Jurnal Hukum dan HAM Wara Sains
Vol. 5, No. 02, Juni 2026, pp. 411-422

Cyber Warfare Sebagai Bentuk Kejahatan Dunia Maya dan Ancaman Terhadap Keamanan Nasional Dalam Perspektif Hukum Pidana

Kurnia Tanu Putra[1], Devina Chandra[2], Fernando Lim[3], Felicia Anter[4], Lioni Anggraini[5], Syamhaikel Pavel Budiman[6], Oky Annisa Rizky Noer Janah[7], Yuni Priskila Ginting[8]

[1] Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Pelita Harapan dan 01051230111@student.uph.edu
[2] Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Pelita Harapan dan 01051230127@student.uph.edu
[3] Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Pelita Harapan dan 01051230139@student.uph.edu
[4] Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Pelita Harapan dan 01051230122@student.uph.edu
[5] Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Pelita Harapan dan 01051230134@student.uph.edu
[6] Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Pelita Harapan dan 01051230193@student.uph.edu
[7] Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Pelita Harapan dan 01051230098@student.uph.edu
[8] Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Pelita Harapan dan yuni.ginting@uph.edu

Article Info

Article history:

Received Jun, 2026
Revised Jun, 2026
Accepted Jun, 2026

Kata Kunci:

Kejahatan Dunia Maya, Cyber Warfare, Keamanan Nasional, Hukum Pidana, Perbandingan Hukum

Keywords:

Cybercrime, Cyber Warfare, National Security, Criminal Law, Comparative Law

ABSTRAK

Perkembangan teknologi informasi dan komunikasi telah melahirkan bentuk ancaman baru terhadap keamanan nasional, salah satunya adalah kejahatan dunia maya (cybercrime) yang dalam perkembangannya dapat mengarah pada cyber warfare sebagai bentuk konflik di ruang siber. Fenomena ini menempatkan ruang siber sebagai domain strategis yang berdampak langsung terhadap kedaulatan negara, stabilitas politik, serta keamanan infrastruktur kritis. Tantangan utama yang dihadapi oleh berbagai negara adalah merumuskan regulasi hukum pidana yang adaptif dan responsif terhadap kompleksitas serangan siber modern yang terus berkembang. Penelitian ini bertujuan untuk menganalisis dan membandingkan pengaturan hukum pidana terkait kejahatan dunia maya sebagai ancaman terhadap keamanan nasional, serta mengidentifikasi kelemahan dan keunggulan sistem hukum dalam merespons ancaman tersebut di era digital. Metode penelitian yang digunakan adalah penelitian hukum normatif dengan pendekatan perundang-undangan (statute approach) dan pendekatan komparatif (comparative approach), dengan mengkaji berbagai regulasi, literatur ilmiah, dan dokumen hukum yang relevan. Hasil penelitian menunjukkan bahwa pengaturan hukum pidana pada umumnya masih berfokus pada penanggulangan cybercrime konvensional yang menitikberatkan pada perlindungan individu dan transaksi elektronik, sehingga belum sepenuhnya mengakomodasi cyber warfare sebagai ancaman keamanan nasional yang bersifat strategis. Selain itu, tantangan yang dihadapi meliputi penegakan hukum, yurisdiksi lintas negara, serta perkembangan teknologi yang lebih cepat dibandingkan regulasi yang ada. Kesimpulan penelitian ini menegaskan perlunya reformulasi kebijakan hukum pidana yang lebih komprehensif, terintegrasi, dan

berorientasi pada keamanan nasional, serta penguatan kerja sama internasional dalam penanggulangan kejahatan dan konflik siber.

ABSTRACT

The development of information and communication technology has generated new forms of threats to national security, one of which is cybercrime that has evolved into cyber warfare as a form of conflict in cyberspace. This phenomenon places cyberspace as a strategic domain that directly affects state sovereignty, political stability, and the security of critical infrastructure. The main challenge faced by many countries is formulating adaptive and responsive criminal law regulations to address the complexity of modern cyber attacks that continue to develop. This study aims to analyze and compare criminal law regulations related to cybercrime as a threat to national security, as well as to identify the strengths and weaknesses of legal systems in responding to such threats in the digital era. The research method used is normative legal research employing statutory and comparative approaches by examining various legal regulations, scientific literature, and relevant legal documents. The results indicate that criminal law regulations generally remain focused on conventional cybercrime prevention, emphasizing the protection of individuals and electronic transactions, and have not fully accommodated cyber warfare as a strategic threat to national security. Furthermore, the challenges encountered include law enforcement limitations, cross-border jurisdiction issues, and technological developments that progress faster than existing regulations. This study concludes that there is a need to reformulate criminal law policies in a more comprehensive, integrated, and national security-oriented manner, as well as to strengthen international cooperation in addressing cybercrime and cyber conflicts.

Corresponding Author:

Name: Yuni Priskila Ginting
Institution: Program Studi Ilmu Hukum, Fakultas Hukum, Universitas Pelita Harapan, JI. Boulevard M.H. Thamrin 1100, Lippo Village, Kelapa Dua, Tangerang, Banten 15811
Email: yuni.ginting@uph.edu

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi dalam beberapa dekade terakhir telah membawa perubahan mendasar terhadap pola keamanan global. Transformasi digital yang pada awalnya bertujuan meningkatkan efisiensi dan konektivitas justru memunculkan berbagai bentuk ancaman baru yang bersifat non-konvensional, salah satunya adalah *cyber warfare*. Dalam situasi ini, ruang siber tidak lagi dipandang sekadar sebagai sarana komunikasi, melainkan telah berkembang menjadi domain strategis yang memiliki posisi setara dengan wilayah darat, laut, dan udara dalam sistem pertahanan negara modern. Sebagaimana dikemukakan oleh Richard A. Clarke (2010), *cyber warfare* merupakan ancaman nyata bagi keamanan nasional karena mampu melumpuhkan

infrastruktur penting suatu negara tanpa harus melibatkan serangan fisik secara langsung. Dengan demikian, cyber warfare tidak hanya berkaitan dengan tindak kejahatan siber biasa (*cybercrime*), tetapi telah berkembang menjadi sarana konflik antarnegara yang digunakan untuk melemahkan kekuatan pihak lawan.

