

## **BAB I**

### **Pendahuluan**

#### **I.1. Latar Belakang**

Perubahan politik dunia yang terjadi di abad ke-21 ini telah menghadirkan suatu kompetisi antar bangsa. Kondisi tersebut cenderung mengarah pada perebutan pengaruh yang sangat ketat, baik secara global, regional maupun internasional. Perkembangan tersebut antarlain meyebabkan terjadinya perubahan pada situasi politik dunia dengan munculnya isu-isu keamanan baru. Di masa Perang Dingin, isu keamanan tradisional cukup menonjol, yakni yang berhubungan dengan geopolitik dan geostrategi, khususnya perebutan pengaruh kekuatan blok barat dan blok timur. Pada masa itu, kekhawatiran dunia terutama pada masalah pengembangan kekuatan militer dan senjata strategis serta hegemoni. Isu keamanan pada dekade terakhir ini makin kompleks dengan meningkatnya peran teknologi informasi di era globalisasi ini.

Perubahan yang mengesankan dari karakteristik perang adalah berakhirnya perang-perang konvensional dengan mengandalkan kekuatan militer secara fisik semata dan kemunculan perang-perang bentuk baru. Pemahaman terhadap perang bentuk baru tersebut memerlukan pembacaan ulang konteks lingkungan politik, ekonomi, dan budaya di masa ini. Perang pun tidak bisa dipisahkan dari kehidupan masyarakat di berbagai zaman. Sebagaimana ditulis oleh ahli strategi Inggris Basil Liddell Hart bahwa *“jika kamu inginkan kedamaian, pahami apa itu*

*perang*.”Pembacaan terhadap bentuk perang baru di abad Globalisasi harus diawali sejak berakhirnya perang dingin. Antara tahun 1989 – 1992 hampir seratus macam perang yang pernah terjadi akhirnya berakhir, dan dalam hal korban peperangan tahun 1990an adalah dekade kekerasan terendah sejak akhir dari Perang Dunia ke-2.<sup>1</sup>

Pada abad globalisasi ini, sejak era paska Perang Dingin, negara menghadapi ancaman-ancaman baru yang semakin tidak dapat diprediksi seperti terorisme, demokratisasi, konflik internal, tindak pidana pencucian uang, kejahatan narkoba dan obat terlarang, serta berbagai konflik budaya dan identitas. Pembacaan ulang terhadap ancaman-ancaman baru tersebut tentunya telah menandai kemunculan perubahan bentuk perang baru di dalam sistem internasional.

Di era teknologi informasi yang mengglobal dan tidak pasti ini, lanskap perang baru telah muncul yang juga melibatkan aktor non-negara. Medan perang fisik telah bertransformasi menjadi ruang-ruang *cyber* dan media global. Menurut Michael Sheehan *battlefields* kini telah berubah menjadi *battlespace*, dengan tiga-dimensi yaitu melibatkan penggunaan kekuatan udara (*air-power*), satelit ruang angkasa (*space satellites*), dan yang mencakup juga gelombang komunikasi dan *cyberspace*.<sup>2</sup>Perang baru yang muncul akibat perkembangan teknologi informasi dan peningkatan konektivitas antar manusia, antar bangsa, ialah sebuah perang yang dinamakan sebagai *cyberwarfare*.

---

<sup>1</sup>John Baylis, Steve Smith, and Patricia Owens; *The Globalization of World Politics: an Introduction to International Relations*; Oxford University Press; New York; 2011; hal 216.

<sup>2</sup>*Ibid*; hal 217.

Aspek perkembangan *cyberspace* dalam globalisasi tersebut sangat berpengaruh terhadap kehidupan sehari-hari masyarakat dan bahkan hingga alam bawah sadar seorang individu. Globalisasi menurut Francis Fukuyama merupakan isu yang lebih besar dari sekedar isu ekonomi.<sup>3</sup> Diskusi-diskusi tentang globalisasi merefleksikan sebagai fenomena di mana dunia menjadi semakin saling terkait dan terpadu, tunduk pada proses homogen dan seragam. Dalam globalisasi, tidak semua kegiatan berlangsung secara global tentunya tapi, *strategically crucial activities and economic factors are networked around a globalized system of inputs and outputs*. Jaringan-jaringan antar manusia dari berbagai bangsa pun terbentuk melalui sarana teknologi informasi. Masyarakat di berbagai negara pun mengakui kemunculan ikon-ikon teknologi informasi global seperti Michael Jackson, Lady Gaga, Justin Bieber, Facebook, Hi5, hingga twitter atau produk-produk yang mendunia seperti Nike atau Mc Donalds. Hal-hal tersebut merupakan bukti sederhana adanya kesadaran global dalam setiap individu di berbagai penjuru dunia. Globalisasi membuat masyarakat dunia menjadi semakin tanpa batas. Hal ini berkaitan erat dengan perkembangan teknologi, komunikasi dan transportasi. Hal inilah yang difasilitasi oleh globalisasi, dimana batasan antar masyarakat dunia menjadi semakin kabur karena keterbukaan.

Thomas L. Friedman mengatakan Globalisasi memiliki Dimensi Ideologi dan Teknologi. Dimensi Ideologi yang dimaksud oleh Thomas L Friedman yaitu kapitalisme dan liberalisme sebagai satu-satunya alternatif ideologi paska perang dingin. Keniscayaan kapitalisme dan liberalisme di era paska perang dingin ini

---

<sup>3</sup>Francis Fukuyama, *The End of History and the Last Man*, (New York: The Free Press, 1992).

pada awalnya diusung oleh Francis Fukuyama dalam bukunya *The End of History and the Last Man*; yang mengklaim bahwa sejarah ideologi telah berakhir dengan pengakuan demokrasi liberal sebagai ‘pemerintahan final umat manusia.

Sedangkan Dimensi Teknologi dari globalisasi adalah teknologi informasi yang telah menyatukan dunia melalui jaringan gelombang komunikasi *cyberspace*. Informasi merupakan asset yang sangat penting karena merupakan salah satu sumber daya strategis yang sangat berguna, baik bagi sebuah individu, organisasi, perusahaan, bahkan Negara. Karena itulah perlindungan terhadap informasi (keamanan informasi) sangat penting untuk diperhatikan. Teknologi internet yang berkembang sangat pesat dewasa ini dan kemampuan masyarakatnya juga yang berkembang sangat pesat juga memperkuat harusnya keamanan informasi dilakukan salah satunya dengan mengontrol jaringan internet.

Salah satu akibat tak terduga dari teknologi informasi adalah gerakan *Arab Spring* yang mampu meruntuhkan kekuasaan politik di jazirah Arab dan Afrika Utara. Penggulingan kekuasaan Muammar Ghadafi di Libya dan Husni Mubarak di Mesir diawali melalui *internet activism* untuk mengumpulkan dan mengorganisir masyarakat. Inilah bentuk dari Globalisasi informasi, yaitu penunjang arus informasi global melalui siaran televisi baik langsung (melalui satelit) maupun tidak lang-sung (melalui paket siaran). Semakin dinamis dan cepat, misalnya berita yang disiarkan secara *realtime* (dari tempat kejadian saat peristiwa terjadi) sehingga langsung dapat dikomunikasikan kepada masyarakat internasional. Bila terdapat informasi tentang pergolakan atau keputusan pemerintah di satu belahan dunia, dapat berpengaruh terhadap lonjakan kurs mata

uang, demonstrasi, aksi protes, dan sebagainya, dengan contoh peristiwa di Mesir tersebut.

Era globalisasi yang saat ini menjadi sebuah keniscayaan yang tidak bisa dihindari oleh bangsa dan Negara manapun di dunia ini. Kondisi ini membuat setiap Negara berusaha keras berinovasi di berbagai bidang untuk tetap menjaga agar tidak tergerus dalam perubahan tersebut. Perubahan mendasar terjadi pada keterbukaan arus informasi khususnya teknologi informasi yang didalamnya mencakup teknologi internet yang saat ini menjadi salah satu kebutuhan pokok. Kondisi ini disadari betul oleh Negara-negara maju yang menjadikan internet atau lebih familiar dengan sebutan dunia maya menjadi sebuah mantra atau dimensi baru yang harus dijelajahi, dikuasai dan dipertahankan setelah darat, laut, udara dan angkasa luar. Dengan dijadikannya internet atau dunia maya menjadi mantra baru, maka beberapa negara Barat maupun negara 'pendatang baru' seperti China dan Rusia membuat berbagai macam berlomba-lomba membangun infrastruktur keamanan dan pertahanan, bahkan, pemerintah Negara-negara tersebut merekrut para ahli yang sangat kompeten di dunia internet melalui kompetisi di universitas-universitas ternama maupun pengamatan di jejaring social. Sebagaimana disebutkan di atas fenomena ini sering disebut sebagai *cyberwarfare*. Dengan melihat dampak dari *cyberwarfare* tersebut, maka pembangunan pertahanan *cyber* adalah sebuah kebutuhan dan keharusan untuk melindungi pertahanan dan keamanan sebuah Negara.

