mendukung pemekaran ketika mereka menyadari dampaknya terhadap anggaran yang bakal diterimanya.

Bagi Pemerintah (Depdagri), yang perlu dilakukan adalah memperbaiki *the legal framework* termasuk di dalamnya proses proposal yang diusulkan. Beberapa isu penting yang perlu disampaikan adalah:

(a) Memperbaiki proses pemekaran melalui kajian secara cermat terhadap proposal-proposal yang diajukan. Indikator kunci yang digunakan adalah kondisi yang jelas dan prediksi terhadap dampak negatif pemekaran.

(b) Menempatkan posisi Pemerintah sebagai satu-satunya pintu masuk bagi usulan pemekaran daerah (prosedur administrasi).

(c) Memperkenalkan kriteria *initial threshold* bagi daerah yang hendak memekarkan diri.

(d) Meperkenalkan waktu yang cukup untuk mempersiapkan langkah-langkah: memasukkan isu tentang proliferasi daerah dalam UU seperti pemisahan sumber-sumber, periode persiapan, lokasi ibukota dll.

(e) Meningkatkan tanggungjawab persiapan pemekaran kepada daerah itu sendiri.

(f) Perlunya konsultasi publik atau pelibatan publik dalam proses pemekaran sehingga masyarakat memiliki andil dalam menilai pemekaran daerahnya.

Selain itu, kerjasama dengan DPD dan masyarakat madani (*civil society*) juga sangat diperlukan untuk mengatasi masalah pemekaran. Dalam konteks ini, langkah yang perlu diambil adalah mengundang aktor-aktor untuk mendiskusikan masalah pemekaran. Kedua, mendorong dialog pusat-daerah untuk menyamakan persepsi.

Langkah terakhir tapi tak kalah pentingnya adalah mencari jalan alternatif untuk mengatasi buruknya pelayanan publik di daerah-daerah terpencil dan terisolasi. Terobosan yang perlu dilakukan dalam konteks realisasi desentralisasi dan otonomi daerah sekarang ini adalah menjadikan kecamatan sebagai pusat pelayanan dan menciptakan kota-kota metropolitan yang dapat memberikan pelayanan di luar batas kota. Dengan kata lain, pemekaran daerah bisa dicegah dengan meningkatkan kualitas pelayanan publik (kesehatan dan pendidikan) dan memberikan insentif bagi daerah-daerah yang berhasil menggabungkan diri.❑

Intelijen di Era Digital

Wawan H. Purwanto

Sulit bagi seorang Presiden dalam menggerakkan roda pemerintahan tanpa dukungan informasi intelijen. Apalagi di era digital yang serba cepat dan didukung teknologi canggih. Siapa tidak siap maka akan tergilas oleh zaman. Apa yang terjadi di suatu kawasan, maka detik itu pula dapat diakses ke seluruh penjuru dunia. Mampukah intelijen menangkap itu semua sebagaimana seorang karateka yang secara reflek menangkis serangan lawan dan menyerang balik?

Aneh jika suatu negara tanpa badan intelijen. Badan intelijen itu perlu karena memang dia merupakan mata, telinga, hidung, lidah, alat peraba yang mampu mendeteksi, mengidentifikasi, mengantisipasi dan melakukan cegah dini terhadap berbagai bentuk dan sifat potensi ancaman, demi kelangsungan hidup bangsa dan negara. [1]

Internet telah memunculkan dan memperkenalkan dunia baru yang disebut

[1] Alex Dinuth, *Sinar Harapan* , 10 September 2001, http://www.sinarharapan.co.id/berita

virtual world atau dunia maya, atau yang disebut pula *cyberspace*, yaitu bentuk dunia yang lain dari pada yang kita kenal selama ini. Dengan kata lain, *virtual world* atau *cyberspace* itu adalah lawan dari dunia yang kita kenal, dimana kita berada dan bernafas, yang disebut *real world* atau *physical world.* [2]

Cyberlaundering menjadi kian marak karena munculnya mata uang baru di *virtual world* yang disebut *electronic money (e-money)* atau *electronic cash (e-cash)* [3] atau *digital cash* atau *digital money*, hal itu dimungkinkan karena sistem-sistem keuangan (*financial system*) memungkinkan nilai ekonomis dinyatakan secara digital oleh pola elektronik.

