KERJA SAMA BILATERAL AS-INDIA TERHADAP CYBER SECURITY (2016-2021)

SKRIPSI

OLEH:

FIKRI FEBRIANT MAHARDIKA

E061181526

HUBUNGAN INTERNASIONAL

FAKULTAS ILMU SOSIAL DAN ILMU POLITIK

UNIVERSITAS HASANUDDIN

MAKASSAR

2024

HALAMAN PENGESAHAN

JUDUL : KERJASAMA BILATERAL AS-INDIA TERHADAP CYBER SECURITY (2016-2021)

N A M A : FIKRI FEBRIANT MAHARDIKA

N I M : E061181526

DEPARTEMEN : ILMU HUBUNGAN INTERNASIONAL

FAKULTAS : ILMU SOSIAL DAN ILMU POLITIK

Makassar, 16 Januari 2024

Mengetahui :

Pembimbing I,	Pembimbing II,
M. Imran Hanafi, MA, M.Ec.	**Nurjannah Abdullah, S.IP, MA.**
NIP. 196307041988031001	NIP. 198901032019032010

Mengesahkan :

Sekretaris Departemen Hubungan Internasional,

Aswin Baharuddin, S.IP, MA.

NIP. 198607032014041002

HALAMAN PENERIMAAN TIM EVALUASI

JUDUL : KERJASAMA BILATERAL AS-INDIA TERHADAP CYBER SECURITY (2016-2021)

N A M A : FIKRI FEBRIANT MAHARDIKA

N I M : E061181526

DEPARTEMEN : ILMU HUBUNGAN INTERNASIONAL

FAKULTAS : ILMU SOSIAL DAN ILMU POLITIK

Telah diterima oleh Tim Evaluasi Sarjana Fakultas Ilmu Sosial dan Ilmu Politik Universitas Hasanuddin Makassar untuk memenuhi syarat-syarat guna memperoleh gelar sarjana pada Departemen Ilmu Hubungan Internasional pada hari Jum'at, 22 Desember 2023.

TIM EVALUASI

Ketua : M. Imran Hanafi, MA, M.Ec. .....

Sekretaris : Abdul Razaq Z Cangara, S.IP, M.Si, MIR. .....

Anggota : 1. Ishaq Rahman, S.IP, M.Si. .....

2. Aswin Baharuddin, S.IP, MA .....

3. Nurjannah Abdullah, S.IP, MA .....

PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini:

Nama : Fikri Febriant Mahardika

NIM : E061181536

Program Studi : Ilmu Hubungan Internasional

Jenjang : S-1

Menyatakan dengan ini bahwa karya tulisan saya yang berjudul:

"KERJA SAMA BILATERAL AS-INDIA TERHADAP CYBER SECURITY (2016-2021)"

Adalah karya tulisan saya sendiri dan bukan merupakan pengambilalihan tulisan orang lain, dan bahwa skripsi ini benar-benar merupakan hasil karya saya sendiri. Apabila di kemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan skripsi ini merupakan hasil karya orang lain, saya bersedia menerima sanksi atas perbuatan tersebut.

Makassar, 29 Januari 2024

Pernyataan,

Fikri Febriant Mahardika

KATA PENGANTAR

Dengan memanjatkan puji syukur atas ke hadirat Allah SWT yang telah memberikan rahmat dan karunia-Nya sehingga Penulis dapat menyelesaikan tugas akhir (skripsi) dengan judul "KERJA SAMA BILATERAL AS-INDIA TERHADAP CYBER SECURITY (2016-2021)" sebagai salah satu persyaratan dalam memperoleh gelar sarjana Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Hasanuddin. Penulis menyadari bahwa dalam penyusunan skripsi ini masih terdapat kekurangan, serta berbagai kendala yang di alami oleh Penulis dalam penyusunan skripsi ini

Skripsi ini masih jauh dari kesempurnaan, untuk itu kritik serta saran yang membangun dari para pembaca tentunya sangat diperlukan agar ke depannya Penulis dapat menghasilkan karya yang lebih baik. Skripsi ini disusun dengan baik berkat bantuan dari banyak pihak yang telah memberikan bimbingan dan dukungan kepada Penulis. Ucapan terima kasih yang sebesar-besarnya Penulis sampaikan kepada keluarga besar, khususnya kedua Orang Tua serta saudara Saya tercinta yang senantiasa memberikan dukungan, motivasi, dan juga doa yang membantu kelancaran penyusunan skripsi ini. Pada kesempatan ini, penulis juga mengucapkan terima kasih yang sebesar-besarnya kepada:

1. Rektor Universitas Hasanuddin, Bapak Prof. Dr. Ir. Jamaluddin Jompa, M. Sc, beserta jajarannya.
2. Rektor Universitas Hasanuddin periode 2014-2022, Ibu Prof. Dr. Dwia Aries Tina Pulubuhu M. A, beserta jajarannya.
3. Dekan Fakultas Ilmu Sosial dan Ilmu Politik, Dr. Phil. Sukri, M. Si dan jajarannya serta seluruh staf fakultas.
4. Ketua Departemen Ilmu Hubungan Internasional, Bapak Prof. Drs. H. Darwis, M.A, Ph. D.
5. Bapak Drs. H.M.Imran Hanafi, MA., M.Ec. selaku dosen pembimbing I, dan Nurjannah Abdullah, S.IP, MA. selaku dosen pembimbing II.

6. Seluruh dosen Departemen Ilmu Hubungan Internasional dan juga seluruh staf Departemen yang telah membantu.
7. Untuk orang tuaku, Tamzil Binawan AP., M.Si. dan Risma Rulani
8. Untuk saudaraku Fitra Adetya Mahaputra
9. Untuk seluruh sahabat-sahabatku, dan teman seangkatan REFORMA 18 serta teman seperjuangan penulis yang selama ini memberikan dukungan dan motivasi kepada Penulis.

Fikri Febriant Mahardika

Penulis

ABSTRAK

Fikri Febriant Mahardika (E061181526) "Kerja Sama Bilateral As-India Terhadap Cyber Security (2016-2021)", di bawah bimbingan Drs. H.M.Imran Hanafi, MA., M.Ec. selaku dosen pembimbing I, dan Nurjannah Abdullah, S.IP, MA. selaku dosen pembimbing II pada Departemen Ilmu Hubungan Internasional, Fakultas Ilmu Sosial dan Ilmu Politik, Universitas Hasanuddin.

Pada era digital yang terus berkembang, Perkembangan teknologi telah menjadi pendorong terhadap meningkatnya produktivitas dan kualitas hidup individu maupun negara. Namun perkembangan tersebut juga mendorong dampak negatif seperti munculnya cyber criminal yang mengeksploitasi teknologi. Keberadaan cyber criminal tentu saja akan mendorong timbulnya permasalahan cyber crime, khususnya pada lingkup cyberspace negara. Negara sendiri mempunyai tanggung jawab untuk melindungi masyarakatnya termasuk dalam bentuk berbagai macam cyber threat. Oleh karena itu dalam upaya menekan aktivitas cyber crime, negara harus memandang akan pentingnya untuk mengembangkan cyber security.

