KEPUTUSAN AMERIKA SERIKAT MELUNCURKAN *CYBER ATTACK* TERHADAP REAKTOR NUKLIR DI IRAN TAHUN 2009

(THE DECISION OF UNITED STATES OF AMERICA'S CYBER ATTACK ON IRAN'S NUCLEAR REACTOR IN 2009)

SKRIPSI

Disusun Untuk Memenuhi Persyaratan Menuju Gelar Strata Satu (S1)
Jurusan Ilmu Hubungan Internasional Universitas Jember

Oleh :

Adrian Sujiwo M

100910101044

JURUSAN ILMU HUBUNGAN INTERNASIONAL
FAKULTAS ILMU SOSIAL DAN ILMU POLITIK
UNIVERSITAS JEMBER
2017

PERSEMBAHAN

Skripsi ini saya persembahkan untuk :

1. Kedua orang tua saya, Sri Mulatsih dan Luhut Malauphase;
2. Guru – guru, pendidik, dan pengajar sejak taman kanak – kanak hingga perguruan tinggi;
3. Almamater jurusan Ilmu Hubungan Internasional Fakultas Ilmu Sosial dan Ilmu Politik Universitas Jember.

MOTTO

“Seseorang dengan semangat hidup mampu menanggung segala beban kehidupan.”

(Friedrich Nietzsche)

SKRIPSI

KEPUTUSAN AMERIKA SERIKAT MELUNCURKAN *CYBER ATTACK* TERHADAP REAKTOR NUKLIR DI IRAN TAHUN 2009

Oleh

Adrian Sujiwo. M

100910101044

Pembimbing :

Dosen Pembimbing Utama : Drs.Muhammad Nur Hasan ,M.Hum

Dosen Pembimbing Anggota : Drs.Abubakar Eby Hara MA,Ph.D

RINGKASAN

Pada tahun 2009 telah terjadi kerusakan pada mesin pengolah pada beberapa reaktor nuklir yang ada di Iran. Laporan – laporan dari para teknisi keamanan di Iran menyatakan bahwa sebuah program komputer tak teridentifikasi yang didesain secara khusus untuk merusak reaktor nuklir telah menyusup ke dalam sistem jaringan pengendali sehingga mengacaukan kinerja mesin di dalamnya. Beberapa tahun setelah insiden tersebut terjadi muncul laporan – laporan serta pernyataan – pernyataan resmi dari tokoh – tokoh keamanan hingga figur politik dari Amerika Serikat yang menyatakan bahwa negara Amerika Serikat yang menjadi dalang dibalik serangan tersebut. Mereka menjuluki program tersebut dengan nama *Stuxnet*. Amerika Serikat mengakui bahwa *cyber attack* itu didasari atas ketakutan utama mereka terhadap kapabilitas Iran dalam mengembangkan energi nuklir yang berpotensi akan menjadi ancaman terhadap keamanan Amerika Serikat dan negara lain di masa depan.

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR SINGKATAN

1. AS = Amerika Serikat
2. CIA = Central Intelligence of America
3. DoS = Denial of Service
4. IAEA = International Atomic Energy Agency
5. MIX = Molybdenum, Iodine dan Xenon
6. NSA = National Security Agency
7. OOG = Operation Olympic Games
8. PBB = Perserikatan Bangsa - Bangsa
9. SQL = Structured Query Language
10. Usstratcom = United States Strategic Command
11. XSS = Cross Site Scripting

BAB I. PENDAHULUAN

1.1 Latar Belakang

Pesatnya kemajuan teknologi informasi di zaman sekarang ini telah menciptakan perubahan yang signifikan dalam kehidupan masyarakat modern. Laju pertumbuhan penyedia layanan telekomunikasi dan infrastruktur serta dukungan perangkat keras – perangkat lunak yang kian canggih mendukung gaya hidup manusia masa kini yang haus akan kebutuhan informasi , berita , dan pengetahuan lainnya yang kini bisa diakses dalam hitungan detik. Efek dari pesatnya kemajuan teknologi informasi ini tak terkecuali dirasakan oleh negara sekelas Iran yang kini memanfaatkan kemajuan teknologi informasi sebagai penunjang salah satu infrastruktur terbesar mereka. Infrastruktur pengembangan energi nuklir yang telah eksis paska era perang dingin di negara tersebut telah mengalami berbagai peningkatan kinerja dan fasilitas yang kini menggunakan bantuan jaringan teknologi informasi dalam memonitor sekaligus mengendalikan pengelolaan kegiatan di dalamnya.

Berbicara mengenai pengembangan energi nuklir , kapabilitas negara Iran dalam mengembangkan energi nuklir telah menjadi sorotan negara – negara besar , terutama negara adidaya. Terhitung hingga saat inipun pengembangan energi nuklir Iran merupakan salah satu isu politik internasional yang tak pernah selesai dibahas dan selama beberapa tahun terakhir ,beberapa upaya ditempuh untuk melucuti kemampuan Iran dalam mengembangkan nuklir mereka. Alasan terbesar yang menjadikan program pengembangan nuklir ini menjadi sorotan adalah sikap dari pemerintah Iran yang kerap tidak mengikuti permintaan dan prosedur dari negara - negara lain dan juga Perserikatan Bangsa – Bangsa (PBB) terkait cara mereka dalam menyikapi pengembangan energi nuklir. Sikap Iran ini lantas menimbulkan paranoid bagi negara – negara penentang mereka yang menganggap bahwa secara diam – diam Iran mengembangkan senjata nuklir hingga ketakutan akan kebocoran program nuklir di masa depan yang akan membawa dampak

negatif bagi lingkungan secara global. Ketakutan tersebut semakin menguat dan menjadi perbincangan hangat di tahun 2002 ketika tercuatnya berita resmi mengenai terkuaknya lokasi reaktor nuklir di Natanz , salah satu kota di Iran , yang aktif mengolah bahan uranium di daerah tersebut. Hal tersebut lantas mengundang perhatian dari *International Atomic Energy Agency (IAEA)* dikarenakan reaktor nuklir yang dibangun tersebut merupakan salah satu reaktor pengembangan energi nuklir yang tidak terdaftar secara resmi dalam daftar proyek reaktor nuklir di negara tersebut[1]. Hasil dari penemuan tersebut lantas membuat Iran masuk dalam radar pengawasan *IAEA* untuk beberapa tahun kedepannya. Hal ini lantas berujung pada peristiwa di tanggal 23 Desember tahun 2006 , dimana PBB memberikan ultimatum bagi negara – negara dunia untuk menghentikan kerja sama terkait suplai material dan bantuan teknologi yang dibutuhkan oleh Iran dalam proyek pengembangan energi nuklir mereka[2]. Menyusul dua tahun kemudian ; di tahun 2008 ; Amerika Serikat mengeluarkan larangan bagi seluruh bank yang ada di negaranya untuk tidak memproses setiap transaksi perbankan yang berhubungan dengan kegiatan ekonomi negara Iran[3]. Kedua langkah yang ditempuh tersebut bertujuan untuk melemahkan Iran secara perlahan dan berharap agar mereka menghentikan proses pengembangan energi nuklir. Namun pada akhirnya sanksi - sanksi yang dijatuhkan kepada Iran tidak membuahkan hasil karena pada akhirnya Iran tidak berhenti mengembangkan nuklir mereka. Mereka bahkan mampu mensukseskan siklus pengembangan energi nuklir dan program – program lain yang berhubungan dengan pengembangan energi nuklir terlepas bahwa mereka telah mendapatkan sanksi ekonomi. Fakta tersebut menjadi inspirasi bagi pihak Amerika Serikat untuk diam – diam membuat rencana untuk melemahkan program energi Iran melalui jalur *backdoor* yang digagas di masa pemerintahan Presiden George W. Bush di tahun 2006. Proyek yang diberi nama *Operation Olympic Games* (OOG) tersebut memfokuskan pada pengembangan senjata digital yang berfungsi untuk merusak sistem teknologi reaktor nuklir Iran

[1] David Albright , et al. 2015. *"Iran's Nuclear Program"* diakses dari http://iranprimer.usip.org/resource/irans-nuclear-program pada 5 Januari 2017.
[2] Kenneth Kazman , "*Iran Sanctions*", *Congressional Research Service*, Januari 2017, hal. 31.
[3] Ibid , hal. 8

secara efektif. Proyek ini berujung kepada pembuatan program *Stuxnet* , sebuah malware dengan ukuran 500 *kilobyte* yang hendak disebar ke dalam jaringan komunikasi digital negara Iran dengan memanfaatkan celah keamanan jaringan internet / intranet yang terkoneksi dengan fasilitas reaktor nuklir yang ada[4]. Pengembangan *malware* ini membutuhkan waktu pengembangan yang cukup lama dan terselesaikan dalam waktu tiga tahun. Senjata ini selesai pada masa awal terpilihnya Presiden Barrack Obama dan akhirnya dilepaskan pada negara sasaran yaitu Iran. Memasuki akhir 2009, reaktor nuklir di Natanz , provinsi Isfahan melaporkan bahwa sistem sentrifugal pengolah uranium di reaktor tersebut mengalami kerusakan yang disebabkan kesalahan pada penanganan sistem[5]. Ketika para teknisi keamanan jaringan diturunkan , mereka menemukan jejak *malware* yang menghinggapi sistem operasi komputer yang digunakan dalam mengontrol kegiatan reaktor tersebut. Mereka beranggapan bahwa celah dalam transfer data baik melalui sirkulasi jaringan internet maupun intranet yang terhubung dengan reaktor telah dimanfaatkan sebagai sarana penyebaran *malware*. Kejadian ini lantas mendapat tanggapan serius dari presiden menjabat saat itu , Mahmoud Ahmadinejad , yang mengeluarkan klarifikasi mengenai serangan *malware* yang merusak reaktor nuklir tersebut.

Kasus di atas menunjukkan Amerika Serikat adalah pihak yang secara langsung bertanggung jawab atas *cyber attack* yang merusak reaktor nuklir di Iran. Beberapa pihak yang terlibat langsung dalam kegiatan pertahanan Amerika Serikat memaparkan beberapa fakta yang membuktikan bahwa kegiatan yang dilakukan pada reaktor nuklir di Iran tersebut sungguh dilakukan atas inisiatif pemerintahan Amerika Serikat. Seorang pakar keamanan yang membocorkan informasi penyadapan komunikasi yang dilakukan oleh *National Security Agency (NSA)* di tahun 2013 yang bernama Edward Snowden mengungkapkan bahwa

[4] Michael Holloway. 2015. "*Stuxnet Worm Attack on Iranian Facilities*" diakses dari http://large.stanford.edu/courses/2015/ph241/holloway1/ pada 3 Januari 2017.
[5] Joby Warrick. 2011. "*Iran's Natanz Nuclear Facility Recovered Quickly From Stuxnet Cyberattack*" diakses dari http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html pada 3 Januari 2017.

malware Stuxnet merupakan produk kerja sama dengan pakar teknologi Israel[6]. Pernyataan tersebut diperkuat dengan adanya pengakuan lain yang diungkapkan oleh Jenderal James E. Cartwright, mantan anggota *United States Strategic Command (USSTRATCOM)* dan Wakil Kepala Staff Gabungan Amerika Serikat yang menjabat di masa pemerintahan presiden George W. Bush dan awal pemerintahan presiden Barrack Obama. Jenderal Cartwright menyatakan bahwa *Stuxnet* merupakan bagian dari proyek OOG dan juga mengakui bahwa dirinya terlibat langsung dalam tim perancang konsep *Stuxnet* dan menawarkan prototip awal senjata digital tersebut kepada presiden George W. Bush[7].

Dari kasus inilah penulis menganggap bahwa motif Amerika Serikat saat itu untuk menciptakan senjata alternatif untuk menyerang Iran melalui jalur *cyber* yang belum pernah ditempuh sebelumnya menjadi pokok bahasan yang menarik untuk diteliti lebih lanjut dalam suatu karya tulis ilmiah dengan judul **Keputusan Amerika Serikat Meluncurkan *Cyber Attack* Terhadap Reaktor Nuklir Iran di Tahun 2009.**

1.2 Ruang Lingkup Pembahasan

Dalam meneliti suatu fenomena Hubungan Internasional yang terjadi di dunia maka diperlukan batasan dalam ruang lingkup pembahasan. Batasan yang ditentukan adalah hal yang diperlukan agar pembahasan yang sedang diteliti tidak berkembang luas atau *out of topic* dari topik utama. Penulis membagi pembatasan dalam batasan materi dan batasan waktu.

---

[6] Graham Cluley. 2012. **"***Stuxnet: How USA and Israel created anti-Iran virus, and then lost control of it*" diakses dari https://nakedsecurity.sophos.com/2012/06/01/stuxnet-usa-israel-iran-virus/ pada tanggal 3 Januari 2017.

[7] Ron Rosenbaum. 2012. "*Richard Clarke On Who Was Behind The Stuxnet Attack*" diakses dari http://www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-160630516/?page=2 pada tanggal 3 Januari 2017.

1.2.1 Batasan Materi

Bahasan penelitian akan difokuskan pada analisis data – data terkait kepada faktor - faktor yang mendorong Amerika Serikat dalam menggagas dan mengeksekusi *cyber attack* terhadap reaktor nuklir di Iran 2009. Selain itu penulis juga akan membahas hal – hal teknis bagaimana serangan tersebut bisa terjadi serta bagaimana dampaknya ketika serangan dilakukan.

1.2.2 Batasan Waktu

Penulis membatasi data – data yang diambil dan diolah untuk penelitian ini dalam rentang waktu tahun 2006 hingga tahun 2009. Walau demikian penulis juga mengambil beberapa data yang terdapat dalam rentang waktu di luar batasan yang ditetapkan untuk memastikan adanya hubungan dari data – data yang didapatkan. Adapun pada tahun 2006 adalah waktu dimana Presiden George W. Bush pertama kali memikirkan gagasan senjata digital untuk menyerang reaktor nuklir Iran dari dalam. Sedangkan pada tahun 2009 adalah awal kepemimpinan Presiden Barrack Obama yang meneruskan program yang telah dikerjakan oleh mantan Presiden Bush dalam 3 tahun tersebut. Pada tahun tersebut pula senjata yang telah diselesaikan tersebut akhirnya diluncurkan pada negara sasaran mereka , Iran.

1.3 Rumusan Masalah

Berdasarkan latar belakang yang di atas , maka penulis mengangkat pokok permasalahan penelitian yang difokuskan kepada rumusan masalah dengan pertanyaan – pertanyaan berikut :

1.Bagaimana Amerika Serikat Melakukan *Cyber Attack* Terhadap Reaktor Nuklir di Iran pada tahun 2009?

2. Apakah yang menjadi motif dibalik serangan tersebut?

1.4 Tujuan Penelitian

Dengan mengangkat topik tersebut sebagai penelitian , penulis bertujuan untuk mencari tahu apa saja yang menjadi *concern* Amerika Serikat hingga mereka memikirkan suatu cara yang sebelumnya belum pernah ditempuh siapapun untuk merusak energi nuklir Iran dari dalam di tahun 2009. Selain itu , penulis berpendapat bahwa dengan mengetahui bagaimana suatu serangan bisa dilakukan akan didapatkan gambaran bagaimana konsep *cyber war* dilakukan dan mengapa hal seperti ini bisa menjadi ancaman serius bagi setiap negara.

1.5 Kerangka Teori

Kerangka teori diperlukan dalam penulisan karya tulis ilmiah sesuai dengan kebutuhan topik yang sedang menjadi fokus penelitian. Kerangka teori digunakan oleh penulis sebagai sarana dalam menganalisis sekaligus menjawab permasalahan yang dihadapi. Dasar dari argumen topik penelitian ini memakai teori utama dari Barry Buzan yakni teori keamanan non-tradisional.

1.5.1 Teori Keamanan Non-Tradisional

Barry Buzan mendeskripsikan keamanan adalah situasi dimana tidak ada perasaan terancam , tidak ada rasa takut akan adanya serangan terhadap suatu nilai[8]. Kemudian lebih lanjut dalam teorinya mengenai keamanan non-tradisional, Barry Buzan mendeskripsikannya dalam pernyataan berikut :

"Non-traditional issues of security reflects post-Cold War changes in the threat environment, particularly globalization's impact in creating new risks, threats and vulnerabilities for states and people, to which governments must now respond."[9]

Pada pernyataan tersebut Buzan berpendapat bahwa konsep keamanan non-tradisional tidak lagi menyangkut mengenai isu klasik pada negara saling

[8] Barry Buzan ,et al. 1998. *Security : A New Framework for Analysis.* Lynne Rienner Publishers, Inc. Hlm.10

[9] Barry Buzan. 2009. *People , States, and Fear Second Edition : An Agenda for International Security Studies In The Post Cold-War Era.* ECPR Press. Hlm.40

memperkuat kekuatan militer sebagai kekuatan utama mereka. Buzan menekankan bahwa paska perang dingin terdapat ancaman – ancaman baru pada beberapa sektor yang akan menimbulkan masalah di masa depan. Ancaman – ancaman baru yang disebutkan dalam tulisan Buzan tersebut lantas membawa penulis pada beberapa konsep yang menjadi topik pembahasan dalam studi keamanan non-tradisional. Dalam hal ini terdapat tiga konsep yakni *cyber security, nuclear deterrence,* dan *pre-emptives war.*

a. Cyber Security

Cyber security mengacu pada konsep keamanan digital yang merupakan produk dari inovasi teknologi informasi yang muncul pada awal era 1990-an terkait jaringan komunikasi antar perangkat komputer[10]. Keamanan digital berfokus pada keamanan informasi – informasi yang telah terekam maupun yang hendak terjadi di antara perangkat komunikasi digital. Isu dalam keamanan digital merupakan *cyber attack* atau serangan yang memanfaatkan celah digital untuk meretas , merusak , ataupun memanipulasi informasi – informasi yang tersimpan dalam perangkat komunikasi yang digunakan oleh penggunanya. Ancaman ini menjadi isu serius dalam zaman modern seperti sekarang dikarenakan seiring berjalannya waktu bukan hanya individu yang merupakan pengguna yang menjadi sasaran dalam *cyber attack* , namun keamanan negara kini perlu diperhatikan sebab tak sedikit kegiatan komunikasi dan pertukaran data penting yang melibatkan kepentingan negara terjadi menggunakan kemudahan teknologi yang semakin berkembang. Kemudahan teknologi dalam transfer informasi secara teknis juga memungkinkan mudahnya seseorang dalam melakukan *cyber attack* terhadap suatu organisasi maupun individu.

[10] Lene Hansen dan Helen Nissenbaum. 2009. *Digital Disaster, Cyber Security , and Copenhagen School.* International Studies Association. Hlm.1

b. *Nuclear Deterrence*

Ancaman senjata nuklir di era perang dingin sejatinya adalah isu dalam teori keamanan tradisional. Dalam perkembangan studi keamanan internasional , *nuclear deterrence* terbagi dalam empat fase. Fase pertama muncul tepat di awal era perang dingin dimulai ketika negara – negara menyadari ancaman nuklir sebagai senjata ancaman terkuat yang sewaktu – waktu dapat menghancurkan siapapun. Fase kedua muncul pada saat perang dingin sedang berlangsung dan mendekati akhir , di mana pada fase ini muncul konsep bahwa senjata nuklir dapat digunakan untuk saling menakuti satu sama lain. Fase ketiga adalah ketika perang dingin memasuki akhir dimana teori mengenai *nuclear deterrence* muncul dan dipelajari lebih mendalam dan negara – negara memikirkan bagaimana untuk menangani masalah serupa ketika hal seperti ini muncul nantinya di masa mendatang. Fase yang terakhir adalah penelitian mengenai *nuclear deterrence* dan ancaman – ancaman baru yang bermunculan paska perang dingin yang menjadi isu dalam keamanan non-tradisional[11]. Ancaman nuklir dalam keamanan non-tradisional kini bukan hanya mengenai bagaimana nuklir digunakan sebagai senjata untuk melawan satu sama lain namun membahas mengenai efeknya bagi lingkungan. Hal ini dibahas dalam salah satu sektor , yakni sektor lingkungan , yang menjadi fokus keamanan modern oleh Buzan. Dalam kasus Amerika Serikat kepada Iran yang diangkat oleh penulis , selain Amerika Serikat merasa terancam atas potensi pengembangan energi nuklir Iran yang sewaktu – waktu dapat disalahgunakan baik oleh pihak Iran atau aktor lain sebagai senjata melawan mereka , AS juga menakuti akan adanya potensi kerusakan lingkungan yang ditimbulkan apabila Iran tidak bertanggung jawab atas kegiatan pengembangan nuklir yang dilakukan.

[11] Frans-Paul Van Der Putten , Minke Meijnders , dan Jan Rood. 2015. *Deterrence as a security concept against non- traditional threats.* Clingendael , Netherlands Institute of International Relations.

c. *Pre-emptive war*

Konsep *pre-emptive war* adalah serangan atau 'perang' yang dilancarkan atau dideklarasikan oleh individu , organisasi , maupun negara pada pihak tertentu guna membasmi atau mencegah ancaman yang diduga berpotensi menjadi pemicu timbulnya perang yang sesungguhnya di masa yang akan datang[12]. Serangan yang dilakukan oleh Amerika sebagaimana yang dibahas oleh penulis dalam karya tulis ini merupakan bentuk dari *pre-emptive war* dikarenakan apa yang telah mereka lakukan diakui sebagai tindakan preventif.

1.6 Argumen Utama

Karya tulis ilmiah hendaknya memiliki argumen utama sebagai jawaban dari rumusan masalah yang dibuat berdasarkan kerangka teori yang digunakan. Pada argumen utama ini , penulis menjelaskan permasalahan yang dibahas sebagai karya ilmiah yang akan diteliti lebih jauh. Adapun berdasarkan latar belakang serta teori dan konsep – konsep yang telah disebutkan sebelumnya , maka penulis mengemukakan argumen utama seperti ini.

Keputusan Amerika Serikat ketika menyerang reaktor nuklir di Iran pada tahun 2009 dilihat melalui teori keamanan non-tradisional : Serangan yang diluncurkan oleh Amerika Serikat kepada sistem jaringan reaktor nuklir di Iran dilakukan melalui jalur digital dan tidak benar – benar melibatkan 'perang' secara langsung seperti yang digambarkan dalam teori keamanan tradisional. Tindakan yang diakui sebagai serangan preventif ini menjadi tindakan yang membuktikan bahwa dalam era keamanan modern, AS telah melihat celah keamanan teknologi informasi sebagai isu keamanan modern yang tak kalah penting untuk dimanfaatkan sebagai alat untuk memenuhi kepentingan mereka , yakni menakut – nakuti suatu pihak yang dianggap menjadi ancaman potensial bagi mereka.

[12] Louis Rene Beres. 1992. *On Assassination as Anticipatory Self-Defense: The Case of Israel.* 20 Hofstra L. Rev. 321. Hlm.20.

1.7 Metode Pengumpulan Data

Data yang digunakan oleh penulis dalam penyusunan karya ilmiah ini didapatkan melalui data – data non-primer yang telah diteliti secara tidak langsung dari sumber data yang ada. Hal tersebut kurang lebih dikarenakan keterbatasan dari penulis dalam mengumpulkan data – data penelitian yang bersumber langsung dari sumber data yang dibutuhkan. Data – data yang dikumpulkan oleh penulis didapatkan melalui buku – buku dari perpustakaan , artikel dari majalah / tabloid dan surat kabar , jurnal ilmiah , dan beberapa data-data elektronik dari situs – situs resmi lembaga telekomunikasi , lembaga pertahanan , lembaga pengembangan energi terbarukan serta beberapa lembaga penelitian lainnya yang masih memiliki keterkaitan dengan penelitian yang diangkat oleh penulis. Adapun penulis mengumpulkan data – data penelitian melalui :

1. Perpustakaan Pusat Universitas Jember
2. Perpustakaan FISIP Universitas Jember
3. Media cetak
4. Situs – situs internet
5. Koleksi pribadi

1.8 Metode Analisis Data

Dalam mengkaji permasalahan yang diangkat oleh penulis , penelitian ini memakai teknik penelitian kualitatif. Dalam upaya mendapatkan hasil penelitian yang lebih optimal dan komprehensif , penulis memakai metode deduktif , dimana pernyataan – pernyataan yang sifatnya umum akan dikumpulkan dan dikaji sebagai kesimpulan. Kesimpulan tersebut berasal dari berbagai pengumpulan data – data dan hasil analisis data empiris yang nantinya akan diuji kebenarannya oleh penulis. Fakta dari data yang ditemukan akan dikumpulkan menjadi kesimpulan tentang bagaimana dan mengapa Amerika Serikat menggunakan *cyber attack* terhadap reaktor nuklir di Iran pada tahun 2009.

1.9 Sistematika Penulisan

BAB I. Pendahuluan

Berisikan latar belakang , pembahasan , rumusan masalah , kerangka teori , argumen utama , metodologi penelitian dan sistematika penulisan.

BAB II. *Cyber Attack* dan *Stuxnet*

Berisikan pengertian mengenai konsep *cyber attack* dan sekaligus membahas mengenai pembuatan dan mekanisme *Stuxnet* yang menjadi sorotan dalam kasus Amerika Serikat terhadap Iran yang dibahas dalam karya tulis ini.

BAB III. Peran Perkembangan Teknologi Informasi Terhadap Program Pengembangan Energi Nuklir Iran

Penulis meneliti tentang aspek teknologi yang digunakan dalam program energi nuklir di Iran dan bagaimana teknologi informasi berperan di dalamnya.

BAB IV. Pembahasan.

Penulis menjabarkan analisa mengenai bagaimana cara Amerika Serikat melakukan *cyber attack* yang merusak kinerja sistem jaringan reaktor nuklir di Iran pada tahun 2009 dan mengapa mereka melakukan serangan tersebut.

BAB V. Kesimpulan

Berisikan kesimpulan dari karya ilmiah ini.

BAB II

CYBER ATTACK DAN *STUXNET*

II.1 Konsep *Cyber Attack*

Ketika pertama kali diperkenalkan sebagai konsep jaringan komunikasi digital di tahun 1990 , internet merupakan realisasi dari konsep dimana manusia dapat saling berinteraksi dalam waktu yang relatif cepat dan tidak terbatas ruang dan jarak. Pesatnya pertumbuhan internet dari masa ke masa telah menciptakan banyak inovasi yang terbukti telah membantu kebutuhan manusia dari segala penjuru dunia. Salah satu dari buah pertumbuhan internet yang sampai sekarang tak luput dari perhatian manusia modern adalah semakin cepat dan mudahnya bagi antar pengguna untuk saling bertukar dan mengakses informasi , terlepas dari mana mereka berasal dan seberapa jauh jarak mereka. Pada saat ini , kemudahan aksesibilitas yang ada telah mengantarkan manusia pada level di mana setiap keputusan dan kendali manusia bisa dikendalikan hanya melalui beberapa perintah dalam suatu perangkat elektronik. Semua interaksi dilakukan secara terkakulasi demi kenyamanan pengguna.

Namun seiring dengan nikmatnya kemudahan dan kecepatan yang ditawarkan , jaringan komunikasi digital tak luput pula dari sasaran para pengguna – pengguna akses digital yang memiliki niatan untuk kepentingan tertentu. Mereka memanfaatkan celah keamanan yang terdapat dalam jaringan digital yang umumnya tidak diketahui oleh para pengguna – pengguna awam. Serangan yang ditujukan kepada siapapun pengguna yang menggunakan fitur akses teknologi komunikasi digital ini disebut sebagai *cyber attack.* Pada awal ketika komunikasi digital ditemukan, hanya sedikit sistem yang terhubung melalui jaringan dan hanya membutuhkan sedikit sekali individu yang terlatih dalam keamanan jaringan untuk mengelola dan mengamankan kegiatan yang melibatkan koneksi jaringan. Semakin bertambahnya tahun dan kebutuhan masyarakat akan

jaringan komunikasi digital, jumlah ahli keamanan yang dibutuhkan justru menurun, Ditambah dengan semakin banyaknya varian perangkat keras yang mampu terhubung dengan jaringan komunikasi digital, seharusnya semakin dibutuhkan pula individu – individu yang memahami seluk beluk kinerja dan keamanan sistem yang terhubung dari perangkat – perangkat yang berbeda.