Perbedaan utama antara negara maju dan negara berkembang adalah kemampuan ilmu pengetahuan dan teknologinya. Kemajuan yang pesat di bidang

ilmu pengetahuan dan teknologi di negara-negara maju karena didukung oleh sistem informasi yang mapan. Sebaliknya, sistem informasi yang lemah di negara-negara berkembang mengakibatkan keterbelakangan dalam penguasaan ilmu pengetahuan dan teknologi. Jadi jelaslah bahwa maju atau tidaknya suatu negara sangat ditentukan oleh penguasaan terhadap informasi yang canggih, karena informasi merupakan modal utama dalam mengembangkan ilmu pengetahuan dan teknologi yang menjadi senjata pokok untuk membangun negara. Sehingga apabila satu negara ingin maju dan tetap eksis dalam persaingan global, maka negara tersebut harus menguasai informasi. Di era globalisasi dan informasi ini penguasaan terhadap informasi tidak cukup hanya sekedar menguasai saja, diperlukan kecepatan dan ketepatan. Sebab hampir tidak ada gunanya menguasai informasi yang telah usang, padahal perkembangan ilmu pengetahuan dan teknologi yang sangat cepat mengakibatkan usia informasi menjadi sangat pendek, dengan kata lain, informasi lama akan diabaikan dengan adanya informasi yang lebih baru.

Begitu pentingnya perkembangan teknologi dan informasi dalam era globalisasi ini membuat setiap Negara berlomba untuk saling meningkatkan system teknologi dan informasinya agar dikatakan sebagai Negara maju yang mengikuti era globalisasi. Sebab itulah seiring dengan berkembangnya teknologi yang begitu pesat, informasi semakin mudah didapatkan. Siapapun dimanapun dengan adanya teknologi yang canggih yaitu internet bisa mendapatkan informasi apapun dari manapun yang diinginkannya. Hal ini memang sangat memudahkan individu untuk memperoleh informasi, namun dengan bebas dan mudahnya informasi

didapatkan tidak sedikit informasi penting yang seharusnya hanya diketahui oleh pihak terbatas bisa menyebar luas kepada khalayak masyarakat. Penyebaran informasi penting yang tidak pada tempatnya juga bisa menjadi salah satu bentuk ancaman.

Masyarakat yang tak luput dari pengaruh globalisasi adalah masyarakat China. Fenomena yang menarik adalah ketika kita menganalisa masyarakat China, karena pada dasarnya memiliki karakteristik dan sejarah yang unik terkait dengan geopolitik dan geostrategi. Secara geopolitik, secara geografi China adalah salah satu negara yang berideologi komunis dimana Barat atau Amerika Serikat membangun kebijakan *containment policy* atau politik pembendungan pada masa Perang Dingin. Sehingga saat ini China dikelilingi oleh negara-negara liberal dan bercirikan pembangunan ekonomi kapitalistik seperti Jepang, Korea Selatan dan Taiwan. Sedangkan secara geoekonomi, posisi China yang dikelilingi oleh negara kapitalistik Asia Timur ini membuat posisi China dalam kacamata ekonomi, mau tidak mau harus turut serta dalam perkembangan regional dimana sedang berlangsung proses globalisasi ekonomi.

China yang merupakan kekuatan baru dunia walau secara diketahui gencar merekrut, membangun dan mempersenjatai negaranya dengan teknologi terkini prajurit dunia maya mereka yang dikenal sebagai blue army. Blue army berada dibawah Chinese *People's Liberation Army* (PLA) Ground Forces yang dipersiapkan untuk bertahan atas serangan cyber terhadap kepentingan china sekaligus mempersiapkan serangan balik yang lebih mematikan. Tercatat beberapa kali para hacker ataupun simpatisan "blue army" menjadi sorotan para pemerhati

keamanan internet menyusul adanya serangan bergelombang yang diduga berasal dari china. Selain menyensor Internet, China juga menetapkan batas-batas unik pada informasi. China merupakan satu-satunya negara penting yang menerapkan suatu sistem penyensoran yang resmi dan rinci yang mewajibkan semua perusahaan yang bergerak di bidang informasi untuk menerimanya. Sebagai akibatnya, mereka yang ingin akses Internet ke situs-situs web yang sensitif terhadap pemerintah China, seperti pembantaian di Alun-Alun Tiananmen atau Dalai Lama, akan menemukan bahwa situs-situs itu diblokir. Berbarengan dengan itu, China tengah mengembangkan peralatan khusus yang berfungsi sebagai mata-mata saiber (cyber) atau serangan-serangan saiber terhadap organisasi-organisasi hak asasi manusia dan, terutama, terhadap perusahaan dan pemerintahan asing, termasuk lembaga-lembaga yang melindungi keamanan nasional Amerika Serikat.

Di China, penyebaran informasi melalui internet berkembang begitu cepat sampai-sampai pemerintah tidak lagi mampu mengendalikannya. Bahkan, pengusaha China muda yang telah belajar di Amerika Serikat membawa mereka dengan model bisnis terbaru Amerika Serikat dan mendirikan perusahaan-perusahaan Internet yang dibiayai oleh perusahaan modal luar negeri. Dengan demikian, internet menjadi salah satu bentuk ancaman tradisional dari informasi, Seperti media yang dikontrol di bawah negara, di China. *Chinese Academy of Social Sciences* menemukan bahwa 67,5 persen pengguna Internet percaya bahwa Internet memungkinkan untuk mengkritik lebih kepada pemerintah daripada mengkritik melalui forum tradisional. Pengguna dapat mengakses situs yang terlarang seperti CNN melalui bantuan perusahaan Barat seperti Safeweb yang

menyediakan hosting internet. Persaingan antara koran dan internet, internet yang dianggap lebih ekonomis untuk memproduksi dan lebih praktis cukup susah dilacak, sehingga dengan menggunakan internet setiap individu lebih merasa independen dan mempunyai kuasa akses yang luas.

Yang menarik lagi adalah kebijakan baru China yang memperketat kontrol penggunaan internet, menyusul penutupan akses luar negeri, seperti Twitter dan YouTube, karena dianggap memungkinkan pengguna situs-situs tersebut mengirimkan video, audio, atau gambar tanpa sensor dari pemerintah. Hal ini menunjukkan bahwa bagi pemerintahan China keamanan informasi sangat penting. Segala macam kejadian bisa terjadi diakibatkan oleh begitu mudahnya tiap orang menjalin komunikasi dengan orang lain di belahan manapun untuk saling bertukar informasi. Informasi yang didapat ataupun diberikan bisa menjadi informasi yang penting atau rahasia. China mengatakan akan memperketat kontrol penggunaan internet untuk menghadapi ancaman hacker dan infiltrasi virus, seperti yang dilansir dalam salah satu berita;

“Kepala Kantor Dewan Informasi Negara, Wang Chen, mengatakan hari Kamis lalu (30/12) bahwa jumlah pengguna internet di China telah mencapai 450 juta pada akhir November ini yang berarti satu dari tiga orang adalah pengguna internet di China, meningkat sekitar 20 persen dari tahun sebelumnya, demikian dilansir dari NHK word hari ini (31/12). Pada saat yang sama, Wang juga mengatakan kantor-kantor pemerintah dan swasta sedang menghadapi peningkatan ancaman dari hacker dan virus, inilah yang menjadi pertimbangan pengetatan kontrol penggunaan internet.”<sup>4</sup>

Di tahun 2008, China memiliki 250 juta pengguna internet, 350 juta telepon selular, 300 juta blog, serta penulis blog dengan jumlah yang tak terhitung

