BAB II

LINIMASA PERKEMBANGAN *CYBER WARFARE* AS-IRAN PASCA 9/11 HINGGA SAAT INI

Proses perjalanan hubungan AS dan Iran dari masa ke masa menunjukkan dinamika yang fluktuatif. Bahkan, kedua negara mengakui serangan dunia maya merupakan inti dari strategi mereka dan sedang dalam tahap membangun kemampuan *cyberspace warfare programs*, diikuti oleh Korea Utara, Inggris, Cina, dan Rusia (Chen, 2010; Gill & Bryant, 2017; Goel, 2011; Spector, 2022). Beberapa pernyataan sebagaimana dituturkan oleh petinggi negara Iran, seperti *"Cyberspace can be an opportunity for us, and we must turn cyber threats into opportunities. And use its opportunities for the benefit of Islam, the revolution and the country.* Ahmad Jannati*"*; *"If we want to compete with other countries in the economy, we have no choice but to develop cyberspace.* Hassan Rouhani*";* dan Direktur DHS's *Cybersecurity and Infrastructure Security Agency* (CISA) AS *"Our critical infrastructure is integrated into a larger global cyber ecosystem, which means that we all need to be resilient or shields up, but certainly be prepared.* Jan Easterly*"* semakin memperkuat spekulasi adanya persaingan di dunia maya yang dilakukan secara terselubung (Eslami & Danesh, 2023). Untuk memahami lebih lanjut, penulis mengupas sejarah serta linimasa perkembangan *cyber warfare* AS-Iran beserta ancaman dan tantangannya pada rangkaian sub-bab berikut:

2.1. Perspektif Historis *Cyber Warfare*

Belum lama berselang, narasi terkait perang dunia maya atau lekat dikenal dengan istilah *"Cyber Warfare"* selalu dihantui oleh pertanyaan-pertanyaan yang menakutkan: Bagaimana jika peretas yang disponsori oleh negara meluncurkan serangan skala penuh yang mampu melumpuhkan seluruh kota? Layanan perbankan ditutup dan ATM dibekukan di seluruh negeri? Haruskah industri perkapalan, kilang minyak, dan pabrik ditutup? Bandar udara dan rumah sakit tidak dapat beroperasi? Pada faktanya, skenario ini tidak lagi spekulatif. Masing-masing dari peristiwa tersebut kini telah terjadi.

Selama berabad-abad, wilayah tempur manusia hanya terbatas pada daratan dan lautan. Manusia menaklukkan daratan dengan relatif mudah, sedangkan lautan hanya dapat diakses melalui bantuan teknologi−kapal layar, kapal uap, dan kapal selam. Kemudian seiring berjalannya waktu *domain* fisik ketiga ditambahkan, yakni: ruang udara. Wilayah ini pun memiliki keterbatasan karena manusia hanya dapat terbang dalam batas tertentu. Pada tahun 1957, wilayah fisik ruang angkasa turut dimasukkan ke dalam daftar. Meskipun masing-masing *domain* fisik diatas memiliki karakteristik, namun ada satu hal yang menarik; dari keempat wilayah fisik tersebut tidak bisa lepas dari penggunaan teknologi untuk mengeksploitasinya.

Sebagaimana kita ketahui bersama, ilmu pengetahuan dan teknologi berkembang pesat selama seratus tahun terakhir. Hal ini tercermin dari bukti bahwa negara dengan kapasitas teknologi yang mumpuni selalu keluar sebagai pemenang (Relia, 2016)**.** *Cyberwarfare* telah dimanfaatkan untuk meneror perusahaan dan

mengganggu seluruh sistem pemerintahan sementara. Dilansir melalui media edukasi *Wired*, satu serangan siber mampu mengakibatkan kerusakan ekonomi hingga mencapai total kerugian $10 miliar (Greenberg, 2019). Karena adanya dependensi yang tinggi terhadap sains dan teknologi, keberadaan dunia maya sebagai *domain* perang kelima menjadikan perang dapat dilakukan melalui media virtual tanpa kehadiran negara yang benar-benar berperang.

Perang sejatinya menjadi bagian tak terpisahkan dari evolusi kehidupan yang panjang. Catatan sejarah menunjukkan bahwa negara-negara pernah terlibat dalam konflik bersenjata sejak zaman prasejarah dan mungkin terus berlanjut di masa depan. Satu-satunya hal yang berubah dan berkembang adalah cara berperang. Konflik dahsyat yang melenyapkan dinasti dan menyebabkan *holocaust* kini menjadi bagian dari sejarah. Dari *"The Age of Tools"* zaman prasejarah hingga 1500 M, suku pemburu-pengumpul menyusun strategi yang menguntungkan serta bertarung dengan kekuatan otot manusia dan hewan. *"The Age of Machine"* merupakan zaman para unit militer besar pada abad ke-18 dan ke-19 menggunakan senjata artileri, berikutnya *"The Age of Systems"* dikembangkan antara Perang Dunia I dan Perang Dunia II dengan mengaplikasikan radar, pesawat jarak jauh, dan serangan darat ke udara yang terkoordinasi radio pemancar. Tepat hingga saat ini kita hidup di abad ke-21, juga dikenal sebagai *"The Age of Automation"* yaitu era kebangkitan kecerdasan buatan (AI) yang memanfaatkan analisis algoritma *machine learning* dan kemampuan sensor untuk mengenali pola dan masalah yang bahkan tidak dapat dilihat oleh manusia (C. C. and K. Geers, 2009).

Nampaknya, transisi fase teknologi informasi telah meningkatkan ketergantungan pada perangkat canggih dan aplikasi digital. Mengubah peperangan yang semula bersifat konvensional bergeser ke dalam bentuk medan perang baru.

2.2. Pengertian Umum *Cyber Warfare*

Untuk memahami ancaman unik yang ditimbulkan oleh perang siber terhadap peradaban, pertama-tama perlu dipahami bagaimana *'Cyber Warfare'* itu sendiri didefinisikan. Tidak ada penjelasan pasti mengenai istilah ini secara universal. *'Rise of the Machines'* yang dikisahkan oleh Thomas Rid melukiskan gambaran perang di masa depan: gagasan tentang perang maya *Terminator* bergaya robotik yang kemudian diganti pada tahun 1990-an dengan gagasan yang lebih berfokus pada komputer dan internet. Sebuah artikel tahun 1993 berjudul *"Cyberwar Is Coming!"* menjelaskan bagaimana *military hackers* dimanfaatkan tidak hanya untuk mengintai dan memata-matai sistem musuh, tetapi juga untuk menyerang komputer musuh melalui perintah dan kontrol (Arquilla & Ronfeldt, 1993).