Karakteristik cyber warfare memiliki perbedaan yang cukup mendasar dibandingkan dengan perang konvensional. Serangan siber tidak dibatasi oleh wilayah geografis tertentu, dapat dilakukan secara anonim, serta memiliki tingkat atribusi yang rendah sehingga menyulitkan proses identifikasi pelaku secara pasti. Menurut P. W. Singer dan Allan Friedman (2014), sifat anonim dan lintas batas dari serangan siber menjadikan *cyber warfare* sebagai ancaman yang kompleks, baik dari segi teknis maupun aspek hukum. Selain itu, dampak yang ditimbulkan oleh serangan siber bersifat luas dan sistemik, yang dapat mengganggu berbagai sektor infrastruktur penting, seperti energi, transportasi, dan komunikasi. Gangguan terhadap sektor-sektor tersebut pada akhirnya berpotensi menimbulkan ketidakstabilan ekonomi serta mengancam keamanan nasional suatu negara.

Dalam perspektif hukum pidana, perkembangan cyber warfare menghadirkan tantangan yang signifikan terhadap konsep-konsep hukum yang selama ini berlandaskan pendekatan konvensional. Pada umumnya, hukum pidana dirancang untuk mengatur perbuatan yang bersifat fisik dengan batas yurisdiksi yang jelas, sedangkan cyber warfare memiliki karakter lintas negara dan kerap melibatkan aktor negara maupun non-negara. Kondisi tersebut menimbulkan berbagai permasalahan, terutama terkait dengan penentuan yurisdiksi, proses pembuktian, serta mekanisme penegakan hukum terhadap pelaku serangan siber. Dalam kajian hukum siber, sebagaimana dikemukakan oleh Robert W. Taylor (2011), perkembangan kejahatan berbasis teknologi menuntut adanya penyesuaian dalam hukum pidana agar mampu mengakomodasi bentuk-bentuk kejahatan baru yang tidak lagi bersifat konvensional.

Indonesia sebagai negara berkembang dengan tingkat digitalisasi yang terus meningkat menghadapi risiko kerentanan yang cukup besar terhadap ancaman serangan siber. Regulasi yang berlaku saat ini, seperti Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah diubah melalui Undang-Undang Nomor 19 Tahun 2016, pada dasarnya masih menitikberatkan pada pengaturan cybercrime dalam lingkup terbatas, seperti akses ilegal, penipuan berbasis daring, dan pencemaran nama baik. Di sisi lain, Kitab Undang-Undang Hukum Pidana juga belum secara tegas mengatur cyber warfare sebagai bentuk ancaman terhadap keamanan nasional. Keadaan ini menunjukkan adanya kemungkinan kekosongan norma hukum dalam menghadapi serangan siber yang bersifat strategis, sistematis, dan terorganisir.

Berbeda dengan kondisi tersebut, Iran menunjukkan pendekatan yang relatif lebih komprehensif dalam menghadapi ancaman di ruang siber. Negara tersebut tidak hanya menjadi sasaran berbagai serangan siber berskala internasional, tetapi juga secara aktif mengembangkan kemampuan pertahanan siber sebagai bagian dari strategi keamanan nasional. Sejumlah laporan strategis menunjukkan bahwa Iran termasuk negara yang telah mengintegrasikan kebijakan siber ke dalam sistem pertahanan negara secara terstruktur dan berkelanjutan.

Salah satu peristiwa yang dianggap sebagai tonggak penting dalam perkembangan cyber warfare di tingkat global adalah insiden Stuxnet pada tahun 2010. Stuxnet merupakan malware berjenis worm dengan tingkat kecanggihan tinggi yang dirancang untuk menargetkan sistem kontrol industri, khususnya yang digunakan pada fasilitas nuklir di Natanz. Malware tersebut diketahui diarahkan pada sistem yang dikembangkan oleh Siemens, terutama perangkat lunak

Step7 yang berfungsi mengendalikan programmable logic controllers (PLC) dalam proses operasional industri.

Dari aspek teknis, Stuxnet beroperasi dengan memanfaatkan berbagai kelemahan keamanan dalam sistem operasi untuk memperoleh akses ke jaringan yang menjadi target. Setelah berhasil menginfeksi sistem, malware ini mengubah instruksi operasional pada mesin sentrifugal yang digunakan dalam proses pengayaan uranium. Dampaknya, mesin-mesin tersebut beroperasi secara tidak wajar hingga mengalami kerusakan fisik tanpa terdeteksi oleh operator. Hasil analisis Kaspersky Lab (2010) menunjukkan bahwa Stuxnet termasuk salah satu malware paling kompleks yang pernah ditemukan, karena mampu mengombinasikan teknik spionase siber dengan tindakan sabotase terhadap infrastruktur fisik.

