BAB I

PENDAHULUAN

1.1 Latar Belakang

Penelitian ini berupaya melihat ancaman seperti apa yang diciptakan oleh pemanfaatan *cyberspace* di Tiongkok terhadap keamanan nasional negaranya. Hal ini berangkat dari kebijakan yang diterapkan oleh pemerintah Tiongkok terhadap pemanfaatan *cyberspace* dinegaranya. Pemerintah Tiongkok yang menerapkan kebijakan sangat bertolak belakang terkait pemanfaatan *cyberspace*, menjadikan penelitian ini menarik demi mengetahui ancaman apa yang diciptakan oleh pemanfaatan *cyberspace* terhadap keamanan nasional Tiongkok sehingga Pemerintah Tiongkok menerapkan kebijakan yang sangat kompleks tersebut.

> *"Technology will make it increasingly difficult for the state to control the information its people receive. The Goliath of totalitarianism will be brought down by the David of microchip"*[1]

Pernyataan diatas dikemukakan oleh Ronald Reagan pada pidatonya di London's Guildhall pada tahun 1989, dimana pada saat itu ide mengenai keamanan masih sangat lekat dengan hal-hal yang bersifat militeristik. Fokus yang sering digunakan ketika membahas isu keamanan berkisar antara kemampuan militer yang dimiliki sebuah negara untuk menghadapi ancaman yang muncul terhadap negaranya. [2] Namun kritik mengenai pembatasan ide yang bias secara budaya (*ethnocentric*) dan terlalu dangkal memunculkan argumentasi-argumentasi mengenai pentingnya

[1] Shanti Kalatil dan Taylor C, Boas. *Open Networks, Closed Regimes* (Washington: Carnegie Endowment for Internastional Peace, 2003) hal. 1
[2] John Baylis, *Internasional and Global Security in Post Cold War Era* (New York: Oxford University Press USA, 2013) hal 253

perluasan kajian, keluar dari batasan sempit keamanan secara tradisional dan menyertakan bahasan lain yang relevan kedalamnya.[3] Hal tersebut memunculkan kajian mengenai isu-isu keamanan non-tradisional yang mencakup isu-isu lain termasuk teknologi. *Cyberspace*[4] adalah bentuk perkembangan teknologi yang belakangan sering dikaitkan dengan kajian keamanan. Nazli Choucri dalam tulisannya yang berjudul *Cyberspace and International Relations; Toward an Integrated System* menyatakan bahwa sebelumnya isu *cyberspace* merupakan permasalahan *low politics*, namun dengan beberapa kejadian seperti kebocoran dokumen rahasia negara di wikileaks, *cyber attack* di Georgia dan Estonia, serta penggunaaan serangan berbasis *cyber* untuk menurunkan kemampuan nuklir iran *cyberspace* sudah merupakan permasalahan yang perlu dibahas di level *high politics*.[5]

Cyberspace dalam kaitannya dengan dinamika hubungan internasional memang memperlihatkan pengaruh yang sangat signifikan belakangan ini. Selain membawa beragam kemudahan bagi berbagai aspek kehidupan bernegara, *cyberspace* juga telah menghadirkan sebuah realitas baru yang menjadi sumber bagi kerentanan, potensi ancaman terhadap keamanan nasional dan kegaduhan terhadap

[3] *Ibid*

[4] Cyberspace didalam *The US National Strategy to Secure Cyberspace* (Februari 2003) mengacu kepada sebuah domain yang dibentuk dari keseluruhan komputer yang saling terhubung satu sama lain, server, router, kabel optik, yang kemudian memungkinkan terjadinya pertukaran informasi dalam jumlah yang sangat besar dan juga memungkinkan berfungsinya infrastruktur-infrastruktur penting negara. Terdiri atas empat elemen: a. Individu yang memakai b. informasi yang beredar di dalamnya c. blok-blok logika (*Logical building blocks)* dan d. fondasi fisik

[5] Nazli Choucri dan David Clark, *Cyberspace and International Relations; Toward an Integrated System* (Massachusettes: MIT press. 2011) hal 2

tatanan internasional.[6] Hal ini bahkan diakui oleh pemerintah Amerika Serikat melalui pernyataan presiden Obama, bahwa ancaman yang hadir melalui *cyberspace* berpotensi melemahkan kepercayaan diri negara dalam sistem informasi yang endasari kepentingan ekonomi dan keamanan nasional negara.[7] Diperkuat dengan pendirian *Cyber Command* di militer AS sebagai pengakuan atas potensi ancaman *cyber* yang dapat melemahkan keamanan dan kesejahteraan negara.[8]

Ancaman yang hadir melalui *cyberspace* menurut Forest Hare dalam artikelnya yang berjudul *The Cyber Threat to National Security; Why Can't We Agree?*, bersifat sangat luas sekaligus juga unik; luas dari cakupan agen pembawa ancaman (*threat agent*) yang bisa saja adalah negara, teroris, pelaku kriminal, ataupun *hacker*, serta luas dari beragamnya bentuk ancaman dan juga targetnya.[9] Namun menurut Hare setiap negara akan memiliki kerentanan yang berbeda terhadap ancaman ini, kerentananan tersebut menurutnya ditentukan oleh karakteristik masing-masing negara. Sebuah ancaman bagi satu negara belum merupakan ancaman bagi negara lain. Bagi negara-negara demokrasi seperti Amerika Serikat sendiri, seperti dinyatakan sebelumnya, *cyberspace* masih merupakan sebuah potensi yang mampu melemahkan kepercayaan diri negara terkait keamanan nasional negaranya, kemudian bagaimana dengan negara otoritarian seperti Tiongkok yang pada kenyataannya juga memanfaatkan *cyberspace* secara maksimal dalam kehidupan bernegaranya.