Namun, beberapa tahun kemudian, *military hackers* tidak serta merta hanya menargetkan komputer musuh. Mereka dengan mudah menyerang bagian terkomputerisasi otomatis dari infrastruktur penting, menciptakan kekacauan, atau menggunakan ruang siber sebagai *platform* propaganda yang dimaksudkan untuk melemahkan kekuatan musuh dengan konsekuensi membawa bencana bagi warga sipil. Adapun merusak begitu banyak sistem vital seperti: rumah sakit, maskapai

penerbangan, bank sentral, bahkan jaringan listrik. Peretasan tidak terbatas pada taktik semata, *cyberattack* bisa menjadi senjata perang. Sebagaimana Bill Clinton mendefinisikan *"Cyber Warfare"* pada tahun 2000 (CNN Transcripts, 2000),

> *"Today, our critical systems, from power structures to air traffic control, are connected and run by computers. And that someone can sit at the same computer, hack into a computer system, and potentially paralyze a company, a city, or a government."*

Sejak itu, definisi *"Cyber Warfare"* dibuat dalam buku *Cyber War* 2010 yang ditulis oleh penasihat keamaan nasional AS, Richard Clarke, mengartikan *Cyber Warfare* sebagai "tindakan oleh *nation-state* untuk menembus komputer atau pertahanan jaringan negara lain dengan maksud untuk menyebabkan kerusakan dan kekacauan". Merujuk dari makna tersebut, menekankan bahwa perang dunia maya sama halnya dengan *"acts of war"* hanya saja diwujudkan dalam bentuk digital.

Di sisi lain, pengertian mengenai *"Cyber Warfare"* menurut Shakarian dkk., (2013) "Perang siber adalah perpanjangan dari kebijakan aktor negara atau non-negara di dunia maya, baik itu merupakan ancaman serius terhadap keamanan suatu negara maupun bentuk respon atas ancaman yang dirasakan bagi keamanan bangsa."

Lain halnya menurut Bernik (2014), dalam bukunya yang berjudul *Cybercrime and Cyberwarfare* melihat perang siber tidak hanya sebagai kegiatan yang bertujuan untuk mencapai dominasi kekuasaan atau supremasi yang dapat memengaruhi sistem informasi, komputer, dan jaringan lawan, melainkan juga

sebagai alat keamanan dan perlindungan dari infrastruktur teknologi informasi mereka sendiri.

> *"It is basically an offensive and defensive operation of (private and public) institutions or groups to obtain and/or use information with the assistance of ICT in order to achieve superiority in the battle with the competition."*

Singkatnya, *Cyberwarfare* adalah konflik berbasis internet yang melibatkan serangan siber bermotif politik dengan berbekal kemampuan informasi sebagai *power* dan mengubahnya menjadi instrumen *national power.*

Cyber warfare, sebagaimana diuraikan dalam *Tallinn Manual,* merupakan aspek penting dalam lanskap konflik internasional terkait operasi siber dan membutuhkan pertimbangan hukum internasional yang cermat. *Manual* ini disusun oleh pakar teknologi informasi dan hukum Eropa di bawah Pusat Keunggulan Pertahanan Siber Kooperatif NATO, sebagai tanggapan atas serangan siber di Estonia pada tahun 2008 dan telah disetujui serta diberlakukan oleh PBB untuk mengatasi kekosongan hukum terkait perang siber. *Tallin Manual*, yang diterbitkan pada tahun 2013 dan diperbarui pada tahun 2017 memberikan analisis komprehensif tentang bagaimana hukum internasional diterapkan pada perang siber. Buku ini mencakup sembilan puluh lima *"black-letter rules"* yang mengatur pelaksanaan operasi siber dan perang siber, memastikan bahwa kegiatan ini dilakukan sesuai dengan prinsip-prinsip hukum humaniter internasional dan hukum perang (Schmitt, 2017).

Rule 30 dari *manual* ini mengadopsi definisi dari *Additional Protocol* I pada Konvensi Jenewa, yang menyatakan bahwa serangan siber dalam konteks perang siber dapat melibatkan organisasi, perusahaan, dan militer dalam upaya merusak atau menyerang sistem komputer pihak lain. Selain itu, *Rule* 41 mendefinisikan *'means of cyber warfare'* sebagai senjata siber dan sistem terkait serta *'methods of cyber warfare*' sebagai taktik, teknik, dan prosedur siber yang digunakan dalam permusuhan. Dalam hukum humaniter internasional, pelaku perang siber dapat termasuk kombatan, non-kombatan, dan sipil yang terlibat langsung dalam konflik, dengan aturan partisipasi diatur dalam Pasal 43(2) dari Protokol Tambahan I yang memberikan hak kepada anggota angkatan bersenjata untuk berpartisipasi langsung dalam permusuhan. *Tallinn Manual* mengidentifikasi bahwa serangan siber dapat dilakukan oleh negara atau aktor non-negara, dan dapat mencakup berbagai metode seperti *hacking, phishing, distributed denial of service* (DDoS), serta penggunaan *honeypots* dan *watering holes* (Suharto, M. A., 2021).

Dalam buku panduan *Tallin* menekankan pentingnya mematuhi prinsip-prinsip perbedaan, proporsionalitas, dan pencegahan dalam pelaksanaan permusuhan. Panduan ini juga menyoroti kebutuhan untuk melindungi sipil dan objek sipil dari dampak serangan siber. Panduan ini tidak dimaksudkan untuk membahas masalah yang berkaitan dengan operasi kinetik ke siber, seperti pemboman udara terhadap pusat kontrol siber, yang diatur oleh hukum perang yang ada. Sebaliknya, fokusnya adalah pada operasi siber ke siber, seperti serangan pada infrastruktur kritis atau sistem kontrol dari pihak lawan (Vihul, 2013).

Dalam analisis hukum konflik bersenjata, tantangan utama bagi para ahli adalah mendefinisikan serangan siber sesuai dengan Pasal 49(1) Protokol Tambahan I, serta masalah terkait mengenai kelayakan melakukan operasi siber yang tidak melukai warga sipil atau merusak properti sipil. Dalam *Tallinn Manual,* serangan termasuk operasi yang menyebabkan cedera atau kematian pada orang atau merusak atau menghancurkan objek (Aturan 30); setiap serangan yang ditujukan terhadap warga sipil atau objek sipil dengan konsekuensi tersebut adalah melanggar hukum (Aturan 31-32).