Selain itu, kasus Stuxnet juga memberikan indikasi kuat mengenai kemungkinan keterlibatan aktor negara dalam pengembangan dan penggunaan senjata siber. Sejumlah kajian menghubungkan serangan ini dengan operasi rahasia yang dikenal sebagai Operation Olympic Games (2010), yang diduga melibatkan beberapa negara maju. Peristiwa ini menunjukkan adanya perubahan paradigma dalam pola konflik internasional, di mana negara tidak lagi hanya mengandalkan kekuatan militer konvensional, tetapi juga memanfaatkan teknologi siber sebagai instrumen strategis dalam mencapai kepentingan nasional.

Dampak dari serangan Stuxnet memiliki konsekuensi yang luas, baik dalam perspektif hukum maupun keamanan internasional. Dari sudut pandang hukum, peristiwa ini memunculkan perdebatan mengenai bagaimana serangan siber dapat dikualifikasikan sebagai tindak pidana, khususnya ketika terdapat dugaan keterlibatan aktor negara. Selain itu, muncul pula berbagai persoalan terkait yurisdiksi lintas negara, proses pembuktian, serta efektivitas mekanisme penegakan hukum terhadap pelaku yang sulit diidentifikasi secara pasti. Dalam ranah hukum internasional, pedoman seperti Tallinn Manual on the International Law Applicable to Cyber Warfare (2013) menunjukkan bahwa regulasi mengenai cyber warfare masih berada dalam tahap perkembangan dan belum sepenuhnya memiliki standar yang mapan secara universal.

Berdasarkan pemaparan latar belakang tersebut, penelitian ini berangkat dari pertanyaan mendasar mengenai bagaimana konstruksi pengaturan hukum pidana terhadap cyber warfare dalam perspektif keamanan nasional, khususnya dalam kerangka sistem hukum di Indonesia dan Iran. Permasalahan ini menjadi penting untuk dikaji mengingat cyber warfare telah berkembang menjadi ancaman strategis yang tidak lagi dapat dipahami sebagai bentuk kejahatan konvensional semata. Selain itu, penelitian ini juga mengkaji perbandingan tingkat efektivitas regulasi hukum pidana di kedua negara dalam merespons ancaman cyber warfare, serta menilai sejauh mana masing-masing sistem hukum mampu beradaptasi terhadap dinamika ancaman siber yang bersifat lintas batas negara dan terus berkembang. Pendekatan komparatif digunakan untuk mengidentifikasi persamaan dan perbedaan dalam sistem hukum kedua negara, sekaligus menemukan praktik-praktik terbaik yang berpotensi dijadikan rujukan dalam pembaruan hukum nasional.

Sejalan dengan rumusan masalah tersebut, penelitian ini bertujuan untuk mengkaji konstruksi serta karakteristik pengaturan hukum pidana yang berkaitan dengan cyber warfare dalam kerangka perlindungan keamanan nasional di Indonesia dan Iran. Penelitian ini juga diarahkan untuk melakukan analisis komparatif guna mengidentifikasi keunggulan dan keterbatasan masing-masing sistem hukum dalam menghadapi ancaman cyber warfare. Melalui pendekatan tersebut, diharapkan penelitian ini mampu memberikan kontribusi terhadap

pengembangan hukum pidana yang lebih responsif terhadap kemajuan teknologi, serta menjadi landasan dalam perumusan kebijakan hukum yang adaptif dalam menghadapi tantangan keamanan nasional di era digital.

2. METODE PENELITIAN

Penelitian ini merupakan penelitian hukum normatif atau yuridis normatif, yaitu penelitian yang berfokus pada kajian terhadap norma-norma hukum yang berlaku, baik yang tertuang dalam peraturan perundang-undangan maupun dalam berbagai sumber hukum lainnya. Penelitian hukum normatif digunakan untuk menganalisis asas-asas hukum, sistematika hukum, serta sinkronisasi peraturan perundang-undangan yang berkaitan dengan cyber warfare sebagai ancaman terhadap keamanan nasional. Dalam konteks ini, hukum dipandang sebagai suatu sistem norma yang menjadi acuan dalam menilai dan mengatur fenomena hukum yang berkembang di masyarakat.

Pendekatan yang digunakan dalam penelitian ini meliputi pendekatan perundang-undangan (statute approach), pendekatan konseptual (conceptual approach), dan pendekatan kasus (case approach). Pendekatan perundang-undangan dilakukan dengan menelaah berbagai peraturan hukum yang relevan, khususnya yang berkaitan dengan hukum pidana dan hukum siber, baik dalam sistem hukum Indonesia maupun Iran. Melalui pendekatan ini, penulis menganalisis sejauh mana regulasi yang ada mampu mengakomodasi perkembangan cyber warfare sebagai ancaman terhadap keamanan nasional.

Selanjutnya, pendekatan konseptual digunakan untuk mengkaji konsep-konsep hukum yang berkembang dalam doktrin dan literatur ilmiah, khususnya yang berkaitan dengan cyber warfare, keamanan nasional, serta hukum pidana. Pendekatan ini bertujuan untuk memperoleh pemahaman yang komprehensif mengenai konsep dan prinsip hukum yang menjadi dasar dalam menganalisis permasalahan yang diteliti, sekaligus untuk mengisi kekosongan norma yang belum diatur secara eksplisit dalam peraturan perundang-undangan.