---

<sup>4</sup>*China Perketat Kontrol Penggunaan Internet.* <http://lintascafe.com/2011/01/01/china-perketat-kontrol-penggunaan-internet/>. Diakses Pada Tanggal 27 Desember 2011.

yang membangun jaringan komunikasi “*all to all*”.<sup>5</sup>Perkembangan media modern yang paling dinamis dapat dilihat dari internet. Pengguna internet diChina menunjukkan tanda-tanda peningkatan dari segi kuantitas, kira-kira 111 juta orang *go online* setiapharinya, dan jumlah ini sendiri terus mengalami peningkatan.<sup>6</sup> Menurut Timothy Cheek, media internet diChina menunjukkan tanda-tanda perubahahan ke arah yang lebih demokratis.<sup>7</sup>Meskipun pemerintah telahmelakukan pengeblokan terhadap sejumlah website internasional, namun praktik liberal dan demokrasi itusendiri mulai nampak di media internet China.Misalkan apabila melihat kasus Wikipedia di China, situsreferensi ini sempat menimbulkan perdebatan ketika seseorang mengekspos esai “*China-centrism*”.Meskipun muncul perdebatan, namun para kontributor setuju pada unsur netralitas Wikipedia, meliputi objektivitasnya dalam isi artikel, kesetaraan bagi pengguna, dan pentingnya konsensus. Hal inilah salah satu yang ditakutkan China sehingga melakukan sensor internet di masyarakatnya.<sup>8</sup>

Dalam Globalisasi, teknologi memiliki kontribusi penting dan besar untuk menciptakan perspektif baru tentang dunia. Jika dalam masa Perang Dingin dinding yang dipandang sebagai symbol dari system Perang Dingin, di era Globalisasi telah diganti oleh *World Wide Web* yang kini telah menyatukan setiap orang di dunia. Hal inilah yang dikhawatirkan oleh China, apabila batas antara individu di satu Negara dan Negara lain sudah hilang dengan salin bertukar

---

<sup>5</sup>James F. Scotton dan William A. Hatchen, hlm. 2.

<sup>6</sup>Jing Wang, *Brand New China: Advertising, Media, and Commercial Culture*(Cambridge: Harvard University Press,2008), hal. 120.

<sup>7</sup>Timothy Cheek, *Living with Reform: China since 1989*, (Nova Scotia: Fernwood Publishing, 2006), hal. 119-120.

<sup>8</sup> *Ibid.*

informasi, system pemerintahan China yang otoriter selama ini dikhawatirkan akan mendapat gonjangan dengan akses informasi keluar maupun ke dalam yang sangat mudah dan perkembangan masyarakat internasional yang lebih terbawa oleh nuansa Demokrasi ala barat yang sangat bertentangan dengan China. Memang dalam sistem Globalisasi salah satu keseimbangan yang dibentuk adalah keseimbangan antara individu dan actor Negara bangsa. Dengan kata lain, Globalisasi telah menghancurkan banyak tembok yang membatasi gerak manusia dan menyatukan dunia melalui jaringan-jaringan (networks). Dengan kata lain Globalisasi memberikan kekuatan tambahan terhadap tiap individu untuk mempengaruhi pasar atau Negara bangsa.

Dengan melihat kebijakan pemerintah China berkaitan dengan keamanan informasi di negaranya, jelas bahwa diatas segalanya, prioritas pertama pemerintah China adalah untuk menjaga stabilitas sosial dan politik di negaranya dari pengaruh informasi dari luar. Pemerintah China khawatir kejadian lama akan terjadi lagi yaitu dengan kerusuhan masyarakat sejak menumpas demonstrasi pro-demokrasi di negara itu pada 1989. Apalagi dengan pengaruh dominasi barat yang semakin meluas dan banyak Negara yang mengapresiasi dan menggunakan ideology dari Barat, menyebabkan China lebih berhati-hati dan mawas diri dalam menjaga keamanan informasi di negaranya. Tidak sedikit peran media, internet, dan jejaring sosial dalam menyumbangkan informasi dan kekuatan mengorganisir pada masyarakat-masyarakat yang sudah jenuh terhadap pemerintahan negaranya yang otoriter. Dan hal ini bagi pemerintah China diharapkan tidak akan terjadi di Negara dan masyarakatnya. Oleh karena itu pembahasan kontrol internet di era

*cyberspace* ini menarik untuk diteliti lebih lanjut apabila dikaitkan dengan perkembangan era globalisasi.

## **I.2. Rumusan Masalah**

Berdasarkan latar belakang masalah di atas, penelitian ini kemudian menetapkan pertanyaan penelitian yang hendak dicari jawabannya eksplorasi penelitian. Pertanyaan kunci dari hal itu adalah:

- Bagaimana upaya China melakukan sekuritisasi terhadap bidang ideologi, bidang politik, bidang pertahanan-kemanan, bidang ekonomi, dan bidang sosial budaya China melalui kebijakan sensor Internet?

## **I.3. Tujuan Penelitian**

1. Mencoba untuk mengkaji permasalahan kontrol internet di China dan upaya China menghadapi perang *cyber*.
2. Untuk memahami apa tujuan China melakukan sensor internet terhadap masyarakatnya.
3. Untuk mengetahui upaya-upaya China dalam melakukan kontrol internet sebagai bentuk sekuritisasi di era globalisasi.

## **I.4. Literature Review**

*Cyberwarfare, Information Warfare, Netwar*, serta *Revolution in Military Affairs* (RMA) merupakan terma-terma yang pertama kali dipopulerkan oleh John Arquilla dan David Ronfeldt pada tahun 1993 melalui sebuah artikel yang ditulis

dalam Jurnal *Comparative Strategy* dengan judul “*Cyberwar is Coming.*”<sup>9</sup> Artikel tersebut mengangkat sebuah isu yang sangat penting mengenai Perang, bahwa perang tidak lagi ditentukan oleh siapa yang memakai senjata paling hebat, prajurit paling kuat, atau anggaran militer paling besar. Perang di masa depan akan lebih ditentukan oleh faktor siapa yang paling hebat dalam menguasai informasi. Artikel tersebut mendapatkan pengakuan dan apresiasi dari militer AS sejak tahun 1995 dan kemudian meluas ke dunia akademis dan para pemangku kebijakan teknologi informasi.

Perkembangan di dunia *cyberspace* dan teknologi informasi tersebut memunculkan reaksi yang ambigu dari Pemerintah China. Artikel dari Nina Hachigian yang ditulis tahun 2001 berjudul “*China’s Cyber Strategy*” menjelaskan bagaimana ambiguitas strategi Pemerintah China dalam menghadapi kemunculan internet ini.<sup>10</sup> Di satu sisi, Pemerintah China memperkenalkan internet untuk mendukung kebijakan modernisasi ekonomi China yang dimulai di era Deng Xiao Ping pada tahun 1978. Namun di sisi lain, Pemerintah China khawatir bahwa keterbukaan informasi yang melekat pada internet akan memunculkan resiko politik bagi legitimasi Partai Komunis China. Sehingga negeri Tirai Bambu tersebut memutuskan untuk memperkenalkan internet sembari tetap memberlakukan kebijakan sensor terhadapnya.

Kebijakan sensor Internet China memang berubah-ubah sesuai dengan konteks perubahan lingkungan. Hal ini diungkap oleh Robert Zheng, Robert R.

---

<sup>9</sup>John Arquilla dan David Rondfelt, *Cyberwar is Coming! Comparative Strategy*, Vol 12, No.2, Spring 1993.

<sup>10</sup>Nina Hachigian; *China’s Cyber-Strategy*; Foreign Affairs, vol. 80, no. 2, March – April 2001.

Ouyang, dan Feng Rui dalam artikelnya berjudul “*Instructional Use of the Internet in China.*” Dalam artikel yang ditulis pada tahun 2001 tersebut mereka menegaskan bahwa Kebijakan Sensor Internet China telah melalui tiga tahapan yaitu tahap *strict censorship*, *half censorship*, dan *limited self autonomy*, serta akan terus berubah mengikuti konteks sosial dan politik yang berkembang.<sup>11</sup> Kebijakan sensor internet tersebut memang di satu sisi menimbulkan resiko politik, namun kepentingan China untuk memasuki persaingan industri teknologi informasi internasional membuat negara tersebut secara perlahan membuka kran kebebasan Internet.