Penelitian ini bertujuan untuk mengetahui hubungan bilateral Amerika Serikat dan India dalam menekan aktivitas cyber crime, serta dampak implementasi kerangka kerja yang di sepakati oleh kedua negara terhadap cyber security. Dalam penelitian ini penulis menggunakan metode penelitian kualitatif dengan mengumpulkan data-data yang relevan terhadap judul penulis melalui studi pustaka. Hasil dari penelitian ini menjelaskan mengenai hubungan bilateral Amerika Serikat dan India, khususnya dalam konteks cyber security serta langkah-langkah yang di ambil oleh kedua negara dalam upaya untuk menekan aktivitas cyber crime. Dalam komitmen kedua negara dalam memerangi cyber crime, terdapat peningkatan terhadap intensitas hubungan bilateral antara Amerika Serikat dan India.

Kata Kunci: Amerika Serikat, India, Hubungan Bilateral, Cyber Security, Cyber Crime, Cyberspace, Cyber Threat, Kerangka Kerja

ABSTRACT

Fikri Febriant Mahardika (E061181526) "US-INDIA BILATERAL COOPERATION ON CYBER SECURITY (2016-2021)", under the guidance of Drs. H.M.Imran Hanafi, MA., M.Ec. as the first supervisor, and Nurjannah Abdullah, S.IP, MA. as the second supervisor the Department of International Relations, Faculty of Social and Political Sciences, Hasanuddin University

In the ever-evolving digital age, technological development has been a driving force behind the increase in productivity and quality of life for individuals and countries. However, this development also drives the negative impact such as the emergence of cyber criminals who exploit technology. The existence of cyber criminals will certainly lead to the emergence of cyber crime problems, especially in the cyberspace of the country. The state itself has a responsibility to protect its citizens, including from various forms of cyber threats. Therefore, in an effort to suppress cyber crime activities, the state must see the importance of developing cyber security.

This study aims to determine the bilateral relationship between the United States and India to suppress cyber crime activities, as well as the impact of the implementation of the framework agreed upon by the two countries on cyber security. In this study, the author used a qualitative research method by collecting data relevant to the author's title through a literature review. The results of this study explain the bilateral relationship between the United States and India, especially in the context of cyber security, as well as the steps taken by both countries in an effort to suppress cyber crime activities. In the commitment of both countries in combating cyber crime, there has been an increase in the intensity of the bilateral relationship between the United States and India.

Keywords: United States, India, Bilateral Relation, Cyber Security, Cyber Crime, Cyberspace, Cyber Threat, Framework

RANCANGAN KOMPOSISI BAB

BAB I PENDAHULUAN

A. Latar Belakang
B. Batasan dan Rumusan Masalah
C. Tujuan Penelitian
D. Manfaat Penelitian
E. Kerangka Konseptual
F. Metode Penelitian

BAB II TINJAUAN PUSTAKA

A. Kerja Sama Bilateral
B. Konsep *Cyber Security*

BAB III GAMBARAN UMUM

A. Hubungan bilateral AS-India Dalam Bidang Cyber Security
B. Kebijakan AS-India Mengenai *Cyber Security*
C. Kebijakan AS-India Dalam Memerangi *Cyber Attack*

BAB IV DAMPAK KEBIJAKAN "THE FRAMEWORK FOR US-INDIA CYBER REALTIONSHIP" DALAM MENGEMBANGKAN CYBER SECURITY

A. Implementasi kebijakan "*The Framework for US-India Cyber Realtionship*"
B. Peluang dan Tantangan Kerja Sama AS-India dalam mengembangkan *Cyber Security*
C. Dampak Kebijakan "*The Framework for US-India Cyber Relationship*" terhadap aktivitas *Cyber Crime*

BAB V PENUTUP

A. Kesimpulan
B. Saran

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

A. Latar Belakang

Pada era digital ini, ilmu pengetahuan dan teknologi telah berkembang pesat yang diikuti oleh implikasi yang bersifat kompleks terhadap kehidupan manusia. Implikasi tersebut juga memberikan dampak terhadap bagaimana negara menjalankan hubungan bilateralnya. Namun dari dampak positif yang diberikan oleh perkembangan tersebut terdapat juga dampak negatif. Seperti munculnya individu yang memiliki pandangan oportunistis dengan tujuan untuk mendatangkan keuntungan untuk diri sendiri, dengan mengeksploitasi kekurangan dalam teknologi. Hal tersebut disebut sebagai "*cyber crime*" yang merupakan kejahatan dengan memanfaatkan *cyberspace*. Dengan demikian terdapat berbagai macam isu *cyber crime* seperti peretasan pada beberapa situs sebagai bagian dari skema kasus pemerasan (Bhattacharjee, 2021). Dalam skema tersebut korban secara tidak sadar memberikan akses kepada *cyber criminal* seperti data identitas yang menjadi privasi korban. Hal tersebut dapat memberikan kerugian besar terhadap korban tersebut. Tidak hanya sebatas itu, dalam gambaran besarnya hal tersebut juga dapat memberikan imbas terhadap infrastruktur kritis negara.

Kasus *cyber crime* sendiri telah dianggap dapat memberikan ancaman terhadap stabilitas suatu negara. Di samping itu, negara *super power* seperti Amerika Serikat juga sulit dalam mengimbangi skema yang dilakukan oleh *cyber criminal* tersebut sebab perkembangan akan teknik dalam meretas

komputer mereka berkembang setiap tahunnya (Ray, 2022). Belum lagi, perkembangan teknologi juga telah memasuki fase *mobile* yang di mana komputerisasi dan akses terhadap *cyberspace* sendiri dapat dilakukan secara leluasa di mana pun dan kapan pun. Sehingga hal tersebut menjadi tantangan tersendiri kepada mereka yang memiliki otoritas untuk memberantas *cyber attack* yang merajalela di setiap tahunnya.

Cyber Security telah menjadi kasus yang semakin mendesak di era digital yang semakin berkembang. Perkembangan *cyber attack* sendiri telah menjadi skema yang kompleks dan sering kali melintasi batas negara. Menimbulkan ancaman serius terhadap infrastruktur kritis, data pribadi, dan stabilitas nasional (Peter W. Singer et al., 2014). Oleh karena itu, hubungan bilateral dalam bidang *cyber security* merupakan tindakan yang sangat penting dilakukan untuk negara untuk memahami lebih dalam mengenai penyebab dari kasus *cyber crime* dengan tujuan untuk menghadapi tantangan tersebut.

Amerika Serikat dan India adalah dua kekuatan dunia yang memiliki perhatian yang sama terhadap *cyber security*. Kedua negara ini menghadapi *cyber attack* yang terus meningkat, baik dari aktor negara maupun kelompok-kelompok *cyber criminal*. Dalam beberapa tahun terakhir, Amerika Serikat dan India telah melakukan upaya untuk memperkuat kerja sama mereka dalam hal *cyber security*, dengan cara melakukan kolaborasi untuk melakukan pertukaran informasi, peningkatan kapasitas, dan penegakan hukum terkait *cyber security* pada pertemuannya (Ray, 2022).