Beberapa ahli memperluas konsep "serangan siber" pada *cyber warfare* yang menyebabkan hilangnya fungsi sehingga memerlukan perbaikan sistem. Isu atribusi operasi siber ke negara juga menjadi masalah mendesak. Isu ini muncul baik dalam konteks pertanggungjawaban negara atas tindakan yang salah secara internasional, hak negara korban untuk menggunakan kekuatan dalam pembelaan diri di bawah *jus ad bellum,* maupun untuk menetapkan adanya konflik bersenjata dalam konteks *jus in bello*. Langkah awal dalam menentukan siapa yang bertanggung jawab atas serangan siber biasanya dimulai dengan melacak jejak digital. Namun, hukum tidak mengharuskan atribusi didasarkan hanya pada data teknis. Sebaliknya, negara korban harus menggunakan standar yang masuk akal dengan mempertimbangkan semua bukti yang ada, seperti data teknis, konteks politik, dan catatan serangan siber sebelumnya, untuk mencapai kesimpulan yang wajar tentang siapa yang bertanggung jawab, mirip dengan bagaimana negara lain akan bertindak dalam situasi yang sama (Schmitt, 2017).

Tallin Manual telah banyak dikutip dan diakui sebagai referensi penting tidak hanya bagi negara dan organisasi, melainkan juga penasihat hukum negara, pembuat kebijakan, serta perencana operasional dalam merumuskan pendekatan mereka terhadap perang siber. Panduan ini menyediakan kerangka kerja untuk memahami implikasi hukum dari operasi siber dan membantu menetapkan pemahaman umum tentang aturan yang mengatur kegiatan-kegiatan ini. Pembaruan dalam panduan mencerminkan sifat perang siber yang terus berkembang dan kebutuhan akan dialog dan kerja sama berkelanjutan di antara negara-negara untuk memastikan bahwa hukum internasional tetap relevan dan efektif dalam mengatasi tantangan yang ditimbulkan oleh konflik-konflik ini.

2.2.1. Definisi *Global Cyber* sebagai *"Non-Traditional Threats"*

Buntut berkembangnya konflik dan perang, turut memperluas laga peperangan dari darat, laut, udara, hingga ke luar angkasa. Sekarang, pertempuran terjadi di arena baru: ruang siber. Kini jarang dijumpai *nation-state* yang secara terang-terangan mengerahkan persenjataan militernya dan memobilisasi angkatan bersenjatanya untuk menganeksasi wilayah negara lain (Vihul, 2013). Namun sayangnya, ini bukan berarti dunia lebih aman dan bebas konflik. Sebenarnya yang terjadi adalah pergeseran dari model konflik tradisional ke model konflik 'non-tradisional' (Rugge, 2018).

Laju perkembangan teknologi semakin pesat seiring dengan pengadopsian *gadget* serta layanan teknologi terkini. Konsep yang diterapkan

dalam dunia teknologi serupa dengan *Moore's Law.* Awalnya, Hukum *Moore* berbicara tentang penggandaan jumlah transistor pada sebuah *chip.* Namun, pada konteks teknologi yang lebih luas, hal ini ditafsirkan sebagai inovasi yang mengarah pada peningkatan kecepatan secara eksponensial—segala sesuatunya bergerak lebih cepat dan canggih dengan adanya inovasi baru. Hadirnya serangkaian potensi ancaman yang terus berubah menghadapkan para profesional keamanan nasional untuk mampu beradaptasi dengan tantangan modern. Teknologi seperti *drone,* 3D *printing*, rekayasa sosial, biometrik, dan kecerdasan buatan (AI) telah mengubah persepsi medan perang dan ruang keamanan (Munirathinam, 2020a).

Konsumsi konsumen yang terus meningkat turut membawa dampak risiko ancaman di bidang keamanan siber. Maka, dibutuhkan aparat keamanan dan pertahanan nasional yang adaptif untuk mengenali dan merespon teknologi baru yang muncul. Dalam pembahasan sub-bab ini, peneliti akan menggali beberapa metode baru yang termanifestasi saat ini dengan melihat secara lebih dekat bagaimana realitas kecerdasan buatan (AI) dapat disalahgunakan untuk tujuan destruktif (Cunningham, 2020; Lin, 2012, hal. 37; Valeriano & Maness, 2015, hal. 25).

Persaingan kekuatan besar dengan cepat mengubah lanskap geostrategis. Pemberlakuan sanksi dan penyebaran pengaruh dalam interaksi antarnegara membuat perang berevolusi menjadi bentuk yang lebih halus, tersembunyi, tiada akhir, tidak dideklarasikan, dan yang utama tanpa batasan

(Sciarrone, 2017). Keadaan ini semakin mengaburkan sekat antara perang dan damai.

Sebelum dibahas lebih lanjut, penting mengenali evolusi persenjataan yang digunakan dalam perang untuk memahami bagaimana peperangan berubah dari waktu ke waktu. Dahulu pada masa perang revolusi dan perang dunia pertama, alat perang akrab dengan penggunaan senapan, tombak, bom, pesawat terbang, tank, kapal, dan lain-lain. Pada Perang Dunia II, kapal dan pesawat terbang dibatasi untuk menembakkan torpedo atau senjata berat dengan jarak tempuh kurang dari 30 mil. Mulai tahun 1960-an, beberapa kapal selam dilengkapi dengan rudal balistik jarak antarbenua. Rudal jelajah yang akurat dimulai pada tahun 1970-an. Lebih dari 75.000 rudal dimiliki oleh 70 negara yang memungkinkan kapal selam dan kapal tempur dapat mencapai target darat yang berjarak ratusan mil dengan persenjataan konvensional (Boot, 2006). Tahun 1980-an menjadi tonggak pesawat masa depan F-117 *Nighthawk,* B-2 *Spirit,* F/A-22, dan F-35 yang dirancang dengan teknologi *"visual stealth"* atau disebut pesawat siluman karena kemampuannya tidak dapat terlihat bahkan di siang hari. Namun seiring berjalannya waktu, jaringan sensor canggih mampu mendeteksi keberadaan pesawat siluman generasi pertama. Serbia berhasil menembak jatuh F-117 pada tahun 1999 dan memakan banyak korban jiwa, sehingga menciptakan ancaman jika mengandalkan pesawat berawak pada misi berisiko tinggi (Boot, 2007; Kaldor, 2012).

Dengan demikian, selama 200 tahun terakhir mulai berkembang alat-alat yang lebih baru, seperti alat peledak improvisasi (IEDs), perang siber, dan kendaraan udara tak berawak (UAVs). Pengembangan senjata nuklir pada

pertengahan abad ke-20 menandai pergeseran penting dalam karakter perang, mendatangkan potensi kehancuran massal dan bencana global (Galeotti, 2022). Kegiatan pengawasan, komunikasi, dan intelijen semakin banyak mengandalkan teknologi internet yang ekspansif dan penggunaan satelit. Kemampuan siber, sistem otonom, dan penyebaran munisi yang dipandu dengan presisi telah mengubah wajah perang. Dengan kemajuan ini, tidak hanya serangan yang lebih terarah dan efektif dapat dilakukan, tetapi juga memungkinkan pihak non-negara untuk terlibat dalam operasi militer yang kompleks. Selain itu, dengan adanya integrasi pembelajaran mesin (ML) dan kecerdasan buatan (AI) dalam sistem militer akan memiliki dampak yang signifikan pada masa depan perang karena memungkinkan pengambilan keputusan yang lebih cepat dan fleksibel (Cunningham, 2020a; Spector, 2022).