Reaksi terhadap kebijakan sensor internet bermunculan yang pada umumnya menghendaki agar Pemerintah China memberikan keleluasaan perkembangan teknologi informasi dan globalisasi. Artikel dari Garry Elijah Dann dan Neil Haddow pada tahun 2006 menjelaskan bagaimana perusahaan-perusahaan teknologi asal Amerika Serikat seperti Google, Microsoft, dan Yahoo! harus mengikuti aturan bisnis di China dengan menyaring informasi yang berlawanan terhadap pemerintah China.<sup>12</sup> Artikel tersebut menyorot bagaimana Google, Microsoft, dan Yahoo telah melanggar hak asasi masyarakat China untuk secara bebas berkomunikasi dan mengelola informasi dengan mengikuti aturan bisnis yang ditetapkan Pemerintah China.

---

<sup>11</sup>Robert Zheng, John R Ouyang, Feng Rui; *Instructional Use of Internet in China*; Journal of Educational Technology Research and Development; Springer Publication; 2002.

<sup>12</sup>Garry Elijah Dann dan Neil Haddow; 2006; *Just Doing Business or Doing Just Business: Google, Microsoft, Yahoo! And the Business of Censoring China’s Internet*; Journal of Business Ethics, Vol 79, Issue 3.

Meskipun mendapat kritik dari banyak Negara, Pemerintah China tetap melanjutkan kebijakan sensor Internetnya. Situasi politik di internal China yang bergejolak, dengan adanya konflik di Provinsi Xin Jiang antara etnis Han dan etnis Uyghur, memaksa negeri tirai bambu tersebut memperketat kebijakan sensor internetnya. Hal ini terungkap dalam artikel Yiyi Lu berjudul “*Online Protests in China*” yang mengungkap bagaimana informasi yang beredar di internet mampu memicu konflik horizontal di China antara dua etnis di Provinsi Xinjiang tersebut.

Kajian tentang kebijakan sensor internet pemerintah China semakin mendapat tanggapan dari dunia akademik dengan adanya konflik di wilayah Xinjiang dan semakin mengetatnya kebijakan sensor internet Pemerintah China. Artikel dari Timothy Farnsworth menyorot tentang bagaimana China pada tahun 2010 membuat manuver politik dengan menjalin kerjasama dengan Rusia untuk mengajukan proposal keamanan *cyber* ke WTO. Dalam artikel tersebut Timothy Farnsworth mengungkap bahwa Pemerintah China berupaya untuk semakin memperketat kebijakan sensor internetnya dengan adanya ancaman-ancaman baru yang ditimbulkan oleh teknologi informasi.<sup>13</sup> Sementara artikel dari Steven Seidenberg menyorot fakta sebenarnya kebijakan sensor internet China telah melanggar klausul kebebasan informasi yang tertuang dalam perjanjian WTO dimana China merupakan salah satu negara yang terikat dengan perjanjian tersebut.<sup>14</sup> Sehingga WTO sebenarnya dapat melakukan komplain dan

---

<sup>13</sup>Timothy Farnsworth, *China and Russia Submit Cyber Proposal*, Arms Control Today, Vol. 41, No.9, November 2011.

<sup>14</sup>Steven Seidenberg; *Breaking China: WTO Complaint Could End “the Great Firewall” of Internet Ban*, ABA Journal, Vol 96-No.11, November 2010

memberlakukan sanksi terhadap Pemerintah China atas kebijakan sensor internet tersebut.

Studi terhadap kebijakan sensor internet pada dasarnya memang relatif baru dalam ilmu hubungan internasional. Kemunculan konsep-konsep baru dalam dunia militer seperti *cyberwar*, *netwar*, *information warfare*, dan *cyberspace* memunculkan sebuah perspektif baru dalam memahami lanskap perang baru di era teknologi informasi. Sebagaimana diungkap oleh Michael Sheehan bahwa medan perang fisik telah bertransformasi menjadi ruang-ruang *cyber* dan media global, sementara *battlefields* kini telah berubah menjadi *battlespace*.<sup>15</sup> Sehingga untuk memahami perang di abad ke-21 ini pemahaman terhadap perang *cyber* diperlukan oleh para pengkaji studi hubungan internasional.

Oleh karena itu, thesis ini sebenarnya lebih menyorot motif dan tujuan China untuk memberlakukan kebijakan sensor internet. Dengan menggunakan teori sekuriti dari Barry Buzan, studi ini akan memfokuskan pada bagaimana peran negara dalam melakukan sekuritisasi terhadap bidang ideologi, politik, ekonomi, pertahanan-keamanan dan sosial budaya. Konsep sekuritisasi yang diajukan Barry Buzan memang tidak terbatas hanya pada bidang militer saja, namun mencakup bidang lain yang menjadi otoritas negara.<sup>16</sup> Kebijakan sensor internet Pemerintah China akan ditinjau dengan berdasarkan sebuah asumsi bahwa kebijakan tersebut merupakan upaya China melakukan sekuritisasi di bidang ideologi, politik, ekonomi, pertahanan-keamanan, serta bidang sosial budaya.

---

<sup>15</sup>John Baylis, Steve Smith, dan Patricia Owens; *op cit*.

<sup>16</sup>*Ibid*, hal 235.

### 1.5. Konsep *Cyberspace*, *Cyberwarfare*, dan *Internet Censorship*

Paska Perang Dingin, para ilmuwan menyaksikan bahwa terdapat perubahan yang sangat signifikan dalam sistem internasional. Para ahli sepakat bahwa era paska Perang Dingin ini adalah era Globalisasi. Globalisasi menyebabkan lingkungan sistem internasional kini tidak lagi didefinisikan sebagai pertarungan antara ideologi kapitalisme yang dipimpin oleh AS dan Sekutu melawan ideologi sosialisme-komunisme. Bahkan Daniel Bell berani menyatakan bahwa konflik ideologi telah berakhir dengan berakhirnya pengaruh sosialisme-komunisme. Kekuatan yang muncul di abad globalisasi ini dalam beberapa hal lebih multipolar, dalam artian bahwa sistem internasional tidak lagi bipolar sebagaimana era Perang Dingin. Kemunculan negara-negara adidaya baru di Asia, China dan India, menjadikan sistem internasional lebih bervariasi dalam kontestasi politik atau hubungan antar-bangsa.

Perkembangan yang paling mengejutkan di abad globalisasi adalah sebuah fakta bahwa negara kini menjadi lebih bergantung pada pencarian dan pertukaran informasi yang disebut sebagai *cyberspace*. Konsep *cyberspace* didefinisikan sebagai oleh Michael Sheehan sebagai ***“total interconnectedness of human beings through computers and telecommunication”***.<sup>17</sup> Dengan kemunculan sistem teknologi *cyberspace* ini negara-negara kini lebih rentan pada konflik baru yang dinamakan sebagai *cyberwarfare*.

Konsep *cyberwarfare* didefinisikan juga oleh Michel Sheehan sebagai ***“state’s ability to attack another state’s computer and information networks in***

---

<sup>17</sup>John Baylis, *op-cit*, hal 217.

*cyberspace and to protect its own capabilities from attacks by adversaries.*”<sup>18</sup> Konsep *cyberwarfare* ini memiliki dua varian lain yaitu *Information Warfare*, dan *Netwar*. Konsep ini mulai populer digunakan oleh para pengamat militer sejak dua dekade lalu. Pada awal tahun 1990an peneliti seperti John Arquilla dan David Ronfeldt yang bekerja pada Rand Corporation menulis sebuah buku bertajuk “*In Athena’s Camp: Preparing for Conflict in the Information Age.*” Di dalam buku tersebut mereka mengidentifikasi sebuah perang ‘*high-tech*’ model baru. Teori yang mereka kemukakan mulai memperoleh pengakuan oleh lembaga militer AS pada tahun 1995.<sup>19</sup> Tentunya konsep *cyberwarfare* ini dapat dengan mudah diartikan sebagai perang di medan *cyberspace*.