Konferensi tingkat tinggi antara Amerika Serikat dan India telah menjadi platform forum penting untuk membahas kasus-kasus *cyber security* dan merumuskan kerangka kerja. Dalam pertemuan-pertemuan ini, kedua negara telah membahas kasus-kasus seperti perlindungan infrastruktur kritis, pertukaran informasi intelijen, dan kolaborasi dalam pengembangan teknologi cyber security. Melalui dialog dan konsultasi yang intensif yang disebut sebagai "*US-India Cyber Dialogue*", Amerika Serikat dan India telah menegaskan komitmen mereka untuk mengatasi *cyber attack* bersama-sama (Ray, 2022).

Dampak dari kerja sama ini sangat signifikan. Pertukaran informasi yang lebih baik antara kedua negara memungkinkan peringatan dini terhadap serangan yang sedang berlangsung dan meningkatkan respons terhadap *cyber attack*. Kolaborasi dalam pengembangan teknologi *cyber security* memungkinkan Amerika Serikat dan India untuk mengembangkan solusi inovatif dan efektif untuk menghadapi serangan yang semakin canggih. Peningkatan kapasitas *cyber security* melalui program pelatihan dan pertukaran pengalaman memperkuat kemampuan kedua negara dalam menghadapi tantangan *cyber security* yang kompleks.

Meskipun telah terjadi kemajuan yang signifikan dalam kerja sama *cyber security* antara Amerika Serikat dan India, tantangan masih belum teratasi sepenuhnya. Aktor-aktor *cyber criminal* terus mengembangkan skema serangan yang lebih canggih, dan kasus-kasus seperti perlindungan data pribadi, penegakan hukum, dan kebijakan *cyber security* masih memerlukan perhatian yang lebih lanjut. Pemerintah Amerika Serikat sendiri telah mengambil

langkah-langkah dalam menanggapi kasus *cyber attack* tersebut seperti menyelenggarakan kerja sama bilateral dengan pemerintah India hingga memberikan edukasi dan pemahaman kepada masyarakat akan bahaya yang mengintai dalam berinteraksi dengan *cyber space* (*U.S. Relations With India - United States Department of State*, 2022). Dalam pandangan Amerika Serikat sendiri, *cyber attack* merupakan ancaman yang dapat merugikan dalam skala global sebab ancaman tersebut memberikan kompromi terhadap infrastruktur kritis dan informasi penting negara (Peter W. Singer et al., 2014). Oleh karena itu, kedua negara melakukan konferensi tingkat tinggi yang di kenal sebagai "*Framework for the US-India Cyber Relationship*" untuk membahas kasus-kasus terkait *cyber security*.

Dalam konteks ini, tulisan ini bertujuan untuk menyelidiki dan menganalisis lebih lanjut kerja Amerika Serikat dan India dalam bidang *cyber security*. Dalam karya tulis ini, akan diidentifikasi peningkatan intensitas hubungan bilateral antara Amerika Serikat dan India, serta langkah-langkah konkret yang dapat diambil untuk memperkuat kerja sama tersebut. Selain itu, dalam karya tulis ini, penulis akan menjelaskan lebih lanjut mengenai kerangka kerja yang pemerintah Amerika Serikat dan India sepakati yaitu "*The Framework for US-India Cyber Relationship*" khususnya dalam aspek *cyber security*. Dengan menggali lebih dalam tentang kerangka kerja tersebut, diharapkan karya tulis ini dapat memberikan kontribusi dalam meningkatkan pemahaman terkait *cyber security* serta peningkatan intensitas hubungan bilateral Amerika Serikat dan India dalam menghadapi *cyber attack* yang terus berkembang di era ini.

B. Batasan dan Rumusan Masalah

Pada penelitian ini, batasan masalah yang dirumuskan oleh peneliti mengacu pada kebijakan yang disepakati oleh pemerintah Amerika Serikat dan India yaitu "*The Framework for US-India Cyber Relationship*". Kebijakan tersebut disepakati di tahun 2016 pada konferensi tingkat tinggi yang disebut sebagai "*US-India Cyber Dialogue*". Mengingat akan luasnya aspek yang disepakati pada kebijakan tersebut peneliti membatasi diri pada aspek *cyber security* dalam kerangka kerja tersebut.

Oleh karena itu, patokan batasan waktu yang diambil oleh peneliti pada tulisan ini mengikuti masa berlaku dari kebijakan "*The Framework for US-India Cyber Relationship*" yaitu pada tahun 2016-2021. Selain itu peneliti juga tertarik untuk mengetahui akan bagaimana hubungan bilateral tersebut dapat berkontribusi terhadap pengembangan *cyber security* dan peningkatan intensitas hubungan bilateral Amerika Serikat dan India dalam memerangi *cyber crime*, serta apa saja langkah kongkret yang diambil oleh kedua negara dalam memperkuat *cyber security*. Mengingat kembali akan banyaknya kasus *cyber crime* pada kedua negara tersebut, apa saja tantangan dan hambatan dalam usaha untuk mengimplementasikan kebijakan tersebut dan dampak apa yang telah ditimbulkan.

Berdasarkan uraian latar belakang yang telah dipaparkan sebelumnya peneliti merumuskan masalah penelitian sebagai berikut:

1. Bagaimana implementasi hasil *cyber dialogue* dalam kerangka kerja "*The Framework for US-India Cyber Relationship*" serta implementasinya
2. Bagaimana peluang dan tantangan yang dihadapi oleh AS-India dalam upaya untuk mengembangkan *cyber security*.
3. Apa dampak kebijakan "*The Framework for US-India Cyber Relationship*" dalam pengembangan *cyber security*.

Dengan batasan dan rumusan masalah tersebut, penelitian ini akan berfokus pada analisis implementasi kebijakan "*The Framework for US-India Cyber Relationship*" dalam konteks *cyber security*, dan peningkatan intensitas hubungan bilateral Amerika Serikat dan India dalam memerangi *cyber crime*, serta memberikan pemahaman yang lebih mendalam tentang langkah-langkah konkret yang telah diambil beserta dampaknya.

C. Tujuan dan Kegunaan Penelitian

1. Tujuan Penelitian

Berdasarkan uraian di atas, penelitian ini dilakukan dengan tujuan:

a. Untuk mengetahui bagaimana implementasi kerangka kerja "*The Framework for US-India Cyber Relationship*".
b. Untuk mengetahui bagaimana peluang dan tantangan yang dihadapi oleh AS-India dalam upaya untuk mengembangkan *cyber security*.
c. Untuk mengetahui dampak kebijakan "*The Framework for US-India Cyber Relationship*" dalam pengembangan *cyber security*.

2. Kegunaan Penelitian

Apabila tujuan penelitian di atas tercapai, maka:

a. Bagi peneliti, penelitian ini diharapkan dapat memberikan pemahaman terkait langkah yang diambil oleh pemerintah Amerika Serikat dan India dalam mengembangkan *cyber security*.
b. Bagi akademisi, penelitian ini diharapkan dapat menjadi informasi dan referensi bagi mahasiswa terkait pembahasan mengenai hubungan bilateral pemerintah Amerika Serikat dan India serta dampaknya terhadap *cyber security*.
c. Bagi perkembangan ilmu pengetahuan, penelitian ini diharapkan dapat memberikan gambaran akan betapa pentingnya perkembangan *cyber security* dalam menyaingi dan menanggulangi perkembangan *cyber crime* sehingga dapat digunakan oleh peneliti lainnya sebagai referensi terhadap permasalahan terkait.

