**Jurnal Kajian Ilmu Humaniora**

JKIH, 8 (6), Juni 2024
ISSN , 24531261

# PERSEPSI KONSEP PERANG SIBER DI INDONESIA DAN IMPLIKASINYA DALAM KRIMINOLOGI TEORETIS

**Farahdina Fairuz Iftinan**
**Email:** farahdinafairuz.i@gmail.com
**Universitas Indonesia**

**Abstrak**: Serangan siber dalam beberapa periode ini telah berkembang menjadi berbagai bentuk dan tingkat eskalasi penyerangan. Tingkatan penyerangan siber yang paling tinggi adalah perang siber. Sebelum melakukan pencegahan dan penanganan, harus dilakukan pemahaman konsep dan definisi perang siber terlebih dahulu. Tanpa adanya pemahaman, maka individu, organisasi, ataupun negara tidak akan pernah mengetahui bahaya yang mengintai dari penggunaan teknologi siber sehari-hari. Penelitian ini merupakan penelitian kualitatif melalui wawancara. BSSN, Kementrian Pertahanan, dan Kepolisian RI dan masyarakat negara Indonesia dengan sampling 10 orang yang tidak memiliki *background* pendidikan dan pekerjaan terkait IT, siber, dan yang berkaitan lainnya. Hasil dari penelitian ini adalah Lembaga pemerintahan yang berkaitan dengan keamanan siber kurang lebih sudah memahami terkait konsep dan definisi perang siber. Namun mayoritas masyarakat yang tidak memiliki latar belakang dan pendidikan terkait IT dan *cyber-related*, kurang memahami konsep dan definisi perang siber.
**Keywords :** Perang Siber, Kriminologi, Definisi Perang Siber.

## PENDAHULUAN

Perkembangan teknologi meningkatkan ketergantungan manusia pada teknologi tidak terkecuali siber. Komunikasi, sektor kesehatan, sistem ekonomi, sekolah, transportasi, dan lainnya telah menggunakan teknologi siber. Peningkatan penggunaan teknologi berarti meningkatkan potensi terjadinya serangan siber. Serangan siber dalam beberapa periode ini telah berkembang menjadi berbagai bentuk dan tingkat eskalasi penyerangan. Salah satu kasus serangan siber dengan skala besar yang menggemparkan dunia terjadi pada fasilitas nuklir di Iran. Iran mengetahui adanya penyerangan siber pada fasilitas nuklirnya pada tahun 2010, peristiwa tersebut dikenal sebagai kasus 'Stuxnet' atau Operasi Olympic Games yang menyerang lebih dari 15 fasilitas nuklir di Iran (Holloway, 2015). Penyerang dan pembuat Stuxnet tidak dapat secara pasti dipertanggungjawabkan, namun menurut studi kasus perang siber yang dilakukan pada tahun 2017 oleh akademisi MIT, Mohan B. Gazula, Amerika Serikat dan Israel adalah negara yang terlibat (Status Quo). Amerika serikat dan Israel merasa terancam dengan adanya fasilitas nuklir yang dimiliki oleh Iran (Pratama, 2016). Penyerangan tersebut biasanya disebut dengan istilah perang siber, yang menyebabkan kerugian ekonomi dan finansial yang sangat besar serta timbulnya ketidakpercayaan dan hubungan politik yang renggang antara Iran dengan negara yang diduga terlibat.

Dilihat dari contoh-contoh kasus tersebut, setiap negara memerlukan keamanan dan pertahanan siber yang kuat terhadap ancaman siber global. Namun, saat ini Indonesia berada pada peringkat tiga terbawah dalam hal keamanan dan kepercayaan internet, dan menempati peringkat ke-83 dari 100 negara dalam hal tingkat kepercayaan terhadap informasi dari media sosial–menunjukkan adanya kekhawatiran terkait keamanan digital (Zahra, 2023). Zahra (2023) mengungkapkan, kurangnya kesadaran dan adopsi praktik-praktik keamanan digital dasar pada responden survei menyiratkan bahwa masyarakat Indonesia rentan terhadap berbagai risiko yang ada pada ruang digital, seperti *malware* dan kejahatan siber. Kerentanan terhadap kejahatan siber, membuat negara Indonesia harus memberikan usaha terbaik untuk melakukan penanganan kejahatan siber, terlebih pada perang siber yang berdampak secara nasional. Sebelum melakukan pencegahan dan penanganan, Pemerintah Indonesia dan masyarakatnya harus memahami konsep dan definisi perang siber terlebih dahulu. Tanpa

pemahaman konsep dan definisi perang siber, maka individu, organisasi, ataupun negara tidak akan pernah mengetahui bahaya yang mengintai dari penggunaan teknologi siber sehari-hari.