2.2.2. *Trend* Perang Dunia Maya Saat Ini

Menurut *the United States Government Accountability Office* (GAO) pada tahun 2020 (GAO, 2020) perkembangan ancaman berbasis dunia maya yang dihadapi negara mencakup ancaman terhadap keamanan nasional, perdagangan dan kekayaan intelektual, dan individu. Sumber ancaman permusuhan terhadap keamanan dunia maya meliputi:

Tabel 2.2.2. Sumber Ancaman *'Adversarial Threats'* terhadap Keamanan Siber

	Sumber Ancaman	Deskripsi
1.	*Bot-net Operators*	Operator jaringan *bot* menggunakan jaringan sistem yang dikendalikan dari jarak jauh yang dikompromikan untuk mengoordinasikan serangan dan untuk mendistribusikan skema *phishing,* spam, dan serangan *malware*. Misalnya: membeli serangan atau layanan penolakan layanan.
2.	*Criminal Groups*	Kelompok kriminal berupaya menyerang sistem untuk keuntungan moneter, biasanya menggunakan *spam, phishing,* dan *spyware/ malware* untuk melakukan pencurian identitas, penipuan online, dan pemerasan komputer. Ini termasuk spionase industri, dan pencurian moneter skala besar atau untuk menyewa atau mengembangkan bakat peretas.
3.	*Hackers*	Peretas membobol jaringan untuk tantangan, balas dendam, penguntitan, keuntungan moneter, aktivisme politik, dan dapat mengunduh skrip dan protokol serangan dari internet dan meluncurkannya terhadap korbannya. CIA menyatakan bahwa

		mayoritas peretas tidak memiliki kemampuan untuk mengancam jaringan kritis AS, namun dalam skala besar, mereka menimbulkan kerusakan yang relatif tinggi.
4.	*Insiders*	Ancaman orang dalam mencakup kontraktor yang dipekerjakan oleh organisasi, serta karyawan yang ceroboh atau kurang terlatih yang mungkin secara tidak sengaja memasukkan malware ke dalam sistem.
5.	*Nation-States*	Bangsa-bangsa bekerja untuk mengembangkan doktrin, program, dan kemampuan peperangan informasi sebagai alat sibernya untuk kegiatan pengumpulan informasi dan spionase. Kemampuan tersebut antara lain terganggunya suplai, komunikasi, dan infrastruktur ekonomi yang mendukung kekuatan militer.
6.	*Phishers*	Individu atau kelompok kecil menjalankan skema phishing dalam upaya mencuri identitas atau informasi untuk keuntungan moneter. Phisher dapat menggunakan *spam* dan *spyware* untuk mencapai tujuan mereka.

7.	*Spammers*	Individu atau organisasi mendistribusikan *email* yang tidak diminta dengan informasi tersembunyi atau palsu untuk menjual produk, melakukan skema phishing, mendistribusikan *spyware* atau *malware,* atau menyerang organisasi.
8.	*Spyware/malware authors*	Individu atau organisasi yang memproduksi dan mendistribusikan *spyware* dan *malware*. Beberapa virus dan *worm* perusak juga telah merusak *hard drive* dan menyebabkan kerusakan fisik pada *critical infrastructures* (CI).
9.	*Terrorists*	Teroris bertujuan untuk menghancurkan atau mengeksploitasi infrastruktur kritis untuk mengancam keamanan nasional, menimbulkan korban jiwa massal, melemahkan ekonomi, dan merusak moral masyarakat.

Sumber: data dikelola oleh peneliti dari berbagai sumber

Jenis serangan yang paling umum dilakukan terhadap *nation-state*, berdasarkan sudut pandang peneliti, adalah melalui spionase dunia maya, baik dengan serangan *Distributed Denial of Service* (DDoS) atau melalui *malware*. *Cyber espionage* adalah praktik memperoleh informasi rahasia *nation-state* atau lembaga, secara khusus menargetkan mereka untuk tujuan

jahat. Serangan DDoS terutama digunakan untuk mengganggu sistem komunikasi negara-bangsa dan jaringan listrik secara bersamaan. Alat serangan dunia maya ini biasanya digunakan untuk membuat layanan online suatu negara-bangsa tidak tersedia dengan membanjirinya dengan lalu lintas yang memiliki permintaan berbeda dari berbagai sumber, yang menyebabkan layanan macet (Digital Attack Map, 2020). Jenis serangan ini terutama menargetkan bank, situs web berita, dan layanan pemerintah, untuk mencegah orang menerbitkan dan mengakses informasi penting. *Malwares*, singkatan dari *'malicious software'*, adalah program perangkat lunak yang merupakan alat populer untuk mengganggu operasi komputer normal. *Malwares* termasuk *virus*, *worm*, *trojan horse*, serta *spywares* (Christensson, 2006).

2.3. Dinamika Hubungan AS-Iran Pasca 9/11

Jika ditarik garis mundur, perjalanan hubungan penuh gejolak antara Amerika Serikat dan Iran dilihat dari sisi historis memang kerap memancing perhatian dunia. Relasi keduanya pada tahun 1985 bahkan sempat terjalin mesra. Secara rahasia Amerika Serikat mengirimkan senjata ke Iran sebagai imbalan atas jasa Teheran membebaskan para sandera yang ditahan oleh gerilyawan Hizbullah (BBC, 2020). Masa ini kemudian dikenal dengan istilah *Iran-Contra Scandal*. Lebih lanjut, memasuki tahun 2000-an tensi kembali memanas karena adanya spekulasi Iran sedang membangun fasilitas pengayaan uranium dan George W. Bush memunculkan istilah *'axis of evil'* bersanding dengan Irak dan Korea Utara

yang diduga tengah mengembangkan *Weapon of Mass Destruction*. 11 September 2001, merupakan kejadian paling memukul Amerika Serikat setelah aksi serangan terorisme menewaskan total 2.996 korban jiwa dan meruntuhkan dua menara kembar, yakni gedung *World Trade Center* dan *Pentagon* (History, 2019). *War on Terrorism* adalah bentuk respon Amerika Serikat pasca serangan 9/11 yang mulai menitikberatkan kebijakan luar negeri dan mendorong masyarakat internasional untuk memerangi segala tindakan terorisme (Chossudovsky, 2005).