D. Kerangka Konseptual

Dalam penelitian ini, kerangka penelitian yang akan digunakan akan berhubungan dengan studi kasus yang akan diteliti yaitu "Kerja Sama Bilateral As-India Terhadap Cyber Security (2016-2021)"

Berhubungan dengan masalah tersebut, maka penulis memerlukan konsep dan juga teori-teori untuk memandu penulis untuk tidak mengalami kekeliruan persepsi dan interpretasi dalam usaha untuk menemukan hasil. Mengenai objek yang akan diteliti oleh penulis tentu saja mempunyai hubungan dan pengaruh dalam konteks hubungan internasional, yang sejatinya Hubungan Internasional itu sendiri merupakan study mengenai interaksi antar aktor-aktor negara. Dengan demikian penulis mendapatkan beberapa tanggapan dari para ahli mengenai hubungan antara teori Hubungan Internasional dan kasus *cyber security* (Michael, 2010). Berikut adalah beberapa tanggapan dari para ahli:

1. Richard A. Clarke dan Robert K. Knake berpendapat bahwa teori klasik dalam Hubungan Internasional, seperti realisme dan liberalisme, masih relevan dalam konteks *cyber security*. Mereka menekankan bahwa negara-negara akan terus berusaha untuk mempertahankan keamanan nasionalnya dan mengambil tindakan yang sesuai dengan kepentingan nasionalnya, bahkan dalam *cyberspace*.
2. Joseph Nye mengembangkan konsep "soft power" yang diadaptasi ke dalam isu *cyber security*. Ia berpendapat bahwa kekuasaan dan pengaruh suatu negara juga tergantung pada kemampuan negara

tersebut dalam mempengaruhi dan mengatur tindakan para aktor di *cyberspace*.

3. L;p..David J. Betz dan Tim Stevens mengemukakan bahwa teori-teori dalam Hubungan Internasional tidak dapat sepenuhnya menjelaskan dinamika *cyber security* karena fenomena ini melibatkan berbagai aktor, termasuk kelompok-kelompok non-negara yang sulit untuk diidentifikasi dan diatur.
4. Erica Chenoweth dan Michael J. Mazarr menekankan bahwa isu *cyber security* harus dilihat dalam konteks hubungan antara negara dan masyarakat sipil, di mana para aktor di *cyberspace* termasuk di dalamnya. Dalam hal ini, mereka mengusulkan konsep "*cyber civil society*" yang dapat berperan sebagai pengawas dan penyeimbang dalam hubungan antara negara dan *cyberspace*.

Dalam konteks *cyber security* sendiri penulis menyimpulkan bahwa *cyber security* mempunyai peran yang penting di era digital ini, sebab dengan berkembangnya globalisasi dalam memanfaatkan teknologi telah menjadi memberikan keuntungan yang signifikan terhadap kehidupan masyarakat. Seperti halnya bagaimana negara dalam berinteraksi dengan negara lainnya, pemanfaatan *cyber space* telah menjadi keperluan untuk negara dalam menjalankan hubungan bilateral dan diplomasinya. Oleh karena itu pengembangan *cyber security* merupakan objek penting oleh negara dalam mempertahankan keamanan nasionalnya.

Hubungan internasional memiliki keterkaitan dengan globalisasi, dalam perkembangan teknologi pun *cyberspace* memberikan dampak yang besar dalam memelopori globalisasi. Sebab perkembangan teknologi sendiri memberikan dampak terhadap intern-konektivitas antar aktor-aktor negara maupun non negara. Dengan demikian, interaksi antar negara dapat dijalankan secara tidak langsung. Salah satu contohnya seperti, negara dapat memperoleh informasi mengenai apa yang terjadi pada negara lainnya secara cepat tanpa menunggu sebuah publikasi pers atau media dengan memanfaatkan internet sebagai aset dalam alat diplomasi.

Kembali membahas mengenai *cyber crime*, di Amerika Serikat sendiri *cyber criminal* mempunyai alasan tersendiri menargetkan masyarakat Amerika Serikat dalam menjalankan skema *cyber attack*. Sebab Amerika Serikat sendiri telah dikenal dalam mengimplementasikan penggunaan teknologi pada mayoritas kehidupan sehari-hari (Michael, 2010). Hal tersebut mengakibatkan, banyak informasi sensitif seperti data pribadi dan finansial dapat dengan mudah diakses oleh *cyber criminal*. Oleh karena itu, para *cyber criminal* mengategorikan Amerika Serikat sebagai target yang menguntungkan.

Pemerintah Amerika Serikat juga memiliki lembaga keuangan dan perbankan yang terkenal, sehingga menjadi target yang menarik bagi para *cyber criminal* yang mencari keuntungan finansial (Suciu, 2021). Dengan memanfaatkan teknik-teknik seperti penipuan online, para *cyber criminal* dapat dengan mudah mengirim spam, serta memalsukan identitas, dengan tujuan untuk mendapatkan informasi pribadi dari korban, yang selanjutnya akan

dimanfaatkan untuk memeras finansial korban. Belum lagi, kurangnya koordinasi dan kerja sama internasional dalam mengatasi *cyber crime* memungkinkan para *cyber criminal* untuk bertindak di luar yurisdiksi negara asal mereka sehingga mereka sulit untuk mendapatkan hukuman. Oleh karena itu, upaya untuk meningkatkan kerja sama dan koordinasi internasional dalam hal *cyber security* sangat penting untuk melindungi masyarakat dari serangan *cyber criminal*.

Dalam sejarah sendiri terdapat insiden yang menjadi dasar untuk pengembangan *cyber security*, insiden tersebut tidak lain adalah *Ransomware WannaCry*. merupakan salah satu serangan *ransomware* yang mengguncang dunia pada tahun 2017 dan memberikan dampak serius bagi pemerintah Amerika Serikat (*Ransomware WannaCry: All you need to know*, 2020). Insiden *WannaCry* tersebut memberikan dampak terhadap pemerintah Amerika Serikat seperti gangguan pada infrastruktur kritis pemerintahan. Dengan menginfeksi beberapa sistem komputer pada infrastruktur melalui sebuah *malware* yang akan mengenkripsi data di dalamnya. Dengan demikian, *cyber criminal* mendapatkan akses ilegal terhadap data negara yang bersifat rahasia atau sensitif dari lembaga pemerintah, yang dapat mengancam keamanan nasional jika terjadi kebocoran. Hal tersebut memberikan gangguan vital pada operasional layanan publik yang memiliki peran penting sebagai infrastruktur kritis (Henriquez, 2022).

Dalam penyerangan tersebut, skema yang dilancarkan oleh *cyber criminal* merupakan sebuah pemerasan. Setelah mereka mendapatkan akses data dari

sistem komputer tersebut, para *cyber criminal* meminta tebusan kepada pemerintah Amerika Serikat dengan jumlah besar untuk mendapatkan kembali akses terhadap data tersebut.