Menurut Farez bin Haouzam, ahli masalah Al Qaeda Arab Saudi, Al Qaeda merekrut anggota melalui internet, tidak seperti anggota-anggota sebelumnya yang direkrut dan dilatih di Afganistan. Melalui pola rekrutmen anggota ini, Al Qaeda dapat melebarkan sayapnya ke seluruh penjuru dunia, tanpa perlu mengadakan kontak langsung dengan calon anggota barunya. Ini berarti ancaman terorisme tidak pudar, tapi meningkat. [4]

Masih ingat ketika Imam Samodra mengakses sumber-sumber keuangan *via lap top* yang diselundupkan ke LP Krobokan Bali. Upaya penggalangan dana *via* internet merupakan celah bagi pendanaan kegiatan terorisme. Kemampuan intelijen dalam melacak pembiayaan teroris sangat diperlukan guna deteksi dini *via* dunia digital. Intelijen perlu terus mengasah diri

---

2 Sutan Remy Sjahdeini, *Seluk Beluk Tindak Pidana Pencucian Uang dan Pembiayaan Terorisme*, Jakarta : Grafiti Cet 1, hlm 53

3 R. Mark Bortner, *Cyberlaundering, Anonymous Digital Cash and Money Laundering. Presented as Final Paper Requirement for Law & the Internet* (LAW 745), A seminar of the University of Miami School of Law, http://www.miami.edu/~froomkin/seminar/papers/bortner.htm. Menurut Mark Bortner : *Electronic cash or digital money, is an electronic replacement for cash. Digital cash has been defined as a series of numbers that have an intrincit value in some form of currency. Using digital cash, actual assets are transferred through digital communications in the form of individually identified representations of bills and coins- similar to serial members on hard currency*

4 Wawan H Purwanto, *Terorisme Undercover, Memberantas Terorisme Sampai Ke Akar-Akarnya, Mungkinkah?* Jakarta : CMB Press, Edisi 1 November 2007, hlm 50

agar dua langkah lebih maju ketimbang lawan.

Masih ingatkan anda ketika sistem KPU (Komisi Pemilihan Umum) dibobol oleh *hacker* Indonesia, yang kemudian terungkap dan pelakunya ditangkap oleh pihak berwajib. Intelijen sudah harus antisipasi lebih jauh akan adanya ancaman dunia maya yang terus berkembang seiring dengan kecanggihan era digital.[5]

Sampai pada era 1990 an, karena makin meningkatnya *cybercrime* para penyidik harus makin peduli akan validitas bukti digital. Maka mulai banyak perangkat dan aplikasi dibuat untuk membantu pengambilan data dari sebuah perangkat digital. *Tools* seperti *Safeback* dan DIBS dibuat pada era ini untuk membantu penyidik mengumpulkan bukti digital tanpa sedikitpun mengubah detil-detil pentingnya. Makin terasa penting dan tinggi tingkat kebutuhannya, *tools* digital forensik dibuat makin canggih dan hebat seiring dengan berjalannya waktu.[6]

Salah satu contoh *tool* yang termasuk cukup hebat yang ada saat ini adalah *Encase*, aplikasi keluaran *Guildance Software*. Tidak hanya dapat membaca data-data yang sudah terhapus, *Encase* juga dapat memberitahukan sistem-sistem yang belum di *patch*, menerima masukan dari *Intrusion Detection System* untuk menyelidiki keanehan jaringan yang terjadi, merespon sebuah insiden keamanan, memonitor pengaksesan sebuah *file* penting, dll. [7]

Di era digital pertimbangan sekuriti menjadi masalah mendesak. Sekuriti penting untuk membangun kepercayaan (*trust*) terhadap sebuah sistem informasi. Karena sistem informasi tersebut diharapkan menjadi sumber

---

5 ITAC *(Information Technology Association of Canada)* pada *International Information Industry Congress (IIIC) 2000 Millenium Congress*" di Quebec tanggal 19 September 2000 menyatakan bahwa *Cybercrime is a real and growing threat to economic and social development around the world. Information technology touches every aspect of human life and so can electronically enable crime.*

6 *Menguak Cybercrime*, http://www.ketok.com/

7 Cybercrime, *Op Cit,* hlm 5. Menurut Roy Suryo, rekaman gambar digital yang sudah terhapus dapat dipanggil lagi, Roy menyarankan agar orang tidak gegabah merekam adegan-adegan seronok karena tetap dapat diakses, apalagi dengan *bluetooth*, gambar mudah disebar.

yang dapat dipercaya. Sekuriti sering dipandang hanyalah merupakan masalah teknis yang melibatkan bisa atau tidak tertembusnya suatu sistem. Pada pandangan makro sekuriti sendiri memiliki konsep yang lebih luas, juga berkaitan dengan ketergantungan suatu institusi terhadap institusi lainnya, atau suatu negara terhadap negara lainnya. [8]

Beberapa aspek sekuriti yang harus dipertimbangkan diantaranya adalah *secrecy, integrity, authentication, non repudiation*, dan *accountability*. Untuk mengaplikasikan sekuriti dalam sebuah sistem informasi diperlukan juga pertimbangan lainnya misal suatu kebijakan sekuriti yang telah tertata dengan baik, teknologi yang memungkinkan diterapkannya kebijakan tersebut, serta kesepakatan sosial.[9]

Sekuriti sesungguhnya terbentuk dari suatu mata rantai yang akan memiliki kekuatan sama dengan mata rantai yang terlemah sekalipun. Buktinya, sebagai misal sistem keamanan yang berbasiskan *certificate authority* (CA) memiliki rantai yang tidak seluruhnya merupakan sistem *kriptografi* (sandi), tetapi manusia juga banyak terlibat.[10]

Menyikapi masalah tersebut, harus diakui bahwa banyak hal yang perlu dipertimbangkan dalam pengaksesan data. Untuk itu, dalam perancangan suatu sistem keamanan, lazimnya kita akan dihadapkan pada beberapa pertimbangan. Pertimbangan tersebut dikenal dengan nama segitiga CIA.

Segitiga CIA terdiri dari pertama, *confidentiality*. Yaitu segala usaha yang berkaitan dengan pencegahan pengaksesan terhadap informasi yang dilakukan pihak lain yang tidak berhak. Kedua, *integrity*. Yaitu sesuatu yang berkaitan dengan pencegahan dalam memodifikasi informasi yang dilakukan oleh pihak lain yang tidak berhak. Ketiga, *availability*. Yaitu pencegahan penguasaan informasi suatu sumber daya oleh pihak lain yang tidak berhak. Dalam pelaksanaan keamanan akan melibatkan 3 M

8 http://rateeh.wordpress.com/2007/09/22/pertimbangan sekuriti

9 *Ibid*

10 Arda Dinata, *Biometri Tawarkan Autentikasi Biologis*, http://www.pikiran – rakyat.com/cetak/2006

(matematika, manajemen, dan manusia).[11]

Teknologi biometrik yang mampu mengenali manusia lewat sidik jari, mata, atau karakter khas bagian tubuh lain kini makin memasyarakat. Teknologi ini dapat diterapkan pada banyak sektor, teknologi ini akan menggusur kata sandi (*password*) sebagai pintu masuk yang punya kelemahan.[12]

Film *Sixth Day* (2001) dengan pemeran utama Arnold Schwarzeneger memperlihatkan betapa biometrik sudah seperti menggantikan kunci. Sidik jari atau mata dapat digunakan sebagai pembuka akses masuk ke ruang kantor, laboratorium, menstarter mobil, atau membayar taksi. Teknologi pengenalan diri itu kini benar-benar mengenali fisik si pemilik, bukan lagi *password* (kata sandi). [13]

Seperti diwartakan *Kompas Cyber Media* yang mengutip hasil penelitian *Central NIC* (perusahaan pendaftar domain di Inggris), hampir separuh responden menggunakan nama atau nama panggilan sendiri sebagai *password*. Sepertiga responden memakai nama tim olahraga kesayangan atau nama bintang pujaan. [14]

Padahal kata sandi punya kelemahan. Selain harus diingat oleh si pemegang sandi, juga gampang ditebak meski yang sulit sekalipun karena ada alatnya. Menurut para ahli keamanan, kini ada *cracking tool* yang mampu memindai kata maupun menebak *password* berupa kombinasi huruf dan angka. *"LofiCrack"*, salah satu program penjebol sandi misalnya, hanya butuh waktu 48 jam untuk mencari seluruh arsip *password* di suatu perusahaan.[15]

Tak heran jika kemudian ada gagasan mencari pendekatan lain yang lebih canggih sebagai pengganti *password*. Jika kata sandi harus diingat (entah *password*-nya sendiri dan atau tempat menyembunyikannya), meng-

---

[11] *Loc Cit. Man behind the gun,* semua kembali kepada kemampuan manusia itu sendiri dalam mengoperasikan peralatan, manusia yang terlatih akan lebih meudah jika sewaktu-waktu berhadapan dengan ancaman.

[12] *Intisari*, Infotekno, Agustus 2001

[13] *Ibid*

[14] *Kompas Cyber Media*, 5 Agustus 2001

[15] Intisari , *Ibid*

apa tidak memakai sesuatu yang melekat di tubuh dan tanpa harus mengingat-ingat segala? Suara manusia, raut muka, atau sidik jari sebagai pembuka akses menjadi peluang besar pengganti kata sandi yang rentan dibobol.[16]

Parameter manusia yang dikenal dengan biometrik itu punya keunggulan sifat tidak dapat dihilangkan, dilupakan, atau dipindahkan dari satu orang ke orang lain. Juga sulit ditiru atau dipalsukan.[17]

Aplikasi teknologi biometrik dapat dicontohkan seperti ketika Anda memberikan tanda masuk ke kantor atau akses ke komputer menggunakan pemindai sidik jari; mengambil uang dari mesin kas yang dapat memindai mata Anda untuk mengenali bahwa Andalah pemilik sah uang itu; mengidentifikasi diri Anda pada bank melalui telepon dengan memakai pengenal suara (*voice recognition*); dan *check in* untuk penerbangan hanya dengan melewati sebuah kamera di bandara yang mengenali Anda sebagai penumpang berlangganan.[18]

Di masa depan, teknologi biometrik akan mirip fenomena komputer yang kemudian menjadi bagian dari sebuah produk kebutuhan hidup sehari-hari. Semua proses kerja di kantor seperti aktivitas akuntansi, pembuatan laporan, penawaran penandatanganan kontrak, dan banyak hal lain disinyalir melibatkan teknologi biometrik. [19]

---

16 *Op Cit.* Apa yang melekat pada manusia memang dapat berubah tatkala seseorang melakukan operasi plastik. Tetapi tidak ada penyamaran yang sempurna, sebagaimana pelarian Gunawan Santosa, buronan kasus pembunuhan Bos Asaba yang berulang kali operasi plastik, namun berkat kecanggihan alat sadap yang digunakan aparat keamanan mampu mengendus jejaknya sehingga tertangkap kembali.

17 *Ibid*

18 *Loc Cit*

19 *Loc Cit.* Tantangan ke depan lebih didasarkan pada kemampuan pengembangan teknologi digital. Indonesia memang lebih mengandalkan *human intelligence* yang terbukti mampu menggulung teroris, namun bantuan peralatan dari luar negeri rupanya sangat membantu dalam mengendus jejak-jejak buronan yang selama ini licin, jadi teknologi digital tetap menjadi tantangan tersendiri. Meskipun demikian seharusnya bangsa Indonesia memodifikasi kunci-kuncinya sehingga kita kuasai teknologi itu versi Indonesia dan tidak dapat di *lock* ketika berhadapan dengan lawan yang kebetulan menjadi pencipta alat tersebut. Ingat ketika F 16 berhadapan dengan Pesawat Hornet AS di pulau Bawean dan pesawat kita di *lock*.

Ada banyak biometrik yang dapat dipakai. Dari yang sudah disebut tadi, sidik jari paling banyak dipakai dalam sistem keamanan. Tinta untuk sidik jari sudah digunakan selama berabad-abad, dan di era digital sekarang sidik jari sudah didigitalisasikan. Sistem elektronik sudah modern menyaring bentuk melengkung *(loop)*, jerat (*arche*), dan lingkaran (*whorl*) dari seluruh jenis sidik jari konvensional ke dalam kode numerik. Parameter sidik jari jauh lebih banyak digunakan karena mudah dan murah. Sebagai gambaran, jika tahun 1998 pangsa pasar sidik jari baru 40 %, dua tahun kemudian meningkat menjadi 84 % (*International Biometrik Group*). [20]

Teknologi sidik jari (*finger scan*) dipertimbangkan sebagai salah satu produk biometrik untuk aplikasi dalam sistem jaringan perusahaan. Perusahaan teknologi menyatakan, kebanyakan telepon yang masuk ke meja operator (*help desk*) adalah meminta bantuan karena lupa *password*.

Biometrik yang terkenal lainnya, *hand geometry*. Tidak seperti pemindaian yang dikenal luas di AS dan Eropa Barat, sistem ini tidak distigmatisasikan oleh sebuah badan keamanan atau intelijen yang memiliki konsekuensi hukum. Produk ini melibatkan pemindaian bentuk, ukuran dan karakter lain (seperti ukuran jari dari sebagian atau keseluruhan tangan). Pemakai diwajibkan membuat beberapa klaim tentang siapa mereka dengan menggesekkan kartu sebagai contoh sebelum pemindaian.[21]

Contoh teknologi ini yang terkenal adalah program *inspass*. Penumpang yang sering terbang ke Amerika boleh melewati antrean di bagian keimigrasian di tujuh bandara besar dengan hanya menggesek sebuah kartu dan menempatkan tangan mereka di atas pemindai. Pemindainya dipasok oleh *Campbell*, California.

Sistem lain, pemindaian mata, dikenal dari cerita mata-mata. Serat-serat, alur, dan bintik-bintik pada selaput pelangi mata (bagian berwarna pada mata) dipindai menggunakan sebuah kamera vidio yang dapat memberikan informasi untuk mengenali seseorang. Tetapi sistem ini di mata pemakai lebih mengganggu

[20] *Op. Cit.*

[21] *Loc. Cit.*

dibandingkan dengan sistem sidik jari.

Meski begitu, sistem pemindaian mata ini telah dicoba sejumlah bank di Inggris, Jepang dan AS. Dengan teknologi ini, tidak diperlukan lagi kartu atau PIN untuk mengakses sebuah rekening. Maskapai AS juga sudah mencoba sistem ini dan dua bandara bagi pelanggan untuk memperoleh kartu penerbangannya. Ini salah satu upaya cegah aksi teroris masuk *via* Bandara sebagaimana terjadi pada serangan 11 September 2001.[22]

Biometri wajah juga bisa dipakai. Teknologi ini bekerja dengan menganalisis sebuah citra vidio atau fotografi dan mengidentifikasi posisi dari beberapa "titik pusat pertemuan" pada raut muka seseorang. Titik pusat pertemuan ini kebanyakan berada diantara dahi dan di atas bibir. Ekspresi maupun keberadaan rambut halus tidak berdampak terhadap analisisnya.

Identifikasi wajah punya kelebihan, yakni orang yang bersangkutan tidak merasa kalau wajahnya sedang dianalisa. Makanya, teknik ini dapat dikembangkan untuk mengetahui keberadaan seorang teroris, misalnya, yang sedang kasak-kusuk hendak beraksi di sebuah bandara. Atau untuk mengacau sebuah pertandingan sepak bola di lapangan dan penipuan di kasino.

Yang agak sulit dikembangkan adalah biometrik suara. Padahal teknologi ini murah biayanya, hanya memerlukan alat penganalisis karakter vokal seseorang (ingat kasus pembuktian rekaman beberapa tokoh oleh pakar multimedia RM. Roy Suryo). Akan tetapi keandalan produk ini rendah dibandingkan dengan produk biometrik lainnya, terutama ketika waktu untuk berbicara cuma sedikit.[23]

---

[22] Robyn Weisman, *Can Cyber-Intelligence Prevent Real-World Terrorism?*, Bookmark to del.icio.us, September 19 th, 2001 menyatakan : *After the tragic event (11 September), many in the intelligence community see a pressing need to make better use of so-called cyber-intelligence to track down enemy activity before future attack can occur. However, no ane has suggested that any combination of traditional intelligence and cyber-intelligence gathering can completely eliminate terrorist attacks*

[23] Roy Suryo sering menjadi saksi ahli dalam berbagai kasus digital. Rekaman adalah petunjuk, baru dapat dijadikan alat bukti setelah ada keterangan ahli. Di era digital sering terjadi animasi, dimana gambar seseorang dipotong dan diganti wajah lain, namun ini semua dapat dilacak jika memnag gambar itu palsu.

Mirip dengan suara adalah tanda tangan. Sistem ini berlandaskan pada teori grafologi bahwa tanda tangan mencerminkan karakter seseorang. Perangkat keras yang digunakan adalah *pen* dan sebuah *pad* untuk mengambil suatu tanda tangan. Tetapi teknologi ini akan bermasalah jika hanya bertumpu pada kebiasaan.

Sementara itu Amerika dan Irlandia telah meloloskan hukum untuk mengesahkan tanda tangan yang dibuat secara digital. Dengan peraturan ini sebuah tanda tangan digital punya kekuatan hukum yang sama dengan tanda tangan yang memakai tinta. Untuk mengatasi tercurinya tanda tangan digital, teknologi ini akan didampingi dengan teknologi biometrik lain, misalnya sidik jari. Dengan begitu sebuah tanda tangan dapat dikeluarkan jika hanya sidik jari pemiliknya ditampilkan.