## TINJAUAN PUSTAKA

### 1. Perang Siber

Perang siber merubah presepsi dan ide yang dimiliki tentang perang. Perang siber menurut adalah bentuk baru dari perang (Sharma, 2009). Clausewitz dalam Sharma (2009) menjelaskan bahwa perang siber adalah perang yang mampu memaksa musuh atau target untuk memenuhi kepentingan dan keinginan penyerang untuk mencapai tujuan tanpa menerapkan kekuatan fisik. Sedangkan menurut Libicki (2009), perang siber diartikan sebagai sesuatu yang terdiri dari jaringan komputer, penyerangan, dan pertahanan. Perang yang biasanya diketahui oleh masyarakat adalah perang antar negara, bangsa, ataupun wilayah yang diperintah oleh pemerintahan atau penguasa untuk mencapai tujuan ekonomi, agama, atau politik dengan menggunakan kekerasan (Paul J, 2017). Namun perang siber merupakan perang yang berbeda, perang tersebut dilakukan dengan melakukan penyerangan di ruang siber, meskipun dalam pelaksanaan lapangannya secara tidak langsung dapat melibatkan fisik sehingga menimbulkan kerugian seperti perang biasanya (Paul J, 2017).

Hal tersebut menyebabkan perdebatan oleh para ahli, apakah fenomena tersebut dapat dikatakan sebagai perang, sebagaimana perang yang diketahui merupakan hal yang identik dengan kekerasan. Sebelum masuknya era digital, perang siber merupakan hal yang sangat tidak dapat dibayangkan oleh masyarakat. Oleh karena tingkat kerusakan dan biaya yang dikeluarkan lebih efektif untuk mencapai tujuan, sehingga perang siber disebut sebagai '*the future of war*' sebagaimana perang yang terjadi di ranah udara, daratan, lautan, dan lainnya disebut sebagai perang primitif (Grayling, 2017). Untuk unggul dalam keamanan siber dalam menghadapi potensi risiko nasional paling serius termasuk perang siber, pemimpin dalam keamanan siber suatu negara harus mencari keseimbangan yang sesuai antara sumber, energi, dan fokus antara ancaman-ancaman siber yang sering dan paling penting (Cutts, 2009).

Meskipun perang siber telah lama ada, namun belum didefinisikan secara baik (Carr, 2012). Tidak ada di dunia internasional yang mengembangkan definisi hukum dari perang siber, sebagaimana perang siber masih belum diatur secara internasional. Carr (2012) juga mengungkapkan apabila LOAC dijadikan sebagai suatu dasar untuk menentukan apakah yang termasuk dalam perang siber, maka penyerangan tersebut harus termasuk dalam ketentuan tertentu. Pertama, konflik bersenjata telah diinisiasi. Kedua, insiden siber yang berkoresponden dengan koflik bersenjata tersebut harus dapat dispesifikasikan kedalam negara tertentu secara langsung ataupun tidak langsung. Yang ketiga adalah adanya tujuan yang membahayakan target yang diserangnya.

Pada Indonesia sendiri, dalam Peraturan Menteri Pertahanan Republik Indonesia No. 82 tahun 2014, perang siber didefinisikan sebagai segala tindakan penyerangan yang dilakukan dengan sengaja, terkoordinasi, dan memiliki tujuan mengganggu kedaulatan negara. Definisi yang dijabarkan dalam Peraturan Menteri Pertahanan Republik Indonesia No. 82 tahun 2014 masih belum sepenuhnya jelas dan sesuai, sebagaimana definisi tersebut mencakup *cyber terrorism* yang seharusnya berbeda dengan perang siber yang mempunyai penyerangan skala negara dengan negara. Namun, dikarenakan anonimitas yang tinggi dalam penyerangan tersebut, membuat batasan definisi tersebut menjadi kurang jelas. Selain itu, tidak dapat dibuktikannya aktor penyerang dalam suatu penyerangan mengakibatkan kebingungan dalam menentukan apakah penyerangan yang sedang terjadi merupakan *cyber terrorism* ataukah perang siber. Sehingga, perang siber yang dimaksud oleh penulis dalam penelitian ini adalah semua aktivitas penyerangan siber yang mengakibatkan dampak dengan skala nasional atau mengganggu kedaulatan nasional, dengan kemungkinan penyerangan tersebut dilakukan oleh negara lain.