Selain itu, pendekatan kasus digunakan dengan menelaah kasus-kasus konkret yang relevan dengan cyber warfare, salah satunya adalah kasus Stuxnet yang menyerang fasilitas nuklir di Iran. Melalui pendekatan ini, penelitian tidak hanya bersifat teoritis, tetapi juga mempertimbangkan praktik nyata yang terjadi di lapangan. Analisis terhadap kasus tersebut memberikan gambaran empiris mengenai bagaimana cyber warfare dapat terjadi serta implikasi hukumnya terhadap keamanan nasional dan sistem hukum yang berlaku.

Bahan hukum yang digunakan dalam penelitian ini terdiri atas bahan hukum primer, bahan hukum sekunder, dan bahan hukum tersier. Bahan hukum primer meliputi peraturan perundang-undangan yang relevan, sedangkan bahan hukum sekunder berupa buku, jurnal ilmiah, dan hasil penelitian yang berkaitan dengan topik yang dibahas. Adapun bahan hukum tersier digunakan sebagai pendukung, seperti kamus hukum dan ensiklopedia. Seluruh bahan hukum tersebut dianalisis secara kualitatif dengan menggunakan metode deskriptif-analitis, yaitu dengan menggambarkan dan menginterpretasikan data hukum yang diperoleh untuk kemudian ditarik kesimpulan yang relevan dengan permasalahan penelitian.

3. HASIL DAN PEMBAHASAN

3.1 Cyber Warfare sebagai Ancaman Keamanan Nasional dalam Perspektif Teoretis

Perkembangan teknologi informasi dan komunikasi telah membawa perubahan signifikan terhadap konsep keamanan nasional yang selama ini dipahami secara konvensional. Ancaman terhadap kedaulatan negara tidak lagi terbatas pada serangan militer tradisional, melainkan telah berkembang ke arah ancaman non-konvensional yang memanfaatkan ruang siber sebagai sarana utama. Dalam konteks tersebut, *cyber warfare* muncul sebagai bentuk baru dari konflik modern, di mana negara maupun aktor non-negara dapat melakukan serangan strategis tanpa harus melibatkan kontak fisik secara langsung. Dalam kajian keamanan siber, Richard A. Clarke (2010) menyatakan bahwa cyber warfare memiliki kemampuan untuk mengganggu bahkan melumpuhkan sistem-sistem penting suatu negara, seperti jaringan listrik, sektor keuangan, dan infrastruktur komunikasi, yang pada akhirnya berpotensi mengganggu stabilitas nasional secara menyeluruh. Pendapat tersebut diperkuat oleh P. W. Singer dan Allan Friedman (2014) yang menegaskan bahwa cyber warfare memiliki karakteristik khas berupa anonimitas pelaku, kecepatan serangan, serta jangkauan yang bersifat global, sehingga menjadikannya sulit untuk dideteksi maupun dikendalikan secara efektif. Martin C. Libicki (2009) menjelaskan bahwa cyber warfare tidak selalu diarahkan untuk tujuan destruktif semata, tetapi juga dapat dimanfaatkan sebagai sarana pencegahan strategis (cyber deterrence) serta instrumen dalam strategi geopolitik suatu negara. Pandangan ini menunjukkan bahwa cyber warfare tidak hanya memiliki aspek teknis, tetapi juga mengandung dimensi politik dan strategis yang kompleks dalam dinamika hubungan internasional.

Dalam konteks hukum internasional, Michael N. Schmitt (2012) menjelaskan bahwa salah satu tantangan utama dalam cyber warfare adalah menentukan apakah suatu serangan siber dapat dikategorikan sebagai penggunaan kekuatan (use of force) atau bahkan serangan bersenjata (armed attack). Ketidakjelasan ini menunjukkan bahwa kerangka hukum yang ada masih belum sepenuhnya mampu mengakomodasi perkembangan cyber warfare. Cyber warfare harus dipahami sebagai ancaman multidimensional yang memerlukan pendekatan komprehensif, baik dari aspek hukum, teknologi, maupun kebijakan keamanan nasional. Kasus Stuxnet sering dipandang sebagai salah satu ilustrasi paling konkret mengenai penerapan cyber warfare dalam praktik nyata. Malware ini pertama kali teridentifikasi pada tahun 2010 dan dirancang untuk menargetkan fasilitas nuklir di Iran, khususnya yang berlokasi di Natanz. Serangan tersebut secara luas dinilai sebagai operasi siber pertama yang berhasil menimbulkan kerusakan fisik terhadap infrastruktur strategis suatu negara, sehingga menjadi tonggak penting dalam perkembangan konflik berbasis teknologi siber.

Menurut Jon R. Lindsay (2013), peristiwa Stuxnet memperlihatkan bahwa cyber warfare memiliki keterbatasan sekaligus peluang strategis yang signifikan. Di satu sisi, keberhasilan serangan ini menunjukkan bahwa senjata siber mampu digunakan secara efektif untuk mencapai tujuan strategis tanpa harus melibatkan konflik militer secara terbuka. Namun demikian, di sisi lain, tingkat kompleksitas teknis serta kebutuhan akan dukungan intelijen yang tinggi menunjukkan bahwa pengembangan kemampuan tersebut tidak dapat dilakukan oleh semua negara secara mudah. Hasil analisis Kaspersky Lab (2010) menunjukkan bahwa Stuxnet dirancang dengan tingkat ketelitian yang sangat tinggi, termasuk kemampuan untuk menargetkan sistem tertentu secara spesifik serta menghindari mekanisme deteksi yang ada. Temuan ini mengindikasikan bahwa cyber warfare telah berevolusi menjadi bentuk serangan yang tidak hanya canggih secara teknis, tetapi juga dirancang secara terarah dan sistematis. James P. Farwell dan Rafal Rohozinski (2011) menyatakan bahwa insiden Stuxnet menandai munculnya paradigma baru dalam peperangan