Di era digital persyaratan sosok intelijen dituntut memiliki nilai tambah berupa ketajaman intelektual serta mobilitas, inovasi dan adaptasi pemikiran yang ditunjang oleh peralatan yang memadai.[24]

Ruth David, mantan Direktur Science dan Teknologi CIA mengatakan *"Technology is only one component. Without supporting policy, effective processes and well trained people, technologies solve nothing. Deployment of facial recognition technologies at border entry point will not ensure apprehension of terrorist."* [25]

Sementara Bill Crowell, mantan Deputy Director of the Supersecret National Security Agency AS menyatakan *"The battle for improved homeland security involves both technology and processes. Technology can be used to make the processes more efficient, predictable and effective."* [26]

Di lain pihak Howard Schmidt, *the Deputy Chairman of the President's Critical Infrastructure Protection Board* menyatakan *"recently that the next national plan for protecting the country critical system and networks will be written with the help of the private sector"*. [27]

Di era digital diperlukan orang-orang

---

[24] Elex Dinuth, *Op. Cit.*, hlm. 4

[25] *Outflanking The Cyberterrorist Threat*, http://www.computerworld.com/

[26] *Loc. Cit.*

[27] *Ibid.*

yang terlatih secara baik, sebab teknologi hanyalah komponen belaka. Dan dengan teknologi maka lebih efesien, efektif dan dapat diramalkan segala sesuatunya. Intelijen memerlukan kemampuan untuk memberikan *early warning, problem solving* dan *forcasting*. Di era digital kemampuan pengawakan teknologi juga perlu orang orang yang mampu memodifikasi termasuk mengubah kunci-kunci sehingga tidak mudah bocor atau disadap. Di sinilah diperlukan keunggulan personil untuk tidak hanya sebagai pengguna tetapi memodifikasi dan mengubah kunci-kunci. Pelibatan swasta dalam pengembangan berbagai modifikasi sangat diperlukan guna mempercepat proses inovasi teknologi.

Ryan Russel, seorang analis kemanan AS yang menguraikan tentang berbagai tragedi di belahan dunia menyatakan bahwa selama ada individu-individu yang memaksakan kehendak dengan tanpa menghormati hak hidup pihak lain maka selama itu pula akan ada ancaman. Ketika seseorang membicarakan pencegahan terhadap serangan di masa datang, mereka akan membicarakan tentang skala / jangkauan serangan itu. Tujuan nyata pencegahan dari serangan lainnya adalah dengan cara mengukur tempat tempat yang mungkin dijadikan target serangan.[28] Kenyataan ini menunjukkan bahwa tantangan di era digital makin berat, tugas ke depan perlu profesionalisme yang tinggi, sesuatu yang sering dipinggirkan karena kepentingan politik. Inilah yang sering menjadi penghambat kemajuan suatu bangsa dalam melakukan *early warning, problem solving* dan *forecasting*.❑

[28] Roby Weisman, *Op. Cit.*, hlm. 1

Etika Profesi Intelijen
(suatu tinjauan psikologi intelijen)

Sartomo.S

Pendahuluan

Pengkhianatan atau pelanggaran terhadap etika moral intelijen dilakukan oleh seorang anggota intelijen Amerika Serikat (AS) dengan initial "JW" beberapa tahun lalu. Sewaktu ada keinginan pemerintah Amerika Serikat (AS) di bawah Jimmy Carter untuk membebaskan sandera warga Amerika Serikat (AS) di Iran ternyata mengalami kegagalan walau pun pemerintah telah menyiapkan sekitar 5000 pasukan. Rencana itu dibatalkan karena satelit mata-mata AS mendeteksi adanya 22 devisi tentara Uni Soviet sedang bergerak menuju Iran. Kemudian diketahui bahwa rencana rahasia AS tersebut telah dibocorkan kepada pihak Uni Soviet oleh "JW" dengan cara menjual kunci persandian sehingga Uni Soviet dengan mudah membuka rencana rahasia AS. Selanjutnya Ray Mc Govern seorang purnabakti anggota Badan Intelijen AS (CIA) mengatakan bahwa ada sementara anggota-anggota intelijen dari CIA sudah tidak lagi memiliki etika moral intelijen sama sekali, keadaan ini mendorong para purnabakti membentuk gerakan yang disebut dengan