---

[6] *Ibid*
[7] Forrest Hare, *The Cyber Threat to National Security; Why Can't We Agree?* (Washington: School of Public Policy, George Mason University. 2010) hal 212
[8] Nazli Choucri dan David Clark, hal.2
[9] Forest Hare, hal. 213

Tiongkok termasuk negara otoriter yang paling awal membuka diri dan memanfaatkan *cyberspace* dalam berbagai lini kehidupan bernegaranya.[10] Hal ini tentu diluar dugaan para penstudi HI mengingat dilema yang dibawa oleh *cyberspace* kepada negara-negara serupa Tiongkok sebagaimana yang dinyatakan oleh Nina Hachigian berikut ini;

> *"The Internet presents a dilemma to leaders of authoritarian states and illiberal democracies. It promises enticing commercial advantages, such as transaction cost reductions, e-commerce possibilities, and foreign trade facilitation. Yet, by giving citizens access to outside information and platforms for discussion and organization, the Internet can also help politically empower populations and potentially threaten regimes"*[11]

Namun terlepas dari hal itu, kebijakan *reform and opening* yang dibuat oleh Deng Xiaoping pada tahun 1978; menjadikan pertumbuhan ekonomi sebagai landasan legitimasi partai yang utama disamping ideologi, menjadi awal penggunaan *cyberspace* secara luas di Tiongkok.[12] Sejak transformasi tersebut, *cyberspace* secara bertahap menjadi ruang yang banyak dimanfaatkan tidak hanya dalam perekonomian namun juga berbagai aspek kehidupan bernegara lainnya di Tiongkok.[13] Selain ditujukan untuk mengawali digitalisasi di jaringan telekomunikasi Tiongkok, pemerintah Tiongkok juga memanfaatkan *cyberspace* sebagai infrastruktur untuk meningkatkan kontrol administrasinya terhadap Pemerintah provinsi dan daerah, meningkatkan kapasitas kepemerintahan dan kewenangannya serta stabilitas

[10] Nina Hachigian, *The Internet and Power in One Party East Asian States* (Washington: The Washington Quarterly, 2002) hal 41
[11] *Ibid*, hal. 41
[12] Nina Hachigian, *China's Cyberstrategy* (New York: Foreign Affairs, 2001) hal. 120
[13] *Ibid*, hal. 120

sosiopolitik.[14] Pada tahun 1998 pemerintah mengumumkan *"Government Online Project"*, 1999 sebagai tahun pemerintahan online dan tahun 2000 ditetapkan sebagai tahun bisnis online. Jaringan *e-government* dan *e-commerce* yang dibangun berhasil meningkatkan kesempatan bisnis dan transparansi informasi mengenai hukum dan perundang-undangan di Tiongkok.[15] Tercatat lebih dari 80% dari pemerintah lokal dan nasional mempunyai website yang walaupun jika dibandingkan dengan negara-negara EU kurang dipelihara dengan baik.[16] Ditambah lagi jumlah penduduk Tiongkok yang memanfaatkan *cyberspace* tergolong sangat banyak, menurut laporan statistik tahun 2015 dari CNNIC (*Chinese Internet Network Information Center)*, terdapat 649 Juta pengguna internet di Tiongkok dengan rasio penetrasi internet[17] sebesar 49,7%.[18] Fakta-fakta tersebut mengimplikasikan pemanfaatan internet sangat luas di Tiongkok.[19]

Permasalahan muncul ketika dalam perkembangannya, Tiongkok kembali menutup celah yang sebelumnya dibuka oleh Deng Xiaoping tersebut dengan pembatasan-pembatasan melalui kebijakan yang diterapkan terkait *cyberspace*. Masuknya Tiongkok ke WTO pada tahun 2000 misalnya; keanggotaan yang mewajibkan kesepakatan negara untuk melonggarkan kontrol terhadap kepemilikan

[14] Chin-fu Hung, *The Political Impact of the Internet in the People's Republic of China: A Critical Perspective* (Coventry. Department of Politics and International Studies University of Warwick) hal. 3

[15] Guoguang Wu. *In the name of good governance: E-government, Internet pornography, and political censorship in China.* dalam X. L.Zhang & Y. N. Zheng. *China's information and Communications technology revolution: Social changes and state responses* (New York: Routledge. 2009) hal. 68–85

[16] *Ibid*

[17] Rasio penetrasi internet dapat diartikan sebagai porsi populasi dari sebuah negara yang mendapatkan akses internet.

[18] CNNIC. *Statistical Report on Internet Development in China* (Beijing: CNNIC, 2015) hal.25

[19] Cristopher R. Hughes, *China and the Globalization of ICTs: Implications for International Relations* (London: Sage Publication, 2002) hal. 207

sektor telekomunikasi, sempat memunculkan optimisme bagi beberapa pihak terhadap peluang-peluang yang akan tercipta di Tiongkok.[20] Namun bergabungnya Tiongkok di WTO tidak membuat aliran investasi ke telekomunikasi negara ini lebih mudah, karena Tiongkok memanfaatkan sebuah pra-kondisi dalam persetujuan tersebut, bahwa didalam operasionalisasi persetujuan ini, negara dapat pula menerapkan peraturan yang berlandas kepada perlindungan konsumen dan penjagaan terhadap keamanan dan kepentingan nasional negara.[21]

Kondisi itulah yang dimanfaatkan oleh pemerintah Tiongkok untuk tetap melakukan kontrol ketat terhadap *cyberspace*. Tiongkok memperkenalkan peraturan untuk meningkatkan kontrol negara terhadap internet pada 25 Desember 2000 yang antara lain mencakup kewajiban semua ISP (*internet service provider*) untuk mengobservasi segala aktifitas dan konten yang ada di server mereka, menyimpan semua data konten dan pemakainya kemudian melaporkannya secara rutin kepada pemerintah. Terdapat banyak sekali konten yang masuk kedalam daftar *blacklist* pemerintah, termasuk didalamnya kejahatan *cyber*, tindakan yang "melanggar prinsip-prinsip dasar konstitusi", "merusak persatuan nasional", "merusak persatuan antar suku", "mengusik kebijakan negara dengan propaganda agama", serta tindakan yang akan "mengganggu stabilitas sosial". Daftar di atas tidak begitu jelas objeknya sampai diketahui bahwa di dalam pasal pertama perundang-undangan Tiongkok disebutkan bahwa ancaman terhadap persatuan tersebut adalah Taiwan, Tibet dan

[20] *Ibid*
[21] *Ibid* hal. 207

wilayah islam di Xianjiang termasuk juga Falun Gong.[22] Ancaman terhadap stabilitas sosial mencakup semua aspek yang tidak terbatas, termasuk didalamnya konten pro demokrasi.[23]

Terdapat lima peraturan lagi yang diumumkan pada tahun yang sama, sebagaimana dikutip sebagai berikut;

> *"In 2000 alone, six major regulations on Internet content control were promulgated by the National People's Congress, the State Council, and the Ministry of Infor-mation Industry, not including the various decrees that were announced by other ministerial units and regulations that were passed by provincial governments."*[24]