modern, di mana senjata siber dapat dimanfaatkan sebagai sarana sabotase strategis terhadap kepentingan vital suatu negara. Peristiwa ini juga mengindikasikan adanya kemungkinan keterlibatan aktor negara dalam proses pengembangan cyber weapon, meskipun keterlibatan tersebut tidak pernah dinyatakan secara resmi. Dari sudut pandang hukum, kasus Stuxnet menimbulkan sejumlah persoalan yang kompleks, antara lain berkaitan dengan atribusi pelaku, penentuan yurisdiksi, serta legitimasi penggunaan kekuatan dalam ruang siber. Michael N. Schmitt (2015) menjelaskan bahwa hukum internasional hingga saat ini masih berada dalam tahap pengembangan dalam mengatur cyber warfare, sehingga berbagai aspek terkait konflik siber belum memiliki kepastian hukum yang memadai.

3.2 Pengaturan Cyber Warfare dalam Hukum Pidana Indonesia

Dalam kerangka penelitian hukum normatif, pengaturan mengenai cyber warfare dalam sistem hukum pidana Indonesia masih memperlihatkan sejumlah keterbatasan, baik dari sisi normatif maupun konseptual. Kondisi tersebut dapat dianalisis melalui tiga pendekatan utama, yakni pendekatan perundang-undangan (statute approach), pendekatan konseptual (conceptual approach), dan pendekatan kasus (case approach). Melalui pendekatan perundang-undangan (statute approach), pengaturan terkait aktivitas di ruang siber di Indonesia pada dasarnya tertuang dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah diubah dengan Undang-Undang Nomor 19 Tahun 2016. Peraturan tersebut mengatur berbagai bentuk tindak pidana, seperti akses tanpa hak terhadap sistem elektronik, intersepsi ilegal, manipulasi data elektronik, serta gangguan terhadap fungsi sistem elektronik. Selain itu, Kitab Undang-Undang Hukum Pidana (KUHP) juga memuat ketentuan umum yang dapat digunakan untuk menjerat perbuatan yang berkaitan dengan perusakan, sabotase, maupun tindak pidana terhadap keamanan negara.

Secara normatif belum terdapat ketentuan yang secara tegas mengatur cyber warfare sebagai bentuk ancaman terhadap keamanan nasional. Regulasi yang ada masih cenderung berorientasi pada cybercrime dalam arti terbatas, yaitu kejahatan yang dilakukan oleh individu atau kelompok terhadap sistem elektronik. Kondisi ini menunjukkan adanya kekosongan norma (normative gap) dalam mengantisipasi perkembangan cyber warfare yang bersifat lintas batas negara dan berpotensi melibatkan aktor negara. Sebagaimana dikemukakan oleh Barda Nawawi Arief (2016), hukum pidana harus senantiasa menyesuaikan diri dengan dinamika perkembangan masyarakat dan teknologi agar tetap mampu mengakomodasi bentuk-bentuk kejahatan baru. Melalui pendekatan konseptual (conceptual approach), dapat dipahami bahwa dalam sistem hukum Indonesia, cyber warfare belum dirumuskan sebagai konsep hukum yang berdiri secara mandiri. Dalam praktiknya, cyber warfare masih sering dipersamakan dengan cybercrime, meskipun keduanya memiliki karakteristik yang berbeda secara mendasar. Cybercrime umumnya bersifat individual dan kriminal, sedangkan cyber warfare memiliki dimensi strategis, politik, dan militer yang berkaitan erat dengan kepentingan keamanan nasional. Dalam hal ini, P. W. Singer dan Allan Friedman (2014) menegaskan bahwa cyber warfare merupakan bentuk konflik modern yang melibatkan aktor negara dan memiliki dampak luas terhadap stabilitas nasional.

Ketidakjelasan dalam aspek konseptual tersebut berdampak pada lemahnya formulasi kebijakan hukum pidana. Tanpa adanya pemisahan yang jelas antara cybercrime dan cyber warfare, hukum pidana akan mengalami kesulitan dalam menentukan kualifikasi perbuatan, subjek hukum yang bertanggung jawab, serta jenis sanksi yang tepat untuk diterapkan. Oleh karena itu, diperlukan

pengembangan konsep hukum yang lebih komprehensif guna mengakomodasi cyber warfare sebagai bagian dari ancaman terhadap keamanan nasional. Melalui pendekatan kasus (case approach), meskipun Indonesia belum pernah mengalami serangan cyber warfare dalam skala besar seperti kasus Stuxnet, peristiwa tersebut memberikan gambaran nyata mengenai potensi ancaman yang dapat terjadi di masa depan. Serangan terhadap infrastruktur strategis, seperti sektor energi, perbankan, dan komunikasi, berpotensi menimbulkan dampak yang signifikan terhadap stabilitas nasional. Menurut Jon R. Lindsay (2013), kasus Stuxnet membuktikan bahwa cyber warfare memiliki kemampuan untuk menimbulkan kerusakan fisik melalui manipulasi sistem digital, sehingga tidak lagi dapat dipandang sebagai bentuk kejahatan biasa.