Konsep *cyberspace* dan *cyberwarfare* sangat penting untuk memahami perang dengan menggunakan teknologi tinggi, dimana AS, mencoba untuk mendominasi domain informasi ketika perang fisik terjadi sehingga mereka mampu melaksanakan operasi militernya tanpa adanya perlawanan berarti dari musuh-musuhnya.<sup>20</sup> Target sasaran dalam perang di dunia maya ini adalah pada jaringan informasi militer suatu negara, dan bahkan pada jaringan sistem ekonomi dan politik suatu negara. Di abad ke-21 ini beberapa negara seperti AS, China, India, Rusia, Kuba, UK, Jerman, dan baru-baru saja Iran telah mengembangkan doktrin pengembangan kapabilitas *cyberwarfare* dalam institusi militer dan pemerintahannya.

---

<sup>18</sup>Ibid.

<sup>19</sup>Edward Halpin, Philippa Trevor, et.al; *Cyberwar, Netwar, and the Revolutions in Military Affairs*; Palgrave Macmillan, New York; 2006; hal 3.

<sup>20</sup>John Baylis, Ibid.

Suatu contoh dari adanya *cyberwarfare* ini adalah pengakuan dari pemerintah Iran pada Juni tahun 2010, bahwa pihaknya telah menjadi korban dari serangan *cyber* melalui sebuah virus yang bernama *Stuxnet*. Virus tersebut dilaporkan berasal dari serangan gabungan AS dan Israel. Pemerintah Iran melaporkan bahwa virus tersebut menyerang fasilitas nuklirnya.<sup>21</sup> Pada tahun 2012 dilaporkan bahwa pemerintah Iran telah melakukan serangan balik terhadap bank-bank di Amerika Serikat, Israel, dan beberapa negara Arab.<sup>22</sup> Michael Joseph Gross bahkan menyebut perang antara AS dan Iran merupakan perang di medan *battlespace* yang pertama dalam sejarah.<sup>23</sup>

Dalam perang *cyber* ini medan peperangan telah berganti dari *battlefield* dalam konsep perang fisik, menjadi *battlespace*. Medan *battlespace* ini meliputi tiga dimensi diantaranya penggunaan kekuatan udara, *air-power*, satelit ruang angkasa, dan juga meliputi jaringan komunikasi *cyberspace*.<sup>24</sup> Kekuatan udara yang dimaksud dalam hal ini adalah penggunaan modus pengintaian udara dengan pesawat siluman atau pesawat tanpa awak, *drone*, dan juga radar-radar berteknologi tinggi.

Internet mulai diperkenalkan di China sejak tahun 1994. Dengan semakin canggihnya peperangan di *cyberwarfare* di medan baru yaitu *cyberspace*, kebijakan negara yang paling mungkin adalah melalui adanya *Internet*

---

<sup>21</sup> *Stuxnet Worms: A Cyber-Missile Aimed At Iran?* 24 Desember 2010 [http://www.economist.com/blogs/babbage/2010/09/stuxnet\\_worm](http://www.economist.com/blogs/babbage/2010/09/stuxnet_worm). diakses tanggal 12 desember 2014. pukul 18:00.

<sup>22</sup> Halliday, Josh. *Stuxnet Worm Is The Work of a National Government Agency*. 24 September 2010; <http://www.guardian.co.uk/technology/2010/sep/24/stuxnet-worm-national-agency>, diakses tanggal 12 desember 2014, pukul 18:19.

<sup>23</sup> Gross, Michael Joseph. *Silent War*; Juli 2013 <http://www.vanityfair.com/culture/2013/07/new-cyberwar-victims-american-business>, diakses tanggal 12 desember pukul 18:22.

<sup>24</sup> John baylis, op-cit, hal 217.

*Censorship*. Konteks yang digambarkan di atas merupakan alasan yang mendasari China mengambil kebijakan *internet censorship* sejak tahun 1998. Pada tahun 1998 pemerintah China merilis sebuah proyek baru yang dinamakan sebagai *Golden Shield Project*. Proyek tersebut mulai dijalankan secara efektif sejak tahun 2003.

Program sensor internet tersebut didasari oleh sebuah ungkapan mashur dari Deng Xiao Ping bahwa *“if you open the window for fresh air, you have to expect some flies to blow in.”* Pernyataan tersebut disampaikan pada tahun 1980an yang berbarengan dengan reformasi ekonomi China. Pernyataan tersebut juga merupakan penegasan bahwa tragedi di masa Revolusi Kultural tahun 1970an dapat terulang kembali dengan upaya China untuk membuka kebijakan ekonomi politiknya di era Deng Xiao Ping.

Pada awal internet masuk di sekitar tahun 1994, ada sejumlah kekhawatiran bahwa internet akan menjadi kontraproduktif bagi masyarakat China. Dengan kekayaan informasi yang terkandung di internet, pemerintah dan sejumlah pengamat di China khawatir bahwa ideologi barat akan mengkontaminasi nilai dan budaya masyarakat setempat. Oleh karena itu pada awalnya pemerintah memberlakukan sensor ketat, dengan membatasi internet bagi beberapa lembaga riset dan beberapa institusi pendidikan tinggi. Pada tahun-tahun berikutnya ada perubahan-perubahan dalam kebijakan sensor internet di China. Menurut Robert Zheng, John R. Ouyang dan Feng Rui kebijakan sensorship oleh

pemerintah China dapat dibedakan menjadi beberapa tahap yaitu: *strict censorship*, *half-censorship*, dan *limited self-autonomy*.<sup>25</sup>

Dengan mempertimbangkan bahwa teknologi informasi merupakan kunci bagi produktifitas dan pendapatan ekonomi nasional Komite Sentral Partai Komunis China secara perlahan membuka akses penggunaan internet dan mengurangi sensor dari *strict censorship* menjadi *limited self autonomy* pada tahun 2001. Kebijakan *limited self-autonomy* berarti pemerintah mengizinkan masyarakat untuk mengakses internet dan bahkan diperbolehkan mengembangkan sendiri materi-materi instruksional di dalam web pagenanya.

Pada tahun 2005, pemerintah provinsi dan pemerintah kota China dilaporkan mulai membuat polisi internet untuk memerangi propaganda anti komunisme di dunia maya. Pembentukan polisi internet ini juga ditujukan untuk memfilter dan mengcounter opini-opini buruk China di dunia *cyberspace*. Pada tahun 2013 dilaporkan bahwa jumlah personil polisi internet ini mencapai 2 juta orang.<sup>26</sup> Jumlah tersebut menandai keseriusan pemerintah China menjalankan program *internet censorship*.

Akhir-akhir ini pemerintah China mulai membuat daftar hitam domain website misalnya domain laman situs dari Jepang ([.jp](#)) dan domain atas ([.com](#)). Selain itu pemerintah China memblacklist beberapa kata kunci seperti *Democracy*, *Human Rights*, *Dictatorship*, *Despotism*, dan lain sebagainya.<sup>27</sup>

---

<sup>25</sup> Robert Zheng, John R Ouyang, Feng Rui; *op-cit*.

<sup>26</sup> Le, Dong. *China Employs Two Million Microblog Monitors State Media Says*. 4 Oktober 2013 <http://www.bbc.co.uk/news/world-asia-china-24396957>, diakses tanggal 24 Desember 2014, pukul 19:00.

<sup>27</sup> *Censorship of Google Searches in China*. <https://en.greatfire.org/search/google-searches>, diakses tanggal 24 Desember 2014 pukul 19.15.

Menurut perkiraan data bahwa jumlah laman web dengan domain asing yang diblokir oleh pemerintah China hingga saat ini berjumlah 4.480.<sup>28</sup>

Berdasarkan penalaran di atas konsep *internet censorship*, *cyberspace*, dan *cyberwarfare* merupakan variable-variable penting dalam penelitian ini. Variable tersebut akan dianalisis dengan menggunakan kerangka teori keamanan dan sekuritisasi yang diungkapkan oleh Barry Buzan sebagaimana dijelaskan dalam poin di bawah ini.

## **I.6. Teori Keamanan dan Sekuritisasi**

Saya merujuk berdasarkan konsep keamanan yang dijelaskan oleh Barry Buzan, bahwa:

*“Security is primarily about the fate of human collectivities, about the pursuit of freedom of threat. The bottom line is about survival, but it also includes a substantial range of concern about a condition of existence. Security is affected by factors in five major sectors: military, political, economic, societal, and environment.”*<sup>29</sup> (keamanan adalah hal utama yang berkaitan dengan nasib sekumpulan manusia, juga berkaitan dengan keyakinan bebas dari ancaman. Permasalahan dasarnya adalah tentang kelangsungan hidup tetapi ini juga mencakup banyak hal atau urusan tentang sebuah kondisi kelangsungan kehidupan. Keamanan dipengaruhi oleh faktor-faktor yang terdiri dari 5 sektor utama yaitu, militer, politik, sosial, ekonomi, dan lingkungan).

