LEMBAGA KAJIAN
SYAMINA
Bekerja Mencegah Kezaliman

NETWORK VS NETWORK

Saat yang Kecil Melawan yang Besar

"Jika aksi militer kita tidak mengarah pada politik Syariat kita yang adil, dan jika tujuan jangka pendek dan kesuksesan kita tidak sejalan dengan tujuan utama kita, maka itu semua adalah sekadar kelelahan, ketegangan, dan ilusi."

— Athiyatullah Al-Liby

"Kemenangan dalam perang bukanlah sesuatu yang berulang, tapi lakukanlah adaptasi bentuk secara terus menerus… Kemampuan untuk meraih kemenangan dengan berubah dan beradaptasi sesuai lawan disebut sebagai kejeniusan."

— Sun Tzu

Sejak serangan 11 September, terorisme menjadi tema yang menjadi *headline* utama di berbagai media dan pemerintah di seluruh dunia. Al-Qaidah, yang diduga berada di balik serangan paling spektakuler dalam sejarah modern tersebut, menjadi sebuah organisasi yang menarik perhatian para analis politik, ahli militer, dan peneliti di Barat untuk dikaji; mulai dari strategi organisasi, propaganda, ideologi, kemampuan operasional, kompetensi kepemimpinan, hingga daya kenyal organisasi tersebut.[1]

Salah satu tema yang menjadi banyak sorotan dan perdebatan adalah mengenai bentuk dan struktur Al-Qaidah. Ada dua pandangan utama mengenai hal tersebut. Pandangan pertama menganggap Al-Qaidah sebagai sebuah hierarki, di mana informasi, akuntabilitas, dan kekuasaan mengalir secara vertikal. Kemampuan Al-Qaidah untuk mengatur serangan simultan di berbagai lokasi yang berbeda seperti di Pentagon dan *World Trade Center* menjadi bukti akan adanya struktur manajerial yang mempengaruhi tujuan dan target organisasi tersebut.

Pemerintah AS juga mendukung pandangan ini dengan menganggap bahwa dengan membunuh para pimpinan inti Al-Qaidah akan menyebabkan hancurnya organisasi tersebut. Mereka melakukan operasi besar-besaran untuk membunuh para pimpinan Al-Qaidah, termasuk diantaranya adalah pembunuhan atas Usamah bin Ladin. Namun kenyataannya, organisasi tersebut masih tetap eksis sampai sekarang. Katherine Zimmerman dalam bukunya yang berjudul *The Al-Qaidah Network: A New Framework for Defining the Enemy* mengatakan bahwa pada tahun di mana Usamah bin Ladin gugur, justru menjadi tahun dimana jaringan Al-Qaidah secara keseluruhan menjadi lebih kuat.[2]

Pandangan yang lain berpendapat bahwa Al-Qaidah adalah sebuah jaringan *(network)*. Mereka berargumen bahwa tekanan dahsyat yang dihadapi Al-Qaidah pascaperistiwa 9/11, menjadikan struktur hierarki tidak mungkin untuk diterapkan. Mereka menganggap bahwa Al-Qaidah sekarang telah bergeser menjadi sebuah jaringan *(network)* yang terdiri atas beberapa simpul dengan jumlah koneksi yang berbeda-beda. Struktur ini dianggap sebagai alasan mengapa Al-Qaidah tidak hancur, meski para pimpinan inti mereka dibunuh, rekening bank dibekukan, dan berbagai bentuk tekanan dahsyat lain diluncurkan oleh Amerika Serikat dan sekutunya. Bentuk jaringan diyakini mampu memberikan daya kenyal dan kemampuan untuk merespon peristiwa-peristiwa eksternal secara cepat.

Mungkin selama ini banyak organisasi, baik perusahaan komersil maupun kelompok perlawanan, baik yang merupakan gerakan populer (rakyat) maupun klandestin (bawah tanah), lebih mengenal model hierarki. Hampir semua perusahaan mengatur anggotanya secara hierarki. Namun, di era informasi ini, model jaringan menjadi bentuk struktur yang sangat dimudahkan dengan perkembangan di dunia teknologi informasi. Kajian ini akan membahas mengenai struktur jaringan, berikut kelemahan dan kekuatannya, serta bagaimana struktur tersebut dikalahkan.

[1] Bruce Hoffman, "Al Qaeda, Trends in Terrorism, and Future Potentialities: An Assessment," Studies in Conflict &Terrorism, 2003, h. 429–442.

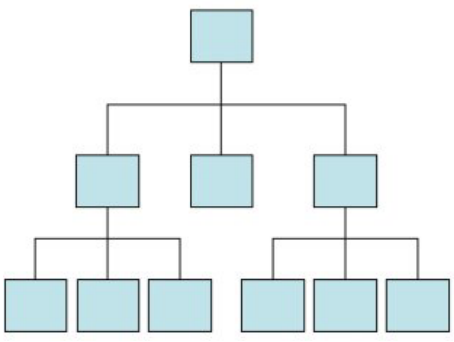
[2] Katherine Zimmerman, "The al Qaeda Network: A New Framework for Defining the Enemy," American Enterprise Institute, September 2013, h. 1.

APA ITU JARINGAN *(NETWORK)?*

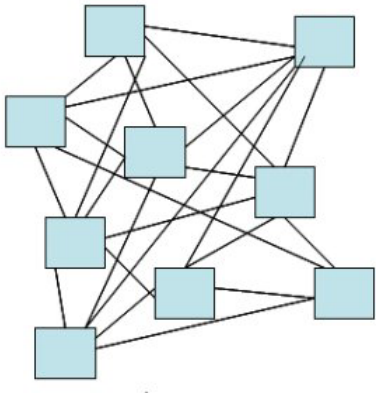
Jaringan *(network)* adalah organisasi yang secara sosial berasal dari komposisi antara para pelaku dan hubungan mereka. Tidak ada perbedaan mengenai karakter tersebut dibandingkan dengan bentuk organisasi yang lain—yaitu sekelompok orang yang bekerja bersama untuk mencapai tujuan bersama. Organisasi menawarkan hasil capaian yang lebih dibandingkan jika hanya dilakukan sendirian. Dua variabel utama yang membedakan berbagai bentuk organisasi adalah frekuensi kontak personal dan letak otoritas. Karakteristik struktural yang membedakan *network* dengan bentuk organisasi lainnya terletak pada (i) otonomi lokal dan informal, (ii) interaksi yang fleksibel di antara para anggotanya berdasarkan hubungan personal, serta (iii) terbatasnya kontrol dari pusat.

Teori organisasi telah menegaskan perbedaan berbagai bentuk organisasi, di mana perbedaan tersebut—secara signifikan—mempengaruhi performa organisasi. Perbedaan tersebut juga berpengaruh pada dinamika *irregular warfare*.[3] Banyak dasar-dasar teori organisasi berasal dari Era Mesin dan berpandangan

Hierarchical organisation structure



Social network



bahwa organisasi itu seperti *mesin, yaitu kumpulan dari beberapa bagian yang perlu distandarisasi dan dikontrol secara terpusat*. Namun, sekarang mulai muncul pemahaman yang menyatakan bahwa organisasi itu seperti sebuah *sistem, di mana hubungan diantara seluruh bagian dan interaksi total mereka menjadi hal yang penting.* Pendapat tersebut memandang organisasi sebagai *kombinasi dari beberapa bagian dan saling terhubung yang berinteraksi dengan lingkungannya, seperti tujuan organisasi, input, tugas, dan output.*

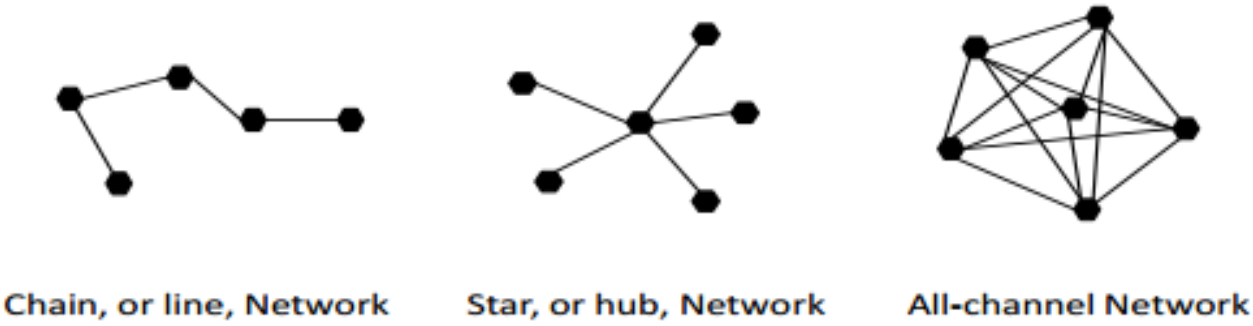
Pendapat yang memandang organisasi sebagai sebuah sistem yang fungsinya terkait dengan lingkungan memicu pada pendapat yang menyatakan bahwa tidak ada bentuk baku organisasi yang ideal. Efektivitas organisasi bergantung pada berbagai aspek dalam lingkungan tersebut.