Lebih lanjut , *cyber attack* didefinisikan sebagai tindakan penyerangan yang berpotensi dilakukan oleh individu , organisasi khusus , institusi resmi , hingga negara yang mengincar jaringan sistem informasi , infrastruktur , atau perangkat digital apapun yang dapat menjadi sarana komunikasi di dunia maya dengan tujuan mencuri / merusak / memanipulasi data – data yang terdapat di sana[13]. Tujuan dari para pelaku *cyber attack* bisa bermacam – macam , mulai dari sekedar kejahatan iseng , balas dendam personal, hingga yang lebih berat seperti kampanye gelap , mempromosikan gerakan radikal atau yang berhubungan dengan terorisme , ataupun mencuri / merusak / memanipulasi suatu data yang diyakini dapat melemahkan pihak tertentu dan memperkuat pihak yang lain[14]. Ada beberapa jenis *cyber attack* yang dapat diidentifikasi[15] :

1. *Malware*

Malware merupakan program atau aplikasi perusak yang dibuat dari bahasa pemrograman yang bervariasi. Program ini dibuat dengan tujuan menyerang perangkat atau sistem operasi yang telah dijadikan sasaran dengan tujuan mengambil alih perangkat / sistem operasi tersebut, merusak stabilitas kinerjanya, merekam sandi rahasia ataupun aktifitas yang dilakukan oleh pengguna dalam perangkat mereka, hingga mengirimkan data – data penting yang dimiliki di dalam perangkat / sistem tersebut kepada koordinat penyerang melalui jaringan yang terkoneksi dengan internet / intranet. *Malware* juga dapat disamarkan sebagai aplikasi maupun format dokumen

[13] Scott W.Beidleman. 2009. *Defining and Deterring Cyber War.* U.S Army War College, Carlisle Barracks. Hlm.2
[14] Ibid. Hlm.11
[15] David A. Wheeler, et al. 2003. *Techniques for Cyber Attack Attribution.* Institute for Defense Analysis. 4850 Mark Center Drive,Alexandria, Virginia. Hlm.9

lain yang kerap kita gunakan dalam kegiatan sehari – hari sehingga tidak menimbulkan kesan dan kecurigaan bahwa perangkat / sistem operasi yang sedang kita gunakan sebenarnya sedang dalam bahaya. Sebuah *malware* dapat disebar baik melalui jaringan yang saling terhubung antar perangkat pengguna ataupun menggunakan akses dari media yang memiliki fitur penyimpanan data yang terhubung dalam suatu perangkat.

2.*Phising*

Phising merupakan jenis serangan dimana penyerang memalsukan tautan yang biasa dikirim melalui email ataupun melalui aplikasi pengirim pesan lainnya yang biasa digunakan dalam perangkat digital yang ada. Pesan yang ada biasanya dipalsukan seolah – olah dikirim oleh seseorang atau organisasi yang punya hubungan dengan kita dan diberi keterangan seolah – olah tautan tersebut berisi hal yang penting untuk dibaca. Ketika seorang pengguna membuka tautan palsu tersebut maka Ia membuka akses bagi penyerang untuk mencuri data – data penting yang dimiliki oleh pengguna yang terjebak tersebut melalui celah tautan.

3.SQL Injection Attack

Structured Query Language (SQL) adalah bahasa pemrograman yang lazim digunakan sebagai basis untuk membuat dan mengelola *database* yang digunakan oleh *server* yang menjalankan layanan atau situs yang diakses oleh banyak orang. Pada umumnya *database* tersebut mengelola data – data pribadi para pengguna dan mengelola sebuah layanan yang spesifik bagi mereka yang membutuhkannya baik melalui intranet ataupun internet. *SQL injection attack* atau serangan injeksi *SQL* mengacu pada kode yang dibuat kompleks oleh suatu penyerang yang mengincar celah dalam *server* berbasis *SQL*. Ketika celah tersebut mampu dieksploitasi maka penyerang mampu mencuri data – data penting yang tersimpan di dalam *database*.

3.***Cross-site Scripting (XSS)***

Sebagaimana pada *SQL injection attack* yang disebutkan di atas , *Cross-site scripting* memanfaatkan celah pada bahasa pemrograman yang digunakan dalam suatu jaringan. Yang membedakannya dari *SQL injection attack* adalah *XSS* tidak mengincar *server* namun mengincar jaringan secara langsung dan hanya akan menyerang saat pengguna menggunakan jaringan. Dalam hal ini , *XSS* lebih mengacu pada serangan yang melibatkan pengguna internet yang kerap mengakses informasi melalui situs – situs yang mereka kunjungi.

4.*Denial of Service (DoS) Attack.*

Setiap jaringan yang menangani koneksi antar pengguna memiliki batas akses yang memperbolehkan *data traffic* atau pertukaran data dalam jumlah tertentu. Hal tersebut untuk memastikan kapasitas *server* yang menangani pertukaran data antar pengguna yang ada mampu beroperasi secara optimal setiap saat. *Denial of Service* merupakan serangan yang memanfaatkan limitasi tersebut. Serangan ini dilakukan dengan cara membanjiri kuota akses data dalam suatu jaringan dengan terus – menerus mengirimkan pertukaran data melebihi kapasitas optimal yang mampu ditangani oleh *server* yang mengelola jaringan. Ketika serangan tersebut berhasil melumpuhkan *server* maka seluruh akses menggunakan jaringan yang dituju akan berhenti secara total dan praktis menghentikan segala aktifitas pengguna yang menggunakan akses jaringan tersebut.

5.*Session Hijacking*

Session hijacking atau pembajakan sesi merupakan serangan yang memanfaatkan celah waktu yang digunakan ketika pertukaran informasi atau data antara pengguna yang terhubung melalui suatu jaringan sedang terjadi. Celah waktu ini disebut *session* dan ketika proses tersebut terjadi , data – data atau informasi pribadi / penting yang dimasukkan oleh pengguna menjadi

'terbuka' untuk beberapa saat dan di sinilah penyerang mampu memanfaatkan *session* untuk mengambil data pengguna.

II.2 *Stuxnet*

Stuxnet masuk ke dalam kategori *malware* yang dibuat menggunakan bahasa pemrograman C++ oleh pakar teknologi informasi yang memahami betul seluk beluk administrasi jaringan dan keamanan digital. Menurut pendapat pakar keamanan digital James P. Farwell, *Stuxnet* sebagai senjata digital merupakan program jahat yang memiliki kemampuan untuk menembus pertahanan digital lawan dengan satu atau beberapa metode dengan tujuan untuk merusak atau mengacaukan sistem mesin atau jaringan yang mengontrol kegiatan mesin di dalam lingkungan industri. *Stuxnet* merupakan hasil penyempurnaan dari *malware* tipe *worm* yang sudah eksis sejak tahun 2003 dan terus berevolusi hingga saat ini.

Yang membedakan *Stuxnet* dengan *malware* serupa yang beredar sebelumnya adalah keunggulannya untuk menginfeksi sistem dalam berbagai cara sebagai terlepas bahwa ia merupakan *malware* dengan ukuran terkecil , *500 kilobyte*, dan termasuk sebagai *malware* yang paling susah untuk diidentifikasi dikarenakan di dalamnya terdapat kode yang membawa sertifikasi digital palsu untuk mengelabui keamanan digital yang sering digunakan di lingkungan industri. Berdasarkan analisa keamanan digital Symantec yang diterbitkan pada tahun 2011[16], *Stuxnet* dirancang dan diluncurkan dengan skenario seperti berikut :

Sistem pengendali industrial yang umumnya digunakan dalam lingkungan industri saat ini dioperasikan dengan *software* pengendali yang mampu diprogram ulang dan berjalan dalam satu sistem operasi. Umumnya pengendali hanya terhubung dalam jaringan intranet dan hampir tidak terkoneksi dengan internet.

Untuk memastikan serangannya berjalan sesuai rencana , penyerang harus mengetahui skema sistem pengendali yang menjadi sasarannya dan bagian mana saja yang dikendalikan. Untuk mendapatkan informasi tersebut biasanya

[16] Nicolas Falliere , et al. 2011. *"W32 Stuxnet Dossier".* Symantec Security. Hlm.3

penyerang memiliki dokumen yang didapat melalui koneksi dari dalam atau bisa pula mencuri dari perangkat yang menyimpan dokumen tersebut menggunakan teknik *cyber attack* yang dikuasainya. Dari dokumen tersebut sang penyerang dapat menyiapkan kode – kode untuk menyusun *stuxnet* sesuai kebutuhannya.

Berikutnya , penyerang membutuhkan pengujian *Stuxnet* menggunakan perangkat keras yang serupa dengan perangkat yang digunakan oleh calon korban. Hal ini demi memastikan kode yang dirancang benar – benar dapat bekerja secara efektif ketika *Stuxnet* menginfeksi sasarannya. Sesi pengujian ini membutuhkan secepat – cepatnya enam bulan dan kelompok pengembang yang terdiri dari paling tidak sepuluh orang dan individu – individu lain yang membantu melancarkan proses pengujian ini. Kemudian Untuk memastikan bahwa sistem sasaran tidak mendeteksi potensi serangan maka tim pengembang menggunakan manipulasi sertifikasi digital yang kerap digunakan sebagai salah satu metode keamanan digital. Mereka mendapatkannya melalui koneksi dari siapapun yang bekerja untuk perusahaan yang menangani sertifikasi digital dan menjual salinan dari sertifikasi digital yang asli ke luar.

Ketika proses pengujian telah dilakukan , tahap berikutnya adalah menginfeksi sasaran. Untuk itu maka *Stuxnet* harus dilepaskan langsung melalui jaringan sistem yang dituju. Ada beberapa metode penginfeksian yang digunakan dalam tahap ini[17] :

1. **Melalui media penyimpanan data :** Target utama *Stuxnet* adalah sistem pengendali yang berjalan dalam satu sistem operasi khusus. Sistem pengendali ini menjalankan setiap perangkat elektronik hingga sistem yang beroperasi dalam lingkungan industri. Sistem pengendali ini umumnya hanya terhubung melalui intranet lingkungan industri dan tak jarang pula beroperasi secara *offline*. Karena keterbatasan jaringan yang ada maka penyerang memanfaatkan media penyimpanan yang mudah digunakan sehari – hari untuk membawa *Stuxnet* dan

[17] Ibid. Hlm.19.

menghubungkannya secara langsung ke dalam perangkat yang terhubung dengan sistem pengendali.

2. **Melalui celah *Win-CC* :** Secara spesifik Stuxnet mengincar sistem operasi yang menjadi *platform* aplikasi Win-CC yang digunakan dalam sistem pengendali yang beroperasi dan menggunakan injeksi kode yang dirancang untuk aplikasi tersebut.
3. **Melalui Jaringan Lokal :** *Stuxnet* mampu masuk ke dalam sistem operasi melalui salah satu *server* yang memperbolehkan akses antar perangkat manapun di dalam lingkungan industri yang dapat saling bertukar data.
4. **Melalui celah *MS100-061 print spooler*** : Menggunakan celah dalam jaringan printer bersama , *Stuxnet* dapat melipat gandakan programnya menggunakan celah ini dan kemudian menjalankan salinannya untuk menginfeksi setiap perangkat yang terhubung ke dalam jaringan.
5. **Melalui celah *Simatic Step7*** : Mesin pengontrol fasilitas elektronik dalam lingkungan industri mayoritas mengandalkan produk dari Siemens yang dibundel dengan piranti lunak dari produsen tersebut yang bernama *SIMATIC Step7* yang digunakan dalam jaringan yang mengendalikan aktivitas perangkat elektronik di dalam lingkungan industri. *Stuxnet* memiliki kode yang mampu memanfaatkan celah di dalam program tersebut.

Seketika *Stuxnet* mulai menginfeksi ke dalam jaringan maka akan terus menyebar hingga ke dalam setiap perangkat keras yang terhubung ke dalam jaringan yang ada dalam lingkungan tersebut hingga akhirnya *Stuxnet* menemukan sistem operasi yang menjadi basis untuk menjalankan sistem pengendali yang terdapat di dalam lingkungan sasaran. Pada tahap ini , penyerang hanya bisa mengendalikan *Stuxnet* melalui perangkat yang terhubung langsung ke dalam jaringan keamanan intranet. Ketika sistem pengendali yang menjadi sasaran ditemukan maka *Stuxnet* akan mengubah kode – kode yang terdapat di dalamnya. Kode – kode tersebut disabotase dan akan merusak kinerja sistem pengendali.

Ketika serangan telah terjadi maka akan sulit bagi korban untuk melakukan verifikasi atas program yang menyerang mereka dikarenakan sertifikasi digital yang terdapat di dalam *Stuxnet* telah mengelabui sistem keamanan mereka dan praktis sistem akan menganggapnya sebagai kesalahan produsen.

Stuxnet yang beredar saat ini secara spesifik menyerang sistem pengendali yang berasal dari produsen Siemens. Adapun sistem pengendali keluaran Siemens sampai saat ini merupakan produk yang telah digunakan oleh sebagian besar lingkungan industri yang ada di hampir seluruh negara dunia. Lebih lanjut menurut James P Farwell , *Stuxnet* dan *malware* yang berpotensi muncul dalam jenis baru di masa depan adalah alat yang ampuh untuk menyerang atau menjatuhkan seseorang atau kelompok tertentu[18]. Beliau mengatakan bahwa terlepas bahwa pembuatan *Stuxnet* akan memakan waktu dan biaya riset yang tidak sedikit jumlahnya , pengeluaran yang diperlukan untuk membuat senjata digital tersebut sangat jauh lebih murah dibandingkan apabila sebuah negara memproduksi senjata militer. Lebih lanjut , spesifikasi *Stuxnet* yang ditujukan untuk merusak industri modern akan menimbulkan kerusakan yang serius pada infrastruktur – infrastruktur yang saat ini mulai didominasi oleh teknologi mutakhir dan berpotensi mengakibatkan kerugian yang setara atau bahkan lebih dari serangan militer[19].

[18] James P. Farwell , et al. *"Stuxnet and the Future of Cyber War".* Januari 2011. Hlm.14
[19] Ibid. Hlm.15

BAB III

PERAN PERKEMBANGAN TEKNOLOGI INFORMASI TERHADAP PROGRAM PENGEMBANGAN ENERGI NUKLIR IRAN

3.I Aspek Teknologi Dalam Program Energi Nuklir di Iran

Program energi nuklir di Iran telah berjalan sejak tahun 1974. Program tersebut digagas pada saat rezim Shiah berkuasa dengan landasan bahwa energi fosil suatu saat akan habis. Pada saat kemunculannya hingga saat ini, negara – negara yang bertentangan dengan Iran telah mengungkapkan ketidak sukaannya terhadap program mereka. Namun tak sedikit pula kelompok – kelompok aktivis hingga pakar – pakar dari dalam dan luar negeri yang membela program Iran ini. Secara dasar terdapat empat pandangan yang menjadi topik utama mengenai program nuklir di Iran[20] :

1. Beberapa pakar energi luar negeri berpendapat bahwa dengan kekuatan ekonomi dan kondisi lingkungan yang mendukung , energi nuklir tak dibutuhkan di Iran. Argumen yang beredar mengatakan bahwa menggunakan nuklir sebagai pembangkit listrik lebih mahal daripada menggunakan alternatif lainnya. Behzad Nabavi , salah satu anggota parlemen dan tokoh reformasi di Iran , mendukung argumen ini meskipun dalam catatan Ia lebih dipengaruhi oleh tokoh – tokoh politik Amerika Serikat.
2. Sementara itu, banyak kelompok dari luar negeri yang justru mendukung Iran untuk mengembangkan energi nuklir dan harus memperdalam teknologi yang mendukung program tersebut. Mereka berpendapat secara ekonomi dalam jangka panjang , nuklir sebagai alternatif energi terbarui akan membawa keuntungan yang lebih baik dan secara prestis akan menempatkan Iran sebagai salah satu negara dunia yang memiliki

[20] Nasser Hadian. 2003. *"Iran's Emerging Security Environment and Relations with the United States: Dynamics and Prospects".* United States Senate Committee on Foreign Relations. Hlm.7

kapabilitas pengembangan energi nuklir yang mumpuni. Lebih lanjut , nuklir adalah teknologi masa depan dan semua negara harusnya memiliki akses untuk mendalami teknologi tersebut lebih dalam. Selain itu , mereka mengatakan bahwa sikap Iran dalam perjanjian nonproliferasi nuklir memastikan mereka tidak akan menggunakan kemampuan mereka untuk mengembangkan senjata nuklir. Pandangan ini didukung oleh pejabat – pejabat Iran serta pakar – pakar dari universitas – universitas besar di negara – negara dunia. Rusia , Jepang , dan beberapa negara Eropa bahkan menyetujui pandangan ini.

3. Beberapa kelompok kecil berpendapat bahwa Iran juga perlu mengembangkan senjata nuklir melalui kemampuan mereka dikarenakan alasan keamanan. Para kelompok tersebut menambahkan bahwa Iran membutuhkannya sebagai faktor deteren untuk menjaga adanya ancaman dari negara – negara lain.
4. Sebagian pakar berpendapat bahwa selain mengembangkan nuklir sebagai alternatif energi di masa depan , Iran juga harus mampu mengaplikasikan energi tersebut dalam skala menengah untuk kebutuhan masyarakat dari segala golongan dan harus melupakan gagasan bahwa mereka harus mengembangkan senjata nuklir. Alasannya selain mereka akan melanggar perjanjian internasional , Iran tak membutuhkan keamanan tambahan dan hal tersebut justru akan menjadikan Iran sebagai musuh negara – negara besar. Para pakar yang menyatakan pandangan ini merupakan kelompok yang mendukung perjanjian nonproliferasi nuklir dan mengkritik sikap Amerika Serikat yang terlalu melebihkan mengenai isu Iran dalam mengembangkan senjata nuklir.

Location	Facility/Reactor as of November 2004	Status
Tehran nuclear research center	Tehran Research Reactor (TRR)	Operating
Tehran	Kalaye Electric Company	Dismantled pilot enrichment facility
Bushehr	Bushehr Nuclear Power Plant (BNPP)	Under construction
Esfahan nuclear technology center	Miniature Neutron Source Reactor (MNSR)	Operating
Natanz	Pilot Fuel Enrichment Plant (PFEP)	Operating (PFEP)
Karaj	Radioactive Waste Storage	Partially operating
Lashkar Ab'ad	Pilot Uranium Laser Enrichment Plant	Dismantled
Arak	Iran Nuclear Research Reactor IR-40	In detailed design phase
Anarak	Waste Storage Site	Waste to be transferred to Jabr Hayan Laboratories (JHL)

Tabel 3.1 : Titik – titik dengan fasilitas pengolahan energi nuklir utama yang aktif di Iran sejak tahun 2004 (Sumber : Iranian Nuclear Sites. Hlm 4.)

Sebagai salah satu negara dengan kapabilitas pengembangan energi nuklir di dunia , Iran telah membuktikan bahwa mereka berambisi untuk mengolah salah satu kekayaan alam mereka dengan tujuan mendapatkan alternatif energi yang lebih baik. Sebagaimana yang telah diungkapkan dalam pandangan – pandangan di atas, program pengembangan ini merupakan salah satu upaya negara tersebut untuk memperoleh energi alternatif yang suatu hari nanti akan menggantikan energi fosil yang semakin hari semakin sulit untuk memenuhi kebutuhan energi dalam negerinya dan semakin besarnya konsumsi tenaga listrik yang membutuhkan pembangkit energi tambahan[21]. Untuk itu hingga per tahun 2004 Iran telah memperkuat program ini dengan membangun fasilitas – fasilitas nuklir pada beberapa titik di negaranya[22]. Dalam mengembangkan reaktor nuklir tersebut

[21]Mohammad Sahimi , et al. "*Energy : Iran Needs Nuclear Power".* Diakses dari http://www.nytimes.com/2003/10/14/opinion/energy-iran-needs-nuclear-power.html pada 30 Maret 2017.

[22] Hussein D. Hassan. 2009. *"Iranian Nuclear Sites "*. Information Research Specialist Knowledge Services Group. Hlm.5

Iran telah mengimplementasikan aspek – aspek teknologi tertentu yang memastikan bahwa proses pengembangan energi nuklir mampu berjalan sesuai rencana.

Salah satu kunci yang membuat program pengembangan energi nuklir di Iran berkembang pesat hingga saat ini adalah penerapan teknologi yang digunakan dalam proyek pengembangan uranium dan plutonium. Untuk memastikan berjalannya proyek pengembangan energi tersebut, Iran mengkreasikan beberapa teknologi yang awalnya mereka pelajari dari negara lain dan menggunakan pemikiran – pemikiran dan rancangan dari ahli – ahli dalam negeri mereka sendiri untuk menciptakan variasi dari teknologi yang telah mereka pelajari. Iran memiliki teknologi sentrifugal gas yang mereka kembangkan sendiri melalui bantuan jaringan dari Pakistan dan teknologi ini berfungsi untuk mengolah uranium dengan lebih efisien[23]. Pada awalnya Iran membuat sentrifugal buatan lokal sebanyak kurang lebih 20.000 unit hanya untuk dua reaktor utama mereka dan kemudian menambah produksi untuk kebutuhan hingga saat ini. Walaupun saat ini mereka mampu memproduksi sentrifugal secara mandiri , bahan – bahan material kualitas tinggi seperti karbon fiber dan besi olah yang dibutuhkan pada awal mereka membangun reaktor nuklir membutuhkan waktu untuk diimpor dari luar negeri. Bahan – bahan ini didapatkan dari koneksi antar negara Timur Tengah dan transaksi tersebut terjadi saat Iran sedang berada dalam situasi dimana PBB dan Amerika Serikat menjatuhkan sanksi ekonomi kepada mereka.

Pusat pengolahan umumnya memuat 164 hingga 174 mesin pengolah uranium dan mendistribusikan hasil olahan kepada beberapa titik. Uranium yang didistribusikan kurang dari 5 persen digunakan sebagai energi untuk menjalankan pembangkit energi nuklir. Sedangkan uranium yang didistribusikan sekitar 20 persen digunakan untuk menjalankan pusat riset energi nuklir[24].

[23] Jeremy Bernstein. 2014.*"Nuclear Iran".* Harvard University Press. Hlm.19
[24] Ibid. Hlm.23

Kemudian untuk proyek pengayaan plutonium , Iran menambahkan teknologi reaktor tenaga air dengan daya 30–50 *megawatt thermal (MWt)* untuk mendukung program pengayaan tersebut[25]. Proyek ini pada awalnya bermaksud mengembangkan dan menggunakan teknologi hasil pengolahan plutonium untuk mengembangkan teknologi alternatif perangkat medis. Seiring berkembangnya teknologi nuklir mereka , tujuan pengolahan plutonium diutamakan sebagai alternatif teknologi pendukung infrastruktur.

Tulang punggung dari pusat pengayaan uranium dan plutonium di Iran adalah mesin pengolah IR-1 yang dibuat dari desain salinan yang dibuat oleh ahli di eropa pada akhir era 1960-an. Pada awalnya , mesin ini tidak dapat beroperasi secara optimal mengingat Iran hanya menggunakan separuh dari kapabilitas rotor yang bekerja di dalamnya sehingga mesin bekerja lebih pelan , lebih ringan tekanan dan mengurangi efisiensinya. Walau demikian IR-1 membawa dampak yang signifikan seiring berjalannya waktu , yakni dengan kecepatan volume produksi. Berbagai permasalahan yang terjadi sebelumnya yang kerap membuat mesin sentrifugal berhenti beroperasi bukan problem besar karena mereka mampu membuat sentrifugal lainnya dengan cepat sehingga tidak menghalangi proses pengolahan uranium dan plutonium. Suplai energi bukanlah masalah bagi mereka. Untuk mengatasi bahaya yang dapat ditimbulkan dari peralatan yang digunakan , Iran lantas menciptakan rangkaian sistem proteksi yang tergolong unik karena sistem ini didesain untuk mengatasi masalah pada sentrifugal dengan menerapkan algoritma toleransi kerusakan yang lebih ketat. Sistem proteksi ini yang hingga saat ini menjadi salah satu faktor penting dalam proyek pengolahan yang dilakukan di reaktor - reaktor nuklir di Iran. Sistem proteksi ini dikendalikan menggunakan mesin pengendali industrial yang diimpor dari luar.

Mesin pengendali industrial tersebut diprogram , diatur , dan dikendalikan oleh program yang dirancang dari pihak ketiga *(third party)*. Pengaplikasian program ini ditemui di lingkungan dengan reaktor nuklir di mana para pekerja di

[25] Andrew Koch , et al. "*Iran's Nuclear Facilities : A Profile", Center for Nonproliferation Studies*. November 1998. Hlm.2

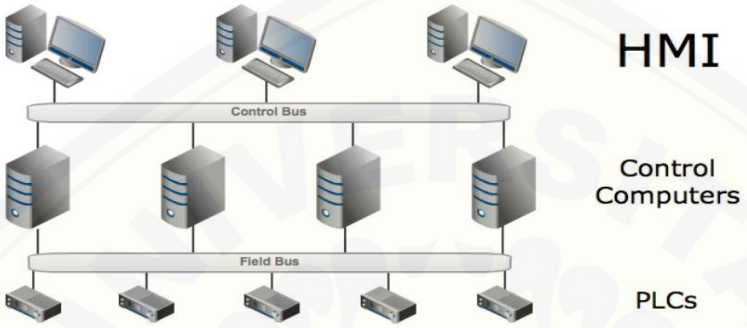
dalamnya telah dibekali perangkat elektronik yang mumpuni dan cukup praktis dikarenakan para penggunanya akan menghabiskan waktu untuk berkeliling di area reaktor nuklir sesering mungkin. Mesin pengendali industrial tersebut nantinya akan terhubung dalam satu jaringan sistem pengontrol di mana pada titik ini teknologi informasi akan menjadi faktor utama.

3.2 Peran Teknologi Informasi

Lingkungan industri atau infrastruktur yang ada saat ini umumnya menggunakan gabungan dua jenis sistem pengontrol : sistem kontrol supervisor dan pengumpulan data yang mengumpulkan data – data lapangan yang tertutup dan sistem pengontrolan distributif yang secara otomatis memanajemen proses produksi. Setiap tahun , sistem – sistem ini mendapat pembaharuan fitur yang membuat keduanya hampir bekerja dengan metode yang sama dan dengan teknologi yang sama. Meskipun demikian , mereka masih sama – sama memiliki perbedaan yang jelas. Perbedaan tersebut ditemui pada sistem pengontrol terintegrasi atau pada instrumen dan kendali yang digunakan. Semua itu berdasarkan penerapan teknologi yang telah digunakan fasilitas yang bersangkutan dari tahun ke tahun.

Sistem pengontrol proses dibuat dengan arsitektur yang rumit dan diprogram dengan beberapa model bahasa pemrograman. Namun pada dasarnya setiap sistem pengontrol proses memiliki satu sifat yang sama. Mereka bekerja dalam satu jaringan yang dikendalikan suatu *server* dan secara langsung mengawasi setiap aktifitas dalam reaktor dan mencatat setiap data yang masuk. Bagian terpenting dari sistem pengontrol proses adalah *human-machine interface* yang mengumpulkan dan menunjukkan data dari reaktor yang berisikan data mengenai perangkat – perangkat yang digunakan dan yang sedang beroperasi dan memungkinkan teknisi untuk mengedit opsi untuk mengatur aktifitas reaktor melalui panel yang tersedia. Interaksi ini terjadi melalui penghubung jaringan kendali yang dijalankan menggunakan perangkat lunak yang berjalan dalam suatu sistem operasi. Komputer – komputer yang saling terhubung tersebut melakukan

pertukaran data melalui *programmable logic controllers* yang secara langsung menghubungkan aktifitas motorik , sensorik , analisa data , serta aktifitas – aktifitas komponen elektronik lainnya yang terdapat di dalam reaktor[26].



Gambar 3.2 : Skema sederhana jaringan sistem pengontrol (Sumber : The Vulnerability of Nuclear Facilities to Cyber Attack. Hlm.2)

Keterangan :

HMI = Human Machine Interface

Control Computers = server

PLCs = Programmable Logic Controllers (mesin pengontrol digital)

Semua jaringan pengontrol terkoneksi dengan jaringan kantor dan hal ini ditujukan agar perusahaan mampu mengatur tujuan mereka dan mengkondisikan kegiatan reaktor sesuai dengan rencana dan juga mengawasi untuk meningkatkan kinerja dan efisiensi di masa yang akan datang.

Mesin pengontrol yang terpasang dan digunakan di reaktor – reaktor nuklir di Iran hingga saat ini menggunakan sistem yang didatangkan dari produsen

[26] Brent Kesler. 2011. *"The Vulnerability of Nuclear Facilities to Cyber Attack".* Strategic Insight, Volume 10. Hlm.2

perangkat elektronik Siemens[27]. Mereka diprogram , diatur , oleh aplikasi yang disebut Simatic. Komputer gegas lebih diutamakan dalam penggunaan program dikarenakan para penggunanya akan menghabiskan waktu untuk berkeliling di area reaktor nuklir sesering mungkin. Dibuat pada tahun 1958 dan diperkenalkan ke Iran pada tahun 1979 , program Siemens yang diberi nama *Simatec Step7* sempat ditarik dari negara itu ketika memasuki era revolusi Islam di Iran. Siemens kembali menjadi produsen yang berperan dalam program pengembangan nuklir di Iran paska tahun 1994. Meskipun perangkat *Simatec Step7* telah menjadi perangkat utama Iran dalam program pengembangan energi nuklir mereka sejak era paska perang dingin , inovasi dalam perangkat tersebut muncul pada tahun 2001 di mana versi *Simatec Step7* yang memiliki fitur konektivitas internet / intranet diperkenalkan. Kemudahan dalam mengunduh , mengedit , serta saling bertukar data muncul dalam perangkat lunak *Simatec Step7 Vol.5, Service Pack 3* di mana kemudian versi – versi berikutnya mengadaptasi fitur konektivitas dari versi tersebut[28]. Hal ini memudahkan para teknisi yang bekerja di dalam lingkungan reaktor nuklir untuk mengawasi kinerja dan aktivitas perangkat – perangkat yang beroperasi di dalam reaktor serta mempercepat pekerjaan mereka dalam berkirim laporan hingga dokumen – dokumen penting lainnya tanpa harus meninggalkan tempat kerja.

Sistem pengontrol sentrifugal menggunakan varian dari *Step7-417* , versi *Step7-315*. Varian *Step7-315* memiliki fisik yang lebih kecil dan difokuskan untuk mengontrol 164 mesin pengendali yang ada dalam reaktor. 164 mesin pengendali disusun dalam satu rak dan ditempatkan dalam 4 baris dan 43 petak. Setiap mesin sentrifugal memiliki mesin penggerak dengan kecepatan maksimum 100.000 *rpm* yang mampu berjalan stabil saat percepatan maupun perlambatan[29]. Fitur ini bisa dicapai dengan adanya konverter frekuensi , sebuah *power supply* yang mengatur kecepatan tertentu melalui arus bolak balik yang diinput menggunakan komputer. Konverter frekuensi disambungkan pada enam sistem pengontrol distribusi yang

[27] Ibid. Hlm.3
[28] Ibid. Hlm 4
[29] Ralph Langner. *"To Kill A Centrifuge", The Langner Group.* November 2013. Hlm 12.

terhubung pada *server* yang menjalankan *Step7-315*[30]. Semua kode dan pertukaran data terjadi di sini.

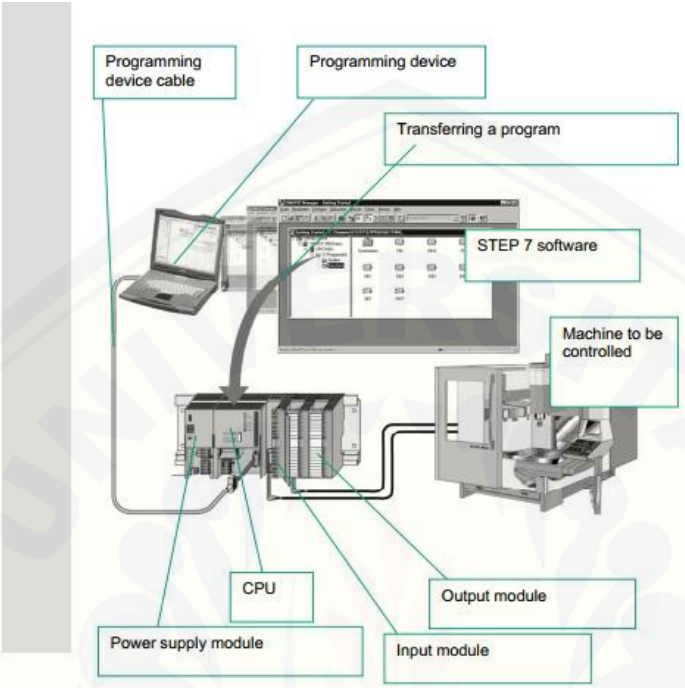
Sistem Proteksi terdiri dari dua lapis , lapis paling rendah terdapat pada level sentrifugal. Tiga katup penutup cepat dipasang di setiap sentrifugal di tiap penghubung pipa sentrifugal dan di bagian pipa lainnya. Dengan menutup katup , sentrifugal yang mengalami masalah dapat diblokir. Setelah terblokir nantinya sentrifugal tersebut akan ditangani oleh teknisi yang menangani permasalahan yang dihadapi.

Pusat pengawasan sistem proteksi menunjukkan status dari setiap sentrifugal yang ditangani tiap *server* – yang sedang berjalan maupun yang diblokir. Ketika salah satu sentrifugal yang mengalami kerusakan sedang beroperasi , maka perlahan sentrifugal tersebut akan diperlambat dan ditutup hingga penanganan lebih lanjut dilakukan demi melindungi alat – alat lainnya dan sistem yang ada. Sebagaimana proteksi berjalan , sistem proteksi tak akan memberitahukan sesuatu kecuali apabila sistem mendeteksi adanya gejala dalam aktivitas reaktor yang tidak normal dan kemudian mencegahnya agar tidak merusak sistem yang berpotensi membahayakan hidup para pekerja di dalamnya.

Iran mempunyai sebuah solusi tersendiri untuk masalah seperti ini – adanya perangkat tambahan yang dipasang pada tiap perangkat yang terhubung pada sentrifugal. Untuk setiap bagian pengayaan uranium , titik tekanan dimonitor dengan sensor tekanan. Apabila terdapat poin tertentu yang melebihi batas normal tekanan maka katup pembuangan yang dikendalikan oleh komputer akan terbuka dan sisa tekanan akan dialihkan ke pembuangan hingga tekanan normal kembali berjalan. Aplikasi pengamanan seperti ini merupakan salah satu penerapan teknologi vakum. Perangkat tambahan ini bisa diakses melalui setiap komputer yang terhubung dengan jaringan monitor proteksi. Opsi proteksi ini pula yang diyakini sebagai faktor krusial bagi Iran hingga dapat membawa program pengembangan energi nuklir mereka dengan pesat seperti sekarang ini.

[30] Ibid. Hlm.14

Di bawah ini adalah skema serta fitur yang dimiliki oleh *Step 7* oleh Siemens yang digunakan dalam lingkungan reaktor nuklir di Iran[31] :



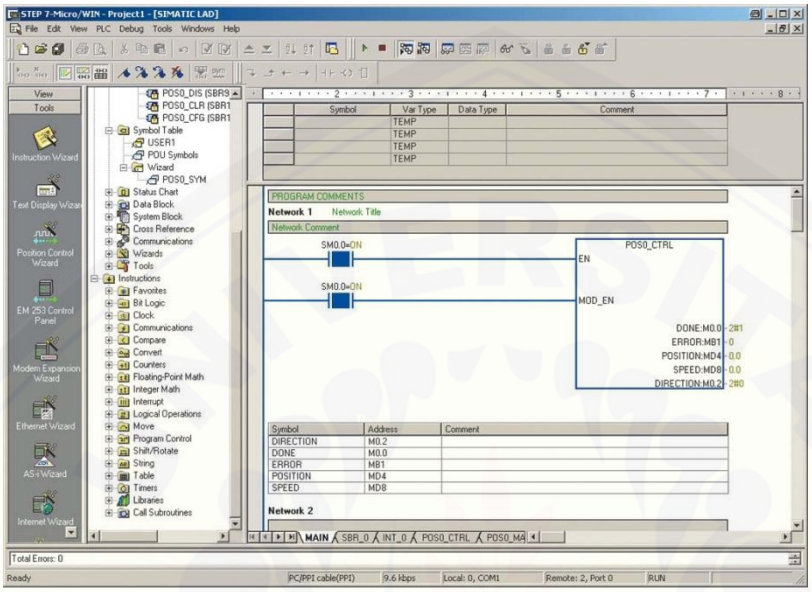
Gambar 3.3 : rangkaian mesin pengendali yang beroperasi menggunakan Step7 (Sumber : Simatic : Work With Step 7. Hlm 20)

Keterangan :

1. *Programming device* : perangkat elektronik yang digunakan untuk memodifikasi program.
2. *Programming device cable* : kabel yang digunakan untuk melakukan koneksi antar perangkat.
3. *Transferring a program :* melakukan pemindahan program.
4. *Step 7 software* : perangkat lunak khusus keluaran Siemens untuk mesin *Step 7.*
5. *Power supply module* : perangkat pensuplai daya untuk menghidupi perangkat.
6. *CPU* : unit pemroses utama.

[31] Anonim. 2006. *"Simatic : Work With Step 7"*. Siemens AG Automation and Drives. Hlm.20

7. *Output module* : modul yang membawa pemrosesan program keluar.
8. *Input module* : modul yang membawa pemrosesan program ke dalam.
9. *Machine* : mesin pengendali yang diatur melalui *programming device.*



Gambar 3.4 : Interface/antarmuka perangkat lunak Step yang terhubung dengan jaringan sistem pengontrol.(Sumber : Simatic : Work With Step 7. Hlm 37)

Di dalam perangkat lunak pada gambar di atas terdapat beberapa opsi yang kerap digunakan dalam proses pengontrolan :

Program offline : Program yang disimpan di dalam media penyimpanan pada perangkat komputer. Di dalamnya terdapat dokumentasi. Salinan dari program offline harus disimpan dikarenakan dokumen yang terafiliasi dengan format program ini tidak tersimpan dalam sistem pengontrol.

Program online :. Program yang digunakan secara online dalam sistem pengontrol.

Download : Hasil program atau dokumen yang diunduh secara online dan disimpan ke dalam sistem pengontrol.

Upload : Membawa program dalam sistem pengontrol dan memasukkannya ke dalam perangkat. Harus menggunakan program offline yang digunakan agar tersimpan dalam media penyimpanan.

Save : Menyimpan blok yang terbuka ke dalam media penyimpanan. Blok yang sedang diedit dapat diunduh oleh mesin pengontrol sekalipun tidak sedang disimpan secara offline.

PG/PC : Komputer atau perangkat elektronik serupa yang menjalankan perangkat lunak SIMATIC milik Siemens.

Nodes : Merupakan perangkat elektronik (seperti mesin pengendali) yang terhubung dengan jaringan dan memiliki alamat IP yang bisa diprogram sesuai kebutuhan.

BAB V

KESIMPULAN

Kerasnya sikap Iran terhadap pengaruh dari negara – negara dunia penentang program energi nuklir mereka telah membawa mereka pada titik di mana negara – negara tersebut mencari jalan alternatif untuk bisa menghentikan program tersebut. Amerika Serikat sebagai salah satu negara yang menentang Iran mendapatkan inspirasi atas momen kebuntuan tersebut dan melakukan langkah yang belum pernah dicapai atau dilakukan oleh negara manapun sebelumnya. Memanfaatkan kemajuan aspek teknologi yang diimplementasikan dalam program pengembangan energi nuklir di Iran, mereka melihat bahwa ada kesempatan untuk menggunakan jalur lain yang memiliki tingkat efektivitas yang lebih tinggi dibanding melalui opsi – opsi yang selama ini telah mereka pertimbangkan , terlepas dari dilema moral mengenai perlu atau tidaknya tindakan seperti ini dilakukan.