Dalam konteks Indonesia, beberapa insiden kebocoran data dan gangguan terhadap sistem pemerintahan dapat dipandang sebagai indikasi awal adanya kerentanan terhadap ancaman siber, meskipun belum mencapai kategori cyber warfare secara penuh. Hal tersebut menunjukkan pentingnya penerapan pendekatan preventif dalam hukum pidana, yang tidak hanya bersifat reaktif terhadap kejahatan yang telah terjadi, tetapi juga mampu mengantisipasi potensi ancaman di masa mendatang. Berdasarkan ketiga pendekatan tersebut, dapat disimpulkan bahwa pengaturan cyber warfare dalam hukum pidana Indonesia masih belum memadai untuk menjawab tantangan keamanan nasional di era digital. Oleh karena itu, diperlukan reformulasi hukum yang meliputi pengakuan terhadap cyber warfare sebagai ancaman strategis, penguatan regulasi yang telah ada, serta pengembangan konsep hukum yang lebih adaptif terhadap kemajuan teknologi. Tanpa langkah-langkah tersebut, sistem hukum pidana Indonesia berpotensi mengalami kesulitan dalam menghadapi dinamika ancaman siber yang semakin kompleks di masa depan.

3.3 Pengaturan Cyber Warfare dalam Sistem Hukum Iran

Dalam kerangka penelitian hukum normatif, kajian terhadap sistem hukum Iran menunjukkan bahwa pengaturan mengenai cyber warfare tidak dirumuskan secara eksplisit sebagai rezim hukum tersendiri, melainkan tersebar dalam sejumlah instrumen hukum yang saling berkaitan. Melalui pendekatan perundang-undangan (statute approach), dapat diidentifikasi bahwa regulasi utama yang mengatur aktivitas di ruang siber adalah Computer Crimes Law Tahun 2009, yang mengatur kriminalisasi terhadap berbagai perbuatan, seperti akses tanpa hak, manipulasi data elektronik, serta gangguan terhadap sistem komputer (Hathaway et al., 2012). Secara normatif, peraturan tersebut tidak secara tegas menggunakan istilah cyber warfare, tetapi mengonstruksinya sebagai bagian dari tindak pidana yang berkaitan dengan keamanan negara, seperti spionase dan sabotase terhadap sistem. Dalam konteks tersebut, cyber warfare ditempatkan sebagai bagian dari kejahatan terhadap keamanan negara (state security crimes), sehingga pendekatan hukum yang digunakan lebih menitikberatkan pada perlindungan kepentingan negara (Schmitt, 2012).

Melalui pendekatan konseptual (conceptual approach), dapat dipahami bahwa dalam doktrin hukum Iran, cyber warfare kerap dipandang sebagai bentuk pengembangan dari praktik spionase dan sabotase yang dilakukan dalam bentuk digital. Pandangan ini sejalan dengan pendapat Martin C. Libicki (2009) yang menyatakan bahwa cyber warfare pada dasarnya merupakan evolusi dari strategi konflik tradisional yang beralih ke ruang siber, bukan sepenuhnya konsep baru yang berdiri secara independen. Dengan demikian, pendekatan yang diterapkan di Iran menunjukkan kecenderungan untuk tidak membedakan secara tegas antara cybercrime dan cyber warfare, melainkan mengintegrasikannya ke dalam kerangka kebijakan keamanan nasional. Selain aspek normatif, Iran juga mengembangkan kebijakan kelembagaan yang bertujuan memperkuat

pengawasan dan pengendalian terhadap aktivitas di ruang siber. Hal ini menunjukkan bahwa regulasi yang diterapkan tidak hanya bersifat yuridis, tetapi juga memiliki dimensi strategis dalam mendukung sistem pertahanan negara. Pandangan ini selaras dengan laporan Center for Strategic and International Studies (2018) yang menyebutkan bahwa Iran telah membangun kapasitas siber yang cukup signifikan sebagai respons terhadap berbagai ancaman eksternal yang dihadapinya.

Melalui pendekatan kasus (case approach), pengalaman Iran sebagai target serangan Stuxnet menjadi salah satu faktor penting dalam pembentukan kebijakan siber nasional. Serangan tersebut membuktikan bahwa infrastruktur strategis suatu negara dapat menjadi sasaran serangan siber yang berdampak langsung pada kerusakan fisik. Menurut Jon R. Lindsay (2013), kasus Stuxnet menunjukkan bahwa cyber warfare memiliki dimensi strategis yang setara dengan konflik konvensional, sehingga membutuhkan respons hukum dan kebijakan yang komprehensif. Secara normatif dapat disimpulkan bahwa sistem hukum Iran mengatur cyber warfare secara tidak langsung melalui kombinasi antara hukum pidana dan kebijakan keamanan nasional. Pendekatan ini mencerminkan karakter hukum yang relatif represif dan strategis, dengan orientasi utama pada perlindungan kedaulatan negara serta kepentingan keamanan nasional.

3.4 Analisis Komparatif dan Implikasi Hukum

Dalam perspektif perbandingan hukum, perbedaan antara Indonesia dan Iran dapat dianalisis melalui tiga pendekatan utama sebagaimana digunakan dalam penelitian ini, yaitu pendekatan perundang-undangan, konseptual, dan kasus. Melalui pendekatan perundang-undangan (statute approach), Indonesia hingga saat ini belum memiliki ketentuan yang secara tegas mengatur cyber warfare sebagai bentuk ancaman terhadap keamanan nasional. Regulasi yang tersedia masih berfokus pada penanggulangan cybercrime dalam pengertian terbatas, sebagaimana tercermin dalam Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik serta Kitab Undang-Undang Hukum Pidana. Sebaliknya, Iran menunjukkan kecenderungan untuk mengintegrasikan isu keamanan siber ke dalam kerangka hukum dan kebijakan nasional, meskipun tidak secara eksplisit menggunakan terminologi cyber warfare dalam regulasinya (Hathaway, 2012).