Dari perspektif organisasi, struktur hierarki melakukan penyaluran otoritas, sumberdaya material, dan ideologi secara vertikal. Di dalam hierarki, terutama yang berdasarkan pada birokrasi ala mesin, tugas-tugas yang kompleks dipecah menjadi pekerjaan-pekerjaan spesifik untuk mencapai efisiensi yang lebih besar. Organisasi bentuk ini membatasi komunikasi dengan pihak di luar bagian mereka. Karenanya, hierarki cenderung mengabaikan pengaruh dari hubungan

[3] *Irregular warfare* adalah perang di mana salah satu atau lebih pihak yang berperang merupakan pasukan non-reguler. Salah satu bentuk *irregular warfare* adalah perang gerilya dan perang asimetris. *Irregular warfare* lebih mengutamakan pendekatan tidak langsung dan asimetris.

formal dan informal dari para pelaku yang sering kali lintas bagian dan lintas batas. Ia juga mengabaikan hubungan sosial harian yang sebenarnya mempengaruhi identitas, perilaku, dan tindakan seseorang.

berbagai gangguan. *Arquilla dan Ronfeldt mendefinisikan network sebagai sekumpulan simpul yang tersebar yang berbagi ide dan kepentingan, serta disusun untuk bertindak secara saling terhubung satu sama lain.*



Gambar 1. Tiga Bentuk Dasar Struktur *Network*

Struktur hierarki cocok untuk masyarakat yang terdiri dari para pekerja berpendidikan rendah. Mereka tidak mempunyai (cukup) pengetahuan atau keterampilan untuk bisa dipercaya melaksanakan suatu tugas secara mandiri dengan efektif atau efisien. Mereka perlu dipandu untuk mengerjakan tugas yang sederhana dan diawasi secara teliti. Karenanya, akuntabilitas menjadi sesuatu yang sangat mungkin untuk diselenggarakan. Pemimpin puncak mampu mengetahui apa yang sedang dilakukan bawahannya, dimana jika suatu tugas tidak berjalan maka 'sumber masalah'bisa segera dicari. Struktur hierarki memberikan peluang dilaksanakannya keputusan secara cepat dan efisien.

Dalam konteks pasukan militer, struktur hierarki cocok untuk mengatur pasukan berpendidikan rendah untuk menjadi pasukan tempur yang efektif. Sementara struktur network sangat cocok diterapkan pada organisasi yang terdiri dari para anggota yang mempunyai keterampilan dan motivasi tinggi.

Secara organisasi, *network* memberikan tingkatan konektivitas yang lebih besar dan lebih ulet dari

JENIS-JENIS JARINGAN (*NETWORK)*

1. **Chain**

   Network jenis ini berbentuk garis linier, dimana hubungan antara satu orang dengan yang lainnya terpisah dalam pola garis. Orang, barang, dan layanan berpindah melalui simpul perantara dalam pola beruntun.

2. **Star atau Hub**

   Dalam jenis *network* ini, beberapa simpul dihubungkan ke satu simpul pusat dalam satu *hub*, dengan bentuk seperti jari-jari. Sumber daya dan komunikasi dilakukan melalui *hub* pusat.

3. **All-Channel**

   Network jenis ini dibentuk dalam sebuah matriks hubungan, dimana setiap simpul terkoneksi satu sama lain dalam pola yang padat.

Menurut Arquilla dan Ronfeldt, tiga bentuk di atas merupakan tiga bentuk utama *network*, meskipun terkadang ada beberapa kombinasi atau variasi dari ketiga bentuk tersebut.

KARAKTERISTIK *NETWORK*

A. Atribut Organisasi

a. Struktur *network* mempunyai tingkat desentralisasi yang tinggi, yang memberikan kelonggaran pada aksi-aksi otonom dan inisiatif operasional yang tinggi.

b. *Network* bertempur dengan simpul yang tersinkronisasi (sel) yang memberikan keuntungan atas pengendalian taktik dan keamanan.

c. Irregular warfare bersifat dinamis, dan *network* mendapatkan keuletan melalui struktur organisasi mereka yang unik.

d. Network yang efektif bersifat fleksibel, dan mampu beradaptasi sesuai dengan kondisi lingkungan, yang membuat mereka resisten dari segala bentuk tekanan.

e. Network dibentuk melalui hubungan yang dibangun atas dasar kepercayaan, yang mampu menopang aktivitas berisiko tinggi dan memberikan keuntungan operasional.

f. Network jarang sekali bersandar pada kontrol dan komando langsung. Hal ini memicu terjadinya fleksibilitas dan otonomi dalam pembuatan keputusan taktis, namun berisiko mengurangi arahan kolektif.

B. Doktrin

Doktrin memberikan bingkai kerja dan prinsip umum dalam sebuah *irregular warfare*. Peran populasi menjadi fitur yang signifikan dalam *irregular warfare*, yang menjadi ciri utama mereka. *Irregular warfare* menegaskan bahwa *perang adalah kelanjutan dari tujuan politik yang diekspresikan dengan cara lain*. **Dalam *irregular warfare*, kehendak masyarakat sama pentingnya dengan kekuatan militer.**

Network mungkin juga akan memperpanjang konflik sebagai cara untuk mendemonstrasikan keinginan kuatnya, atau untuk menggapai kemenangan yang cepat dan menentukan.

a. Network bertempur menggunakan doktrin yang unik dan terkombinasi yang mengaburkan antara atribut ofensif dan defensif.

b. Network menggunakan *swarming*[4] sebagai aspek fundamental dalam doktrin mereka. *Swarming* juga menjadi elemen pembeda antara *network* dengan bentuk *irregular warfare* yang lain.

c. Network mampu untuk bertempur secara berlarut-larut, mampu untuk mengambil inisiatif pada saat yang memungkinkan, mendemonstrasikan kekuatan yang ada, serta memanfaatkan kesempatan untuk mencapai kemenangan yang cepat.

d. Network sangat bergantung pada tipu daya, dalam bentuk *concealment*, untuk memastikan kondisi yang mendukung baik dalam tingkatan teknik maupun strategis.

e. Network menyerang kelemahan dengan melakukan gangguan sistem, dibandingkan melakukan konfrontasi langsung dengan pasukan musuh yang lebih kuat—meski pilihan kedua juga diambil oleh *network*. Penggunaan strategi tidak langsung ini meningkat pada era informasi ini, yang memberikan kemudahan konektivitas antarelemen dan lebih mudah untuk melakukan pembongkaran sistem-sistem vital musuh.

[4] *Swarming* adalah perilaku di mana beberapa unit pasukan yang otonom atau semi otonom melakukan serangan atas musuh dari berbagai arah yang berbeda dan kemudian berkumpul kembali.

C. Metode Operasional

a. Network secara umum mempunyai sumberdaya yang lebih sedikit dibandingkan lawannya. Meski demikian, bersenjata ringan bisa juga memberikan keuntungan operasional yang berlipat.

b. Network mempunyai derajat siluman yang tinggi *(high degree of stealth)*, yang merupakan atribut fundamental dalam pembuatan keputusan taktis mereka.

c. Network membutuhkan kejutan, yang menjadi elemen yang menentukan dalam serangan terhadap musuh yang lebih kuat.

d. Network membutuhkan mekanisme klandestin untuk mempertahankan kerahasiaan mereka, namun hal tersebut bisa menciptakan inefisiensi operasional.

D. Strategi Informasi

a. Network berusaha menyebarkan informasi secara cepat, yang membawa pada inovasi taktik dan pemberian inspirasi secara cepat.

b. Network melakukan aktivitas operasional untuk mempengaruhi persepsi publik. Langkah ini membutuhkan sinkronisasi dengan strategi informasi.

c. Network membutuhkan tingkat intelijen yang tinggi, di mana penggunaannya secara sistemik akan menentukan kecepatan operasional mereka.

d. Network menggunakan teknologi informasi modern untuk mencapai keunggulan informasi stratejik atas lawannya.