### *2. Routine Activity Theory*

Korban dari perang siber dapat dijelaskan oleh teori *routine activity*. Fattah (2000) mengemukakan bahwa viktimisasi dapat dijelaskan oleh teori *routine activity*. Dalam teori ini dijelaskan bahwa terjadinya viktimisasi dikarenakan adanya tiga elemen, yaitu *motivated offenders*, *suitable targets*, dan tidak adanya *capable guardians*. Maksud dari *motivated offenders* adalah aktor yang termotivasi dan memiliki keinginan untuk melakukan kejahatan. Banyak faktor-faktor yang dapat mempengaruhi aktor tersebut untuk melakukan kejahatan diantaranya seperti adanya pengaruh sosial, kebutuhan ekonomi, dan lainnya. Sedangkan elemen *suitable targets* adalah target korban baik itu objek, individu, atau properti yang dinilai menarik, layak, dan mudah oleh aktor kejahatan. Pelaku/aktor kejahatan melihat nilai, aksesibilitas, visibilitas, dan kelemahan target korban. Sedangkan tidak adanya *capable guardians* adalah tidak adanya bentuk penjagaan yang dapat mengurangi kesempatan aktor untuk melakukan kejahatan. *Capable guardians* dapat dilihat dari berbagai bentuk seperti kebijakan, organisasi, dan teknologi.

## METODE

Penelitian ini merupakan penelitian kualitatif melalui wawancara. Pendekatan kualitatif memungkinkan peneliti untuk mengekplorasi dan menganalisis lebih jauh tanpa dibatasi oleh statistik ataupun pendekatan kuantitatif. Data dalam penelitian ini menggunakan data primer dan data sekunder. Data primer dikumpulkan dengan wawancara pada 3 lembaga pemerintahan yaitu BSSN, Kementrian Pertahanan, dan Kepolisian RI dan masyarakat negara Indonesia dengan sampling 10 orang yang tidak memiliki *background* pendidikan dan pekerjaan terkait IT, siber, dan yang berkaitan lainnya. Diambilnya ketiga lembaga tersebut, dikarenakan ketiga lembaga tersebut merupakan lembaga pemerintah yang berwenang dalam penanganan kejahatan dan serangan siber di Indonesia. Data sekunder menggunakan data dari Laporan Publikasi, Kebijakan, atau dokumen terkait lainnya. Hasil temuan analisis akan dianalisis lebih lanjut dengan teori *Routine activity*.

## HASIL DAN PEMBAHASAN

### 1. Pemahaman Definisi dan Konsep Perang Siber di Indonesia

Perbedaan persepsi terhadap perang siber sering ditemukan diakibatkan oleh adanya kompleksitas dan batasan konsep, aktor yang terlibat, perkembangan dan keragaman teknologi, dan lainnya. BSSN menjelaskan bahwa terdapat banyak pengertian tentang perang siber. Perang siber sifatnya berbeda dengan perang konvensional. Adanya perang konvensional akan dideklarasikan secara formal oleh negara lawan yang berlangsung dalam jangka waktu tertentu, lain halnya dengan perang siber yang berlangsung secara senyap. Perbedaan antara perang siber dengan kejahatan siber dilihat dari aktor penyerangnya. Apabila yang terlibat dalam suatu serangan siber merupakan *state actor* ataupun *state-sponsored actor* dengan tujuan menyerang infrastruktur, fasilitas dan aset milik pemerintah negara lain, maka hal tersebut lebih dikategorikan pada perang siber.