---

<sup>28</sup> *Online Censorship in China*. <https://en.greatfire.org/>, diakses tanggal 24 Desember pukul 19.10.

<sup>29</sup> Anak Agung Bayu Perwita, *“Human Security Dalam konteks Global dan Relevansinya Bagi Indonesia”*, Analisis CSIS Tahun XXXII/2003 No. 1, Jakarta, CSIS, 2003, hal.70.

Jika dikontekstualisasikan kepada permasalahan sensor internet di China, konsep keamanan disini akan dianalisis berdasar beberapa aspek yaitu: aspek ideologi, aspek politik, aspek pertahanan - keamanan, aspek ekonomi, dan aspek sosial budaya.

Lima sektor konsep keamanan yang dijelaskan oleh Barry Buzan di atas mengalami perkembangan yang cukup signifikan, yaitu:

1. *The origin of threats*

Pada masa perang dingin ancaman yang akan dihadapi oleh sebuah Negara adalah ancaman dari Negara lain dalam bentuk perang konvensional. Dalam dunia hubungan internasional, hal ini disebut sebagai konsep keamanan tradisional. Namun dewasa ini ancaman bisa berasal dari wilayah domestik maupun global, bahkan melalui jaringan komunikasi seperti internet. Sebagaimana dijelaskan di atas ancaman tersebut diantaranya adalah kejahatan-kejahatan yang timbul di ruang *cyber* seperti *cyber attack*, *cyber terrorist*, *cyber crime*, dan suatu konsep besar yang merujuk pada perang baru yang biasa disebut dengan *cyberwarfare*.

2. *The nature of threats*

Pada masa perang dingin, ancaman lebih berupa ancaman militer, namun dewasa ini ancaman bersifat sangat kompleks seperti, terorisme dan ancaman dalam bentuk keamanan informasi. Lanskap keamanan telah berubah menjadi ruang-ruang di dunia maya, *cyberspace*. Dalam ruang *cyber* sulit menentukan siapa yang berseberangan secara politik dan kepentingan apa yang tersembunyi di ruang *cyber* tersebut.

### 3. *Changing response*

Pada masa perang dingin dalam merespon suatu ancaman terhadap keamanan lebih fokus dalam bentuk materialistik, namun dewasa ini lebih berkembang dan bergeser pada perkembangan-perkembangan sosial, budaya, politik, dan hukum dalam mewujudkan sebuah keamanan yaitu melalui media informasi seperti internet.

### 4. *Changing responsibility of security*

Pada masa Perang Dingin, actor atau pihak yang paling bertanggungjawab terhadap keamanan adalah Negara, namun dewasa ini tercapainya suatu keamanan bukan hanya peran dari sebuah Negara. Masalah keamanan yang sangat rawan dan mulai menjadi perhatian bersama, menuntut semua pihak untuk berperan aktif untuk mewujudkan satu keamanan.

### 5. *Core value of security*

Pada masa Perang Dingin nilai-nilai keamanan terfokus pada nilai-nilai kemerdekaan, kedaulatan, dan integritas territorial. Namun dewasa ini keamanan menjadi lebih rumit menyangkut pada penghormatan atau penghargaan terhadap Hak Asasi Manusia, Demokrasi, dan upaya memerangi kejahatan-kejahatan transnasional, termasuk kebebasan individu untuk mengakses data informasi melalui internet.

Dengan menggunakan 5 konsep di atas, akan bisa dianalisa mengapa internet merupakan variable yang berpengaruh terhadap berkembangnya konsep keamanan di era globalisasi ini dan mengapa perluanya suatu Negara yaitu China

dalam pembahasan ini untuk melakukan pengamanan informasi dengan mengontrol akses internet pada masyarakatnya.

Menurut Barry Buzan dalam bukunya yang berjudul *Security, A New Framework for Analysis*, ancaman-ancaman politis ditujukan kepada stabilitas negara. Tujuannya bisa berbeda, mulai dari menekan pemerintah terkait dengan kebijakan yang telah dibuatnya, sampai menggulingkan pemerintah, dan menginterupsi struktur politik negara untuk memperlemah. Inti dari sebuah negara adalah identitas nasionalnya dan mengorganisir ideologi, serta institusi-institusi biasanya merupakan target utama dari ancaman. Karena negara merupakan entitas politik, ancaman-ancaman politis pun biasanya sama ditakutinya dengan ancaman militer. Apalagi, jika target adalah negara yang lemah.

Pendapat Buzan itu menunjukkan betapa sulitnya untuk mendefinisikan keamanan politik, sekaligus betapa sulitnya untuk membatasinya, terutama dalam kaitannya dengan keamanan sosial dan militer-sosial berhubungan dengan identitas nasional, militer dengan penggunaan kekuatannya.

**Sekuritisasi** sendiri dapat diartikan sebagai versi ekstrim dari politisasi.<sup>30</sup> Dalam sekuritisasi, aktor melakukan perluasan cakupan keamanan nasional ke dalam berbagai bidang sehingga semua masalah bisa dilihat sebagai keamanan nasional melalui proses politik. Melalui sekuritisasi, terjadi pergeseran isu dari yang mulanya hanya isu politik biasa, menjadi isu yang diasumsikan urgent dan memerlukan penanganan cepat, bahkan tanpa peraturan normal dan aturan-aturan pembuatan keputusan lainnya. Inilah esensi dari sekuritisasi. Ada beberapa konsep

---

<sup>30</sup>Barry Buzan, Ole Waever, Jaap de Wilde; *Security: A New Framework for Analysis*, (London: Lynne Rienner Publisher, 1998), hlm. 23.

dalam sekuritisasi yang menunjukkan bagaimana aktor melakukan sekuritisasi. Konsep-konsep tersebut yaitu aktor sekuritisasi, *speech act*, *existential threat*, *referent object*, dan *audience*.<sup>31</sup> Sesuai namanya, aktor sekuritisasi adalah pihak yang mengusahakan sekuritisasi. Aktor tersebut akan melakukan usaha-usaha sosialisasi ide atau yang disebut juga *speech act*, dengan cara mengampanyekan *existential threat*, yaitu isu-isu ancaman eksistensial yang diwacanakan. Usaha sekuritisasi ini ditujukan kepada *audience*, atau pihak-pihak yang ingin dipengaruhi oleh aktor untuk mempercayai *existential threat*, dan akan berpengaruh pada *referent object*, yaitu pihak yang akan terancam jika isu tersebut tidak disikapi secara serius. Cara terbaik untuk menentukan *securitizing actors* adalah dengan melihat logika dari sebuah pernyataan sekuritisasi. Ketika seorang individu mendeklarasikan sebuah pernyataan sebagai isu sekuritisasi dengan menggunakan logika negara, maka *securitizing actor* dari proses tersebut adalah Negara dan bukan individu.

### **I.7. Thesis Statement**

Ide dasar penulisan tesis ini adalah kemunculan fenomena baru Politik Internasional di era globalisasi yang dinamakan sebagai *Cyberspace*. Perang-perang konvensional telah ditinggalkan dan kini muncul perang baru di dunia maya yaitu *cyberwarfare*. Negara pun mengantisipasi perang *cyber* tersebut dengan kebijakan *internet censorship*.

Untuk menjawab rumusan masalah bagaimana upaya China melakukan sekuritisasi terhadap bidang ideologi, bidang politik, bidang pertahanan-kemanan,

---

<sup>31</sup>*ibid.*

bidang ekonomi, dan bidang sosial budaya China melalui kebijakan sensor Internet, penulis memiliki beberapa asumsi dasar, yaitu: benar China melakukan sensor internet sebagai upaya untuk membentengi dari pengaruh besar pertukaran informasi di dunia *cyber* seperti masuknya pengaruh nilai-nilai ideologi barat. Kekhawatiran tersebut tidak saja terfokus pada aspek nilai ideologis, namun juga berimbas pada pengaruh lain di bidang politik, ekonomi, pertahanan, dan sosial budaya.