KEKUATAN DAN KELEMAHAN *NETWORK*

Kekuatan dan kelemahan *network* didapatkan dari pemahaman secara menyeluruh atas karakteristik *irregular warfare*. Beberapa tumpang-tindih muncul pada kekuatan dan kelemahan mereka; dan ini menjadi suatu ciri umum dalam aspek, doktrin, bahkan sistem fisik dari sebuah organisasi. Dalam banyak cara, karakteristik tersebut bak pedang bermata dua bagi sebuah organisasi; bisa menguatkan atau justru membahayakan. Mengetahui kekuatan dan kelemahan adalah sebuah langkah kritis dalam memahami musuh dan mencari titik rentan mereka.

A. Kekuatan *Network*

a. Sifat *network* yang terdesentralisasi memberikan otonomi yang lebih besar pada saat konflik, dan memberikan keleluasaan pada inisiatif operasional dan penyelarasan mandiri (*self-synchronization*).

b. Kurangnya peran pemimpin dalam memberikan arahan membuat *network* tidak terlalu bersandar pada kontrol langsung.

c. Simpul yang saling terhubung memberikan peluang pada kontrol taktis yang tersinkronisasi dan memberikan keamanan yang lebih besar dalam bentuk persembunyian (*concealment*) dan kompartemen.

d. Struktur berbentuk *network* lebih ulet dari tekanan luar. Jika satu simpul gagal, keseluruhan *network* masih bisa tetap berjalan.

e. Struktur *network* memberikan fleksibilitas yang lebih tinggi, di mana mereka lebih mampu untuk beradaptasi atas terjadinya perubahan lingkungan dibandingkan hierarki.

f. Network mendapatkan kekuatan melalui hubungan yang dibangun atas dasar kepercayaan. Hubungan tersebut mampu

menopang aktivitas-aktivitas berisiko tinggi dan meningkatkan efektivitas operasional.

g. Kemampuan *network* untuk melakukan persembunyian *(concealment)* di tengah-tengah populasi memberikan keuntungan yang sangat besar bagi mereka.

h. Elemen yang bersenjata ringan memberikan keuntungan yang lebih besar dalam melakukan mobilitas dan *concealment*.

i. *Network* menggunakan teknologi informasi untuk mencapai keuntungan dalam komunikasi stratejik.

j. Informasi teknologi memberikan peluang bagi *network* untuk melakukan mobilisasi, melatih, merekrut, dan melakukan pendanaan dengan biaya yang sedikit serta akses yang luas.

B. Kelemahan *Network*

a. Desentralisasi membuat organisasi tersebut sulit untuk melakukan kontrol atas sebuah operasi dan juga sulit untuk melakukan penguatan atas langkah-langkah keamanan.

b. Simpul yang kecil akan berada dalam kerugian yang besar jika mereka tidak melakukan serangan kejutan dalam tingkat taktis, yang seringkali bisa dicapai melalui tipu daya yang berorientasi pada *concealment (concealment-oriented deception)*

c. Struktur *network* memang memberikan tingkat keuletan yang tinggi, namun ia juga lebih rentan yang bisa menyebabkan keruntuhan total (*total collapse*) jika sejumlah besar *hub* gagal.

d. *Network* terbatasi oleh kemampuan mereka untuk mencapai keseimbangan antara kegigihan dan operasi (niat vs. kemampuan).

e. Hubungan yang berdasarkan kepercayaan memberikan sebuah alat atau cara untuk mengidentifikasi para pelaku dalam *network* tersebut. Selain itu, hubungan tersebut juga bisa menjadi poin potensial akan terjadinya keretakan.

f. Koneksi seluruh kanal *(all-channel connections)* meningkatkan potensi infiltrasi di dalam *network*.

g. *Network* harus bersiap untuk bertempur dalam jangka panjang serta menyeimbangkan antara kemenangan yang menentukan dengan kemampuan untuk tetap bertahan.

h. Tuntutan kerahasiaan membutuhkan mekanisme untuk sembunyi, yang menciptakan terjadinya inefisiensi komunikasi.

i. Kecepatan operasional terbatasi oleh kemampuan intelijen, karena penggerebekan dan penyergapan, bahkan *swarming*, membutuhkan data intelijen dalam jumlah yang signifikan.

j. Ketergantungan *network* pada teknologi informasi publik semakin meningkat—di mana teknologi tersebut bisa menguatkan dan juga bisa membahayakan.

k. Kurangnya kontrol pusat atas para anggota berpotensi memicu munculnya aksi-aksi otonom yang bertentangan dengan tujuan organisasi secara umum.

l. Kurangnya akuntabilitas, karena otoritas tersebar dan kontrol terbatas.

Dengan melihat kekuatan dan kelemahan *network*, kita bisa mencatat peran penting organisasi dan informasi. Di antara kekuatan yang ada, tingkat otonomi yang tinggi dan desentralisasi mampu menghasilkan aksi operasional yang cepat, namun juga menciptakan

kesulitan untuk membentuk konsensus dan mengoordinasikan aksi-aksi yang kompleks.

Aspek organisasional memberikan pengaruh yang paling besar pada kekuatan dan kelemahan, namun peran informasi juga tidak kalah penting, di mana jika ia dikerjakan dengan skill tinggi akan memberikan peningkatan kemampuan yang signifikan dari sebuah jaringan yang secara dasar lemah.

Informasi juga memiliki hubungan yang unik dengan kemampuan *network* untuk tetap tersembunyi. Di satu sisi, pihak yang ingin melawan *network* harus memiliki informasi yang diperlukan untuk menemukan simpul *network*, di mana mereka seringkali harus bekerja keras untuk mendapatkannya. Di sisi lain, *network* juga seringkali harus berusaha untuk tampak dan aktif di bidang informasi, demi keuntungan stratejik dan kebutuhan operasional mereka.

BAGAIMANA CARA MELAWAN *NETWORK*?

Melawan *network* pada abad ke-21 ini memberikan tantangan yang berbeda jika dibandingkan dengan melawan kekuatan militer tradisional dan pasukan gerilyawan klasik. Organisasi *network* saat ini memanfaatkan dunia teknologi informasi untuk menciptakan hubungan dan berbagai kemungkinan baru yang membuat mereka menjadi musuh yang sangat berat bagi pasukan militer tradisional. Perang dalam era informasi ini memberikan ancaman yang berbeda secara signifikan, meningkatkan kompleksitas dan kemampuan yang ditunjukkan oleh bentuk organisasi tersebut.

Perang modern saat ini menggunakan seluruh jaringan yang ada—politik, ekonomi, sosial, dan militer—untuk meyakinkan para pembuat keputusan di pihak lawan bahwa tujuan strategis mereka susah dicapai atau terlalu berbiaya dibandingkan keuntungan yang akan mereka dapatkan. Pendekatan perang secara tradisional yang mengasumsikan pertempuran dengan pasukan militer profesional, dengan doktrin yang sama dan kekuatan teknologi yang sama, saat ini tidaklah relevan. Keunggulan unik *network* di era informasi ini, dengan melakukan sinkronisasi teknik pertempuran, dianggap telah memberikan tantangan yang sangat signifikan di era modern ini.

Sejarah telah menunjukkan beberapa contoh kesuksesan para gerilyawan berhasil mengalahkan pasukan militer negara. Usaha mujahidin Afghanistan pada akhir 1980-an menjadi contoh nyata bagaimana sebuah organisasi gerilyawan mampu mengalahkan pasukan militer negara sebesar Uni Soviet. Suku Habr Gedir juga berhasil memaksa pasukan AS menarik diri dari Somalia pada tahun 1993. Yang lebih aktual, pasukan militer profesional berhasil dibuat frustasi oleh gerilyawan di Afghanistan dan Irak.

Lebih dari sepuluh tahun berperang, pasukan koalisi internasional masih dipaksa untuk bertempur melawan musuh yang tidak punya pasukan angkatan laut, angkatan udara, atau angkatan darat. **S**atu hal yang secara gamblang menandaskan bahwa ada faktor lain yang lebih penting dari sekadar keunggulan teknologi dan pasukan yang lebih kuat.

Selain itu, paduan antara *network*, senjata yang unik, dan kemampuan penyebaran informasi memberikan keuntungan tersendiri pada jaringan-jaringan non-negara. Karenanya, para pengamat menilai bahwa *network* akan memberikan tantangan yang lebih besar dibandingkan tantangan yang diberikan oleh konflik yang terjadi saat ini.

Yang menarik, dari sebuah studi tentang tiga puluh pemberontakan yang terjadi antara tahun 1978-2008,

hanya delapan di antaranya yang berhasil dimenangkan oleh pasukan negara dengan kekuatan yang lebih superior.[5] Catatan ini, ditambah dengan semakin meningkatnya kekuatan *network*, membuat beberapa negara kini berusaha mencari cara yang tepat untuk menghadapi *network* di era informasi ini.

"Berhadapan dengan kemampuan perang tradisional AS, musuh kita nampaknya akan memilih menggunakan paduan antara kemampuan mengacaukan, menghancurkan, *irregular,* dan kemampuan tradisional sebagai cara untuk mencapai tujuan strategis mereka. Strategi musuh kita adalah untuk menumbangkan, menarik, dan membuat kita lelah dibandingkan mengalahkan kita secara militer. Mereka akan berusaha untuk mengikis dan meruntuhkan kekuatan nasional, pengaruh, dan kehendak AS dan sekutu stratejiknya."[6]

Aspek utama dari ancaman ini adalah bahwa semua tipe lawan akan menggunakan cara-cara diluar cara militer tradisional, namun mereka tetap bertujuan untuk mengalahkan AS dalam konflik tersebut. Ahli militer China, Qiao Lang dan Wang Xiangsui, dalam bukunya *Unrestricted Warfare,* menegaskan tentang meningkatnya tren kekuatan-kekuatan asimetris yang berusaha mengambil keuntungan dengan mengombinasikan antara kekuatan militer dan non-militer dalam cara-cara yang baru. Mereka melihat perang saat ini berada di tengah-tengah perubahan yang dramatis, karena prinsip perang yang baru tidak lagi menggunakan pasukan bersenjata untuk memaksa musuh mengakui keinginan seseorang. Namun, mereka kini menggunakan semua cara, termasuk kekuatan bersenjata dan tidak bersenjata, militer dan non-militer, cara-cara yang mematikan dan tidak mematikan untuk memaksa musuh mereka agar menerima kepentingan seseorang.[7]

Beberapa studi tentang *irregular warfare* menekankan akan pentingnya usaha untuk melakukan gangguan secara langsung atas sebuah jaringan. Menurut Carley, ada *tiga indikator utama terjadinya destabilisasi sebuah jaringan, yaitu berkurangnya aliran informasi, kesulitan untuk mencapai konsensus umum, dan berkurangnya efektivitas pelaksanaan tugas secara keseluruhan.*[8]

Pemerintah AS sendiri menegaskan bahwa "musuh kita barangkali adalah sebuah jaringan yang longgar atau sebuah entitas yang tidak memiliki struktur hierarki yang terlihat. Namun, mereka memiliki sebuah titik rentan yang bisa dieksploitasi dalam sistem politik, militer, ekonomi, sosial, informasi, dan infrastruktur mereka yang saling terhubung. Mereka sering melakukan konflik jangka panjang sebagai usaha untuk mementahkan keinginan pemerintahan sebuah negara. Dalam hal ini, operasi militer saja tidaklah cukup untuk mengatasi konflik semacam itu."[9]

Selain itu, doktrin militer AS yang lainnya juga menyatakan bahwa musuh yang berbentuk jaringan mempunyai beberapa kelemahan yang bisa dieksploitasi, di mana gangguan pada beberapa simpul dalam jaringan tersebut memberikan kesempatan bagi

[5]Paul, Clarke dan Gill, "Victory Has a Thousand Fathers: Evidences of Effective Approaches to Counterinsurgency", 1978–2008, h. 12.

[6] U.S. Department of Defense, *Irregular Warfare Joint Operating Concept*, Ver. 1.0, Washington, D.C.: U.S. Joint Chiefs of Staff, Januari 2007, h. 15–16.

[7]Qiao Lang and Wang Xiangsui, *Unrestricted Warfare,*Beijing: PLA Literature and Arts Publishing House, 1999, h. 4 (http://www.cryptome.org/cuw.zip).

[8]Carley, Lee, and Krackhardt,"Destabilizing Networks," h. 90.

[9]U.S. Department of Defense, Joint Publication 1, *Doctrine for the Armed Forces of the United States*, I–1.

pengumpulan data intelijen dan/atau untuk melakukan usaha isolasi yang lebih efektif.[10]

Struktur berbentuk *network (*jaringan) mempunyai titik rawan yang berbeda dengan struktur hierarki. Dari identifikasi beberapa kekuatan dan kelemahan *network*, dihasilkan beberapa hal yang bisa menjadi titik rawan atau peluang untuk melakukan gangguan atas *network*, di mana beberapa hal yang menjadi kekuatan dari *network* berpeluang juga menjadi potensi titik rawan.

Beberapa titik rawan jaringan *(network)* adalah sebagai berikut:

- Sifat *network* yang terdesentralisasi memberikan peluang terjadinya inisiatif yang besar, namun ia bisa dilawan dengan unit yang serupa dengan menggunakan *offensive swarming.* (Organisasi/Doktrin).
- Sinkronisasi yang kompleks antara unit-unit yang terdesentralisasi membutuhkan tujuan yang melingkupi semuanya dan komunikasi yang luas. (Strategi Informasi/Organisasi/Doktrin)
- *Network* sangat bergantung pada kemampuan mereka untuk menyembunyikan diri. (Doktrin)
- Struktur *free-scale network* memberikan keuletan dan fleksibilitas yang tinggi, namun ia rentan akan serangan yang diarahkan atas *hub*-nya. (Organisasi)
- Hubungan kuat yang berdasarkan atas kepercayaan memberikan alat untuk mengidentifikasi dan membongkar jaringan tersebut. (Organisasi)
- Mekanisme klandestin mampu memelihara kerahasiaan jaringan tersebut, namun bisa menghambat komunikasi internal. (Doktrin)
- Aktivitas operasional terbatasi oleh kemampuan intelijen dan kebutuhan untuk mempengaruhi persepsi publik. (Metode Operasional/Strategi Informasi)
- Struktur *network* yang saling terhubung memberikan peluang terjadinya infiltrasi. (Organisasi)

Selain beberapa titik rawan di atas, faktor kontekstual dan lingkungan juga harus diperhatikan dalam memerangi *network*. Seperti, apa strategi utama jaringan tersebut? Apakah ia termasuk pemberontakan yang populer (merakyat), ataukah dia semacam jaringan bawah tanah yang hanya sedikit hubungannya dengan populasi yang lebih besar?