Serangan tersebut menjadi latar belakang akan urgennya dalam meningkatkan pertahanan *cyber security* negara. Amerika Serikat dengan India sebagai negara yang menjadi korban dengan kerugian yang besar mengadakan konferensi tingkat tinggi yang disebut "*US-India Cyber Dialogue*". Terkait dengan keinginan kedua negara untuk meningkatkan kerja sama dalam bidang *cyber security* dan teknologi informasi (Ray, 2022). Konferensi ini merupakan platform yang penting bagi Amerika Serikat dan India untuk berdiskusi tentang kasus-kasus terkait *cyber security*, pertukaran informasi, kolaborasi teknologi, dan peningkatan kerja sama dalam menghadapi *cyber threat* (*Framework for the U.S.-India Cyber Relationship - U.S. Embassy & Consulates in India*, 2016). Pada konferensi tersebut kedua negara menyepakati kerangka kerja yang disebut "*The Framework for US-India Cyber Relationship*"

Dalam konteks ini, kebijakan "*The Framework for US-India Cyber Relationship*" menjadi landasan penting bagi kerja sama kedua negara dalam aspek *cyber security*. Kebijakan ini memberikan kerangka kerja yang jelas dan komprehensif untuk memperkuat kerja sama bilateral, mengidentifikasi langkah-langkah konkret yang harus diambil, serta menegaskan komitmen kedua negara dalam memerangi *cyber crime*. Amerika Serikat sendiri memandang bahwa kasus *cyber crime* sebagai ancaman global dan memerlukan kolaborasi untuk menanggulanginya (*Framework for the U.S.-India Cyber*

Relationship - U.S. Embassy & Consulates in India, 2016). Dalam menanggapi *cyber criminal* tersebut pemerintah Amerika Serikat mengambil langkah-langkah seperti:

1. Kerja sama dengan pemerintah India: Amerika Serikat berkolaborasi dengan India dalam menanggulangi *cyber crime* seperti melakukan pertukaran informasi serta pemahaman teknologi untuk meningkatkan kemampuan kedua negara dalam melawan *cyber crime*.
2. Penegakan hukum: Amerika Serikat juga berkolaborasi dalam jalur hukum dalam menangani kasus-kasus *cyber crime*. Amerika Serikat bekerja sama dengan penegak hukum India dalam menangani *cyber crime*.
3. Pendidikan dan Kesadaran Masyarakat: Pemerintah Amerika Serikat dan India juga melakukan upaya untuk meningkatkan kesadaran masyarakat mengenai *cyber security* dan risiko yang terkait dengan *cyberspace*. Ini dilakukan melalui program pendidikan dan sosialisasi mengenai praktik-praktik *cyber crime*.
4. Teknologi dan Inovasi: Pemerintah Amerika Serikat dan India juga berkolaborasi dalam mengembangkan teknologi dan inovasi baru untuk menangani *cyber crime*, termasuk pengembangan sistem *cyber security* yang lebih efisien, program pelatihan *cyber security*, serta pengembangan alat analisis data yang canggih untuk mendeteksi *cyber crime*.

Dengan demikian, peneliti menetapkan konsep yang memiliki relevansi terhadap penelitian yang akan dikaji mengenai kerja sama bilateral dari pemerintah Amerika Serikat dan India. Hal tersebut meliputi:

1. Hubungan Bilateral

   Kerja sama bilateral antara pemerintah Amerika Serikat dengan India didasari sebagai langkah Amerika Serikat dalam menanggapi kasus *cyber crime* yang terus meningkat di setiap tahunnya yang memakan korban banyak dari warga Amerika Serikat. Oleh karena itu, kerja sama dari kedua belah pihak melakukan pertukaran informasi dengan menyelenggarakan pertemuan yang disebut "*US-India Cyber Dialogue*" di tahun 2015 dengan membahas tentang kasus *cyber security* dan teknologi informasi (*Framework for the U.S.-India Cyber Relationship - U.S. Embassy & Consulates in India*, 2016). Dialog yang didiskusikan oleh kedua belah pihak, seperti:

   a. Ancaman *cyber security* yang saling berbagi: Baik Amerika Serikat maupun India menghadapi ancaman serius dalam bentuk *cyber attack* dan *cyber crime*. Kedua negara menyadari bahwa kolaborasi dan pertukaran informasi yang erat dapat membantu melawan ancaman tersebut dan memperkuat *cyber security*.
   b. Pertumbuhan sektor teknologi informasi: Baik Amerika Serikat maupun India memiliki industri teknologi informasi yang berkembang pesat. Kerja sama dalam bidang *cyber security* dan

teknologi informasi dapat memperkuat kedua negara dalam menjaga keberlanjutan pertumbuhan sektor ini.

c. Hubungan bilateral yang kuat: Amerika Serikat dan India telah lama menjalin hubungan bilateral yang kuat dalam berbagai bidang, termasuk politik, ekonomi, dan keamanan. Kerja sama dalam *cyber security* dan teknologi informasi dapat menjadi bagian dari upaya untuk memperkuat hubungan bilateral yang sudah ada.
d. Keinginan untuk melindungi kepentingan nasional dan masyarakat sipil: Dalam era digital yang semakin berkembang, kedua negara memiliki kepentingan yang sama untuk melindungi infrastruktur kritis, data pribadi masyarakat sipil, dan kepentingan nasional mereka dari *cyber attack*.
e. Potensi untuk saling menguntungkan: Kerja sama dalam *cyber security* dan teknologi informasi dapat memberikan manfaat saling menguntungkan bagi Amerika Serikat dan India. Hal ini meliputi pertukaran teknologi, peningkatan kapasitas, dan kemampuan bersama untuk mengatasi ancaman yang kompleks dan saling terkait di *cyber space*.

Dengan suksesnya kerja sama bilateral tersebut, pemerintah Amerika Serikat dan India menandatangani kebijakan yang disebut "*The Framework for US-India Cyber Relationship*" di tahun 2016.

2. *Cyber Security*

Cyber security memiliki keterkaitan yang erat dengan ilmu hubungan internasional karena *cyber security* tidak hanya mempengaruhi individu atau organisasi di dalam suatu negara, tetapi juga dapat mempengaruhi hubungan internasional. Ancaman *cyber security* yang timbul dari *cyber attack*, *cyber war*, dan *cyber espionage* dapat memiliki dampak yang signifikan terhadap stabilitas politik, keamanan nasional, dan hubungan antar negara (Bjola et al., 2015).

Dalam konteks lain, dampak yang ditimbulkan oleh *cyber attack* terhadap sebuah negara tidak lain seperti:

a. Pertama, *cyber attack* terhadap infrastruktur kritis seperti listrik, air, dan telekomunikasi dapat mengakibatkan gangguan yang signifikan terhadap perekonomian suatu negara dan bahkan dapat mempengaruhi hubungan antar negara. Sebagai contoh, *cyber attack* terhadap sistem keuangan suatu negara dapat mengakibatkan kerugian ekonomi yang signifikan dan menimbulkan ketegangan dalam hubungan antar negara.
b. Kedua, *cyber security* dapat mempengaruhi kebijakan luar negeri suatu negara. Kebijakan luar negeri suatu negara dapat berubah sebagai akibat *cyber attack* atau *cyber espionage* yang dilakukan oleh negara lain. Hal ini dapat memicu konflik antar negara dan mempersulit hubungan internasional.