Rangkaian peraturan ini dilanjutkan pada tahun 2002; pemerintah Tiongkok menyensor sebagian besar isi dari sumber informasi dan hanya memperbolehkan pidato yang "benar secara politik" untuk dipublikasikan melalui *cyberspace*, yang berarti bahwa konten yang dirasa berbahaya bagi kepentingan dan reputasi negara akan dihapus.[25]

Tidak sampai disana saja, pada bulan oktober 2011, Kementerian Keamanan publik (*Ministry of Public Security*) Tiongkok mendesak polisi untuk menggunakan *microblogs*[26] untuk menggiring opini publik dan memperhatikan isu-isu yang tengah hangat dibicarakan melalui *cyberspace*.[27] Pemerintah Tiongkok menciptakan kesatuan

---

[22] *Ibid*
[23] *Ibid*
[24] Annes.Y. Cheung, *The Business of Governance: China's Legislation on Content Regulation in Cyberspace* (Los Angeles: Conference Paper pada China and the Internet Conference, 2003)
[25] *Ibid* hal. 3
[26] Microblogs adalah gabungan antara *social networking* dengan *mini blogging*, dimana konten dengan kuantitas yang minim (dikenal dengan istilah "Update") didistribusikan secara online dan juga melalui jaringan *Mobile Phone*. Twitter jelas-jelas adalah *leader* dalam bagian ini
[27] Richard Fontaine dan Will Rogers. *China's Arab Spring Cyber Lessons* http://thediplomat.com/2011/10/03/China%E2%80%99s-arab-spring-cyber-lessons/ Diakses pada 4 november 2012

khusus yang disebutnya *cyber police* untuk melaksanakan pengawasan terhadap internet di Tiongkok. Kompleksitas upaya kontrol yang dilakukan oleh pemerintah Tiongkok terhadap penggunaan *cyberspace* ini bahkan menempatkan Tiongkok sebagai negara dengan rezim filtering internet tercanggih di dunia.

> *"The OpenNet Initiative project (ONI), a partnership of researchers at the University of Toronto, Harvard Law School and Cambridge University, has a mission "to investigate and challenge state filtration and surveillance practices". Its country study on China, released in April 2005, concludes that "China's Internet filtering regime is the most sophisticated effort of its kind in the world," and that it "involves numerous state agencies and thousands of public and private personnel."*[28]

Kebijakan yang kompleks ini tentu menimbulkan sebuah pertanyaan mengenai apa yang mendasarinya. Sementara menurut Jennifer Jackson Preece, keamanan nasional dapat mengacu kepada kebijakan publik yang dengannya negara mengusahakan kelangsungan dan kedaulatannya sebagai sebuah institusi dan juga keamanan dan kesejahteraan bagi rakyatnya.[29]

Penjelasan diatas menjadikan penelitian ini menarik demi mengetahui ancaman apa yang diciptakan oleh pemanfaatan *cybrspace* terhadap keamanan nasional Tiongkok. Dan seperti yang dinyatakan oleh Hare dalam artikelnya bahwa setiap negara memiki kerentanannya masing-masing dalam isu *cyber-security* maka ancaman bagi keamanan pemerintah AS atau negara lainnya belum tentu merupakan ancaman keamanan bagi pemerintah Tiongkok. Berdasarkan uraian di atas, maka

---

[28] Joseph Y. S Cheng, *The Chinese Authorities' Control of the Internet and the Challenge of Democratisation* (Karlsruhe: Zentrum für Angewandte Kulturwissenschaft und Studium, 2012) hal. 1

[29] Jennifer Jackson-Preece. *Security in International Relations* (London: University of London, 2011) hal. 30

menarik untuk dikaji mengenai ancaman apa yang diciptakan oleh pemanfaatan *cyberspace* di Tiongkok terhadap keamanan nasionalnya.

1.2 Rumusan Masalah

Pemanfaatan *cyberspace* secara masif di Tiongkok adalah kebijakan yang berada diluar dugaan penstudi Hubungan Internasional, mengingat keberadaan Tiongkok sebagai negara sosialis dan *cyberspace* sebagai domain yang memungkinkan kebebasan pertukaran informasi dalam jumlah yang sangat besar. Ditengah pemanfaatan ini pemerintah Tiongkok juga melakukan kontrol ketat terhadap pemanfaatan dan perkembangan *cyberspace* yang bahkan menempatkannya sebagai negara dengan sistem filtering internet paling canggih di dunia. Hal ini tentu memunculkan keingintahuan mengenai hal-hal yang melatar belakangi kebijakan pemerintah yang sangat bertolak belakang tersebut.

1.3 Pertanyaan Penelitian

Berdasarkan latar belakang dan rumusan masalah diatas maka pertanyaan penelitian ini adalah *ancaman seperti apakah yang diciptakan oleh pemanfaatan cyberspace terhadap keamanan nasional Tiongkok?*

1.4 Tujuan Penelitian

1. Mendeskripsikan *cyberspace* sebagai isu kontemporer yang muncul dalam kajian keamanan.
2. Mendeskripsikan perkembangan *cyberspace* di Tiongkok serta kebijakan-kebijakan yang diterapkan oleh pemerintah Tiongkok dalam mengontrolnya.
3. Menganalisis pengaruh pemanfaatan *cyberspace* terhadap keamanan nasional Tiongkok; ancaman seperti apa yang disebabkannya.

1.5 Manfaat Penelitian

a. Memberikan kontribusi dalam mengambangkan khasanah ilmu pengetahuan, sehingga dapat memperkuat teori-teori mengenai pengaruh *cyberspace* terhadap dinamika hubungan internasional
b. Meningkatkan kemampuan penulis dalam menjalankan aktivitas dan usaha-usaha penelitian dan merumuskan analisis dalam rangka memenuhi tanggung jawab sebagai akademisi
c. Menambah referensi dan pengetahuan bagi peneliti selanjutnya.

1.6 Studi Pustaka

Beberapa ahli dan sarjana ilmu sosial telah mencoba mengkaji pengaruh yang disebabkan oleh *cyberspace* terhadap tidak hanya pada aspek keamanan negara saja, tetapi berbagai aspek dari kehidupan bernegara lainnya. Pada penelitian ini, akan ditampilkan beberapa tulisan yang juga menelaah mengenai permasalahan ini dan kemudian akan mendukung penelitian penulis.