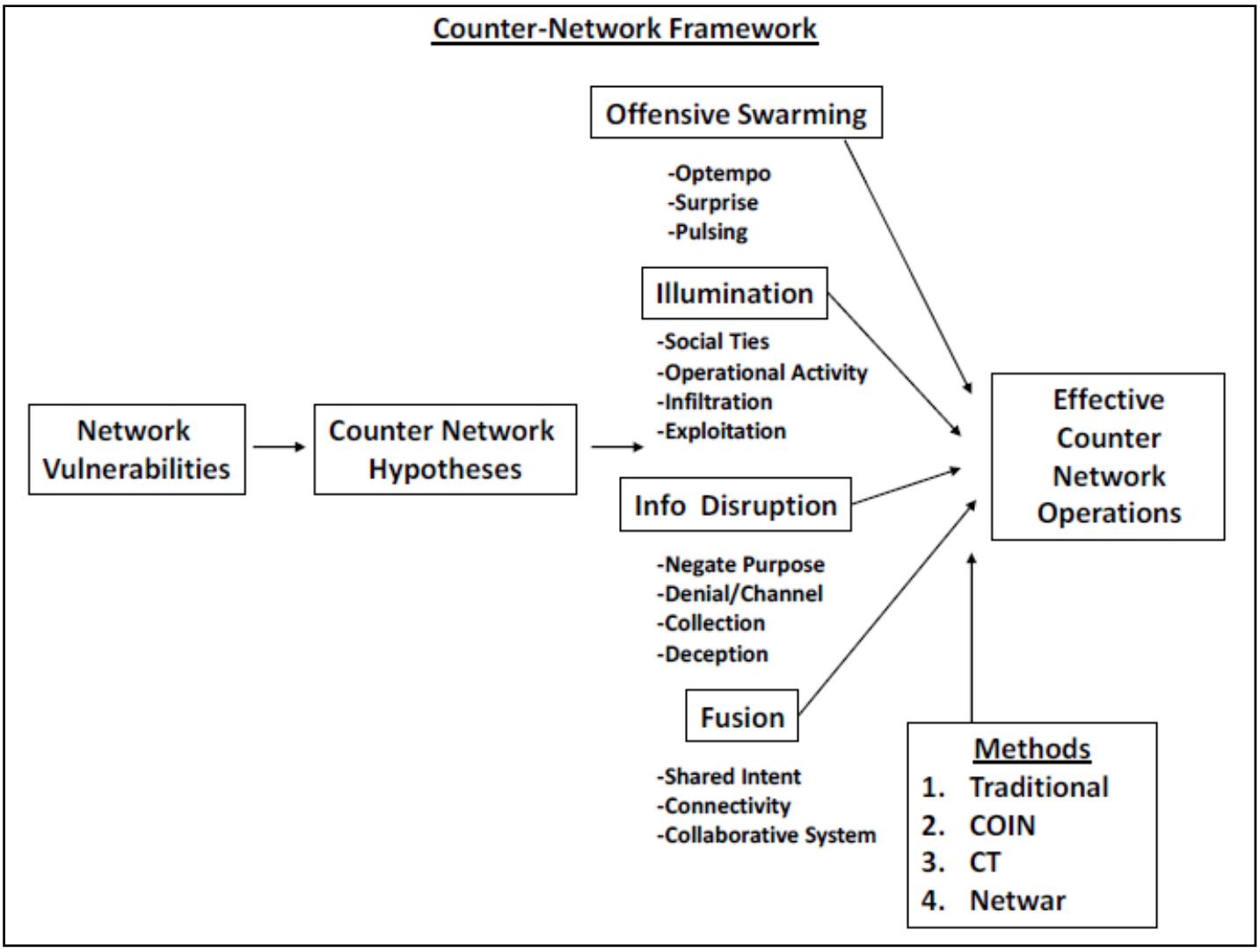
Sebuah organisasi *network* adalah elemen dari struktur jaringan sosial masyarakat yang lebih besar, dan memahami populasi di mana mereka berinteraksi juga tak kalah penting dengan usaha untuk mengacaukan mereka. Organisasi *network* bukanlah organisasi militer standar, di mana dalam banyak kasus usaha yang paling penting untuk mematahkan mereka adalah dengan melakukan bujukan pada persepsi masyarakat.[11]

Kompleksitas mengenai apa, bagaimana, dan mengapa masyarakat berinteraksi adalah aspek yang penting dalam pengumpulan data intelijen. Begitu juga dengan faktor budaya. Gordon Hahn menyatakan bahwa "usaha untuk memecah kelompok pemberontak tidak akan sukses tanpa pemahaman yang rinci akan pembagian politik, sosial, kesukuan, dan ekonomi jaringan tersebut. Pengetahuan secara detail atas sejarah, budaya, ideologi politik, dan seluk beluk struktural juga hal yang esensial."[12]

[10] U.S. Department of Defense, Joint Publication 3-26, *Counterterrorism*, III–15.

[11]Michael T. Flynn, Matt Pottinger, dan Paul D. Batchelor, *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan*, Washington, D.C.: Center for a New American Security, 2010, h. 24

[12]Gordon Hahn,"The Jihadi Insurgency and the Russian Counterinsurgency in the North Caucasus," Post-Soviet Affairs 24, no. 1 (January–March 2008): 3,



Gambar 2. Bingkai kerja kontra jaringan

Berikut adalah beberapa variabel yang diperlukan untuk melawan jaringan:

A. Illumination (Penerangan)

Iluminasi adalah sebuah usaha untuk mengidentifikasi dan menentukan letak simpul dalam sebuah jaringan. Ada empat cara untuk membuka aspek gelap dalam memerangi *network*. Keempat aspek tersebut akan berjalan lebih efektif jika dilakukan secara kombinasi, dibanding jika hanya fokus pada satu cara.

(i) *Metode pertama* adalah dengan memanfaatkan pertalian sosial, atau basis dukungan dan jaringan masyarakat di mana jaringan tersebut dibentuk. Jaringan sangat memanfaatkan pertalian yang kuat diantara struktur masyarakat. Pertalian yang kuat adalah aspek yang sangat penting dalam pembentukan jaringan, namun hubungan sosial yang membentuk pertalian tersebut terjadi dalam cara yang terbuka dan tidak aman.

Dalam sebuah artikel yang menyerukan adanya restrukturisasi usaha pengumpulan intelijen di Afghanistan, Jendral Michael Flynn menyoroti tentang pentingya mendapatkan pengetahuan tentang konteks lokal dari sebuah operasi dan perbedaan antara Taliban dan masyarakat Afghanistan pada umumnya. Pengetahuan ini

sangat penting untuk memahami hubungan antara para pejuang dengan penduduk lokal.

Sebagaimana yang dijelaskan sebelumnya, pemberontakan yang berisiko tinggi dan bersifat klandestin mengembangkan pertalian yang sangat kuat diantara para anggotanya, yang dicirikan dengan tingkat kepercayaan yang tinggi. Hubungan berdasarkan kepercayaan tersebut terutama terjadi berdasarkan pertemanan dan pertalian keluarga.

Hubungan tersebut memberikan alat yang kuat untuk mengidentifikasi segmen inti dari sebuah jaringan, meski mereka berusaha untuk tetap tersembunyi. Selain itu, metode ini juga bisa dilakukan dengan melakukan pengikisan kepercayaan dan menciptakan ketidakstabilan di dalam jaringan tersebut.

(ii) *Metode kedua* adalah dengan memaksa jaringan tersebut untuk menampakkan diri sendiri. Metode ini dilakukan dengan memaksa mereka untuk melakukan operasi serangan, yang membuat simpul-simpul operasional menjadi kelihatan dan bisa menjadi target. Aspek operasional adalah fungsi yang memaksa jaringan untuk sembunyi atau menghindar.

Kedua pilihan tersebut memerlukan mekanisme klandestin. Namun, semakin bersifat klandestin karakter sebuah jaringan maka semakin tidak efisien jaringan tersebut. Jaringan yang sangat tersembunyi akan menghasilkan struktur berbentuk sel, dan memerlukan otoritas yang lebih untuk menguatkan. Untuk mempertahankan sifat klandestin, mereka berusaha untuk membatasi komunikasi, perjalanan, dan lain-lain, dengan mengurangi hubungan, memperlambat komunikasi, dan menghilangkan banyak aspek dalam seluruh kanal yang selama ini membuat mereka efektif secara operasional.

Oleh karena itu, adanya tekanan dan aspek operasional tersebut membawa jaringan pada pilihan fundamental; apakah akan tetap mempertahankan aktivitas operasional yang nantinya akan berdampak pada tekanan yang meningkat, ataukah mengurangi aktivitas operasional dan menjadi lebih tersembunyi yang dalam prosesnya akan membuat mereka menjadi semakin terstruktur dan terisolasi. Dengan memaksa sebuah jaringan untuk membuat pilihan yang sulit, jaringan tersebut akan berada dalam ujung sebuah dilema yang kompleks.

(iii) *Metode ketiga* adalah melakukan eksploitasi atas jaringan tersebut. Eksploitasi disini meliputi interogasi dan pengumpulan informasi mengenai jaringan tersebut dari berbagai sumber, termasuk melakukan *human intelligence* (HUMINT). Elemen utama dari HUMINT dalam konteks ini adalah melakukan spionase klasik dan interogasi atas para tahanan.

Doktrin COIN *(Contra Insurgency)* modern menekankan pentingnya interogasi dan perannya dalam memahami sifat ancaman dalam sebuah lingkungan yang *irregular*.[13] Mereka menganggap bahwa tahanan yang bisa diinterogasi adalah harta yang sangat berharga. Bahkan, barangkali menjadi satu-satunya alat yang memungkinkan untuk mengetahui kemampuan sebuah jaringan secara lebih rinci. Contoh sukses dari hal ini adalah penangkapan dan informasi yang didapat dari seorang warga Jerman bernama Ahmed Sidiqi,

[13] U.S. Department of Defense, Field Manual 3-24, *Counterinsurgency*, 3–27.

yang membuat tercegahnya beberapa rencana serangan di Eropa.