Sejatinya, apabila kita telah bersusah payah membangun usaha bertahun-tahun dan tiba-tiba ada yang mengusik ketenangan itu, tentu dapat menyulut emosi dan sudah merupakan sifat alami manusia memunculkan reaksi untuk melakukan pembalasan. Senada dengan Iran, pasca mengalami serangan dan berbagai sanksi yang dijatuhkan oleh Amerika Serikat lantas tidak membuat Iran berdiam diri begitu saja. Dengan cepat Iran meningkatkan kemampuan sibernya menggunakan strategi dan organisasi sebagai instrumen *national power* (Center for Strategic & International Studies, 2019). Tercatat pada tahun 2009, cikal bakal kemampuan siber Iran berasal dari upaya *hacktivism* untuk memperluas pengawasan dan kontrol domestik. Kelompok pasukan atas nama *'Iranian Cyber Army'* melakukan propaganda dengan menyebarkan pesan politik anti-Amerika melalui media sosial Twitter dan *search engine* Baidu di China sebagai respon terhadap *Green Movement*. Gerakan reformasi menggunakan simbol berwarna hijau ini merupakan protes pemilihan umum presiden Iran tahun 2009 atas kemenangan Mahmoud Ahmadinejad yang dinilai oleh oposisi Mir-Hossein Mousavi, terdapat rekayasa dan manipulasi pemungutan suara (Foreign Affairs, 2019). Akibatnya, Twitter tidak

dapat diakses selama lebih dari satu jam dan pengguna berulangkali diarahkan ke *link* Twitter yang bermuatan pesan politik. Bahkan, *Iranian Cyber Army* turut meretas media berita asing, seperti BBC dan *Voice of America* (VOA).

Aksi saling balas antara dua kubu Amerika Serikat dan Iran pasca peristiwa 9/11 nampaknya berbuntut panjang. Situasi ini semakin diperkeruh oleh Amerika Serikat setelah meluncurkan serangan virus Stuxnet tahun 2010 yang menargetkan fasilitas nuklir Iran, sehingga memicu adanya retaliasi *tit for tat* (Cunningham, 2020). Dalam *Game Theory,* strategi *tit for tat* digunakan untuk menggambarkan relasi timbal balik antara kedua belah pihak berdasarkan pada hubungan sebab-akibat (kausalitas) (Springer, 2015). Apabila salah satu pihak melakukan pengkhianatan, kecurangan, dan melanggar perjanjian atau kesepakatan kerjasama, maka pihak yang lain akan melakukan hal serupa. Sederhananya, *tit for tat* dimaknai sebagai suatu tindakan pembalasan, di mana kebaikan akan dibalas dengan kebaikan dan sebaliknya kejahatan akan dibalas dengan kejahatan. Hal ini dapat tercermin dari perjalanan hubungan antara kedua negara. Ketika Amerika Serikat bersikap kooperatif, maka Iran akan melunak dan menerima tawaran untuk bekerjasama. Sebaliknya, ketika Amerika Serikat 'mencederai' Iran, maka Iran akan membalas dengan perbuatan yang setimpal.

Selanjutnya, peristiwa *cyber warfare* paling *sophisticated* yang tak kalah menggemparkan dunia adalah infeksi virus Stuxnet di Iran pada bulan Juli 2010. Serangan siber ini tergolong unik dan tidak dapat diprediksi sebelumnya, dikarenakan virus Stuxnet menyerang secara *offline* sistem operasi Microsoft Windows dan piranti lunak Siemens *Step* 7 melalui *Zero-Day Exploit* dan *USB flash*

drive yang telah terinfeksi. Disamping itu, Stuxnet tidak melakukan peretasan atau pencurian informasi, melainkan merusak secara fisik sistem industri (*Industrial Control Systems*/ICS) yang dikendalikan oleh komputer dengan cara sabotase (Forbes, 2010; McAfee, 2020). Dengan kata lain, Stuxnet dirancang untuk menargetkan infrastruktur dunia nyata seperti pembangkit tenaga listrik, pembangkit tenaga air, dan unit industri. Badan intelijen Amerika Serikat (*U.S. National Security Agency* dan *Central Intelligence Agency)* berkoalisi dengan Israel melakukan operasi gabungan yang didesain secara khusus menargetkan *Programmable Logic Controllers* (PLCs) untuk menyerang jaringan komputer program nuklir Iran menggunakan *worm* bernama Stuxnet, atau dikenal pula dengan sebutan *Operation Olympic Games* (Shakarian et al., 2013). Serangan ini dinilai sukses, bahkan teknisi nuklir Iran sekali pun dibuat kebingungan karena tidak mampu mengungkapkan penyebabnya. Infiltrasi Stuxnet berjalan sangat mulus dan tidak terdeteksi, semua indikator berada dalam mode normal namun menyebabkan efek destruktif secara diam-diam.

Badan pusat kajian siber New Jersey melaporkan, *malware* Stuxnet mampu memanipulasi kecepatan sentrifugal dan berhasil menghancurkan 1.000 sentrifugal pengayaan uranium Iran di Nathanz (NJCCIC, 2017; Rosenzweig, 2013; Stanford University & Holloway, 2015). Apabila dianalogikan, perang saat ini seperti *Pandora's Box* yang telah mengubah strategi militer global di abad ke-21. Hal ini diindikasikan dengan adanya intervensi Amerika Serikat yang memiliki dana besar (*state-sponsored attack*) untuk menyusup keamanan nasional Iran. Penulis pun

sependapat sebagaimana dikatakan dalam (Foreign Policy & Langner, 2013), bahwa *"nuclear proliferators come and go, but cyberwarfare is here to stay"*.

Terbukti pada tahun 2012, Iran melangsungkan *Operation Cleaver* yang menargetkan *critical infrastructures* Amerika Serikat, yakni: militer, sistem transportasi, rumah sakit, institusi perbankan, sektor energi dan sumber daya, sektor minyak dan gas, jaringan telekomunikasi dan teknologi, institusi pendidikan, perusahaan kimia, dan pemerintahan (Siboni & Kronenfeld, 2014). Tidak hanya itu, retaliasi lain seperti *Shamoon* dan *Operation Ababil* turut diluncurkan oleh Iran. *Hacker group* bernama *"Cutting Sword of Justice"* menggunakan virus Shamoon berjenis *Wiper* untuk menyerang perusahaan minyak Saudi Aramco. Serangan siber ini mampu menginfeksi 30.000 komputer yang bertujuan mengganggu aliran minyak Arab Saudi. Cara kerja virus Shamoon adalah menghapus data, berupa: dokumen, *spreadsheets, e-mail,* dan *files*, kemudian menggantinya dengan foto bendera Amerika Serikat yang terbakar.

Satu tahun berikutnya, Iran berafiliasi dengan *hacker group* bernama *Izz ad-Din Al-Qassam* meluncurkan serangan Operasi Ababil yang merupakan rangkaian dari serangan DDoS dan menargetkan beberapa institusi perbankan Amerika Serikat seperti *SunTrust*, *JPMorgan Chase*, *HSBC*, *Capital One*, dan *New York Stock Exchange* (Mazanec & Bradley, 2015; Slavin & Healey, 2013). Meskipun *Operation Cleaver* ditujukan untuk membalas serangan Amerika Serikat atas Stuxnet, namun dampak yang ditimbulkan akibat serangan ini berbeda. Jika Stuxnet lebih berfokus pada kerusakan fisik yang ditimbulkan dalam jangka pendek untuk memperlambat upaya pengayaan uranium Iran, sementara *Operation Cleaver* lebih

memikirkan efek jangka panjang dengan mencuri *intellectual property* atau data yang akan diperjualbelikan untuk memperoleh keuntungan ekonomi. Dari serangkaian serangan yang telah diluncurkan oleh Iran, nampaknya menjadi jelas bahwa Amerika Serikat khawatir akan kekuatan Iran belajar dari peristiwa Stuxnet yang mana semakin diperkuat oleh pernyataan Jenderal William Shelton selaku kepala *Air Force Space Command, "Iran is a force to be reckoned with, with the potential capabilities that they will develop over the years and the potential threat that will represent to the United States"* (Shalal-Esa, 2013).

Polemik ketegangan antara Amerika Serikat dan Iran semakin memuncak semenjak Presiden Trump menjabat pada Januari 2017, dan diikuti oleh serangkaian kebijakan baru terkait kepemilikan nuklir Iran. Pada tanggal 8 Mei 2018 secara unilateral Amerika Serikat resmi menarik diri dari kesepakatan nuklir atau *Joint Comprehensive Plan of Action* (JCPOA) yang telah dibangun pada tahun 2015 (Telegraph, 2018). JCPOA merupakan upaya negara-negara P5+1 (Amerika Serikat, Tiongkok, Inggris, Perancis, Rusia, dan Jerman) untuk mengendalikan program nuklir Iran dengan hasil negosiasi pencabutan dari berbagai macam sanksi ekonomi sebagai bentuk harapan mencapai dunia yang lebih aman. Namun adanya inkonsistensi dari persepsi masa pemerintahan Obama dan Trump, Washington kembali menerapkan sanksi penuh terhadap Iran. Trump menilai JCPOA hanya menguntungkan sepihak bagi Iran yang tetap ingin mempertahankan status hegemon regionalnya untuk memulihkan krisis ekonomi Iran dan diam-diam membangun pengayaan uraniumnya sebagai senjata pemusnah massal.

Kompleksnya hubungan Amerika Serikat dan Iran yang kerap mengalami pasang surut, membuat penulis merasa topik ini menarik untuk diteliti. Terlebih, di balik berbagai serangan saling berbalas antara Amerika Serikat dan Iran terdapat faktor-faktor yang tidak lepas dari adanya intrik politik. Eskalasi konflik kedua negara semakin meningkat setelah terbunuhnya petinggi militer pasukan Quds, Jenderal Qasem Soleimani (The Guardian, 2020). Serangan tersebut dikomando langsung atas perintah Presiden Trump menggunakan pesawat nirawak atau *drone* MQ-9 Reaper nyaris tak bersuara yang membawa misil Hellfire H9X. Dilansir dari Cambridge University Press, keberadaan Soleimani di Bandara Internasional Baghdad diamati oleh *drone* canggih yang memiliki sensor sensitif terhadap waktu dan mampu menembakkan rudal tepat pada target sasaran (Cambridge University Press, 2020). Trump, dalam pidato di kediamannya Mar-A-Lago Florida menyatakan alasan pembunuhan terhadap Jenderal Soleimani dikarenakan ingin melindungi Amerika dan dunia dari teror yang mengguncang Timur Tengah selama 20 tahun terakhir yang termaktub sebagai berikut:

> *"Under my leadership, America's policy is unambiguous: to terrorists who harm or intend to harm any American, we will find you; we will eliminate you. We will always protect our diplomats, service members, all Americans, and our allies."*
>
> *"Soleimani has been perpetrating acts of terror to destabilize the Middle East for the last 20 years. What the United States did yesterday should have been done long ago. A lot of lives would have been saved"* (White House, 2020)

Soleimani disebut-sebut sebagai orang yang harus bertanggungjawab atas kematian warga sipil Amerika dan sedang merencanakan serangan terhadap diplomat serta personel militer Amerika. Maka tindakan itu harus segera dihentikan untuk mengakhiri perang.

> *"For years, the Islamic Revolutionary Guard Corps and its ruthless Quds Force – under Soleimani's leadership – has targeted, injured, and murdered hundreds of American civilians and servicemen. The recent attacks on U.S. targets in Iraq, including rocket strikes that killed an American and injured four American servicemen very badly, as well as a violent assault on our embassy in Baghdad, were carried out at the direction of Soleimani."*
>
> *"Soleimani was plotting imminent and sinister attacks on American diplomats and military personnel, but we caught him in the act and terminated him."*
>
> *"We took action last night to stop a war."*
>
> *"We did not take action to start a war"* (White House, 2020).

Akibatnya, pada 4 Januari 2020 *DHS's National Terrorism Advisory System* merilis buletin, yang menetapkan Iran sebagai *"State Sponsor of Terrorism"* sejak tahun 1984 karena secara aktif terlibat dalam serangkaian tindakan kekerasan dan mematikan yang mengancam *national security* Amerika Serikat. Lebih lanjut,

dalam peringatan tersebut Amerika Serikat menetapkan *Islamic Revolutionary Guard Corps (IRGC)* sebagai organisasi teroris pada 15 April 2019 karena keterlibatan langsungnya dalam perencanaan kegiatan terorisme (Department of Homeland Security, 2020). Pasca tewasnya Soleimani, dunia dibuat geger dengan ramainya tagar *#WorldWarThree* dan #HardRevenge di media sosial yang bermunculan. Bahkan, banyak pihak meramalkan perang berskala besar akan terjadi. Sebagaimana yang diketahui Iran sudah belasan tahun membangun pengaruhnya di beberapa negara Timur Tengah, seperti Lebanon, Yaman, Suriah, hingga Irak. Hal ini membuat khawatir dunia apabila Iran akan mengibarkan bendera perlawanan bersama dengan para sekutunya.