Kepolisian RI mengungkapkan bahwa perang siber dapat dilihat dari dua bentuk, yang pertama *computer related* dan *computer based*. *Computer/IT related* merupakan gangguan pertahanan negara yang menggunakan komputer atau teknologi informasi. Salah satu contohnya adalah dengan adanya opini atau komentar yang dapat menggerakkan dan merubah suatu bangsa dari pemikiran dan identitas lamanya. *Computer/IT based* merupakan perang siber yang melakukan penyerangan pada komputer atau infrastruktur teknologi informasi lainnya, seperti misalnya hacking pada fasilitas kritikal negara. Hal tersebut diaplikasikan dalam 3 sub-bagian pada Direktorat Tindak Pidana Siber (Dittipidsiber) yaitu Subdit *Computer Related*, Subdit *Computer Crime*, dan Subdit Bantuan Teknis (Seperti bidang kerjasama, laporan forensik, dan lain-lain). Selain itu, perang siber dapat dibagi menjadi dua yaitu nyata dan tidak nyata. Nyata dimaksudkan bahwa perang

siber secara nyata merusak ruang fisik seperti misalnya fasilitas kritis negara. Sedangkan tidak nyata dimaksudkan sebagai fungsi mata-mata, tidak merusak secara fisikal namun mengintai kebiasaan negara, algoritma, atau lainnya yang dapat dipakai sebagai senjata dikemudian hari. Menurut Kepolisian RI, perang siber tidak terbatas dalam mengganggu dan pengrusakan fasilitas kritikal, namun juga pada persiapannya seperti penanaman ideologi baru pada Masyarakat Indonesia.

Menurut Kementrian Pertahanan perang siber adalah perang yang asimetris. Istilah asimetris disematkan dikarenakan antara serangan dan pertahanan yang dilakukan sifatnya tidak seimbang. Serangan siber dapat dilakukan dengan modal yang rendah, usaha yang tidak sulit, maupun SDM yang sedikit, namun pertahanannya membutuhkan usaha yang besar, biaya yang besar, dengan jumlah SDM yang cukup. Dari ketiga lembaga tersebut, bahwa terdepat perbedaan persepsi terkait konsep dan definisi perang siber. BSSN menekankan pada penyerangan dilakukan oleh Negara. Kepolisian RI menekankan bentuk penyerangan ada pada dua bentuk. Sedangkan, Kementrian Pertahanan menekankan perang siber pada dampak terganggunya keamanan dan kedaulatan negara Indonesia. Dapat disimpulkan bahwa perang siber adalah perang yang dilakukan oleh suatu negara dengan menyerang fasilitas kritis ataupun lainnya dalam teknologi siber yang mengganggu keamanan dan kedaulatan negara.

Dari hasil wawancara pada 10 narasumber sampling masyarakat Indonesia dapat disimpulkan bahwa mayoritas masyarakat Indonesia tidak memahami ataupun tidak pernah mendengar istilah perang siber. Terdapat 1 orang dari 10 orang narasumber yang memahami perang siber adalah penyerangan siber dari negara lain terhadap fasilitas kritis negara Indonesia maupun dalam bentuk propaganda. Hal tersebut menunjukkan bahwa pemahaman terkait istilah dan konsep perang siber di Indonesia masih dalam tahap awal. Terdapat kesenjangan pengetahuan terkait isu-isu keamanan siber di Indonesia. Meningkatnya penggunaan teknologi siber di Indonesia seharusnya diiringi dengan peningkatan kesadaran masyarakat maupun lembaga pemerintahan pada isu dan potensi risiko yang dapat terjadi di Indonesia.