(iv) *Metode keempat* adalah dengan melakukan infiltrasi. Sifat jaringan yang menghubungkan seluruh kanal dan penggunaan pertalian yang lemah untuk menghubungkan seluruh segmen dalam jaringan memberikan peluang terjadinya infiltrasi. Meski konektivitas yang tinggi memberikan keuntungan akan cepatnya aliran informasi, namun ia juga berpotensi meningkatkan terjadinya kontak dan akses pada informasi tersebut dibandingkan yang terjadi pada bentuk organisasi lainnya.

Selain itu, pertalian lemah yang menjadi jembatan dalam sebuah jaringan berarti akses awal menuju jaringan tersebut, yang biasanya kurang diteliti dengan cermat. Pertalian yang dibentuk untuk melakukan rekrutmen, penggalangan dukungan, dan bahkan pertemanan, memberikan jalan untuk mengakses dan membuka aktivitas sebuah jaringan. Kasus Ramzi Yousef yang dikhianati oleh teman yang ia jumpai di Universitas Islam Internasional di Islamabad adalah salah contohnya.[14]

Contoh lain adalah Shannon Rossmiller, yang menggunakan jejaring sosial di internet untuk mencari teman jihadi, dan kemudian mengkhianati mereka.[15] Selain penggunaan penetrasi intelijen, langkah lain yang bisa dilakukan adalah dengan melakukan *pseudo-operation* (operasi semu), karena dalam sebuah jaringan yang tersebar luas sangat potensial untuk disusupi adanya *false group* (kelompok palsu) dan *decoy activities* (aktivitas umpan).

B. Offensive Swarming

Swarming merupakan alat yang paling valid untuk melawan sebuah jaringan. Sebuah organisasi berbentuk jaringan biasanya terdiri dari beberapa simpul yang tersebar, yang jika mereka berkumpul sekalipun tetap susah untuk disasar, karena mereka biasanya pandai mengelak dan menghindar. Karenanya, diperlukan kontra-simpul yang mempunyai kegesitan dan kecepatan yang mampu melawansimpul tersebut. Dalam hal ini unit *counter-swarming* bisa menjadi salah satu jawaban.

Unit *counter-swarming* akan melakukan serangan secara mengejutkan untuk terus menerus memaksa jaringan tersebut untuk bersembunyi atau menghindar. Melawan jaringan sangat memerlukan efek kejutan untuk bisa berjalan secara efektif. Efek kejutan ini bisa dilakukan dengan melakukan inisiatif mengawali serangan, yang akan sangat menguntungkan karena lawan biasanya dalam kondisi tanpa penjagaan. Ini sebagaimana yang dikatakan oleh William McRaven ketika menjelaskan sifat unit operasi khusus yang kecil; bahwa kejutan adalah kombinasi dari tipu daya, *timing*, dan mengambil keuntungan atas kerentanan yang terjadi pada musuh.[16] Sementara *swarming* mampu memberikan metode tersebut untuk melakukan

[14] Jones, *Exploiting Structural Weaknesses in Terrorist Networks: Information Blitzkrieg and Related Strategies,*h. 11.
[15]Noah Shachtman, *Some of Her Best Friends are Terrorists, WIRED*, 23 Oktober 2007 (http://www.wired.com/dangerroom/2007/10/some-of-her-bes).

[16]William H. McRaven, *Spec Ops: Case Studies in Special Operations Warfare: Theory and Practice,*Novato, CA: Presidio Press, 1995, h. 17.

kejutan secara konsisten dan memberikan tekanan operasional pada lawan.

Salah satu aspek kunci dari *offensive swarming*[17] adalah *pulsing. Pulsing* adalah fungsi dari melihat dan menunggu yang diimbangi dengan serangan cepat saat melihat ada kerentanan pada lawan, kemudian diikuti dengan pengumpulan kembali simpul-simpul. *Pulsing* memanfaatkan data intelijen yang didapat dari iluminasi untuk menentukan tempo dan sifat serangan atas sebuah jaringan. Jarak antar-serangan dalam *pulsing* mungkin relatif pendek. Meski demikian, masih memungkinkan untuk dilakukannya identifikasi titik rawan baru dan sinkronisasi atas data intelijen baru tersebut.

Selain itu, *offensive swarming* juga dicirikan oleh tempo operasi yang sangat tinggi yang dimaksudkan untuk menghancurkan *hub* secara cepat. Hal ini akan berdampak pada runtuhnya jaringan tersebut, karena organisasi jaringan biasanya tidak mampu bertahan dari angka kehilangan yang tinggi, terutama pada elemen-elemen yang aktif secara operasional, yaitu *hub* yang berfungsi menyatukan dan menjadi elemen kritis dari struktur tersebut.

Memang, beberapa pihak menyatakan bawah hilangnya beberapa elemen dalam sebuah jaringan bisa diisi dengan mudah oleh para penggantinya. Namun, dalam banyak kasus, masih perlu diuji apakah penggantinya tersebut memiliki tingkat keahlian yang sama dengan pendahulunya.

Selain itu, hilangnya elemen kunci tersebut diduga juga akan 'mengasah' sebuah jaringan, di mana para pengganti akan termotivasi dan terasah dari pengalaman pahit tersebut. Untuk mengurangi dampak tersebut, aktivitas operasional yang signifikan harus difokuskan pada usaha iluminasi yang ekstensif, dan memastikan bahwa dampak kerusakan yang ditimbulkan atas struktur jaringan tersebut lebih besar jika dibandingkan dengan nilai simpul penggantinya.

C. Information Disruption (Pengacauan Informasi)

Pengacauan informasi berfungsi untuk melawan ketergantungan jaringan yang tinggi pada informasi, dan mencoba mengeksploitasi kelemahan yang terungkap dalam strategi informasi jaringan tersebut. Sebagaimana yang diungkapkan oleh Berkowitz, faktor yang paling penting dalam dunia militer di era informasi ini adalah *'kemampuan untuk mengumpulkan, mengomunikasikan, memproses, dan melindungi informasi.'* Untuk memenangkan perang informasi kita perlu membuat sistem informasi kita menjadi lebih *capable* (mampu)*, reliable* (handal)*,* dan lebih aman, atau dengan menyerang sistem informasi lawan sehingga membuat mereka menjadi kurang *capable,* kurang *reliable,* dan kurang aman.[18]

Menurut Lawrence Freedman, dalam perang *irregular*, superioritas dalam hal fisik hanya akan bernilai kecil kecuali jika bisa diterjemahkan ke dalam keuntungan di dunia informasi.[19] Kilcullen menguatkan pernyataan tersebut dengan

[17] *Swarming* memang tampak tak berbentuk, namun sebenarnya mereka terstruktur secara bebas dan terkoordinir sebagai salah satu cara strategis untuk melakukan serangan dari segala arah. Salah satu caranya adalah dengan melakukan *pulsing,* baikdengan pasukan maupun dengan senjata, baik dari jarak dekat maupun jarak jauh.

[18] Bruce Berkowitz, *The New Face of War: How War Will be Fought in the 21st Century,* New York: The Free Press, 2003, h. 21.

[19] Lawrence Freedman, *The Transformation of Strategic Affairs,*Abingdon, NY: Routledge, 2006.

menambahkan bahwa 'saat ini benar-benar terjadi perang informasi. Saat kelompok pemberontak menyerang kendaraan AS di Irak, bukan berarti mereka melakukannya karena ingin mengurangi jumlah Humvee AS, tapi lebih dikarenakan mereka ingin liputan media yang spektakuler atas aksi peledakan Humvee tersebut.[20]

Dinamika tersebut membuat strategi informasi yang tepat sangatlah penting. Di samping itu, usaha untuk melakukan kontra jaringan (*counter-network*) harus melibatkan komponen pengacauan informasi. Komponen ini bukanlah komponen yang berdiri sendiri, tetapi melibatkan juga usaha operasional digabung dengan usahailuminasiyang lebih besar.

Aspek paling penting dalam variabel ini berfokus pada menyangkal tujuan umum lawan. Elemen penyatu yang cukup kuat dalam pembuatan sebuah jaringan adalah adanya pandangan bersama yang menyatukan berbagai simpul yang terpencar dan otonom. Narasi tersebut merupakan faktor penggerak tentang bagaimana jaringan bertindak dan merupakan motivator dari berbagai aksi jaringan tersebut. Pengacauan informasi dimaksudkan untuk melawan tujuan tersebut melalui pelemahan, pembelokan, atau bahkan penolakan atas tujuan yang dinyatakan oleh sebuah organisasi jaringan.