2.4. Ancaman *Cyber Warfare* dalam Ranah Politik Internasional

2.4.1. Kejahatan Siber oleh *State* maupun *Non-State Actors*

Dalam mendukung perencanaan strategis Iran, tiga organisasi militer memainkan peran utama di bidang *cyber* (Slavin & Healey, 2013): 1) *the Iranian Revolutionary Guard Corps* (IRGC) memiliki *Cyber Defense Command* yang bertugas untuk merekrut dan melatih ribuan orang untuk mengintai para pembangkang di internet serta menyebarkan *statement* politik pemerintah Iran (Fassihi, 2012). IRGC adalah pelaku di balik serangkaian insiden yang ditujukan untuk menyerang *critical infrastructures* Amerika Serikat, Israel, Arab Saudi, dan *Gulf States;* 2) *Basij*, merupakan sebuah organisasi paramiliter sipil yang dikendalikan oleh

IRGC. Memiliki 120.000 sukarelawan *cyberwar* sebagai penghubung antara universitas dan sekolah agama untuk merekrut *proxy hackers;* dan 3) *Iran's "Passive Defense Organisation"* (NPDO), dibentuk pada masa pemerintahan Ali Khamenei untuk memerangi ancaman berbasis internet serta bertanggungjawab pada perlindungan infrastruktur. Organisasi ini beranggotakan pejabat senior militer dan badan intelijen resmi yang tergabung dalam *"Supreme Council of Cyberspace*", untuk memastikan koordinasi antara *cyber offense* dan *cyber defense* dalam rangka mengurangi *national vulnerabilities* dan secara bersamaan meningkatkan stabilitas negara terhadap ancaman asing tanpa penggunaan kekuatan bersenjata.

Secara pertahanan *(cyber defense),* Iran berupaya untuk mewujudkan dua tujuan pokok: *Pertama,* Iran menciptakan *"technological envelope"* untuk melindungi infrastruktur kritis dan informasi sensitif negara sebagai respon balasan atas serangan virus Stuxnet. *Kedua,* Iran membentuk program yang memiliki jaringan komunikasi independen untuk menggagalkan aktivitas *cyberspace* oleh oposisi maupun mengatur kegiatan kelompok anti-rezim. Sementara secara penyerangan *(cyber offensive),* Iran menggunakan taktik *asymmetrical warfare* yang dipadukan dengan *cyberspace warfare*. Iran melihat, penggunaan strategi *cyberspace warfare* ternyata sama efektifnya dengan *asymmetrical warfare* seperti terorisme dan *guerilla warfare* karena memberikan efek *'damage'* pada lawan yang memiliki keunggulan militer dan teknologi (Siboni & Kronenfeld, 2012).

Dengan demikian, Iran selama ini cenderung melancarkan serangan sibernya ke Amerika Serikat yang menargetkan *critical infrastructures,* seperti institusi perbankan, rumah sakit, sistem transportasi, dan infrastruktur energi dan sumber daya.

2.4.2. Siber Ofensif Iran terhadap *Critical Infrastructures* AS

Serangan dunia maya menggunakan *cyber tools* dan *cyber weapon* yakni berupa *software* dan *hardware*. Identifikasi dari serangan siber tidak mudah untuk dideteksi, terutama dalam hal motif dan juga pelaku dari serangan siber. Saat ini, aktifitas yang terjadi di ruang maya menjadi perhatian dunia dikarenakan telah memasuki sendi-sendi tiap kehidupan. Ancaman siber memiliki potensi yang dapat membahayakan keamanan nasional dari suatu negara, dunia maya yang terjadi saat ini merupakan medan pertempuran di mana memungkinkan terjadinya transfer data secara langsung dan upaya penahanan.

Dengan adanya perkembangan di era globalisasi yang saat ini membuat dunia semakin terdigitalisasi, keberadaan *cyber warfare* memungkinkan serangan taktik dan strategi menggunakan remot dengan risiko minim dari penyerang. Sulitnya untuk melakukan pelacakan sumber dari serangan dan identifikasi penyerang, penggunaan biaya yang murah, dan celah kerentanan dalam sistem komputer menyebabkan *cyber warfare*

bersifat *asymmetric*. Secara ofensif, strategi dunia maya dalam taktik yang dilakukan oleh Iran adalah penggunan *the use of force*.

Iran banyak meluncurkan serangan kepada *critical infrastructures* milik Amerika Serikat dan sekutunya termasuk infrastruktur energi, keuangan, sistem transportasi. Dalam rangka merealisasikan tujuan dari strateginya, Iran mengalokasikan sekitar $1 miliar untuk membangun teknologi dan merekrut ahli yang terlatih. Iran memiliki jaringan pendidikan dan institusi penelitian yang berhubungan dengan IT. Kapabilitas dari *non-state actors*, seperti *The Revolutionary Guards* digadang-gadang menjadikan Iran sebagai salah satu negara yang mengikuti perkembangan dalam *cyber warfare* (Siboni & Kronenfeld, 2014).

2.4.3. *Cyber Insecurity* AS-Iran dalam Perang Siber

Bukan hal yang mengejutkan apabila kemampuan siber Iran perlahan menunjukkan kemajuan yang signifikan. Dalam akhir-akhir ini kampanye Iranian *Cyber Espionage* berhasil ditelusuri menggunakan rekayasa sosial atau *social engineering* dan *phishing* untuk mengumpulkan informasi data dari institusi penting negara-negara besar seperti Amerika Serikat, Israel, dan Inggris. Meskipun Iran tidak terindikasi menggunakan alat teknologi yang canggih, namun Iran menunjukkan adanya perkembangan dalam operasi kapabilitas Iran dalam pengumpulan

informasi rahasia *(intelligence sharing)* dan penggunaan operasi infrastruktur yang kompleks.

Teknologi siber yang inovatif telah membantu bisnis AS untuk mencapai efektivitas dan pelaksanaan tugas-tugas infrastruktur vital. Namun tidak bisa dipungkiri, adanya peluang yang luar biasa besar erat kaitannya pula dengan adanya kerentanan dalam dunia maya. Misalnya saja, *cyber space* juga dipenuhi oleh aktor-aktor yang dapat membawa kerugian besar seperti penjahat terorganisir, mata-mata pemerintah dan industri esensial yang berpotensi sebagai ancaman. Dalam menilai ancaman Iran ke AS perlu menyelidiki motivasi, peluang, dan kapabilitas dari negara lawan. Misalnya, embargo AS ke Iran dan serangan siber pada infrastruktur nuklir dan minyak baru-baru ini memotivasi Iran untuk melakukan serangan balik ke AS. Sebagaimana dikutip dalam situs resmi pemerintahan AS, ancaman siber tidak memiliki batasan. Data merupakan kerentanan besar bagi suatu negara karena dapat diakses, diserang kapan saja dan oleh siapapun. Pelaku *'cyber threat'* Iran terus meningkatkan kemampuan *offensive cyber* mereka. Iran telah menggunakan kemampuan sibernya yang semakin canggih untuk menekan aktivitas sosial dan politik tertentu, serta merugikan musuh regional dan internasional. Dilansir dari *Cybersecurity and Infrastructure Agency* (CISA), komunitas intelijen dan berbagai organisasi sektor swasta AS telah mengidentifikasi IRGC sebagai kekuatan pendorong di belakang serangan siber yang disponsori oleh negara Iran.