Pertama untuk melihat signifikansi isu *cyber-security* di dalam kehidupan negara, Forrest Hare dalam tulisannya yang berjudul *The Cyber Threat to National Security: Why Can't We Agree* ia mencoba meyakinkan pendapatnya mengenai signifikansi *cyber threat* atau ancaman dari dunia maya terhadap keamanan negara. Signifikansi tersebut menjadikan *cyber threat* isu yang layak dibahas dalam studi keamanan sehingga relevan untuk dikaji dengan teori dan konsep-konsep yang ada dalam kajian keamanan. Banyak sekali isu *cyber threat* yang kemudian mempengaruhi keamanan sebuah negara, yang prioritas dan solusinya belum disepakati dalam level multilateral. Fakta ini kemudian berpengaruh kedalam proses

pemecahan masalah tersebut, sebab jika belum ada rumusan yang jelas secara multilateral mengenai isu mana yang harus diprioritaskan dan langkah-langkah apa yang akan ditempuh maka tentu proses penyelesaiannya belum dapat dilaksanakan.[30]

Didalam tulisan ini Hare juga menawarkan sebuah kerangka berpikir untuk menganalisis masalah *cyber threat*, selama belum ada kesepakatan multilateral mengenainya, yaitu dengan menggunakan kerangka berpikir yang dikembangkan oleh Buzan. Melalui model tersebut, analis dapat mengklasifikasikan sensitifitas negara terhadap isu *cyber security*, menurutnya masing-masing negara memiliki titik rentan masing-masing terhadap isu *cyber threat* yang dapat dianalisis melalui kekuatan (*power)* dan kepaduan sosial politik (*socio-politic cohesion*) sebuah negara. Dengan klasifikasi ini analis dapat melihat dan mengevaluasi prioritas serta kebijakan yang diambil negara dalam ranah *cyber threat*.

Secara umum tulisan Hare ini menggambarkan variasi ancaman yang disebabkan oleh *cyberspace* terhadap negara. Beragamnya ancaman tersebut menurut Hare menyebabkan kesulitan penyelesaian secara multilateral. Tulisan Hare ini sangat mendukung penelitian yang akan penulis lakukan dengan menggambarkan signifikansi *cyber threat* terhadap kajian keamanan terutama keamanan nasional negara.

Literatur kedua berjudul *Cyber Security Threat Characterization* merupakan laporan penelitian oleh Neil Robinson dkk atas permintaan dari *Swedish Cabinet Office and Department of Defence* kepada Akademi Pertahanan Nasional Swedia dan Pusat kajian Ancaman Asimetris yang kemudian dilimpahkan kepada RAND eropa

[30]Hare, hal 212

demi mengetahui karakteristik ancaman dari *cyber security* negara. Negara-negara yang menjadi studi kasus adalah sepuluh negara meliputi Inggris, Kanada, Denmark, Estonia, Finlandia, Perancis Jerman, Belanda, Rusia, dan Amerika Serikat ditambah dua Organisasi Internasional meliputi NATO dan EU. Penelitian mereka ditujukan untuk menjawab pertanyaan: pertama, bagaimana cara memprioritaskan *cyber threat* dan bagaimana hubungannya dengan isu di level keamanan nasional lainnya? Kedua, apa tipe spesifik dari ancaman yang datang dari cakupan *cyber security?* Ketiga, Organisasi mana yang memiliki kebijakan terkait peran, tanggung jawab dan *agencies' scope*? Peran apa yang dimainkan oleh agen "penegak hukum" dan di konteks mana mereka sesuai?

Dari penelitian yang mereka lakukan dapat disimpulkan bahwa ancaman terhadap *cyber security* sudah menjadi isu keamananan yang diletakkan dalam prioritas tinggi pada evaluasi *national risk* di lima tahun terakhir ini. Namun menurut penelitian mereka, walaupun isu ini berada pada prioritas utama, respon yang diperlihatkan negara tidak sama; disebutkan bahwa Perancis, Jerman, Inggris dan Amerika Serikat termasuk negara yang memberikan alokasi sumber daya yang tergolong tinggi kepada area ini khususnya berupa aliran dana. Negara lain seperti Belanda memasukkan isu ini kedalam priritas utama namun belum memberikan komitmen formal untuk mengalokasikan dana.

Untuk negara-negara lainnya, dikarenakan definisi dari *cyber security* dalam dokumen kebijakan beragam mulai dari perlindungan infrastruktur dan perlindungan terhadap komunitas informasi, langkah yang diambil Pemerintah tidak terlalu

signifikan, intinya adalah bahwa setiap negara memiliki kebijakan dan prioritas yang berbeda mengenai isu ini.

Penulis menggunakan tulisan ini sebagai bahan perbandingan sekaligus panduan dalam menganalisis ancaman yang jika didalam tulisan ini bersifat umum dan dilakukan terhadap banyak objek, sementara penulis hanya akan mengkaji Tiongkok namun mendalam terhadap karakter ancaman yang dihadapinya.

Tulisan selanjutnya adalah buku karangan Zixue Tai yang berjudul *The Internet in Tiongkok; Cyberspace and Civil Society*, yang merupakan buku yang akan membantu penulis dalam melihat dampak apa yang diberikan *cyberspace* terhadap pergerakan masyarakat di Tiongkok, apakah pergerakan masyarakat kemudian memberikan ancaman serupa gerakan masyarakat dalam fenomena Arab Spring atau malah kemudian sama sekali tidak membahayakan pemerintah Tiongkok? Karenanya dalam bukunya ini, Tai mencoba untuk menganalisis hubungan sebab akibat antara internet dan *civil society* dalam konteks Tiongkok dengan melihat kepada *historical trajectory*-nya.

Dalam temuan penelitiannya ia mendapatkan bukti yang jelas menerangkan bahwa internet telah menjadi alat emansipasi dan *empowering* bagi *civil society* di Tiongkok serta membuka kesempatan yang baru bagi revitalisasi kekuatan *civil society* sendiri. [31] Ia juga mengatakan bahwa ada beberapa dampak lagi yang diberikan oleh internet kepada Tiongkok dan rakyatnya, seperti menyediakan warga Tiongkok cakupan informasi yang lebih luas, walaupun kemudian pemerintah

[31]Zixue Tai, *The Internet in China; Cyberspace and Civil Society,* (New York: Routledge, 2006) hal. 255

melakukan tindakan sensor, masyarakat Tiongkok bahkan kemudian berupaya menembus barikade tersebut sehingga menjadikan internet sebagai salah satu alat produksi perubahan yang sangat kuat untuk masyarakat. Kedua internet menjadi ruang publik yang melibatkan masyarakat dalam berbagai diskusi terkait isu sosial dan politik yang terbatas, namun tetap menjadi barometer untuk opini dan sentimen publik. Kemudian internet juga memungkinkan individu untuk mengemukakan opini yang lepas dari pengaruh negara dan menyampaikannya secara bebas dalam forum online. Internet juga mengubah peran tradisional dari media di Tiongkok dan menjadi pusat dari *collective action* dari *civil society* di Tiongkok.[32]

Buku ini membantu penulis untuk melihat perubahan apa sajakah yang dihasilkan oleh eksistensi internet di Tiongkok khususnya terhadap *civil society* dan pengaruhnya terhadap negara.