Di bidang politik, China berupaya membendung arus besar demokratisasi yang masif terjadi di negara dunia kedua dan negara dunia ketiga, terutama sejak era paska Perang Dingin. Indikasi ini dapat dilihat dari kebijakan pemerintah China yang akhir-akhir ini memblokir beberapa kata kunci di situs pencari (Google dan Yahoo) khususnya yang berkaitan dengan ‘demokrasi,’ ‘otoritarianisme,’ dan despotisme, serta kata kunci yang berhubungan dengan tokoh nasional demokrat China seperti Sun Yat Sen, Chiang Kai Sek, Zhou Enlai, dan tokoh-tokoh aktifis demokrasi lainnya.

Di bidang pertahanan keamanan kebijakan sensor internet merupakan upaya pemerintah China membangun sistem *firewall* (pertahanan komputer) bagi jaringan informasi dan fasilitas militernya. Sistem pertahanan di bidang teknologi informasi ini penting bagi China mengingat saat ini dunia kemiliteran di China telah mengalami perubahan sejak diperkenalkannya komputerisasi persenjataan dan penggunaan satelit dalam sebuah program yang dikenal dengan konsep *revolution in military affairs (RMA)*.

Di bidang ekonomi, kebijakan sensor internet China relevan dengan upaya China untuk menguasai perekonomian global dewasa ini. Sistem ekonomi yang berkembang kini menuntut kemajuan teknologi informasi sebagai kunci utama bagi daya kompetitif suatu bangsa dalam kontestasi global. Sehingga upaya-upaya untuk membangun bisnis teknologi informasi yang kuat diperlukan oleh suatu negara. Kebijakan sensor ketat pemerintah China merupakan upaya proteksi Pemerintah China terhadap perusahaan teknologi informasi lokal seperti Baidu, Tencent, dan Alibaba di tengah kompetisi dengan perusahaan teknologi informasi asing seperti Google, Yahoo, Youtube, Facebook.

Di bidang sosial budaya, China saat ini tengah berupaya membendung arus *westernisasi* dan masuknya pengaruh budaya-budaya luar terhadap kehidupan sosial budaya masyarakat China. Kemunculan internet mawadahi pertukaran informasi, nilai, dan gagasan yang cenderung bebas antara masyarakat di suatu negara dengan masyarakat di negara lain. Oleh karena itu kebijakan sensor internet ini merupakan upaya paling cermat dalam menghadang pengaruh-pengaruh budaya dari luar masuk ke China daratan. Pemerintah China berupaya memproteksi jaringan informasi dari adanya intervensi dunia luar dalam konflik di daerah *Xinjiang* antara Pemerintah melawan kelompok separatis islam *Uyghur*.

## **1.8. Metodologi**

### **1.8.1. Unit Analisa dan Unit Eksplanasi Penelitian.**

Ilmu hubungan internasional adalah studi yang sangat luas yang mencakup studi tentang perilaku individu, negara, dan juga isu-isu dalam sistem

internasional. Dalam hal ini Mochtar Mas'oe'd menyebutkan tentang perlunya sebuah klasifikasi tentang **unit analisa** dan **unit eksplanasi** dalam studi hubungan internasional. **Unit analisa** adalah obyek yang perilakunya akan dianalisa, atau yang disebut sebagai *dependent variable*. Sementara **Unit Eksplanasi** adalah obyek yang memberikan penjelasan terhadap perilaku **unit analisa**, atau yang mempengaruhi perilaku unit analisa. **Unit Eksplanasi** disebut juga sebagai *independent variable*.

Lebih lanjut Menurut Mochtar Mas'oe'd terdapat tiga hubungan antara *dependent variable* dan *independent variable* atau antara unit analisa dan unit eksplanasi; yaitu model korelasionis, model induksionis, dan model reduksionis.<sup>32</sup> Pengklasifikasian antara unit analisa dan unit eksplanasi beserta model hubungannya dijelaskan dalam tabel sebagai berikut:

**Tabel 1.1. Unit Analisa dan Unit Eksplanasi dalam Studi Hubungan Internasional**

		Unit Analisa		
		Individu	Negara-bangsa	Sistem regional dan global
Unit Eksplanasi	Individu	<b>korelasionis</b>	<b>reduksionis</b>	<b>reduksionis</b>
	Negara-bangsa	<b>induksionis</b>	<b>korelasionis</b>	<b>reduksionis</b>
	Sistem regional & global	<b>induksionis</b>	<b>induksionis</b>	<b>korelasionis</b>

Sumber: Data diolah dari buku Mochtar Mas'oe'd, *Ilmu Hubungan Internasional: Disiplin dan Metodologi*.

<sup>32</sup>Mochtar Mas'oe'd; *Ilmu Hubungan Internasional: Disiplin dan Metodologi*; Jakarta: LP3ES; 1994; hal 40 – 42.

Merujuk pada fokus penelitian dan klasifikasi Mochtar Mas' oed di atas maka penelitian ini menempatkan unit analisa negara-bangsa dan unit eksplanasi sistem internasional. Unit analisa negara bangsa disini menempatkan kebijakan pemerintah China dalam melakukan sensor internet sebagai variabel dependen. Kebijakan sensor internet disini memiliki kaitan dengan kebijakan China di bidang sekuritisasi ideologi, politik, pertahanan-keamanan, ekonomi, dan bidang sosial budaya.

Sementara unit eksplanasi atau obyek yang mempengaruhi kebijakan pemerintah China adalah munculnya sistem jaringan informasi internet yang disebut dengan *cyberspace*. Jaringan informasi internet ini mampu menjangkau seluruh negara di Dunia sehingga merupakan bagian dari Unit Analisa Sistem Internasional.

Menurut J. David Singer, dalam level analisis negara bangsa ada sebuah keuntungan diamana dalam analisis ini peneliti akan menemukan perbedaan-perbedaan signifikan antara aktor-aktor dalam hubungan internasional. Hal itu disebabkan dalam level analisis ini peneliti tidak memerlukan pertalian kesamaan-kesamaan antara negara-negara bangsa, namun level analisis ini memungkinkan peneliti untuk menguji negara bangsa tertentu secara lebih mendetail. Kelemahannya adalah bahwa dalam level analisis ini peneliti tidak akan mampu melakukan perbandingan kebijakan luar negeri antara satu negara dengan negara lainnya.<sup>33</sup>

---

<sup>33</sup>J. David Singer; *The Level of Analysis Problem in International Relations*; Journal of World Politics, Vol.14, No.1, The International Systems: Theoretical Essays; 1961; hal 82.

### 1.8.2. Jenis Penelitian

Jenis penelitian yang digunakan dalam penulisan penelitian ini adalah penelitian kualitatif. Menurut Bogdan dan Taylor penelitian kualitatif adalah prosedur penelitian yang menghasilkan data deskriptif berupa kata-kata tertulis atau lisan dari orang-orang atau perilaku yang dapat diamati.<sup>34</sup> Penelitian kualitatif menghasilkan penemuan-penemuan yang tidak dapat dicapai dengan menggunakan prosedur statistik atau dengan cara-cara kuantifikasi. Penelitian kualitatif dapat menunjukkan gejala kehidupan masyarakat, sejarah, tingkah laku, fungsionalisasi organisasi, pergerakan sosial, dan hubungan kekerabatan.<sup>35</sup>

Penelitian kualitatif mencoba berupaya menganalisis data-data yang bersifat *interpretivisme*, berupaya memahami fenomena sosial (*understanding*), dan memahami alasan tindakan sosial (*reasons*).<sup>36</sup> Data-data dianalisis dari fenomena sosial atau lingkungan sosial yang terdiri atas pelaku, kejadian, tempat, dan waktu. Latar sosial tersebut digambarkan sedemikian rupa sehingga dalam peneliti melakukan pengembangan pertanyaan-pertanyaan dasar yaitu apa dan bagaimana kejadian itu terjadi, siapa yang terlibat dalam kejadian tersebut, kapan terjadinya, serta bagaimana runtutan dan logika dari kejadian tersebut.

Titik picu penelitian itu adalah munculnya fenomena globalisasi yang melahirkan gejala-gejala sosial baru di masyarakat. Gejala tersebut secara lebih spesifik adalah kebijakan sensor internet oleh Pemerintah China. Penelitian ini akan menjelaskan keterkaitan logis antara sebab munculnya kebijakan tersebut

---

<sup>34</sup>Lexy Moleong; *Metodologi Penelitian Kualitatif (Ed. Revisi)*; Bandung: PT Remaja Rosdakarya; hal 4.