Pada tanggal 20 Juli 2021, Pemerintah AS mengaitkan aktivitas kontrol industri dengan aktor siber Iran, para pelaku *nation-state actor* ini diamati telah menyebarkan *malware* Shamoon terhadap ICS. Berikut adalah laporan aktivitas siber berbahaya Iran berdasarkan analisis CISA, U.S. *Department of Defense,* dan FBI (CISA, 2021):

Tanggal Penerbitan	Nama Aktivitas Serangan Siber	Deskripsi
20 Juli 2021	*JSAR-12-241-01B: Shamoon/DistTrack Malware (Update B)*	Pemerintah AS mengaitkan dengan publikasi kegiatan sebelumnya yang menargetkan sistem kontrol industri aktor siber *nation-state* Iran.
30 Oktober 2020	*CISA and FBI Joint Cybersecurity Advisory: Iranian Advanced Persistent Threat Actor Identified Obtaining Voter Registration Data*	CISA dan FBI merilis CSA Gabungan pada aktor APT Iran yang menargetkan situs web negara bagian AS, termasuk situs web pemilihan, untuk mendapatkan data pendaftaran pemilih. Penasihat memberikan indikator kompromi (IOCs) dan mitigasi yang direkomendasikan untuk entitas yang terkena dampak.
22 Oktober 2020	*CISA-FBI Joint Cybersecurity Advisory: Iranian Advanced*	CISA dan FBI merilis peringatan Penasihat tentang aktor APT Iran yang kemungkinan berniat mempengaruhi

	Persistent Threat Actors Threaten Election-Related System	dan mengganggu pemilihan AS 2020 untuk menabur perselisihan di antara pemilih dan merusak kepercayaan publik dalam proses pemilihan AS.
15 September 2020	*CISA-FBI Joint Cybersecurity Advisory: Iran-Based Threat Actor Exploits VPN Vulnerabilities MAR-10297887-1.v2 – Iranian Web Shells*	CISA dan FBI merilis CSA Gabungan pada aktor siber berbahaya yang berbasis di Iran dan menargetkan beberapa agen federal AS serta jaringan berbasis AS lainnya. Penasihat menganalisis taktik, teknik, dan prosedur (TTPs) aktor ancaman; IOC; dan mengeksploitasi Kerentanan dan Eksposur Umum. MAR merinci fungsionalitas file berbahaya—termasuk beberapa komponen *China Chopper Web Shell*—yang digunakan oleh aktor siber berbahaya yang berbasis di Iran.
6 Januari 2020	*CISA Alert: Potential for Iranian Cyber Response to U.S. Military Strike in Baghdad*	Mengingat meningkatnya ketegangan antara Amerika Serikat dan Iran, CISA merilis analisis Peringatan dan *"Insights"* yang memberikan TTP kepada pemerintah Iran dan aktor ancaman siber yang berafiliasi dengan

	CISA Insights: Increased Geopolitical Tensions and Threats	TTP dan gambaran profil ancaman siber Iran.

Sumber: CISA

2.5. Tantangan *Cyber Warfare* AS dan Retaliasi *Tit-for-Tat* Iran

Serangan siber yang paling berkesan antara Iran dan AS adalah virus Stuxnet pada tahun 2010, berhasil menginfeksi fasilitas pengayaan uranium Iran dan menyebabkan sentrifugal mereka tidak berfungsi. Meskipun tidak ada negara yang mengaku bertanggung jawab, namun berdasarkan bukti-bukti mengarah pada AS dan didukung oleh negara Israel. Saat ini, kemampuan perang siber AS sangat beragam, terorganisir, dan tingkatnya sangat tinggi. Pada Oktober 2019, AS telah meluncurkan operasi siber rahasia terhadap infrastruktur propaganda Iran menyusul dugaan serangan *drone* dan rudal Iran terhadap fasilitas minyak Arab Saudi (Reuters, 2021).

Di sisi lain, ditemukan pada tahun 2013 bahwa peretas Iran yang diduga melakukan pekerjaan untuk pemerintah Iran telah menembus kontrol komputer sebuah bendungan kecil di utara *New York City.* Peretas yang sama juga meluncurkan serangan siber terhadap sejumlah lembaga keuangan besar dan memblokir pelanggan untuk mengakses akun mereka secara online. Dalam iklim saat ini, Iran dapat mempertimbangkan untuk menggunakan kemampuan serangan sibernya sebagai bagian dari pembalasannya atas pembunuhan Soleimani.

Mengakui kemungkinan serentetan serangan siber dari pihak-pihak yang berafiliasi dengan Iran, Departemen Keamanan Dalam Negeri AS memperingatkan perusahaan-perusahaan AS untuk mempertimbangkan dan menilai kemungkinan dampak serangan semacam itu terhadap bisnis mereka. Bertentangan dengan adanya kekhawatiran ini, kemampuan Iran untuk meluncurkan serangan siber besar yang dapat memengaruhi sebagian besar populasi AS telah diremehkan oleh beberapa pakar keamanan siber.

Cyberwarfare bisa menjadi ancaman serius dan Iran dapat mengambil kendali infrastruktur penting untuk melumpuhkan target militer atau membahayakan publik. Tindakan perang bisa sewaktu-waktu terjadi yang melibatkan negara dan kekuatan militer. Serangan dapat dilakukan dari jarak jauh dan oleh kelompok peretas yang tidak dipekerjakan secara terbuka oleh pemerintah yang terlibat. Di bawah hukum internasional, negara-negara dapat secara sah membela diri jika diserang. AS secara eksplisit memiliki hak untuk menanggapi serangan siber dengan kekuatan militer. Tetapi, pembenaran untuk serangan balik apapun akan melemah jika tidak jelas apakah negara yang dituduh berada di balik serangan siber karena tidak ada bukti yang kuat menyatakan bahwa suatu negara adalah dalang dibalik kejadian tersebut akibat penggunaan proxy untuk menyamarkan identitas pelaku.