Keempat, dalam artikel terbitan *Center for Technology and Nation Security Policy* yang berjudul *Cyber Influence and International Security*, Franklin D. Kramer dan Larry Wentz menulis bahwa pengaruh *cyberspace* merupakan sumber kekuatan yang masih terus berkembang dalam area kemanan internasional. Walaupun Amerika Serikat memiliki kapasitas yang besar dalam teknologi informasi, namun pengaruh *cyberspace* tidak hanya terletak pada kapasitas tersebut. Kompleksitas pengguna *cyberspace* dan latar belakang budaya pengguna yang berada pada dunia informasi internasional membuat objek audien kepada efektifitas yang dapat berperan dalam proses pengaruh dalam sektor keamanan.

[32] *Ibid*

Amerika Serikat misalnya, negara yang memiliki 40% dari total penyimpanan informasi dan pusat telekomunikasi.[33] Dalam transaksi data yang internet di AS, setiap lebih dari 12 miliar tampilan *website*, dan 184 miliar klasifikasi iklan dari media massa. 6 miliar iklan dari majalah-majalah, 2,6 juta iklan komersial dari radio, 330.000 iklan komersial televisi, dan 40 juta dari transaksi surat elektronik.[34] Di seluruh dunia pada tahun 2002 lebih dari 18 *exabytes* (10^{18}*bytes*) informasi baru yang dihasilkan melalui saluran elektronik (telepon, radio, televisi, internet) dan 5 *exabytes* informasi yang dihasilkan melalui percetakan, film, dan media penyimpanan.[35] Tahun 2006 terjadi peningkatan dalam pemakai layanan *e-mail* yang mencapai 25 miliar transaksi surat elektronik setiap harinya. Belum termasuk pesan di *spam*, yang mengambil bagian 60% dari seluruh *e-mail* tersebut.[36] *Bytes* tidak hanya menjadi indikator dalam mengukur arus informasi yang ada. Contohnya Wikipedia memiliki ruang penyimpanan data sebesar 100 *gigabyte*. Lebih dari 1,2 juta kabel telepon dan 2,1 juta telepon seluler digunakan diseluruh dunia.[37] Lebih dari 1 juta penduduk dunia (18,9 % dari total populasi dunia) menggunakan jasa internet.[38] Dari tahun 2000-2007 penggunaan internet mengalami kenaikan sebanyak 244,7 %. Secara global, tingkat persentase tertinggi di tempati oleh Afrika (874,6%) dan Timur Tengah (920,2).

---

[33] University of California Berkeley, *How Much Information? 2003*, Executive Summary pada http://www2.sims.berkeley.edu/research/projects/howmuch- info-2003/execsum.htm diakses pada 4 November 2012

[34] Michael Pfau and Roxanne Parrott, *Persuasive Communication Campaigns* (Boston: Allyn and Bacon, 1993)

[35] *Ibid*

[36] Ferris Research http://www.ferris.com/research-library/industry-statistics diakses pada 9 November 2012

[37] *The World Fact Book* (Washington, DC: Central Intelligence Agency, 2007) tersedia pada https://www.cia.gov/cia/publications/factbook/geos/xx.html

[38] Internet World Stats http://www.internetworldstats.com/stats.htm

Kramer juga menjabarkan bahwa pemerintahan AS memiliki beberapa mekanisme dalam membuat pengaruh di level *cyberspace* internasional. Sebagai contoh instansi publik di Gedung Putih, *Department of State* (DOS), Agensi pembangunan internasional (USAID), dan Departemen Pertahanan (DOD) menggunakan media televisi, radio dan akses di *website* untuk menyampaikan pesan-pesannya. Informasi ini tersedia secara global, dan dapat di akses tanpa biaya. Begitu juga dengan setiap kedutaan AS di seluruh dunia yang menggunakan fasilitas yang sama dan memiliki akses dalam kapabilitas internet.

Hal ini menunjukkan bahwa kapasitas *cyberspace* yang dimiliki AS memungkinkan adanya penyampaian pesan secara masal. Kapasitas ini digunakan untuk meningkatkan dan mempengaruhi arus informasi secara global. Pemerintah AS memiliki kepentingan untuk menyebarkan informasinya di area publik untuk menarik audien di seluruh dunia guna terlibat didalam pembentukan makna sesuai dengan tujuan nasional AS sendiri.

Kelima adalah sebuah Jurnal yang ditulis oleh Ashley Esarey dan Xiao Qiang yang berjudul *Digital Communication and Political Change in Tiongkok* yang secara umum bercerita mengenai perkembangan dan populernya teknologi media digital di Republik Rakyat Tiongkok yang menurutnya menyebabkan fenomena *liberalization of public discourse* dan tersedianya wadah advokasi politik bagi rakyat Tiongkok. Popularitas dan perkembangan yang begitu pesat kemudian memberikan jaringan

sosial baru ini sebuah kekuatan yang luar biasa kepada rakyat Tiongkok untuk melawan hebatnya propaganda negara.[39]

Didalam artikelnya ini Ashley dan Xiao melakukan upaya analisis konten terhadap koran dan blog-blog yang ada di Tiongkok untuk menguji teori rezim informasi (*information regime theory*) untuk membuktikan adanya transformasi di kepemilikan komunikasi politik. Dalam proses ini ditemukan bahwa dibandingkan dengan koran, kritik terhadap negara lebih banyak ditemukan di blog, sementara kebanyakan koran berisikan hal-hal yang malah membangun atau mendukung negara. Perbandingannya adalah dari 100% blog dan koran, 61% blog berisikan kritik sementara hanya 19% dari koran yang berani menyatakan kritiknya.

Disini juga dijelaskan bahwa kebijakan internet Tiongkok sangat unik, melibatkan pembangunan industri internet (*internet industrial development*), kemudian regulasi yang sah mengenai komunikasi digital (*legitimate regulation of digital communications*) dan penyensoran secara politik (*political cencorship*).

1.7 Kerangka Konseptual

1.7.1 Keamanan Nasional

Dalam menjelaskan konsep keamanan nasional, para ahli atau penstudi yang menggunakan konsep ini biasanya beranjak dari definisi keamanan secara umum. Hal ini dapat diamati melalui pemakaian konsep dalam beberapa literatur berikut; Poppy dalam *paper*-nya yang berjudul "*Kabut Asap; Sebagai Isu Ancaman Non-tradisional dalam Kajian Keamanan Regional*" menyatakan bahwa konsep keamanan

[39]A.M Brady, *Marketing dictatorship: Propaganda and thought work in contemporary China* (New York: Rowman and Littlefield Publishers, 2008)

negara atau *national security* merupakan salah satu kategori dari konsep keamanan secara umum.[40] Dr. Kusnato Anggoro dalam makalahnya yang berjudul *Keamanan Nasional, Pertahanan Negara dan Ketertiban Umum* juga mencoba mendefinikan keamanan nasional dengan terlebih dahulu menjelaskan keamanan secara umum

> "Dalam konsep-konsep tradisional, para ilmuwan biasanya menafsirkan keamanan - yang secara sederhana dapat dimengerti sebagai suasana bebas dari segala bentuk ancaman bahaya, kecemasan, dan ketakutan - sebagai kondisi tidak adanya ancaman fisik (militer) yang berasal dari luar"[41]

Arnold Walfer dalam bukunya "*National Security*", mengemukakan bahwa keamanan nasional adalah sebuah keadaan yang tersusun atas ketidakhadiran ancaman terhadap sebuah nilai.[42] Menurut Bambang Darmono dalam bukunya yang berjudul "Keamanan Nasional: Sebuah Konsep dan Sistem Keamanan Bagi Bangsa Indonesia" keamanan nasional dapat dimaknai baik sebagai sebuah kondisi maupun sebagai fungsi. Sebagai fungsi, keamanan nasional akan memproduksi dan menciptakan rasa aman dalam pengertian luas, yang di dalamnya tercakup rasa nyaman, damai, tenteram dan tertib.[43] Konsep ini menurut Bambang menekankan pada kemampuan pemerintah dalam melindungi integritas teritorialnya dari ancaman yang baik datangnya dari luar maupun dari dalam.

---

[40] Poppy Irawan, *Kabut Asap : Sebagai Isu Ancaman Non-Tradisional Dalam Kajian Keamanan Regional*. 2007. Dipresentasikan pada persidangan 50 tahun hubungan Indonesia-Malaysia, dipublikasikan pada Working Paper University Malaya, Malaysia. Sebagaimana dikutip dari Ardila Putri, *Sekuritisasi Isu Pangan di Indonesia; Studi Pada Kebijakan Food Estate Pemerintah Republik Indonesia*, Proposal penelitian, Padang: FISIP Universitas Andalas

[41] Koesnanto Anggoro. *Keamanan Nasional, Pertahanan Negara dan Ketertiban Umum*, (CSIS, 2003) hal. 1

[42] David A. Baldwin hal.13

[43] Bambang Darmono. Keamanan Nasional Sebuah Konsep dan Sistem Keamanan bagi Bnagsa Indonesia (Jakarta: Sekretariat Jendral Dewan Ketahanan Nasional. 2010) hal iv

Keamanan nasional dapat diartikan sebagai kemampuan sebuah negara untuk melindungi dirinya dari bahaya dan ancaman yang berasal dari luar. Tujuan akhir dari keamanan sebuah negara adalah untuk men-*deter*, mencegah atau sama sekali menghilangkan resiko serangan terhadap negara dan populasinya. [44] Keamanan nasional juga dapat mengacu kepada kebijakan publik yang dengannya negara mengusahakan kelangsungan dan kedaulatannya sebagai sebuah institusi dan juga keamanan dan kesejahteraan bagi rakyatnya.[45] Keamanan nasional disusun atas dua komponen penting, yaitu keamanan institusi kenegaraan (*state security*) dan keamanan individual rakyat yang mendiami negara tersebut (*personal security)*[46].

Menurut teori liberal dua komponen keamanan nasional ini adalah *analogous*, yang berarti secara teori negara tidak mungkin menjadi ancaman bagi rakyatnya dan demikian sebaliknya.[47] Kedua komponen memiliki pengaturan timbal balik dimana negara berfungsi sebagai penyedia keamanan baik bagi institusi maupun personal segenap rakyatnya; dalam waktu yang sama rakyat memiliki kewajiban untuk bertindak dalam koridor pengaturan hukum yang telah ditetapkan negara.[48] Namun hal ini menjadi berbeda penerapannya jika dilihat dari sudut pandang negara-negara otoriter seperti Bekas Jerman Timur, Korea Utara atau Tiongkok, dimana ketidak cocokan antara *state security* dengan *personal security* sangat mungkin terjadi. [49] Keamanan bagi Pemerintah dapat menjadi ketidak-amanan bagi rakyatnya secara

[44] Jennifer Jackson-Preece, Halaman 18
[45] *Ibid* hal. 30
[46] *Ibid* hal. 26
[47] *Ibid*
[48] *Ibid* hal. 30
[49] *Ibid* hal. 32

personal dan sebaliknya; keamanan personal dapat menjadi ancaman bagi keamanan institusi negara.

Barry Buzan dalam bukunya ”*People, State and Fear”* menyatakan bahwa keamanan nasional memiliki tiga landasan: landasan ideasional, landasan institusional dan landasan fisik.[50] Landasan fisik berupa penduduknya, wilayah serta sumber daya yang terletak di lingkup otoritas teritorialnya; landasan institusional berupa segala mekanisme kenegaraan, termasuk lembaga legislatif dari eksekutif maupun ketentuan hukum, prosedur dan norma-norma kenegaraan; landasan ideasional dapat mencakup berbagai hal termasuk gagasan tentang “wawasan kebangsaan”.[51]

Konsep ini akan penulis gunakan untuk mendefinisikan keamanan bagi Tiongkok didalam kerangka dunia *cyber*. Definisi diatas akan memudahkan analisis korelasi antara kebijakan yang dikeluarkan dalam mengontrol perkembangan dan pemanfaatan internet dengan ancaman yang diciptakan oleh pemanfaatan *cyberspace* terhadap keamanan nasionalnya.