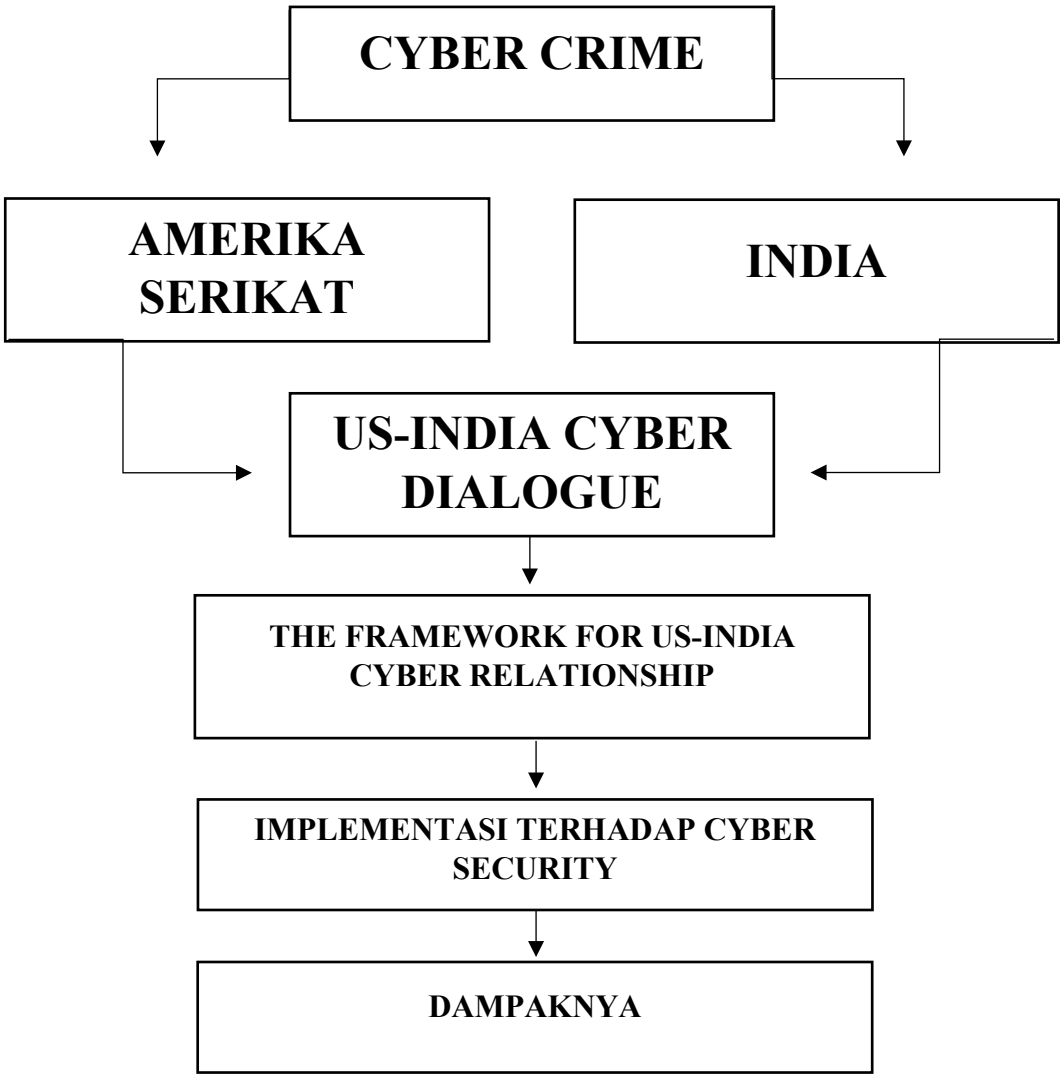
c. Ketiga, *cyber security* juga dapat mempengaruhi diplomasi internasional. *Cyber attack* terhadap institusi pemerintah atau perusahaan dapat menimbulkan ketegangan di antara negara-negara yang terlibat dan mempengaruhi upaya diplomasi internasional. Sebagai contoh, *cyber attack* terhadap sistem pemilu suatu negara dapat menimbulkan ketidakpercayaan dan mempengaruhi upaya diplomasi internasional.

Dalam konteks ini, ilmu hubungan internasional dapat membantu dalam memahami dampak *cyber security* terhadap hubungan internasional dan memberikan kerangka konseptual untuk memahami hubungan antar negara yang kompleks dan terus berubah akibat ancaman *cyber security*. Oleh karena itu, ilmu hubungan internasional dan *cyber security* saling terkait dan saling mempengaruhi satu sama lain.

3. Batasan Penelitian atau Fokus Penelitian

Variabel Independen	Indikator	Variabel Dependen	Indikator
Kerja sama bilateral	Adanya MoU yang disepakati oleh kedua negara	*Cyber Security*	1. Mengurangi risiko *cyber attack* 2. Peningkatan pertahanan cyber yang kuat dan efektif

4. Model Analisis



E. Metode Penelitian

1. Tipe Penelitian

Tipe penelitian yang akan digunakan peneliti adalah metode kualitatif. Metode ini dipilih dikarenakan pendekatan dalam penelitian berfokus pada analisis deskriptif dari data-data yang telah terkumpulkan dan rangkum sekaligus mempermudah penulis dalam menggambarkan fenomena dan petunjuk secara deskriptif. Metode ini dapat membantu peneliti dalam menganalisasi data-data tersebut secara deskriptif akan bagaimana kerja sama pemerintah AS-India dalam mengembangkan *cyber security*.

Alasan peneliti memilih metode kualitatif karena peneliti dapat mendalami apa yang dibutuhkan dari objek penelitian yang diteliti seperti analisis deskriptif mengenai topik terkait.

2. Teknik Pengumpulan Data

Dalam pengumpulan data, peneliti akan menerapkan studi literatur dengan merangkum data dari berbagai sumber informasi, seperti jurnal, buku, artikel berita, serta dokumen pendukung terkait kebijakan "*The Framework for US-India Cyber Relationship*" dalam usaha untuk mengembangkan *cyber security*. Setelah mengumpulkan sumber data, penulis lalu mengambil bagian yang terkait dengan tema untuk mendukung penelitian ini.

3. Jenis Data

Dikarenakan terdapat keterbatasan akses dan jarak dalam merangkum sumber data primer, peneliti memutuskan untuk memanfaatkan data sekunder dalam merangkum material yang mendukung penelitian ini melalui buku, jurnal, artikel berita, serta dokumen pendukung yang dapat dirangkum melalui media internet untuk memberikan informasi terkait kerja sama US-India terhadap *cyber security*.