Dari sudut pandang konseptual (conceptual approach), Indonesia masih menempatkan cybercrime sebagai bentuk kejahatan individual yang bersifat kriminal, sementara Iran cenderung memandang aktivitas siber sebagai bagian dari konflik strategis yang berkaitan dengan kepentingan negara. Pandangan ini sejalan dengan pendapat P. W. Singer dan Allan Friedman (2014) yang menegaskan bahwa cyber warfare memiliki dimensi strategis yang melampaui sekadar kejahatan siber biasa dan berkaitan erat dengan stabilitas nasional. Melalui pendekatan kasus (case approach), peristiwa Stuxnet memberikan pelajaran yang signifikan bagi kedua negara. Bagi Iran, serangan tersebut menjadi momentum penting untuk memperkuat sistem pertahanan siber serta meningkatkan kapasitas keamanan nasional. Di sisi lain, bagi Indonesia, kasus tersebut menunjukkan adanya potensi ancaman yang belum sepenuhnya diantisipasi dalam sistem hukum yang berlaku. Sebagaimana dikemukakan oleh James P. Farwell dan Rafal Rohozinski (2011), insiden Stuxnet menandai awal transformasi cyber warfare menjadi instrumen strategis dalam dinamika hubungan internasional.

Implikasi hukum dari hasil perbandingan tersebut menunjukkan perlunya reformulasi hukum pidana di Indonesia agar lebih responsif terhadap perkembangan cyber warfare. Reformasi tersebut tidak hanya terbatas pada perluasan norma hukum, tetapi juga mencakup perubahan

paradigma dalam memandang ancaman siber sebagai bagian yang tidak terpisahkan dari keamanan nasional. Dalam hal ini, Michael N. Schmitt (2012) menegaskan bahwa sistem hukum harus mampu menyesuaikan diri dengan kemajuan teknologi agar tetap relevan dalam mengatur bentuk-bentuk konflik modern. Analisis komparatif ini menunjukkan bahwa efektivitas regulasi hukum pidana sangat dipengaruhi oleh kemampuan negara dalam mengintegrasikan pendekatan normatif, konseptual, dan empiris secara seimbang. Tanpa adanya integrasi tersebut, hukum berpotensi tertinggal dari perkembangan teknologi serta dinamika ancaman global yang semakin kompleks.

4. KESIMPULAN

Cyber warfare merupakan bentuk ancaman baru terhadap keamanan nasional yang memiliki karakteristik berbeda dari kejahatan konvensional maupun cybercrime secara umum. Ancaman ini tidak hanya berdampak pada sistem informasi, tetapi juga berpotensi menimbulkan kerusakan fisik terhadap infrastruktur strategis negara, sebagaimana tercermin dalam kasus Stuxnet yang menyerang fasilitas nuklir di Iran. Peristiwa tersebut menunjukkan bahwa cyber warfare telah berkembang menjadi instrumen konflik modern yang memiliki dimensi strategis, politik, dan militer yang kompleks. Dalam perspektif hukum pidana, pengaturan cyber warfare di Indonesia masih menunjukkan berbagai keterbatasan yang cukup mendasar. Melalui pendekatan perundang-undangan, dapat diketahui bahwa Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik yang telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, serta Kitab Undang-Undang Hukum Pidana, masih menitikberatkan pada pengaturan cybercrime dalam arti terbatas dan belum secara tegas mengakomodasi cyber warfare sebagai ancaman terhadap keamanan nasional. Dari sisi konseptual, belum adanya pemisahan yang jelas antara cybercrime dan cyber warfare dalam sistem hukum Indonesia turut menyebabkan lemahnya perumusan kebijakan hukum yang responsif terhadap perkembangan teknologi.

Sistem hukum Iran menunjukkan pendekatan yang relatif lebih terintegrasi dalam menghadapi ancaman cyber warfare. Meskipun tidak secara eksplisit mencantumkan istilah cyber warfare dalam peraturan perundang-undangannya, Iran telah mengonstruksikan ancaman siber sebagai bagian dari kejahatan terhadap keamanan negara serta mengintegrasikannya dalam kebijakan pertahanan nasional. Pendekatan ini diperkuat oleh pengalaman empiris Iran sebagai target serangan siber, yang mendorong penguatan regulasi dan kelembagaan di bidang keamanan siber. Melalui analisis komparatif yang dilakukan, dapat disimpulkan bahwa perbedaan mendasar antara Indonesia dan Iran terletak pada paradigma dalam memandang ancaman siber. Indonesia cenderung menggunakan pendekatan yang bersifat reaktif dan berorientasi pada penegakan hukum terhadap pelaku kejahatan individual, sedangkan Iran menerapkan pendekatan yang lebih strategis dengan mengintegrasikan aspek hukum, kebijakan, serta pertahanan negara. Perbedaan tersebut menunjukkan perlunya reformulasi hukum pidana di Indonesia agar lebih komprehensif, adaptif, dan responsif terhadap perkembangan cyber warfare. Penelitian ini menegaskan pentingnya penguatan sistem hukum pidana di Indonesia melalui pengakuan terhadap cyber warfare sebagai ancaman strategis terhadap keamanan nasional, pengembangan konsep hukum yang lebih sistematis, serta harmonisasi dengan perkembangan hukum internasional. Tanpa adanya pembaruan tersebut, sistem hukum pidana Indonesia berpotensi mengalami kesulitan dalam menghadapi dinamika ancaman siber yang semakin kompleks di era digital.