Sesuai dengan kerangka teori yang digunakan dalam penelitian ini, apa yang telah dilakukan oleh Amerika Serikat terhadap Iran merupakan contoh nyata dari tantangan yang dihadapi dalam keamanan modern. Perang kini tak lagi dilakukan dengan adu kekuatan militer secara fisik namun berpotensi terjadi dalam lingkup ruang dunia maya yang kini menjadi faktor utama dalam kegiatan pertukaran informasi dan data. Selain pada kasus Amerika Serikat terhadap Iran ini kita bisa mengambil pula kesimpulan bahwa kejadian ini juga mampu menimpa negara manapun selama faktor teknologi informasi berperan dalam kegiatan sehari – harinya. Mengingat bahwa setiap tahun selalu terdapat inovasi teknologi informasi dan semakin bergantungnya masyarakat maupun negara terhadap kemudahan yang ditawarkan oleh kemajuan teknologi informasi , maka sudah sepantasnya isu mengenai keamanan dalam ruang digital menjadi perhatian besar oleh negara demi melindungi kepentingannya dan melindungi informasi rakyatnya dari serangan pihak – pihak yang berniat buruk pada mereka. Seperti pula yang dijelaskan pada bab – bab di atas, tantangan ini akan membutuhkan

peran sumber daya manusia yang benar – benar ahli di bidangnya dan diperlukan pula pengetahuan yang cukup mengenai bagaimana sebuah jaringan komunikasi harus dijaga.

DAFTAR PUSTAKA

Buku

Angelo, Jr, Joseph A. 2004. *Nuclear Technology*. Greenwood Press, 88 Post Road West, Westport.

Beres, Louis Rene. 1992. *On Assassination as Anticipatory Self-Defense: The Case of Israel.* 20 Hofstra L. Rev.

Bernstein, Jeremy. 2014. *Nuclear Iran.* Harvard University Press.

Buzan , Barry. 2009. *People , States, and Fear Second Edition : An Agenda for International Security Studies In The Post Cold-War Era.* ECPR Press,2009. Brighton , Sussex.

Buzan , Barry ,et al. 1998. *Security : A New Framework for Analysis.* Lynne Rienner Publishers, Inc. England.

Falliere, Nicolas., Liam O Murchu, Eric Chien. 2011. *"W32 Stuxnet Dossier".* Symantec Corporation World Headquarters 20330 Stevens Creek Blvd.

Hemmer, Christopher. 2007. "*Parameters : United States Army War College Quarterly".* Army War College.

Kazman , Kenneth. 2017. "*Iran Sanctions*". Congressional Research Service. Diane Publishing Co.

Mohseni, Payam. 2015. *Iran and the Arab World after the Nuclear Deal.* Belfer Center for Science and International Affairs, Harvard Kennedy School.

Moleong , Lexy. J. 2004. Metodologi Penelitian Kualitatif. Bandung. Remaja Rosda Karya.

Sanger, David E. 2013. *Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power*. Crown Publishing Group.

Wheeler, David A., Gregory N. Larsen, Task Leader. 2003. *Techniques for Cyber Attack Attribution.*
Institute for Defense Analyses. 4850 Mark Center Drive, Alexandria, Virginia

Jurnal dan Artikel Ilmiah

Anonim. 2003. *Implementation of theNPT safeguards agreement in the Islamic Republic of Iran – GOV 2003/40.* International Atomic Energy Agency.

Anonim. 2003. *Implementation of the NPT safeguards agreement in the Islamic Republic of Iran – GOV 2003/75*. International Atomic Energy Agency.

Al-Buaniain, Yusuf. 2008. *Iran Nuclear Threat : An Environmental Perspective.* United States Marine Corps, Command and Staff College, Marine Corps University 2076 South Street, Marine Corps Combat Development.

Beidleman, Scott W. 2009. *Defining and Deterring Cyber War.* U.S Army War College, Carlisle Barracks.

Farwell, James P, Rafal Rohozinski. *Stuxnet and the Future of Cyber War*. Januari 2011. Routledge Informa Ltd.

Hadian, Nasser. 2003. *Iran's Emerging Security Environment and Relations with the United States: Dynamics and Prospects.* United States Senate Committee on Foreign Relations.

Hansen , Lene dan Helen Nissenbaum. 2009. *Digital Disaster, Cyber Security , and Copenhagen School.* International Studies Association.

Hassan, Hussein D. 2007. *Iranian Nuclear Sites.* Information Research Specialist Knowledge Services Group. Agustus 2007.

Kahn, Tzvi. 2016. *The Future of Iranian Terror and Its Threat to the US Homeland.* The House Committee on Homeland Security's Subcommittee on Counterterrorism and Intelligence.

Kesler, Brent. 2011. *The Vulnerability of Nuclear Facilities to Cyber Attack.* Strategic Insight, Volume 10.

Koch, Andrew, Jeanette Wolf. *Iran's Nuclear Facilities : A Profile.* Center for Nonproliferation Studies.

Langner, Ralph. *To Kill A Centrifuge,* The Langner Group. November 2013.

Mueller, Paul, Babak Yadegari. 2012. *The Stuxnet Worm.* University of Arizona.

Van Der Putten , Frans Paul , Minke Meijnders , dan Jan Rood. 2015. *Deterrence as a security concept against non- traditional threats.* Clingendael , Netherlands Institute of International Relations.

Internet

Al-Nusf, Sami. 2006. *"The Iranian Nuclear Dossier Is More Dangerous Than Israel's"*. Diakses dari http://www.meri-k.org/publications/the-iranian-nuclear-dossier-is-more-dangerous-than-israel pada tanggal 5 Mei 2017.

Albright , David dan Andrea Sticker. 2015. "*Iran's Nuclear Program"* diakses dari **http://iranprimer.usip.org/resource/irans-nuclear-program** pada tanggal 5 Januari 2017.

Anonim. 2010. *"Ahmadinejad Admits Centrifuges Damaged by Virus"* diakses dari http://www.jpost.com/International/Ahmadinejad-admits-centrifuges-damaged-by-virus pada tanggal 5 Mei 2017

Anonim. 2015. "*What The Heck Was Stuxnet?"* diakses dari https://null-byte.wonderhowto.com/news/what-heck-was-stuxnet-0160816 pada tanggal 5 Mei 2017.

Anonim. 2016. "*Stuxnet Part 1 : The Perfect Crime"* diakses dari http://www.bluekaizen.org/stuxnet-part1-the-perfect-crime/ pada tanggal 15 Mei 2017.

Cluley, Graham. "*Stuxnet: How USA and Israel created anti-Iran virus, and then lost control of it*" diakses dari https://nakedsecurity.sophos.com/2012/06/01/stuxnet-usa-israel-iran-virus/ pada tanggal 3 Januari 2017.

Fogarty, Kevin. 2012. *"U.S admits cyber attacks on Iran , others"* diakses dari http://www.itworld.com/article/2727364/security/u-s--admits-cyberattacks-on-iran--others.html pada tanggal 15 Mei 2017.

Hadley, J. Stephen. 2010. *"Iran Primer : The George W. Bush Administration"* diakses dari http://www.pbs.org/wgbh/pages/frontline/tehranbureau/2010/11/iran-primer-the-george-w-bush-administration.html pada tanggal 15 Mei 2017.

Holloway , Michael. 2015. "*Stuxnet Worm Attack on Iranian Facilities*" diakses dari http://large.stanford.edu/courses/2015/ph241/holloway1/ pada 3 Januari 2017.

Keck, Zachary. 2015. *"Exposed : Iran's Super Strategy to Crush America In a War"* diakses dari http://nationalinterest.org/feature/exposed-irans-super-strategy-crush-america-war-13152 pada tanggal 15 Mei 2017.

Katz, Yaakov. 2010. "*Stuxnet Virus Set Back Iran's Nuclear Program By 2 Years"* diakses dari http://www.jpost.com/Iranian-Threat/News/Stuxnet-virus-set-back-Irans-nuclear-program-by-2-years pada tanggal 5 Mei 2017.

Khaitous, Tariq. 2008. *"Why Arab Leaders Worry About Iran's Nuclear Program"*. Diakses dari http://thebulletin.org/why-arab-leaders-worry-about-irans-nuclear-program pada tanggal 5 Mei 2017.

Matar, Hosam. 2012. *"Saudi Nuclear Program : A Mirage of Process"*. Diakses dari http://english.al-akhbar.com/node/4064 pada tanggal 5 Mei 2017.

Ngan, Mandel. 2007. *"Why The U.S Can't Afford to Attack Iran"* diakses dari https://www.thetrumpet.com/4207-why-the-u-s-can-t-afford-to-attack-iran pada tanggal 5 Mei 2017.

Rosenbaum , Ros. 2012. "*Richard Clarke On Who Was Behind The Stuxnet Attack*" diakses dari http://www.smithsonianmag.com/history/richard-clarke-on-who-was-behind-the-stuxnet-attack-160630516/?page=2 pada tanggal 3 Januari 2017.

Sahimi, Mohammad, Pirouz Mojtahed-zadeh, Kaveh L. Afrasiabi. 2003. "*Energy : Iran Needs Nuclear Power"* diakses dari http://www.nytimes.com/2003/10/14/opinion/energy-iran-needs-nuclear-power.html pada tanggal 5 Mei 2017.

Warrick , Joby. 2011. "*Iran's Natanz Nuclear Facility Recovered Quickly From Stuxnet Cyberattack*" diakses dari http://www.washingtonpost.com/wp-dyn/content/article/2011/02/15/AR2011021505395.html pada 3 Januari 2017.