<sup>35</sup>Ibid.

<sup>36</sup>Burhan Bungin, *Metodologi Penelitian Kualitatif*; Jakarta: PT Raja Grafindo Persada; hal 46.

dan untuk apa kebijakan tersebut dibuat dalam sebuah *setting* masyarakat yang saling terhubung melalui jaringan komunikasi *cyberspace*. Upaya untuk memperkuat kontrol pemerintah terhadap internet ini salah satunya adalah satu bagian dari strategi besar dalam perang baru yang disebut sebagai *cyberwarfare*.

### 1.8.3. Metode pengumpulan data

Data yang digunakan dalam penelitian ini lebih banyak berasal dari pengumpulan data sekunder. Data sekunder merupakan sumber data penelitian yang diperoleh peneliti secara tidak langsung melalui media perantara (diperoleh dan dicatat oleh pihak lain). Data sekunder umumnya berupa bukti, catatan atau laporan historis yang telah tersusun dalam arsip (data dokumenter) yang dipublikasikan maupun yang tidak dipublikasikan.

Perolehan data sekunder ini adalah dengan menggunakan teknik pengumpulan data yang disebut sebagai studi literatur. Dalam studi literatur sumber utama data yang valid berasal dari buku-buku dan jurnal yang telah melalui proses *peer review*. Sedangkan sumber data yang lain berasal dari data-data dari media massa dan internet yang berkaitan dengan topik penelitian akan disaring secara hati-hati dan memperhatikan aspek relevansi data dengan topik penelitian.

### 1.8.4. Metode analisis data

Menurut J. David Singer ada tiga macam model analisis dalam ilmu hubungan internasional yaitu analisis deskriptif, eksplanatif, dan prediktif. Dalam analisis **deskriptif** peneliti harus menyajikan data mengenai fenomena sosial secara holistik dan tidak menyimpang untuk memperoleh gambaran lengkap

mengenai realitas obyektif. Namun kelemahan dari model analisis ini adalah kesulitan peneliti untuk menggambarkan fenomena sosial secara menyeluruh, bahkan hal itu hampir tidak mungkin tercapai. Misalnya kita ambil contoh dari analogi seseorang pembuat peta (*cartographer*) yang diberikan tugas untuk membuat gambar tentang bentang alam sebuah pulau. *Cartographer* tersebut akan menemui kesulitan memindahkan gambar multi-dimensi dari sebuah bentang alam menjadi peta dua dimensi tanpa adanya distorsi (penyimpangan dari kenyataan) atau penyederhanaan melalui skala-skala tertentu.<sup>37</sup>

Sementara itu metode analisis **eksplanatif** memungkinkan peneliti untuk mencari hubungan antar fenomena yang sedang diinvestigasi. Metode analisis eksplanatif memungkinkan peneliti untuk mengkaji hubungan sebab akibat antar variabel. Model **Prediktif** memerlukan sebuah pengkajian yang mampu menjawab pertanyaan peneliti mengenai prediksi terhadap suatu fenomena. Namun bukan berarti model Prediktif ini memiliki derajat kesulitan yang lebih besar daripada model eksplanatif dan deskriptif.<sup>38</sup> Misalnya kita mampu secara akurat memprediksi bahwa suatu negara akan merespon suatu fenomena politik antar bangsa dengan kekuatan militer. Tentunya prediksi tersebut yang merupakan hasil dari deskripsi tentang fenomena dan adanya eksplanasi antar variabel penelitian.

Berdasarkan uraian-uraian dalam *literature review* dan level analisis di atas, penulis menetapkan bahwa model analisis data yang digunakan dalam penelitian ini adalah metode **analisis deskriptif**. Peneliti akan menggambarkan secara holistik jawaban dari pertanyaan penelitian mengenai sejauh mana

---

<sup>37</sup>J. David Singer; Op.Cit; hal 78.

<sup>38</sup>Ibid.

kebijakan sensor internet oleh Pemerintah China merupakan upaya sekuritisasi terhadap ideologi, politik, pertahanan keamanan, ekonomi, dan sosial budaya. Penggambaran tersebut juga akan meliputi penjelasan tentang bagaimana realitas sistem internasional sebagai unit eksplanasi mempengaruhi kebijakan pemerintah China memberlakukan sensor internet. Penulis juga akan mendeskripsikan fenomena kemunculan perang di ruang *cyber* yang disebut dalam konsep akademik sebagai *cyber warfare*.

#### **1.8.5. Ruang Lingkup Penelitian**

Penelitian ini memfokuskan pada kebijakan Negara dalam melakukan sekuritisasi di bidang ideologi, politik, pertahanan – keamanan, ekonomi, dan sosial budaya melalui kebijakan sensor internet. Kebijakan sensor internet mulai diberlakukan oleh Pemerintah China sejak awal tahun 1990an ketika negara tersebut mulai membuka diri terhadap dunia luar. Kebijakan tersebut hingga kini masih berlangsung dan menjadi sorotan dunia internasional mengingat China merupakan salah satu negara yang berani melakukan kebijakan sensor yang kuat di bidang teknologi informasi.

Sementara itu topik lain yang menjadi pokok bahasan adalah konteks lingkungan internasional yang dipilih menjadi unit eksplanasi dari penelitian ini. Dalam penelitian ini penulis menetapkan bahwa perkembangan dunia *cyberspace* dan *cyberwarfare* adalah unit eksplanasi dalam penelitian ini. Unit eksplanasi tersebut memang cukup luas mengingat merupakan bagian dari unit eksplanasi sistem internasional.

### 1.8.6. Sistematika Penulisan

Thesis ini terdiri dari lima bab yang dapat dibaca secara terpisah maupun secara berurutan. Bab I adalah bagian pendahuluan yang terdiri dari latar belakang masalah, pertanyaan penelitian, tujuan penelitian, *thesis statement*, dan metodologi penelitian. Dalam Bab 1 penulis mencoba mengeksplorasi asal muasal persoalan sensor internet di China dengan melihatnya dari kaca mata perubahan politik paska Perang Dingin. Dalam bagian ini penulis juga mengerucutkan permasalahan yang berkaitan dengan tema dalam bentuk pertanyaan penelitian, serta membuat pernyataan dugaan (*thesis statement*). Penulis juga menjabarkan pisau analisa metodologis yang dipakai dalam penelitian ini.

Bab II mendeskripsikan *Internet Censorship* di China khususnya mengenai sejarah kemunculan fenomena tersebut dalam dunia hubungan internasional. Bab II ini terdiri dari beberapa sub-bagian yang diantaranya menjelaskan sejarah kemunculan internet dan dampaknya terhadap misi penyadapan di abad ke-21 dan munculnya revolusi sistem persenjataan di tubuh militer.

Pada Bab III penulis memfokuskan pembahasan pada strategi atau kebijakan China menghadapi bentuk perang baru dengan nama *cyber attack*, *cyber terrorism*, dan *cyber warfare*. Beberapa sub bagian di dalamnya terdiri dari penjelasan-penjelasan tentang konteks penerimaan internet di China dan perubahan kebijakan pemerintah dalam mensensor internet. Dalam sub bagian terakhir penulis melengkapi pembahasan ini dengan mengemukakan fakta-fakta baru seputar kebijakan sensor internet di abad ke-21.

Pada Bab IV penulis mengerucutkan permasalahan sensor internet di China pada teori sekuritisasi yang dikemukakan oleh Barry Buzan. Sebagaimana yang dijabarkan oleh Buzan dalam teori sekuritisasi, bab ini akan dibagi menjadi lima sub bagian yang masing-masing membahas motif dan tujuan China dalam melakukan sekuritisasi di bidang Ideologi, Politik, Pertahanan-Keamanan, Ekonomi, dan Sosial Budaya. Bab ini sekaligus bertujuan untuk menjawab pertanyaan penelitian dan mencocokkan apakah *thesis statement* yang dibuat pada Bab I sesuai dengan temuan-temuan fakta selama proses penelitian.

Bab V merupakan kesimpulan penulis tentang keseluruhan penelitian ini. Pada bab ini penulis mensarikan temuan-temuan fakta dalam tiap bab untuk membuat ikhtisar atau menemukan intisari dari penelitian ini.