Aspek kedua pengacauan informasi difokuskan pada menyangkal, atau menyalurkan, kemampuan jaringan untuk berkomunikasi. Upaya ini bertujuan untuk mengurangi arus informasi baik di dalam jaringan maupun komunikasi eksternal di luar jaringan. Upaya untuk mengurangi arus informasi internal berfokus pada usaha mengisolasi aktor yang seharusnya berfungsi sebagai *hub* komunikasi, serta menabur ketidakpercayaan untuk memperlambat dan bahkan memblokir informasi yang seharusnya dapat dibagi. Upaya ini bisa memberikan efek gangguan yang cukup dahsyat pada sebuah jaringan.[21]

Aspek ketiga pengacauan informasi adalah membiarkan jaringan untuk berkomunikasi sebanyak mungkin, dan menggunakan informasi yang diberikan untuk lebih memahami dan menerangi jaringan. Teknik ini semakin mungkin di era di mana kecerdasan verbal, terutama dalam bentuk SIGINT *(Signal Intelligence)*, bisa memberikan informasi yang cukup. Teknik ini memerlukan keseimbangan yang besar antara kegiatan operasional dan kemampuan untuk mendapatkan informasi tambahan pada sebuah jaringan.

[20]George Packer, *Knowing the Enemy: Can Social Scientists Redefine the War on Terror?* The New Yorker,18 Desember 2006, h. 65–66 (http://www.newyorker.com/archive/2006/12/18/061218fa_fact2).

[21] J. Bowyer Bell, *Aspects of the Dragonworld: Covert Communication and the Rebel Ecosystem*, International Journal of Intelligence and Counterintelligence 3, no. 1 (1989): 27–31.

Terakhir, dalam usaha pengacauan informasi diperlukan kemampuan melakukan tipu daya. Tipu daya merupakan alat yang penting dalam melawan tujuan suatu jaringan dan terbukti efektif dalam mengganggu aliran informasi baik internal maupun eksternal.

D. Fusion (Penggabungan)

Fusi adalah usaha untuk melawan koneksi tersinkronisasi yang digunakan oleh jaringan. Fusi memiliki elemen organisasi dan elemen doktrin. Secara organisasi, fusi membutuhkan konektivitas tingkat tinggi diantara unsur-unsurnya sebagaimana jaringan, dan hal ini sangat penting dalam sebuah usaha kolaboratif. Secara doktrin, fusi melibatkan penggabungan berbagai kemampuan operasional dan upaya analitis dalam sebuah proses pemecahan masalah yang sistematis. Fusi merupakan *gabungan antara mendapatkan data intelijen yang sangat luar biasa dan melakukan aksi operasional yang mampu mengacaukan lawan irregular.*

Dalam lingkungan konflik *irregular*, intelijen memainkan peran utama, dan bahkan operasi harus dirancang dalam rangka menghasilkan data intelijen. Menurut Frank Kitson, jika masalah utama dalam mengalahkan musuh sangat tergantung pada usaha untuk menemukan mereka, maka sangat bisa dipahami akan pentingnya informasi yang baik. Sejarah *irregular warfare* menunjukkan bahwa ketidakmampuan untuk mengenali sifat lingkungan *irregular warfare* menyebabkan ketergantungan pada kegiatan operasional sederhana untuk menemukan musuh, yang akhirnya berujung pada kegagalan.

Penggabungan antara operasi dan intelijen memberikan tingkat konektivitas yang memudahkan sinkronisasi aksi dan data intelijen yang diperlukan untuk mencapai keberhasilan dalam setiap variabel sebelumnya. Jika tiga variabel sebelumnya difokuskan pada tindakan yang diambil terhadap jaringan, fusi berfokus pada kemampuan inti yang diperlukan untuk melakukan tindakan tersebut.

Kesamaan tujuan sangat diperlukan dalam melawan jaringan. Fusi membutuhkan kesamaan tujuan untuk menyatukan berbagai elemen yang berbeda dan memberikan arah untuk mencapai target yang spesifik. Kesamaan tujuan ini akan menyatukan tujuan dan fokus yang berbeda-beda dalam sebuah organisasi dan memaksimalkan kontribusi dari masing-masing satuan tugas. Meskipun fusi memberikan konektivitas dan inovasi yang lebih besar pada tingkat yang paling rendah, tetapi peran pemimpin sangat penting dalam menyediakan dan menekankan tentang tujuan bersama yang hendak dicapai.

Konektivitas yang komprehensif antara orang, informasi, dan aksi akan memberikan sinergi yang diperlukan untuk memudahkan tindakan seperti iluminasidan *swarming*. Lingkungan *irregular warfare* memerlukan sistem yang memfasilitasi adanya fusi. Seluruh operasi menuntut adanya intelijen, karena operasi yang tidak terlalu kuat—ditambah dengan respons adaptif dari musuh—memberikan peluang bagi mereka terus mengubah lokasi dan struktur.

Dari dinamika tersebut, sebuah operasi membutuhkan dan menghasilkan data intelijen, menciptakan sebuah siklus dengan tujuan akhir

adalah untuk mendapatkan pemahaman yang lebih besar tentang musuh. Fokus dari sistem ini adalah mendukung dan menghasilkan data intelijen pada level yang paling rendah.

Sistem fusi ini adalah sistem yang mana baik pengumpul data intelijen dan pemakainya memerlukan kolaborasi tingkat tinggi. Pengumpulan data intelijen adalah fokus utama dari sebuah operasi, untuk kemudian data tersebut digunakan untuk mendukung operasi berikutnya. Contoh dari hal ini adalah fungsi intelijen, pengawasan, dan pengintaian lintas udara *(Airborne Intelligence, Surveillance, and Reconnaissance)* dalam siklus penargetan.

Airborne ISR telah menjadi aspek penting dalam perang saat ini karena mampu menawarkan pengamatan yang terus menerus—dengan tingkat visibilitas yang rendah dari kemungkinan diketahui musuh—dan kemampuan untuk mendeteksi, mengidentifikasi, dan melacak musuh dalam lingkungan dengan tingkat kontras yang rendah, baik di lingkungan pedesaan maupun di perkotaan. ISR memberikan kemampuan yang unik yang memungkinkan dilakukannya penggabungan masukan dari aksi operasional dan data intelijen dari semua sumber.

STUDI KASUS

A. IRAK 2003 – 2006

a. Offensive Swarming

Komponen utama dalam *offensive swarming* adalah kejutan, kecepatan operasi, dan *pulsing.* Seluruh elemen tersebut membutuhkan data intelijen yang akurat mengenai lokasi target, kesabaran untuk mengumpulkan data intelijen, dan kemampuan untuk menyerang tanpa harus membuka diri. Dalam kasus Perang Irak 2003 – 2006, pasukan AS mengalami kekurangan data intelijen mengenai pemberontakan yang terjadi di wilayah tersebut. Bahkan, pada awal konflik, mereka menyangkal adanya pemberontakan tersebut.

Ketidakpahaman atas kultur lokal membuat AS berusaha menyerang kelompok perlawanan dengan melakukan operasi berskala besar dalam menyisir tempat persembunyian mereka. Hasilnya, operasi ini hanya memberikan pengaruh kecil pada jaringan Al-Qaidah Irak (AQI) yang cukup kompleks. Berbagai serangan di Fallujah menjadi bukti kemampuan AQI untuk mengelak dari serangan terdahsyat sekalipun; meskipun mereka bertempur di sana, banyak pejuang dan sebagian besar pimpinan AQI yang menyebar ke tempat lain.