**2. Implikasi Perbedaan Persepsi Perang Siber**

Kurangnya pemahaman konsep perang siber, memperbesar potensi negara Indonesia menjadi korban. Ketidakpemahaman membuat kurangnya pengambilan langkah-langkah pencegahan dan keamanan yang memadai. Potensi viktimasi perang siber dapat dijelaskan oleh teori *routine activity*. Fattah (2000) mengemukakan bahwa viktimisasi dapat dijelaskan oleh teori *routine activity*. Dalam teori ini dijelaskan bahwa terjadinya viktimisasi dikarenakan adanya tiga elemen, yaitu *motivated offenders*, *suitable targets*, dan tidak adanya *capable guardians*. Dalam elemen *motivated offenders*, aktor negara yang menyerang Ketidakpemahaman tentang perang siber membuat individu, organisasi, atau negara tidak menyadari motivasi dan teknik yang digunakan oleh aktor, sehingga memperbesar probabilitas gagal dalam mengantisipasi serangan yang terjadi. Sedangkan dalam elemen *suitable targets*, ketidakpemahaman tentang perang siber menjadikan potensi target yang menarik oleh aktor penyerang. Sebagaimana tanpa pemahaman perang siber, persiapan terkait keamanan dan pertahanan siber tersebut masih kurang dan lemah. Dalam elemen tidak adanya *capable guardians*, tidak adanya penjagaan yang dapat mencegah perang siber terjadi membuat suatu negara akan selalu rentan terhadap penyerangan yang dilakukan negara lain. Kebijakan yang memadai, sistem organisasi yang efektif, serta kesadaran bersama dari masyarakat terkait perang siber merupakan salah satu penjagaan yang dapat dilakukan dari potensi viktimisasi perang siber. Serangan yang dilakukan oleh negara tertentu bisa terjadi dimana saja seperti sektor pemerintahan, perusahaan kritikal seperti perbankan, ataupun penyerangan sistem komunikasi masyarakat Indonesia. Sehingga, tanpa adanya usaha bersama baik dari lembaga Pemerintahan, organisasi, serta individu, keamanan siber akan tetap lemah.

## KESIMPULAN

Perbedaan persepsi perang siber timbul akibat kurangnya awareness terkait perang siber itu sendiri. Pemahaman mendalam terkait perang siber membuat pemerintah dan masyarakat melaksanakan pencegahan dan penanganan yang efektif, yang dapat mengurangi potensi viktimisasi perang siber. Namun saat ini pemahaman perang siber belum merata sepenuhnya merata. Lembaga pemerintahan yang berkaitan dengan keamanan siber kurang lebih sudah memahami terkait konsep dan definisi perang siber. Namun mayoritas masyarakat yang tidak memiliki latar belakang dan pendidikan terkait IT dan *cyber-related*, kurang memahami konsep dan definisi perang siber. Tanpa adanya pemahaman perang siber yang kuat, Indonesia tidak dapat menerapkan pencegahan dan penanganan yang kuat juga (adanya *capable guardians*). Sebagaimana negara yang bertujuan melakukan penyerangan terhadap Indonesia tidak dapat diketahui dengan pasti.

## DAFTAR PUSTAKA


Carr, Jeffrey. (2012). *Inside Cyber Warfare Mapping The Cyber Underworld*. Sebastopol: O'reilly Media.

Cutts, Andrew. (2009). *Warfare and the Continuum of Cyber Risks: A Policy Perspective*. The Virtual Battlefield: Perspectives on Cyber Warfare, IOS Press.

Fattah, Ezzat A. (2000). *Victimology: Past, Present and Future*. Criminologie, Vol. 33, No. 1: 17-46.

Gazula, Mohan B. (2017). *Cyber Warfare Conflict Analysis and Case Studies*. Cambridge: Massachusetts Institute of Technology.

Grayling, A.C. (2017). *War an Enquiry*. New Haven CT: Yale University.

Holloway, Michael. (2015). *Stuxnet Worm Attack on Iranian Nuclear Facilities*. Diakses pada laman: http://large.stanford.edu/courses/2015/ph241/ holloway1/.

Kementerian Pertahanan Republik Indonesia. (2014). Peraturan Menteri Pertahanan Republik Indonesia Nomor 82 Tahun 2014 Tentang Pedoman Pertahanan Siber.

Libicki, Martin C. (2009). *Sub Rosa Cyber War*. The Virtual Battlefield: Perspectives on Cyber Warfare, IOS Press.

Paul J. (2017). *Encyclopedia of Cyber Warfare*. Colorado: ABC-CLIO. Springer.

Pratama, Ryscha Yuliardi. (2016). *Penggunaan Cyberwar Melalui Stuxnet Project Oleh Amerika Serikat dalam Merespon Perkembangan Proyek Nuklir Iran di Natanz*. Jurnal Analisis Hubungan Internasional, Vol. 5 No. 2.

Sharma, Amit. (2009). *Cyber Wars: A Paradigm Shift from Means to Ends*. The Virtual Battlefield: Perspectives on Cyber Warfare, IOS Press.

Zahra, Natasya. 2023. *Meningkatkan Inklusi dalam Indeks Literasi Digital Nasional: Dari Pengukuran hingga Pemberdayaan*. Ringkasan Kebijakan No. 19.