung jawab.

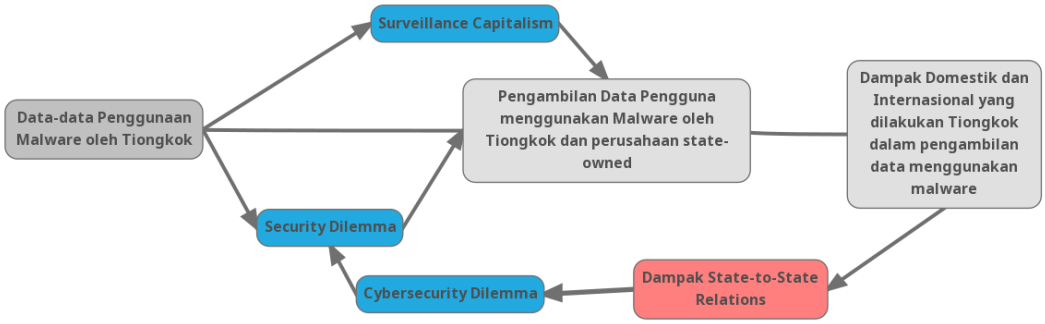
Pada penelitian ini juga bahwa *Big Data* sebagai sebuah akomodasi yang diambil dikarenakan menjadi hal penting bagi negara yang digunakan. *Surveillance capitalism* merupakan sebuah konsep pemahaman yang muncul pada tahun 2014an, yang dikembangkan oleh Shoshana Zuboff dalam bukunya yang berjudul *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* disebutkan bahwa terjadinya Surveillance capitalism ini dimana adanya transaksi terbarukan; yang dimaksud ditemukannya sebuah material baru dalam sebagai barang transaksi. Konsep ini menjelaskan bahwa material baru yang disebutkan merupakan sebuah Big Data, Big Data yang dimaksud ialah sebuah kebiasaan manusia yang terekam secara online dan disimpan dalam sebuah cloud

[21] Ibid.
[22] Ibid.

server.[23] Sebuah aktor dalam melakukan transaksi ini memiliki sebuah kepentingannya sendiri. Konsep ini berkembang dimana pada saat awal mula perkembangan teknologi yang semakin pesat; dan juga dimana orang pada saat itu menggunakan data-data untuk *advertisement*. Aktor pertama dalam melakukan ini adalah perusahaan, perusahaan menggunakan big data untuk mempelajari *human natural habits on their smartphone*; perusahaan mempelajari hal itu untuk mencari target dari pasar mereka. Lalu, Platform seperti google dan beberapa media online lainnya melakukan penjualan data untuk mengambil keuntungan.[24]

Tulisan ini akan menggunakan konsep-konsep telah dijelaskan tersebut untuk memaparkan dan menganalisa dampak penggunaan *malware* yang dilakukan oleh Tiongkok dan beberapa perusahaan. Kerangka pemikiran tersebut dapat dijelaskan melalui gambar bagan di bawah ini:

Gambar 1.1: Operasionalisasi Teori



[23] Zuboff, S. (2020). The age of surveillance capitalism: The fight for a human future at the new frontier of power. New York: PublicAffairs.
[24] *The social dilemma*. Dir. Jeff Orlowski. Netflix, 2020. Documentary.

1.6 Metode Penelitian dan Teknik Pengumpulan Data

1.6.1 Metode Penelitian

Metode penelitian yang digunakan adalah metode penelitian secara *mixed method*, namun *mixed method* yang digunakan akan fokus kepada kualitatif. Dikarenakan peneliti akan menggunakan data sebagai sumber utama dengan menggunakan teori secara *explicit* sebagai landasan utama dalam melakukan penelitian ini. Metode ini juga bertujuan untuk mengkonstruksikan realita sosial dengan melibatkan makna dan nilai-nilai secara eksplisit dengan data-data yang ditemukan oleh penulis.[25] Penulis akan meneliti dari data yang tersedia dalam bentuk sumber teks dan gambar.[26] Penelitian *mixed method* ini fokus kepada kualitatif juga akan bertujuan untuk memperoleh pemahaman mendalam mengenai pengalaman, perspektif, dan hubungannya dengan aktor dengan menggunakan secara konteks sensitif.

1.6.2 Teknik Pengumpulan Data

Hal ini dilakukan agar penulis dapat memahami nilai-nilai yang digunakan oleh Tiongkok dalam menggunakan kekuatannya untuk menggapai suatu kepentingan yang diperoleh. Dalam hal ini, Tiongkok menggunakan Data dalam *Big Data Privacy* untuk memperoleh informasi yang diinginkan. Metode penelitian kualitatif yang digunakan akan merefleksikan data dengan menganalisa data yang disajikan. Data tersebut akan direpresentasikan untuk menunjukkan hasil potensial

[25] John W. Creswell, "The Selection of a Research Design" dalam Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, 3rd ed., (California: SAGE Publications Inc., 2009)
[26] John W. Creswell, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, 4th ed., (Thousand Oaks: SAGE Publications Inc., 2014)

yang dapat dicapai.[27] Teknik pengumpulan data yang dilakukan dalam penelitian ini menggunakan media, dan berita yang akan dianalisis pada penelitian nanti. Media dan berita nanti akan menjadi pendukung dalam melakukan penelitian ini.

1.7 Sistematika Pembahasan

Penelitian ini akan dibagi ke dalam empat bab. Pada bab satu, penulis akan membahas latar belakang masalah yang diteliti mengenai permasalahan yang dialami Tiongkok sebagai aktor dalam melakukan pengambilan data secara illegal. Penulis juga akan menyajikan identifikasi masalah, pembatasan masalah, perumusan masalah, tujuan dan kegunaan penelitian, teori dan konsep yang akan dipakai, metode penelitian, serta teknik pengumpulan data yang akan digunakan. Pada bab kedua, akan membahas pergerakan Revolusi Industri hingga masuk ke dalam ranah 4.0, dan penjelasan mengenai perannya Big Data *dan Internet of Things* (IoT) dalam negara Tiongkok. Lalu, pada bab ini juga membahas terdapat ancaman baru di dalam Revolusi Industri 4.0. Lalu, pada bab ketiga akan menjelaskan pergerakan Tiongkok dari tahun 2010-2019 dan apa yang menjadi target dari Tiongkok. penulis juga akan membahas bagaimana Tiongkok menggunakan data-data dan apa kepentingannya bagi Tiongkok itu sendiri. Lalu, bagaimana tiongkok menggunakan data tersebut. Pada bab ini akan dianalisis menggunakan konsep-konsep *surveillance capitalism* dan teori *security dilemma* yang memiliki konsep tersendiri dalam Revolusi Industri 4.0 yaitu konsep *cybersecurity dilemma* dari Tiongkok. Dalam bab ini juga penulis akan membahas pengaruh dan dampak *state-to-state relations* yang dilakukan oleh Tiongkok

[27] Ibid. 183.

berdasarkan negara-negara yang menjadi target dari Tiongkok. Pada bab keempat, penulis akan menarik sebuah kesimpulan berdasarkan analisis dan penelitian pada penulisan ini.