4. Teknik Analisis Data

Dalam menganalisis data, peneliti akan menerapkan teknik analisis kualitatif sebab teknik analisis tersebut dapat digunakan untuk menganalisis informasi dan data-data secara deskriptif yang diperoleh dari pengumpulan data sekunder dari berbagai sumber yang kredibel dengan tujuan menjawab pertanyaan penelitian.

5. Metode Penulisan

Dalam penelitian ini, penulis akan menggunakan metode deduktif dengan melakukan analisis secara deskriptif terhadap topik penelitian berdasarkan data-data yang diperoleh. Hasil dari analisis tersebut akan diklasifikasikan ke dalam sub-topik penelitian untuk menjawab pertanyaan penelitian hingga peneliti dapat menarik kesimpulan dari keseluruhan analisis tersebut.

BAB II

TINJAUAN PUSTAKA

A. Kerja Sama Bilateral

Dalam konteks kerja sama bilateral merujuk pada bentuk kolaborasi antara dua negara. Dengan melibatkan pertukaran sumber daya, informasi, teknologi, atau dalam berbagai bidang yang dapat menguntungkan kedua pihak yang terlibat. Konsep ini memainkan peran penting dalam hubungan internasional dan memiliki keterkaitan yang signifikan dengan dinamika politik, ekonomi, dan sosial di tingkat global. Berikut adalah beberapa aspek utama terkait konsep kerja sama bilateral dan keterkaitannya dengan hubungan internasional:

1. Diplomasi Bilateral: Kerja sama bilateral sering kali menjadi hasil dari negosiasi diplomatik antara dua negara. Melalui dialog dan perundingan, kedua pihak mencapai kesepakatan yang menguntungkan baik untuk kepentingan mereka maupun untuk mencapai tujuan bersama.
2. Pembangunan Ekonomi: Kerja sama bilateral dapat melibatkan pertukaran perdagangan, investasi langsung, dan proyek-proyek ekonomi bersama antara dua negara. Ini membantu meningkatkan pertumbuhan ekonomi dan menciptakan peluang kerja.
3. Keamanan dan Pertahanan: Beberapa kerja sama bilateral melibatkan bidang keamanan dan pertahanan, termasuk pertukaran intelijen,

pelatihan militer, atau kerja sama dalam penanganan ancaman keamanan bersama.

4. Pengembangan Sosial dan Budaya: Program-program pertukaran pelajar, budaya, dan seni sering kali menjadi bagian dari kerja sama bilateral. Ini membantu memperdalam pemahaman antara dua negara dan membangun ikatan sosial dan budaya.
5. Penyelesaian Konflik: Dalam beberapa kasus, kerja sama bilateral dapat menjadi instrumen untuk menyelesaikan konflik antara dua negara. Melalui dialog dan kerja sama, negara-negara dapat mencari solusi damai untuk perbedaan mereka.
6. Keterkaitan Global: Meskipun kerja sama bilateral melibatkan dua negara, hasilnya dapat memiliki dampak lebih luas dalam konteks hubungan internasional. Kesepakatan dan inisiatif bilateral dapat memengaruhi dinamika regional dan bahkan global, terutama jika kedua negara tersebut memiliki peran penting dalam arena internasional.
7. Hubungan Diplomatik Lebih Baik: Kerja sama bilateral dapat memperkuat hubungan diplomatik antara dua negara. Ini menciptakan dasar yang kuat untuk bekerja sama dalam isu-isu global dan meningkatkan kestabilan di tingkat internasional.

Dalam konteks *cyber security* sendiri, realisme menekankan negara untuk bertindak berdasarkan kepentingan nasional mereka. Negara juga wajib untuk mempertahankan atau meningkatkan kekuasaan dan keamanan mereka dalam

cyberspace, sebab *cyberspace* sendiri memiliki sistem internasional yang anarkis (Petallides, 2012). Salah satu alasan pengembangan *cyber security* adalah dalam sejarah sendiri telah tercatat akan peningkatan dari aktivitas *cyber attack* di setiap tahunnya. Di tahun 2021 sendiri telah tercatat kerugian yang ditimbulkan oleh *cyber attack* telah mencapai 6.9 Miliar US$ ("Internet Crime Report 2021," 2021).

Liberalisme sendiri menekankan akan kerja sama dan saling ketergantungan antar negara dalam menyelesaikan suatu permasalahan. Jika diartikan dalam konteks *cyber security*, pandangan ini menyarankan agar negara melakukan kolaborasi atau kerja sama serta memfasilitasinya untuk mencapai tujuan bersama (Isnarti, 2016). Dalam hubungan bilateral Amerika Serikat dan India, untuk menanggapi urgensi akan pengembangan *cyber security* dengan mengadakan kolaborasi dalam bentuk konferensi tingkat tinggi yang disebut sebagai "*US-India Cyber Dialogue*" di tahun 2015 ("Brief on India-U.S. Relations", 2017). Dalam diskusi tersebut, kedua negara membahas tentang kebijakan internasional mengenai *cyber security*, membandingkan strategi negara dalam menanggapi kasus *cyber security*. Di ikuti oleh tahun selanjutnya, dalam diskusinya kedua negara menyepakati kerangka kerja yang dikenal sebagai "*The Framework for US-India Cyber Relationship*". Diskusi dan pertukaran intelijen tersebut merupakan usaha kedua negara dalam meningkatkan usaha mereka untuk memerangi *cyber attack*. Di mana pada akhirnya usaha tersebut akan berkontribusi dalam pengembangan *cyber security*.

Jika kita melihat dalam pandangan *soft power*, kerangka kerja "*The Framework for US-India Cyber Relationsip*" yang disepakati oleh Amerika Serikat dan India merupakan sebuah tanggapan terhadap urgensi pengembangan *cyber security* (Yang et al., 2021). Dengan dasar tersebut dapat disimpulkan alasan kedua negara melakukan hubungan bilateral, sebab terdapat kesamaan faktor dalam kasus-kasus *cyber attack* yang dihadapi oleh Amerika Serikat dan India. Faktor tersebut, menumbuhkan kepentingan dari kedua negara yang akan mendorong terjadinya kolaborasi. Faktor-faktor tersebut meliputi:

1. *Cyber Threat* yang Semakin Kompleks: *Cyber Threat* semakin berkembang dan kompleks, termasuk serangan dari aktor-aktor negara dan kelompok-kelompok *cyber criminal*. Kedua negara menyadari bahwa tantangan ini memerlukan kerja sama dan koordinasi yang erat untuk meningkatkan ketahanan dan melawan *cyber threat* (Prasad et al., 2022).
2. Keamanan Nasional dan Kestabilan Kawasan: Keamanan nasional dan kestabilan kawasan menjadi prioritas bagi Amerika Serikat dan India. Kerja sama dalam *cyber security* membantu melindungi infrastruktur kritis, data pribadi, dan sistem informasi penting, serta mencegah serangan siber yang dapat mengganggu stabilitas di kawasan tersebut (Prasad et al., 2022).
3. Kekuatan Teknologi dan Inovasi: Amerika Serikat dan India merupakan negara-negara dengan kekuatan teknologi dan inovasi yang signifikan.

Kerja sama dalam *cyber security* memungkinkan pertukaran teknologi, keahlian, dan penelitian di aspek *cyber security*, yang dapat menguntungkan kedua belah pihak (Prasad et al., 2022).