1.7.2 *Cyber Vulnerabilities Model*

Framework ini sebenarnya terdapat didalam buku Barry Buzan *People, State, and Fear* dan tidak secara khusus ditujukan untuk isu di *cyberspace* namun Forest Hare mengoperasionalisasikannya untuk isu *cyber threat* di dalam artikelnya yang berjudul *The Cyber Threat to National Security: Why Can't We Agree?*. Untuk mengkonstruksi kerangka berpikirnya Buzan berfokus pada dua aspek dari negara

[50] Koesnanto Anggoro. hal. 2
[51] *Ibid*

bangsa yaitu *Power* dan kepaduan sosial politiknya (*socio-political cohesion*).[52] Melalui kombinasi dua faktor tersebut Buzan menyediakan klasifikasi yang dapat digunakan untuk menilai signifikansi relatif sebuah ancaman dari perspektif negara-negara tertentu yang dapat digambarkan melalui matrix berikut:

Tabel 1. Vulnerabilities (kerentanan) dan Tipologi Negara

		Socio-political Cohesion	
		Weak	Strong
Power	Weak	Highly vulnerable to most types of threats	Particularly vulnerable to military threats
	Strong	Particularly vulnerable to political threats	Relatively invulnerable to most types of threat (less inclined to characterize issues as military)

Sumber: Forest Hare, "The Cyber Threat to National Security; Why Can't We Agree, 215

Negara yang lemah secara *power* (P-W) dan juga lemah dari segi kepaduan sosial politik (SC-W) tentu saja akan menjadi negara yang paling rentan akan semua jenis ancaman dari segala sektor dan level.[53] Ketika negara ini memiliki sumber daya yang berharga bagi negara lain, ia menjadi sasaran ancaman berkelanjutan yang akan terus menghambat perkembangan negaranya.[54] Negara dengan kategori P-S (*power strong*) /SC-W (*socio-political cohesion weak*) dan P-W (*power weak*) /SC-S (*socio-political cohesion strong*) akan memiliki ancaman keamanan yang lebih bervariasi.

[52] Hare. hal 215
[53] *Ibid*, hal.216
[54] *Ibid*

Negara P-S/SC-W memperlihatkan prioritas kepada negara yang relatif kuat militernya tetapi relatif lemah SC nya. Menurut model ini, negara-negara tersebut paling fokus terhadap ancaman pada kemampuan negara untuk mempertahankan kontrol terhadap penduduknya. Sebagaimana dinyatakan oleh buzan bahwa [55]

> *"Weak states, and those with narrowly cast ideological orthodoxies, will be impelled by their domestic conditions to push the qualifications for threats to have 'national security problem' status down towards the low end of the threat spectrum. When political threats dominate, the national security agenda can become very wide-ranging indeed"*

Sementara negara yang berada di kanan atas memiliki perspektif yang berbeda secara fundamental terkait kerentanan terhadap ancaman atas keamanan nasionalnya.[56] Menurut model ini, negara-negara ini memiliki karakteristik berupa ketidakmampuan mereka untuk menghasilkan kekuatan militer yang siginifikan tetapi mereka memiliki fondasi kepaduan sosial politik yang kuat (P-W/SC-S). Negara-negara sejenis ini memiliki institusi yang stabil dan kuat serta tidak terlalu khawatir dengan ancaman yang bersifat politis dan ideologis terhadap eksistensi mereka. Namun negara ini sangat rentan terhadap kemampuan militer negara sekitarnya. Keterbatasan sumber daya "memaksa" negara jenis ini untuk berspesifikasi di ekonomi namun tidak sama sekali menghilangkan kerapuhannya sebagai sebuah negara.[57]

Dengan argumentasi bahwa ancaman dapat hadir melalui *cyberspace*, Hare kemudian mengoperasionalisasikan model dari Buzan kepada isu *cyber security*:

---

[55] *Ibid*
[56] *Ibid*
[57] *Ibid*

Tabel 2. *Cyber Vulnerabilities* dan Tipologi Negara

		Socio-political Cohesion	
		Weak	Strong
Power	Weak	De-stabilizing political actions in cyberspace, attacks on Internet infrastructure, criminal activities	DDOS and other major attacks on critical infra-structure*
	Strong	De-stabilizing political actions in cyberspace	Criminal activities in cyberspace

Sumber: Forest Hare, "The Cyber Threat to National Security; Why Can't We Agree, 218

P-W/SC-W akan rentan terhadap semua jenis ancaman yang dapat terjadi di *cyberspace* termasuk website berbasis forum-forum yang dapat menyebabkan ketidakstabilan politik, serangan pada infrastruktur berbasis internet maupun aksi-aksi kriminal melaluinya. Sementara negara dengan P-S/SC-S tindakan criminal merupakan asal ancaman yang paling signifikan. P-W/SC-S biasanya merupakan negara yang maju dan memiliki ketergantungan yang besar pada *cyberspace* untuk sebagian besar infrastruktur dan juga administrasi sehingga sangat rentan terhadap *cyber attack*. Negara P-S/SC-W menganggap *cyberspace* sebagai tantangan bagi rezim yang menginginkan kontrol dalam persebaran informasi yang mereka anggap *subversive*. Negara seperti ini menganggap *cyberspace* dan pengaruhnya sebagai tantangan bagi stabilitas upaya mereka memperkuat kepaduan sosial politik. Negara P-S/SC-W akan sangat tertarik dalam memberlakukan langkah-langkah yang akan

membenarkan kontrol yang lebih besar terhadap aliran informasi di *cyberspace* baik di dalam wilayah kedaulatan mereka maupun dari komunitas internasional.

Dalam proses analisis, *power* dapat dinilai melalui perbandingan dengan kemampuan militer yang dimiliki oleh negara lain didalam sistem internasional khsusnya dari negara sekitar dan negara-negara great powers.[58] Negara yang tergolong lemah dari segi harus memaksimalkan kemapuan ekonomi mereka untuk kesejahteraan negaranya. Tetapi tetap belum sepenuhnya mengurangi kerentanannya terhadap ancaman. Negara yang kepaduan sosial politiknya (*social political cohesion*/SC) lemah, sangat rentan kepada ancaman ide mengenai negara, institusinya dan bahkan kesatuan teritorialnya.

Walaupun model ini tidak didesain untuk mengklasifikasi secara komprehensif semua tipe-tipe negara, tidak pula menunjukkan semua potensi ancaman yang akan menghadang negara yang dianggap rentan.[59] Namun, model klasifikasi kasar ini memudahkan peneliti untuk memahami persimpangan dari dua polemik mengenai power dan kepaduan sosial politik dan bagaimana karakteristik ini berpotensi untuk mempengaruhi agenda keamanan negara.

Framework ini akan penulis gunakan untuk menspesifikasi ancaman yang disebabkan pemanfaatan *cyberspace* bagi keamanan nasional Tiongkok.

[58] *Ibid*, hal. 215
[59] *Ibid* , hal.216

1.8 Metodologi Penelitian

Metode ialah suatu prosedur atau cara untuk mengetahui sesuatu yang mempunyai langkah-langkah sistematis.[60] Metode penelitian adalah cara ilmiah untuk mendapatkan data dengan tujuan dan kegunaan tertentu.[61] Metode penelitian yang digunakan dalam penelitian ini bersifat kualitatif dengan model deskriptif-analitis, yaitu suatu pendekatan yang digunakan untuk menjelaskan suatu fenomena sosial yang diteliti secara mendalam.

Metode penelitian yang bersifat kualitatif digunakan untuk dapat memahami *cyberspace* tidak hanya sebagai kemajuan teknologi semata namun merupakan ruang yang berpengaruh besar terhadap dinamika hubungan internasional atau dalam penelitian ini sebagai ancaman bagi keamanan nasional Tiongkok. Deskriptif dipakai sebagai teknik untuk menjelaskan.[62] Analisis deskriptif dipakai untuk memaparkan secara teruji seperti apa ancaman yang disebabkan oleh pemanfaatan *cyberspace* di Tiongkok terhadap keamanan nasionalnya.

Deskripsi kualitatif dimaksudkan disini sebagai cara menafsirkan data dan informasi, yaitu dengan interpretasi, tanpa melakukan pengujian lebih lanjut untuk menetapkan mana yang mejadi komponen-komponen analisis yang paling bermakna. Rangkaian informasi disusun menurut fakta-fakta yang dikumpulkan untuk memastikan objektivitasnya.

---

[60]Prof. Dr. Husaini Usman dan Purnomo Setiady Akbar, *Metodologi Penelitian Sosial*, (Jakarta: Bumi Aksara, 2011) Hal 41

[61]Prof.Dr. Sugiyono, *Metode Penelitian Kuantitatif, Kualitatif dan R&D* (Bandung: Penerbit Alfabeta, 2011) hal. 244

[62]Lexy J. Moleong, *Metodologi Penelitian Kualitatif*, (Bandung: Remaja Rosdakarya, 2007), hal.6

1.8.1 Batasan Penelitian

Analisa akan dibatasi dari tahun dimana *cyberspace* dipakai secara masif di Tiongkok yaitu pada tahun 1998 sampai tahun 2015. Tahun 1998 merupakan tahun dimana pemakaian internet di Tiongkok menjadi sebuah tren yang terhentikan. Pemanfaatannya bersifat sangat luas sehingga pemerintah Tiongkok bahkan melakukan penyesuaian di birokrasinya dengan pendirian Kementrian Industri dan Informasi (KII). Sampai sekarang tren ini masih terus mengalami perkembangan.

1.8.2 Tingkat Analisa dan Unit Analisa

Tingkat analisa merupakan tingkat dimana pengetahuan itu berada, sementara unit analisa merupakan unit yang perilakunya hendak dideskripsikan, dijelaskan, dan diramalkan. [63] Tingkat analisa dalam penelitian ini adalah sistem internasional sementara unit analisa nya adalah negara Tiongkok.

1.8.3 Metode Pengumpulan Data

Sementara itu, pengumpulan data dalam penelitian ini menggunakan teknik penelitian kepustakaan *(library research)*. Data dan informasi yang akan digunakan dalam penelitian ini adalah data sekunder yang didapat dari beberapa sumber yaitu penelitian-penelitian sebelumnya yang juga membahas tentang *cyberspace* baik di Tiongkok maupun di negara lain yang terkait serta ancaman yang diciptakan oleh pemanfaatan *cyberspace* terhadap keamanan negara, buku-buku, jurnal-jurnal ilmiah terkait, artikel-artikel tentang keduanya.

[63] Mohtar Mas'oed, *Ilmu Hubungan Internasional – Disiplin dan Metodologi*, (Jakarta: LP3ES, 1990) hal. 35

1.8.4 Teknik Pengolahan dan Analisa Data

Analisa data adalah proses mencari dan menyusun secara sistematis data yang diperoleh dari hasil pengumpulan data dengan cara mengorganisaikan data ke dalam kategori, menjabarkan kedalam unit-unit, melakukan sintesa, menyusun kedalam pola, memilih mana yang penting dan yang akan dipelajari, dan membuat kesimpulan sehingga dapat difahami.[64]

1.9 Sistematika Penulisan

BAB I Pendahuluan

Pengantar yang berisi latar belakang, rumusan masalah, pertanyaan penelitian, tujuan penelitian, manfaat penelitian, studi pustaka, kerangka teoritik dan konseptual, metodologi penelitian, pembatasan masalah dan sistematika penulisan. Menggambarkan secara keseluruhan tentang penelitian yang akan dilakukan.

BAB II Keamanan Nasional Tiongkok

Bab ini akan menjelaskan konsepsi keamanan nasional menurut Tiongkok

BAB III Dinamika Pemanfaatan *Cyberspace* di Tiongkok

Bab ini mendeskripsikan perkembangan pemanfaatan *cyberspace* di Tiongkok serta kebijakan-kebijakan apa saja yang diterapkan oleh pemerintah Tiongkok dalam mengontrol perkembangan dan pemanfaatan *cyberspace* di negara mereka.

BAB IV Analisis Ancaman *Cyberspace* terhadap Keamanan Nasional Tiongkok

Bab ini akan menganalisis hubungan saling mempengaruhi antara *cyberspace* dengan keamanan nasional Tiongkok.

BAB V Kesimpulan

[64]Prof. Dr. Sugiyono, hal. 244

Bab ini berisi kesimpulan dari pembahasan yang berdasarkan kepada pertanyaan penelitian yang diangkat.


UNIVERSITAS ANDALAS
UNTUK
KEDJAJAAN
BANGSA