b. Illumination

Kurangnya pemahaman budaya dan sifat perjuangan kelompok *irregular*, membuat AS tidak memiliki pengetahuan dan kemampuan yang dibutuhkan untuk mengungkap jaringan AQI. Sebagian besar usaha AS dalam melakukan iluminasi berfokus pada aktivitas operasional musuh saat serangan terjadi, bom meledak,

atau terjadi penculikan. Mereka berhenti pada insiden tersebut, dan tidak menjadikan insiden tersebut sebagai pintu masuk untuk memahami jaringan AQI. Usaha pengumpulan data intelijen juga terhambat oleh kurangnya kemampuan para intelijen AS. Menyusul terbongkarnya skandal Abu Ghuraib pada April 2004, banyak tahanan yang dipindahkan ke penjara yang lebih besar, dan sebagian besar justru dibebaskan. Kelemahan tersebut, ditambah dengan lemahnya manajemen dan pembagian informasi serta kurangnya fusi organisasi membuat usaha iluminasi menjadi sulit bagi AS. Hal ini menjadi bukti akan sebuah ungkapan: sebuah pemberontakan tidak akan bisa dikalahkan jika mereka tidak bisa diidentifikasi.[22]

c. Information Disruption

Kemampuan pengacauan informasi sangat bergantung pada strategi informasi secara keseluruhan, satu hal yang pada periode ini AS cukup lemah. Tujuan AQI adalah melakukan jihad melawan penjajahan AS dan menolak kontrol Syiah di Irak, dan banyak tindakan AS justru mendukung tujuan AQI tersebut. Bahkan Gedung Putih juga memperkuat pesan AQI tersebut dengan membuat pernyataan bahwa 'kita sedang berperang melawan teroris asing, yang datang dari luar untuk melakukan apa yang mereka yakini sebagai jihad yang sangat penting.'[23]

Usaha untuk mencegah atau mengalihkan aliran informasi AQI juga tidak ada karena AQI dengan mudah mengakses berbagai sumber komunikasi, terutama internet. Memang usaha pengumpulan informasi sudah ada, namun kurang fokus. Sebagian besar usaha tipu daya masih terpecah-pecah dan belum menyatu.

d. Fusion

Fusi lebih menekankan pada penyatuan niat dan tujuan yang nantinya akan menimbulkan konektivitas dalam organisasi dan sinkronisasi doktrin. Awalnya, pasukan AS mempunyai kesepahaman yang sama akan tugas utama mereka—yaitu untuk mengalahkan dan menggulingkan rezim Saddam Hussein—namun saat tujuan tersebut tercapai, sebagian besar tekad tersebut memudar.

Alasan utama melemahnya tekad tersebut disebabkan kurangnya pemahaman akan doktrin bersama, yaitu pesan-pesan mengenai bagaimana perang tersebut dilakukan dan bagaimana masa depan pasukan AS. Bahkan pada pertengahan 2006, banyak tentara AS yang bersiap untuk pulang dan melimpahkan sebagian besar tugas mereka kepada Pasukan Keamanan Irak (ISF).

Kurangnya strategi bersama membuat masing-masing unit dalam pasukan AS menjadi kurang terhubung, dimana tiap unit hanya berfokus pada area tanggungjawab mereka masing-masing. Mereka hanya bekerja dengan kelompok lain jika diperlukan, itupun tidak dalam pola yang terintegrasi.

[22] Bing West, "Iraq and a Singular Information Failure," yang dimuat dalam *Ideas As Weapons: Influence and Perception in Modern Warfare*, editor G. J. David Jr. dan T. R. McKeldin III (Washington, DC: Potomac Books, 2009), h. 225.

[23] The White House, "Interview of National Security Advisor by KXAS-TV, Dallas, TX," November 2003.

B. IRAK 2006 – Sekarang

a. Offensive Swarming

AS menggunakan seluruh aspek *offensive-swarming* untuk melawan Al-Qaidah Irak (AQI) pada periode ini. Integrasi antara pengumpulan data intelijen dan fusi membuat AS mampu meningkatkan tempo serangan. Mereka menggunakan data intelijen sebagai pengarah operasi. Bahkan, hanya dengan sedikit tanda adanya aktivitas AQI, itu bisa menjadi titik awal menuju pengumpulan data yang lebih banyak dan penting.

Mereka melakukan serangan mengejutkan secara gencar, cepat, dan tepat, di mana informasi yang didapatkan dari satu serangan menggiring pada target berikutnya. Mereka melakukan *pulsing* secara efektif dengan lebih memahami konteks lingkungan lokal. Mereka menganggap bahwa aspek operasi yang paling penting dalam pembunuhan Abu Mush'ab Az-Zarqawi bukanlah gugurnya Az-Zarqawi, tapi 405 serangan berikutnya yang dilakukan dalam selang waktu sepekan.

Swarming dilakukan dalam waktu 24 jam sehari dan 7 hari dalam sepekan atas simpul-simpul yang terlihat. Selain itu, AS juga diuntungkan dengan adanya serangan cepat dari *Abna'ul Iraq* (*Sons of Iraq*/SOI) atas AQI di tempat-tempat yang menjadi basis AQI.

b. Illumination

Langkah awal AS dalam melakukan iluminasi adalah dengan melakukan pemahaman atas hubungan sosial dan jaringan kesukuan di Irak. Kemudian mereka menggunakan siklus F3EA (*Find, Fix, Finish, Exploit, Analyze)* untuk mengumpulkan data intelijen.

Siklus F3EA ini penting untuk memetakan kelompok klandestin dan pendukung mereka, menggunakan seluruh data intelijen untuk menyibak kondisi lingkungan lokal, jaringan sosialnya, dan para pembuat keputusan diantara mereka. Salah satu aspek penting dari siklus ini adalah penggunaan *drone* untuk melakukan pengawasan dan pengumpulan data intelijen. Selain itu, usaha iluminasi juga dimudahkan oleh konflik sektarian dan pertempuran diantara para pemberontak yang memaksa AQI untuk muncul ke permukaan.

Cara berikutnya adalah dengan mengelola sistem penahanan secara ramah dan efisien, melakukan teknik interogasi secara efektif, dan cara lain yang membuat para tahanan mau memberikan informasi yang berharga.

c. *Information Disruption*

Pengacauan informasi ini sangat diuntungkan atas "kesalahan besar" AQI yang sering melakukan "serangan brutal dan tanpa pandang bulu". Kampanye media AS selama ini gagal dalam menyanggah kampanye perlawanan AQI, sampai AQI membuat "kesalahan" dengan mengecam umat Islam "Sunni moderat".

AS berhasil mendiskreditkan AQI dengan menyorot aspek-aspek 'horor' dari aksi-aksi AQI. Strategi informasi AQI semakin kalah saat suku-suku lokal melakukan kampanye media untuk menyudutkan AQI, yang membuat popularitas AQI semakin melorot dan menguatkan usaha-usaha AS.

Selain itu, AS juga melakukan pengumpulan data intelijen dari berbagai sumber sebagai alat untuk mengacaukan sumber-sumber teknis, dibarengi dengan kehadiran secara fisik di lapangan yang mencoba untuk menghentikan penggunaan kurir dan mekanisme-mekanisme dukungan lainnya. Pengusiran AQI dari 'persembunyian amannya' juga memicu mereka untuk meningkatkan komunikasi dalam rangka memulihkan diri; satu hal yang akhirnya digunakan untuk pengumpulan data baru bagi AS.

"Organisasi *network* bukanlah organisasi militer standar, di mana dalam banyak kasus, usaha yang paling penting untuk mematahkan mereka adalah dengan melakukan bujukan pada persepsi masyarakat."

d. *Fusion*

Fusi dilakukan AS dengan menyatukan beberapa agensi dan kelompok ke dalam satu unit kerja. Unit tersebut disatukan oleh niat dan tujuan yang sama, di mana *sense of urgency*, tujuan, dan komitmen untuk menyelesaikan satu misi menyatukan beberapa elemen tersebut. Masing-masing personal mengutamakan dedikasi mereka atas tugas tersebut dibanding kepada organisasi induk mereka.

(K. Mustarom)

ABOUT US

Laporan ini merupakan sebuah publikasi dari Lembaga Kajian Syamina (LKS). LKS merupakan sebuah lembaga kajian independen yang bekerja dalam rangka membantu masyarakat untuk mencegah segala bentuk kezaliman. Publikasi ini didesain untuk dibaca oleh pengambil kebijakan dan dapat diakses oleh semua elemen masyarakat. Laporan yang terbit sejak tahun 2013 ini merupakan salah satu dari sekian banyak media yang mengajak segenap elemen umat untuk bekerja mencegah kezaliman. Media ini berusaha untuk menjadi corong kebenaran yang ditujukan kepada segenap lapisan dan tokoh masyarakat agar sadar realitas dan peduli terhadap hajat akan keadilan. Isinya mengemukakan gagasan ilmiah dan menitikberatkan pada metode analisis dengan uraian yang lugas dan tujuan yang legal. Pandangan yang tertuang dalam laporan ini merupakan pendapat yang diekspresikan oleh masing-masing penulis. Untuk komentar atau pertanyaan tentang publikasi kami, kirimkan e-mail ke: lk.syamina@gmail.com.

Seluruh laporan kami bisa didownload di website: www.syamina.org