4. Pertukaran Intelijen: Kerja sama dalam *cyber security* memungkinkan pertukaran intelijen dan informasi tentang *cyber threat* yang sedang berlangsung, memungkinkan kedua negara untuk menghadapi serangan secara efektif dan meningkatkan tanggapan terhadap ancaman tersebut.
5. Perlindungan Data dan Privasi: Dalam era digital dan berkembang, perlindungan data dan privasi menjadi penting bagi kedua negara. Kerja sama dalam *cyber security* dapat membantu mengembangkan kerangka kerja dan standar bersama untuk melindungi data dan privasi pengguna di kedua negara (Prasad et al., 2022).
6. Tantangan Bersama: Amerika Serikat dan India menghadapi tantangan yang sama dalam menghadapi *cyber threat*, seperti serangan ransomware, *cyber attack*, dan perang informasi. Kerja sama bilateral memungkinkan kedua negara untuk berbagi pengalaman dan terlibat dalam upaya bersama dalam mengatasi tantangan ini (Prasad et al., 2022).

B. Cyber Security

Cyber security adalah serangkaian tindakan yang dilakukan untuk melindungi sistem komputer, jaringan, perangkat *mobile*, data, dan informasi digital lainnya dari serangan, akses tidak sah atau ilegal, perusakan, perubahan, dan pencurian oleh pihak yang tidak berwenang ("What Is Cybersecurity?", 2021). Tujuan utama dari *cyber security* adalah untuk memastikan kerahasiaan, integritas, dan ketersediaan data dan sistem digital.

Cyber security mencakup berbagai aspek, termasuk perlindungan terhadap virus, *malware*, serangan *phishing*, *hacking*, dan *cyber attack* lainnya. Beberapa langkah yang dilakukan dalam kerangka *cyber security* meliputi:

1. Pengamanan jaringan: Memastikan bahwa jaringan yang digunakan oleh suatu organisasi aman dan tidak mudah diakses oleh pihak yang tidak berwenang (Kamble, 2013).
2. Enkripsi data: Melindungi data dengan enkripsi sehingga hanya orang yang berwenang yang dapat membaca atau mengaksesnya (Kamble, 2013).
3. Identifikasi dan validasi: Memastikan bahwa hanya pengguna yang sah yang memiliki akses ke sistem dan data (Kamble, 2013).
4. Penilaian risiko: Mengidentifikasi ancaman yang mungkin terjadi pada sistem dan data, dan mengambil tindakan untuk meminimalkan risiko tersebut (Kamble, 2013).

5. Pemantauan dan analisis: Memantau aktivitas sistem secara terus-menerus dan menganalisis data untuk mendeteksi *cyber attack* mungkin terjadi (Kamble, 2013).
6. Pelatihan dan kesadaran: Melakukan pelatihan kepada pengguna sistem untuk meningkatkan kesadaran mereka tentang pentingnya keamanan digital dan bagaimana melindungi diri dari *cyber attack* (Kamble, 2013).

Cyber security sangat penting dalam *cyberspace* saat ini, karena terjadi peningkatan terhadap kasus yang berkaitan dengan *cyber security,* dan memberikan kerugian kepada individu dan negara. Oleh karena itu, negara harus memastikan bahwa mereka mengambil langkah-langkah yang tepat untuk melindungi sistem dan data mereka dari *cyber attack*.

Jika dilihat dari kemajuan teknologi yang dimiliki oleh Amerika Serikat dan India, dapat terlihat perbedaan aspek *cyber security* di kedua negara. Hal tersebut dipengaruhi beberapa faktor yang di dalamnya termasuk perbedaan infrastruktur teknologi informasi, kebijakan pemerintah, tingkat kesadaran masyarakat terhadap *cyber security*, serta kompleksitas ekosistem teknologi masing-masing negara. Berikut adalah beberapa perbedaan utama antara *cyber security* di Amerika Serikat dan India:

1. Kebijakan Pemerintah dan Regulasi: Amerika Serikat memiliki sejarah yang lebih panjang dalam pengembangan dan penerapan kebijakan *cyber security*. Mereka memiliki berbagai badan pemerintah dan lembaga yang berfokus pada *cyber security*, seperti *National Institute of Standards and*

Technology (NIST) dan *Cybersecurity and Infrastructure Security Agency* (CISA) ("About Cybersecurity and Infrastructure Security Agency", 2018). Di India, kesadaran tentang *cyber security* terus berkembang, dan pemerintah telah meningkatkan upaya untuk memperkuat infrastruktur *cyber security* dengan berbagai kebijakan dan inisiatif. Seperti mendirikan "*National Critical Information Infrastructure Protection Centre*" (NCIIPC) dan "*National Technical Research Organisation*" (NTRO) ("About National Critical Infrastructure Information Protection Centre", 2014).

2. Infrastruktur Teknologi dan Keamanan Jaringan: Amerika Serikat memiliki infrastruktur teknologi yang lebih matang dan rumit dengan lebih banyak perusahaan besar yang beroperasi dalam berbagai sektor. Ini juga berarti mereka menghadapi lebih banyak ancaman keamanan. Di India, infrastruktur teknologi berkembang pesat, dan tantangan *cyber security* dapat bervariasi dari perusahaan besar hingga usaha mikro, kecil, dan menengah (Lostri et al., 2022).
3. Peran Swasta dan Publik: Di Amerika Serikat, perusahaan swasta memainkan peran besar dalam mengembangkan dan menerapkan solusi *cyber security*. Mereka juga sering bekerja sama dengan pemerintah dalam upaya meningkatkan *cyber security*. Di India, sementara sektor swasta juga penting, ada penekanan yang lebih besar pada peran pemerintah dalam memastikan keamanan infrastruktur teknologi dan data nasional (Lostri et al., 2022).

4. Pelatihan dan Sumber Daya Manusia: Amerika Serikat memiliki sejumlah besar ahli dalam bidang *cyber security*, perusahaan keamanan, dan program pelatihan yang diakui secara global. Di India, sementara ada pertumbuhan dalam industri *cyber security*, perluasan sumber daya manusia terlatih masih merupakan tantangan (Lostri et al., 2022).
5. Tingkat Kesadaran Publik: Amerika Serikat mungkin memiliki tingkat kesadaran yang lebih tinggi tentang *cyber security* di kalangan masyarakat umum. Di India, kesadaran tentang ancaman *cyber security* terus berkembang dan menjadi fokus penting dalam kampanye kesadaran publik (Lostri et al., 2022).

Meskipun ada perbedaan dalam pendekatan dan tingkat kematangan, baik Amerika Serikat maupun India menyadari betapa pentingnya *cyber security* dalam era digital yang semakin berkembang. Keduanya berusaha untuk meningkatkan kapabilitas keamanan mereka guna melindungi infrastruktur dan data dari *cyber threat* yang semakin kompleks dan beragam. Dengan demikian, kedua negara berkolaborasi dalam mengembangkan infrastruktur dan pemahaman *cyber security* dengan tujuan untuk mencari metode yang efektif untuk menekan dan mengurangi aktivitas *cyber criminal*.