SARAN

1) Diperlukan reformulasi hukum pidana nasional dengan mengakomodasi cyber warfare sebagai kategori tersendiri dalam sistem hukum Indonesia. Pengaturan yang saat ini masih bertumpu pada Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik sebagaimana telah diubah dengan Undang-Undang Nomor 19 Tahun 2016, serta Kitab Undang-Undang Hukum Pidana, perlu dikembangkan agar mampu menjangkau ancaman siber yang bersifat strategis, terorganisir, dan berpotensi melibatkan aktor negara. Reformulasi ini penting untuk menutup kekosongan norma yang selama ini menjadi salah satu kelemahan dalam pengaturan hukum pidana nasional.
2) Diperlukan penguatan konsep hukum yang jelas dalam membedakan antara cybercrime dan cyber warfare. Ketidakjelasan batasan konseptual antara kedua istilah tersebut dapat menyulitkan aparat penegak hukum dalam menentukan kualifikasi perbuatan dan bentuk pertanggungjawaban hukum yang tepat. Oleh karena itu, pengembangan kajian akademik dan doktrinal perlu ditingkatkan sebagai landasan dalam merumuskan kebijakan hukum yang lebih adaptif terhadap perkembangan teknologi. Dalam hal ini, pengalaman negara lain yang telah mengintegrasikan isu keamanan siber ke dalam kebijakan nasional dapat dijadikan sebagai bahan perbandingan dalam proses pembaruan hukum nasional.
3) Penguatan kelembagaan serta peningkatan kapasitas sumber daya manusia di bidang keamanan siber menjadi aspek yang sangat penting. Penanganan cyber warfare membutuhkan keahlian teknis yang tinggi serta koordinasi yang efektif antar lembaga. Oleh karena itu, diperlukan sinergi antara aparat penegak hukum, lembaga pertahanan, dan institusi terkait lainnya dalam membangun sistem keamanan siber nasional yang terintegrasi dan responsif terhadap berbagai bentuk ancaman digital.
4) Peningkatan kerja sama internasional perlu menjadi prioritas dalam menghadapi cyber warfare yang bersifat lintas batas negara. Mengingat karakteristik ancaman siber yang tidak mengenal batas wilayah, penanganannya tidak dapat dilakukan secara sepihak oleh suatu negara. Kerja sama internasional, baik melalui perjanjian bilateral maupun multilateral, diperlukan untuk memperkuat mekanisme pencegahan, penanggulangan, serta penegakan hukum terhadap serangan siber. Selain itu, harmonisasi dengan prinsip-prinsip hukum internasional juga penting agar kebijakan nasional selaras dengan perkembangan regulasi global.

Diperlukan penguatan pendekatan preventif dalam sistem hukum pidana Indonesia. Pembentukan regulasi yang komprehensif harus diimbangi dengan langkah-langkah pencegahan, seperti peningkatan kesadaran masyarakat terhadap keamanan digital, perlindungan terhadap infrastruktur kritis nasional, serta penguatan sistem keamanan teknologi informasi secara berkelanjutan. Dengan demikian, hukum pidana tidak hanya berfungsi sebagai instrumen represif, tetapi juga sebagai sarana strategis dalam menjaga stabilitas dan keamanan nasional di era digital.

DAFTAR PUSTAKA

Arief, Barda Nawawi. (2016). *Bunga rampai kebijakan hukum pidana*. Jakarta: Kencana.

Center for Strategic and International Studies. (2018). *Iran's cyber threat: Espionage, sabotage, and attack*. Washington D.C.: CSIS.

Clarke, Richard A. (2010). *Cyber war: The next threat to national security and what to do about it*. New York: HarperCollins.

Computer Crimes Law 2009 (Republik Islam Iran).

Farwell, James P., & Rohozinski, Rafal. (2011). Stuxnet and the future of cyber war. *Survival*, 53(1), 23–40. https://doi.org/10.1080/00396338.2011.555586

Hathaway, Oona A., Crootof, Rebecca., Levitz, Philip., Nix, Haley., Nowlan, Aileen., Perdue, William., & Spiegel, Julia. (2012). The law of cyber-attack. *California Law Review*, 100(4), 817–885.

Kaspersky Lab. (2010). *The Stuxnet worm: A cyber missile targeting Iran's nuclear program*. Diambil dari https://www.kaspersky.com

Kitab Undang-Undang Hukum Pidana (KUHP).

Libicki, Martin C. (2009). *Cyber deterrence and cyberwar*. Santa Monica: RAND Corporation.

Lindsay, Jon R. (2013). Stuxnet and the limits of cyber warfare. *Security Studies*, 22(3), 365–404. https://doi.org/10.1080/09636412.2013.816122

North Atlantic Treaty Organization Cooperative Cyber Defence Centre of Excellence. (2013). *Tallinn manual on the international law applicable to cyber warfare*. Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9781139169288

Schmitt, Michael N. (2012). Cyber operations and the jus ad bellum revisited. *Villanova Law Review*, 56(3), 569–606.

Schmitt, Michael N. (Ed.). (2013). *Tallinn Manual on the International Law Applicable to Cyber Warfare*. Cambridge: Cambridge University Press.

Singer, P. W., & Friedman, Allan. (2014). *Cybersecurity and cyberwar: What everyone needs to know*. Oxford: Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199918096.001.0001

Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.

Undang-Undang Nomor 19 Tahun 2016 tentang Perubahan atas Undang-Undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik.