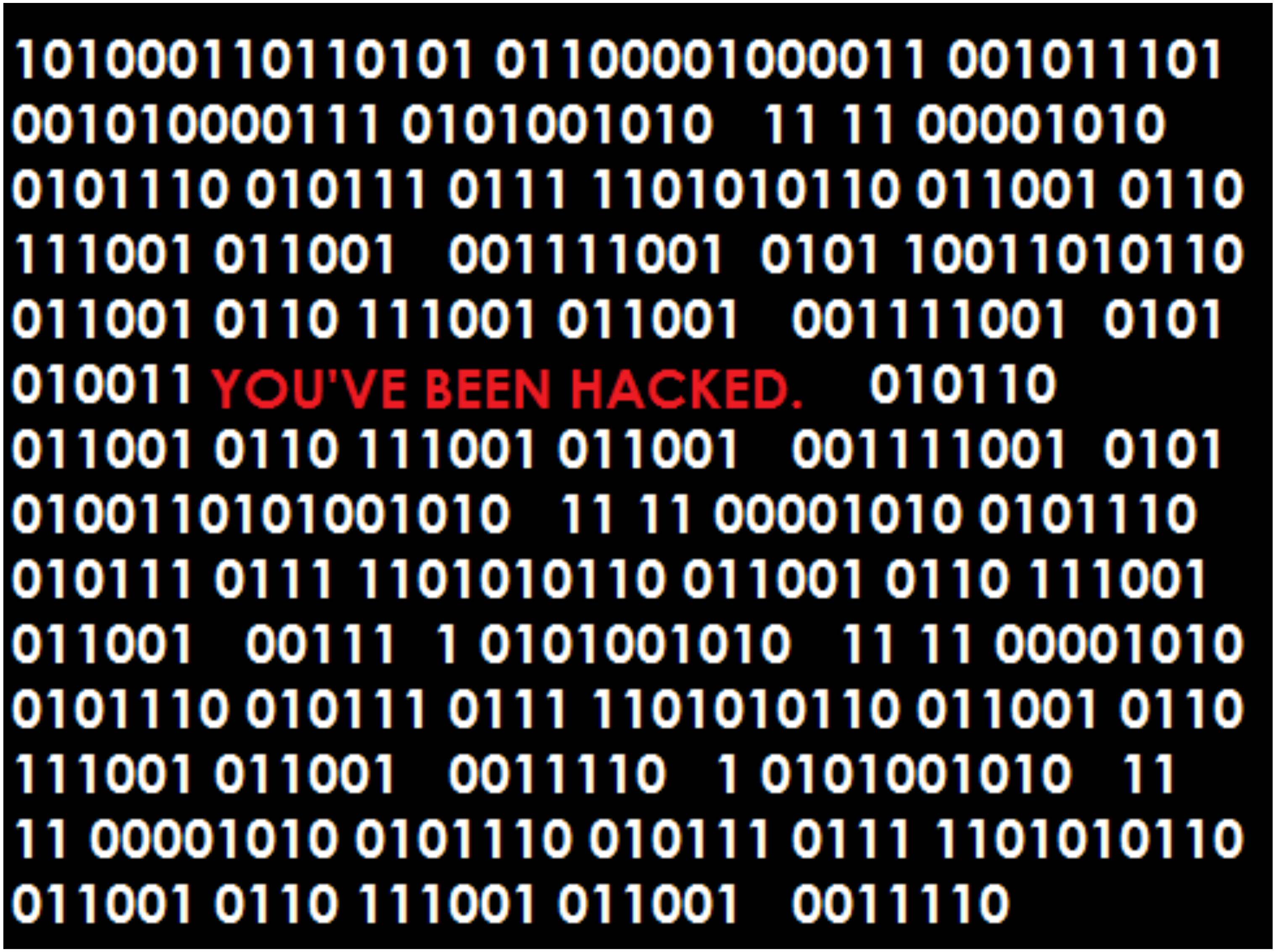
```
./hydra -l username1 -p password1 -vV -f www.mysite.com
ftp
Hydra v7.4.1 (c)2012 by van Hauser/THC & David Maciejak
- for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at
2012-11-30 11:00:30
[VERBOSE] More tasks defined than login/pass pairs
exist. Tasks reduced to 1.
[DATA] 1 task, 1 server, 1 login try (l:1/p:1), ~1 try
per task
[DATA] attacking service ftp on port 21
[VERBOSE] Resolving addresses ... done
[ATTEMPT] target www.mysite.com - login "username1" -
```

```
root@localhost# wget http://www.microsoft-
.com/mysqldump.sql
--2013-04-30 00:10:10--  http://www.microsoft-
.com/mysqldump.sql
Resolving www.microsoft.com... 00.00.07.17
Connecting to www.microsoft.com|00.00.07.17|:80...
connected.
HTTP request sent, awaiting response... 200 OK
Length: 41043000 (400M) [application/zip]
Saving to: "mysqldump.sql"

 4% [==============================>          ] 20,722,000
1.10MB/s  eta 4m 40s
```

Comparative Study: Iran, Russia &國人民共和國 Cyber Conflict

19 JULY 2013
HITCON 2013
台北, 中華民國


1010001110110101 0110000100011 001011101
001010000111 0101001010 11 11 0001010
0101110 010111 0111 1101010110 011001 0110
111001 011001 001111001 0101 10011010110
011001 0110 111001 011001 001111001 0101
010011 YOU'VE BEEN HACKED. 010110
011001 0110 111001 011001 001111001 0101
010011010101001010 11 11 00001010 0101110
010111 0111 1101010110 011001 0110 111001
011001 00111 1 0101001010 11 11 00001010
0101110 010111 0111 1101010110 011001 0110
111001 011001 0011110 1 0101001010 11
11 00001010 0101110 010111 0111 1101010110
011001 0110 111001 011001 0011110

Comparative Study: Iran, Russia & PRC Cyber Conflict

Presentation Abstract:
Nation State Motivations for Using the Cyber Realm – Comparative Study of Islamic Republic of Iran, Russian Federation & the People's Republic of China (中華人民共和國)…

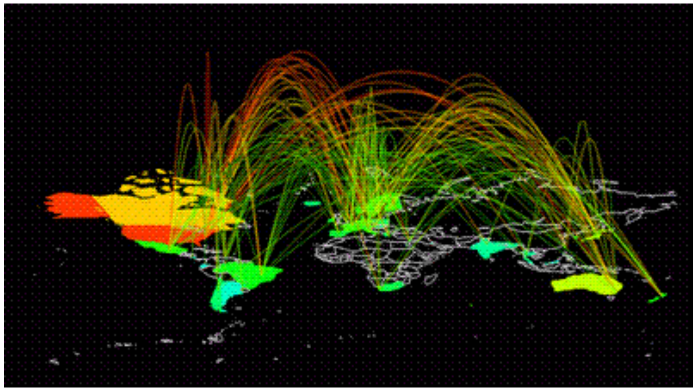
International governments including the Islamic Republic of Iran, Russian Federation and the People's Republic of China (中華人民共和國)...

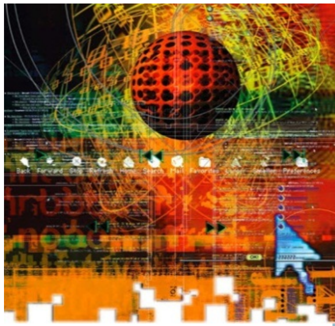
all have very well developed cyber capabilities both offensively and defensively;

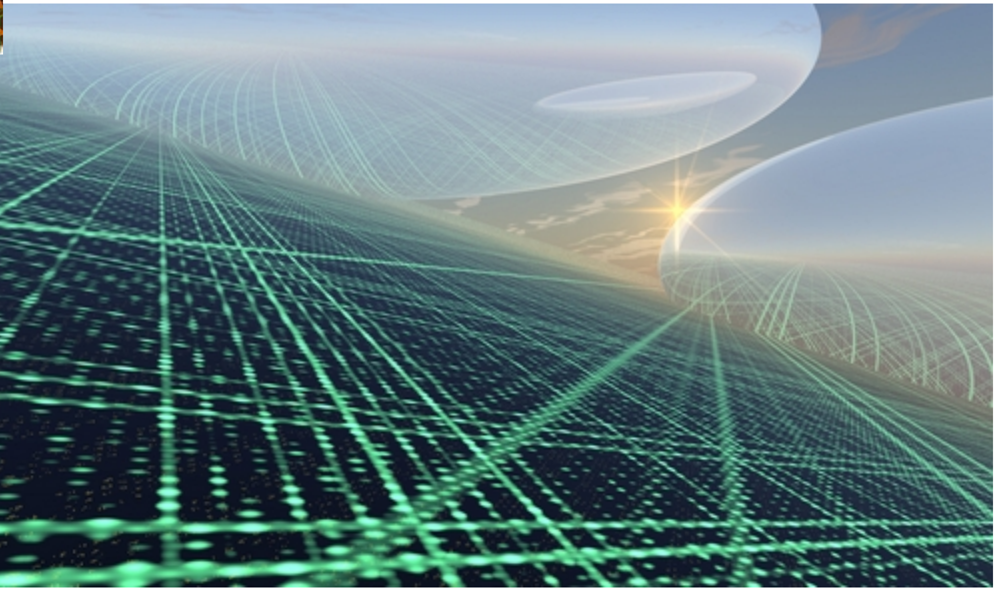
this is the Western world view.

During this presentation a foreigner's international experience reviewing, studying and researching these three nation states will be presented. Included in this 360 degree review will be both the Western/foreigner's perspective and the distinct motivations by each country to feel compelled to develop such technologically advanced national security weapons in the information realm.

The international lens used to review the nation state cyber weapons platform development will incorporate cultural, historical, linguistic, military, political and technological foci…

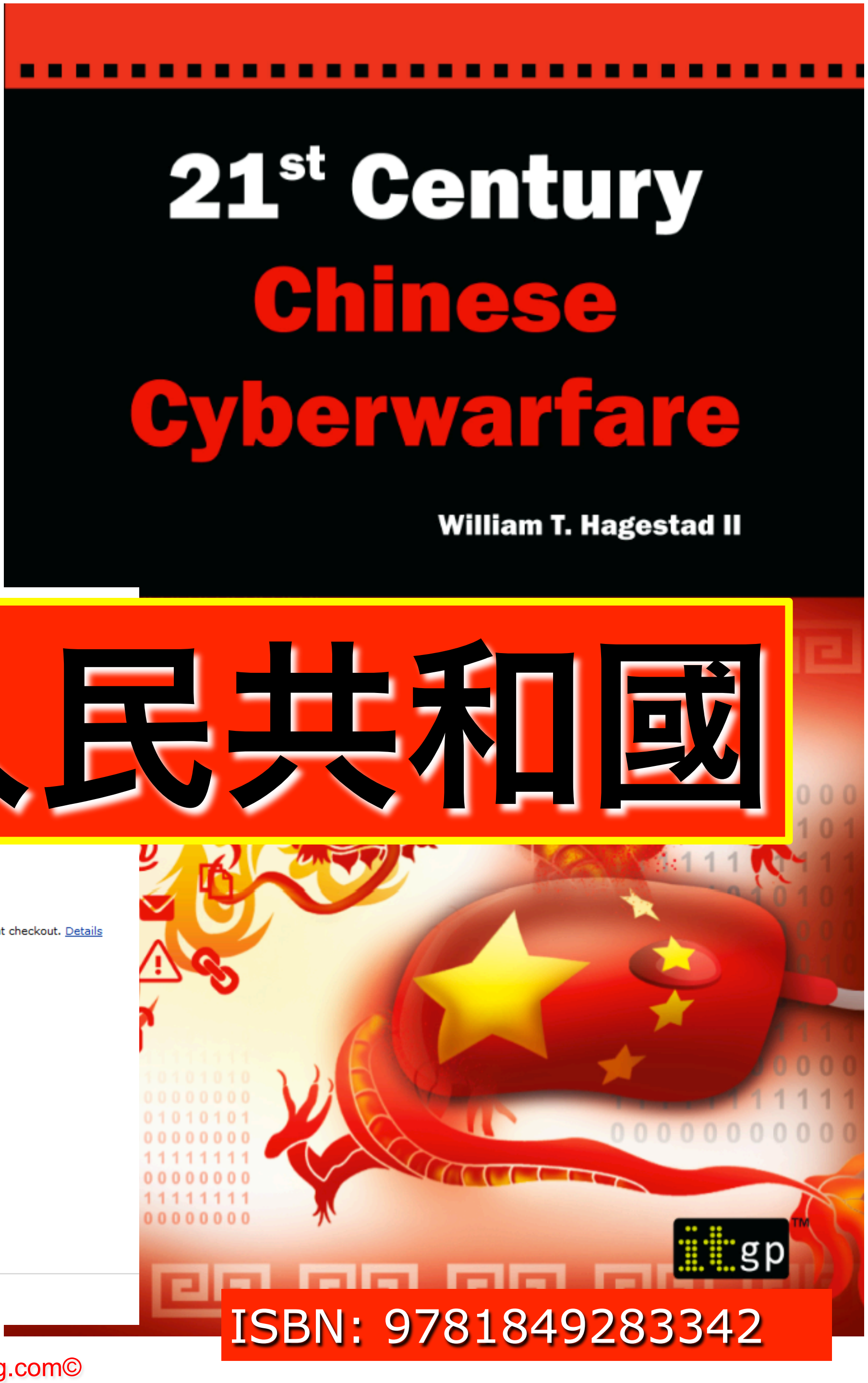


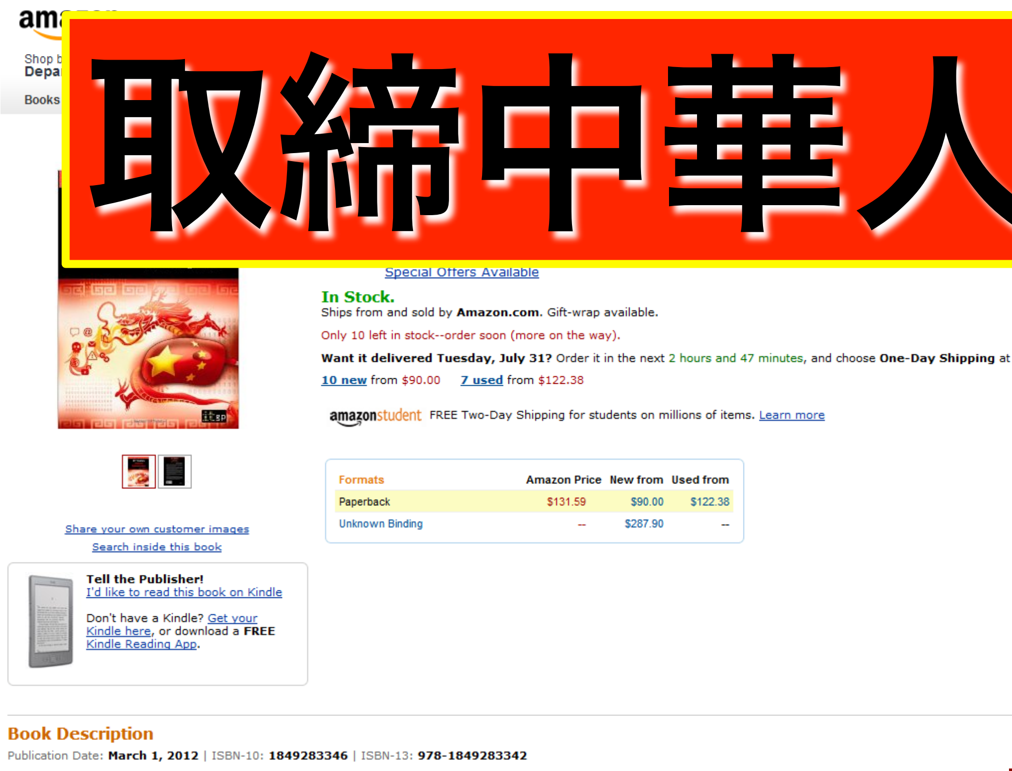




“21st Century Chinese Cyber Warfare”

“二十一世紀中國網絡戰”





Special Offers Available

In Stock.
Ships from and sold by **Amazon.com**. Gift-wrap available.

Only 10 left in stock--order soon (more on the way).

Want it delivered Tuesday, July 31? Order it in the next 2 hours and 47 minutes, and choose **One-Day Shipping** at checkout. Details

10 new from $90.00   7 used from $122.38

amazonstudent FREE Two-Day Shipping for students on millions of items. Learn more

Formats	Amazon Price	New from	Used from
Paperback	$131.59	$90.00	$122.38
Unknown Binding	--	$287.90	--

Share your own customer images
Search inside this book

Tell the Publisher!
I'd like to read this book on Kindle

Don't have a Kindle? Get your Kindle here, or download a **FREE** Kindle Reading App.

Book Description
Publication Date: **March 1, 2012** | ISBN-10: **1849283346** | ISBN-13: **978-1849283342**

取締中華人民共和國

ISBN: 9781849283342

"The Pentagon's Cyber Strategy"

Future Cyber Capabilities “The capabilities being sought would allow U.S. cyber-warriors to "deceive, deny, disrupt, degrade and destroy" information and computers around the globe”.

5 basic principles of the future US CYBER strategy:

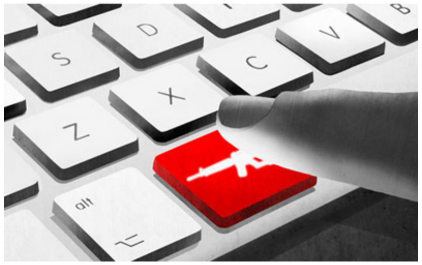
- Cyber must be recognized as a warfare domain equal to land, sea, & air;

- Any defensive posture must go beyond “good hygiene” including sophisticated & accurate operations that allow rapid response;

- Cyber defenses must reach beyond the department’s dot-mil world into commercial networks, as governed by DHS;

- Cyber defenses must be pursued with international allies for an effective “shared warning” of threats; and…

- US Defense Department must help to maintain & leverage U.S. technological dominance…improve acquisitions process… keep up with the speed & agility of the information technology industry…



William J. Lynn III W. Defending a New Domain: The Pentagon's Cyberstrategy.// Foreign Affairs. September/October 2010. http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain(29.08.2010)
Webster S. Pentagon may apply preemptive warfare policy to the Internet. August 29, 2010. http://www.rawstory.com/rs/2010/0829/pentagon-weighs-applying-preemptive-warfare-tactics-internet/(30.08.2010)

Cyber Adversary Taxonomy

Cyber Threat	Motive	Targets of Opportunity	Methodologies	Capabilities
Nation States ~ Peace Time	Economic, Military, National Secrets, Political	Commercial Enterprises, Intelligence, National Defense, Governments, National Infrastructure	Military & Intel specific cyber doctrine, hacktivists	Asymmetric use of the cyber domain short of kinetic
Nation States ~ War Time	Economic, Military, Political	Commercial Enterprises, Intelligence, National Defense, Governments, National Infrastructure	Military & Intel specific cyber doctrine, hacktivists	Asymmetric use of the cyber domain including kinetic
Cyber Terrorists & Insurgents	Political	Infrastructure, Extortion and Political Processes	Combination of advanced persistent threats (APT)	Developing – will be a concern in 2012
Cyber Criminals – Grey & Black Markets	Financial	Intellectual Property Theft, Fraud, Theft, Scams, Hijacked Network & Computer Resources, Cyber Crime for Hire	Exploits, Malware Botnets, Worms & Trojans	Cell-based structure as an APT
Criminal Organizations – RBN	Financial		Use of above with distinct planning	Highly professional, dangerous
Rogue Organizations – Anonymous, LulzSec	Financial Military, National Secrets, Political	Intellectual Property Theft, Direct & Indirect pressure on OGA Resources	Organic hacking capabilities unsurpassed	Organized yet de-centralized

OCINX Report

Office of the National Counterintelligence Executive (ONCIX)…2011 Report "Foreign Economic and Industrial Espionage"

COUNTERINTELLIGENCE

OFFICE OF THE NATIONAL COUNTERINTELLIGENCE EXECUTIVE

FOREIGN SPIES STEALING US ECONOMIC SECRETS IN CYBERSPACE

Report to Congress on Foreign Economic Collection and Industrial Espionage, 2009-2011

October 2011

7 NOV 2011

Nefarious Nation States…

Orientation…

中華人民共和國…

俄國…

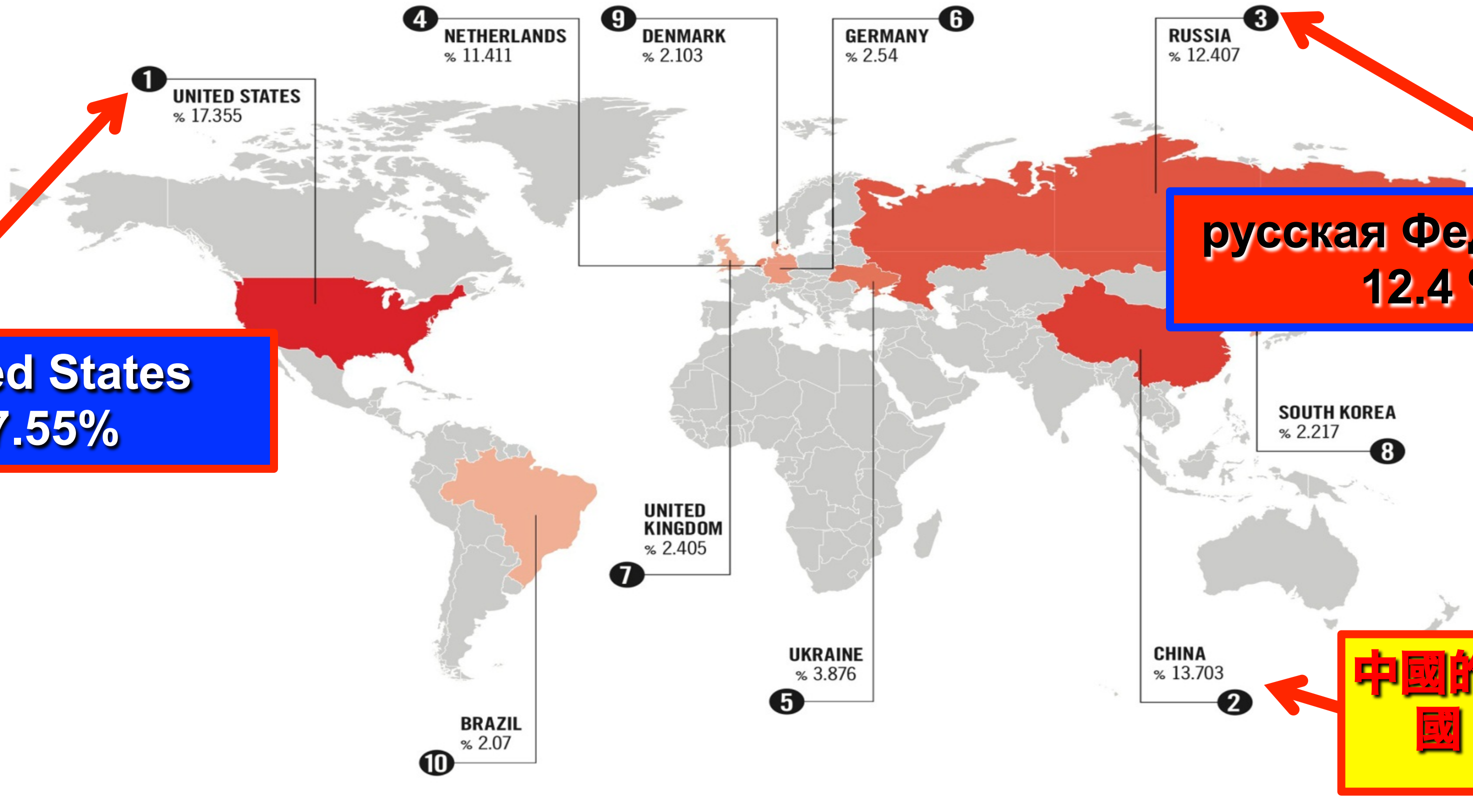
伊朗…

Red-DragonRising.com©

ORIGIN OF HACKS

% BY COUNTRY OF ORIGIN

nccgroup
freedom from doubt



United States
17.55%

русская Федерация
12.4 %

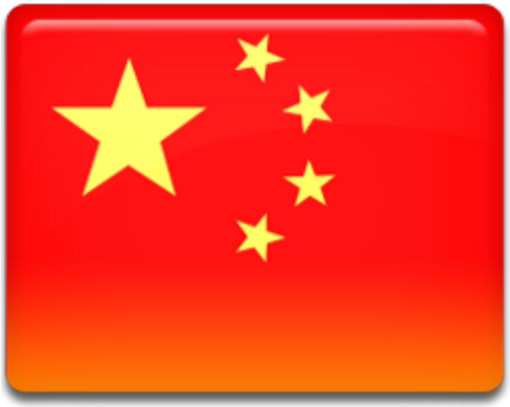
中國的人民共和國 13.7 %

Russia has also shown a large increase, with over 12%
This huge leap has cemented Russia's position in 3rd, behind the United States and China.

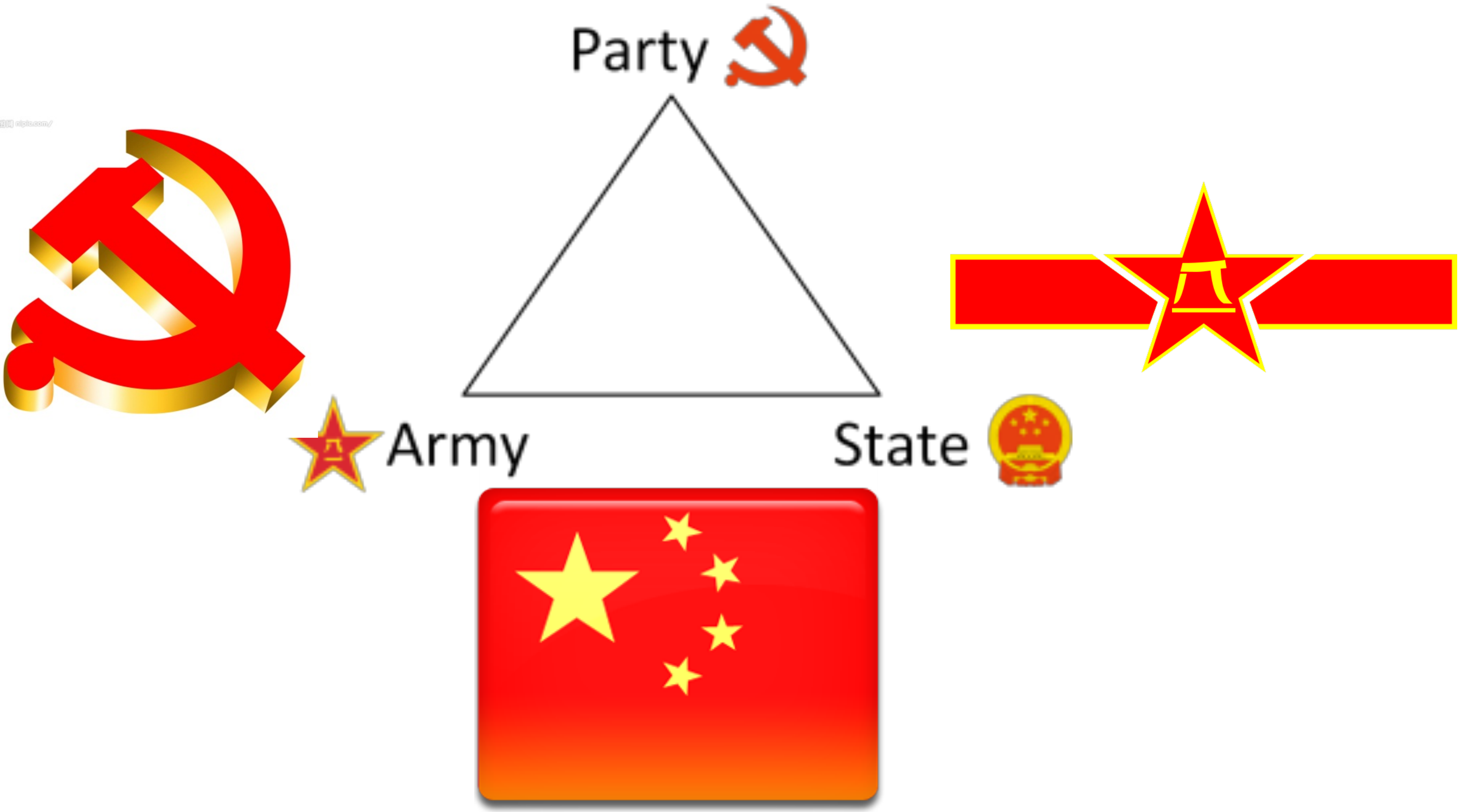
Significant rise in hacks from the Netherlands, up from 3.1% to over 11%, moving it into 4th place in the hacking chart.

www.nccgroup.com/media/169256/origin_of_hacks_q3_2012.pdf

中華人民共和國



中國是誰?



Red-DragonRising.com©

http://www.zerohedge.com/contributed/2013-02-19/meet-latest-boogey-monster

中國人民解放軍
1949 Information Warfare (IW)

“要取得勝利，我們必須盡可能讓敵人盲，聾，密封他的眼睛和耳朵，和他的指揮官在他們的頭腦中製造混亂分心。”

毛泽东 Mao Tse-Tung

人民解放军

500 BC **孫子兵法** - Basis

300 BC **孫臏兵法** - Continued

1995 - Major General Wang Pufeng –

- **Founding father of Chinese Information Warfare (IW)**

1999 - ***War Beyond Limits*** – **超限战**

- **PLAAF Senior Colonel's Qiao Liang & Wang Xiangsui**

2002 - PLA's Information Warfare W strategy spearheaded

- Major General Dai Qingmin -

Integrated Network-Electronic Warfare (INEW)

中國IW官方聲明

20 JUL 2010 – ‘ordered by President Hu Jintao to handle cyber threats as China enters the information age, & strengthen the nation's cyber-infrastructure’

General Staff Directorate’s (GSD) Cyber Warfare ‘Princelings’…

General Zhang Qinsheng 章沁生
General Chen Bingde 陈炳德
General Ma Xiaotian 马晓天
Vice Admiral Sun Jianguo 孙建国
Major General Hou Shu sen 侯树森

漢族…Han Chinese Communist… Technologists… PLA Leaders…. &

中國人

Chinese Military …. Future OPS

“…train a new type of high-caliber military personnel in large numbers, intensively carry out military training under computerized conditions, & enhance integrated combat capability based on extensive IT application…”;

“…implement the military strategy of active defense for the new period, and enhance military strategic guidance as the times so require”;

“…strengthen national defense aim to safeguard China's sovereignty, security and territorial integrity and ensure its peaceful development…“;

“…enhance the capability to accomplish a wide range of military tasks, the most important of which is to win local war in an information age…“;

8 NOV 2012: President Hu JinTao:
“China will speed up full
military IT Applications by 2020”

http://news.xinhuanet.com/english/special/18cpcnc/2012-11/08/c_131959900.htm

Red-DragonRising.com©

Cyber Initiative Comparison

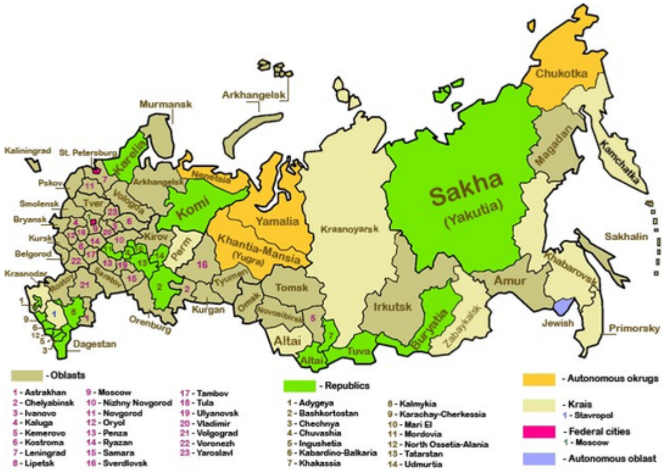
Characteristics	Iran	Russia	China
Started IW/EW			1995
Founding Father			Major General Wang Pu Feng (少將王浦峰)
Used as Combined Arms?			Yes - 2011
Use of Hacktivism as a Proxy?			Yes
Official Military Command			2010
External Motivators			United States of America
Internet Controls?			Yes
Criminal Cyber Capability?			Yes
Impact on Commerce?			Yes

俄國 Russian Federation

KGB (КГБ)

ФЕДЕРАЛЬНАЯ СЛУЖБА БЕЗОПАСНОСТИ

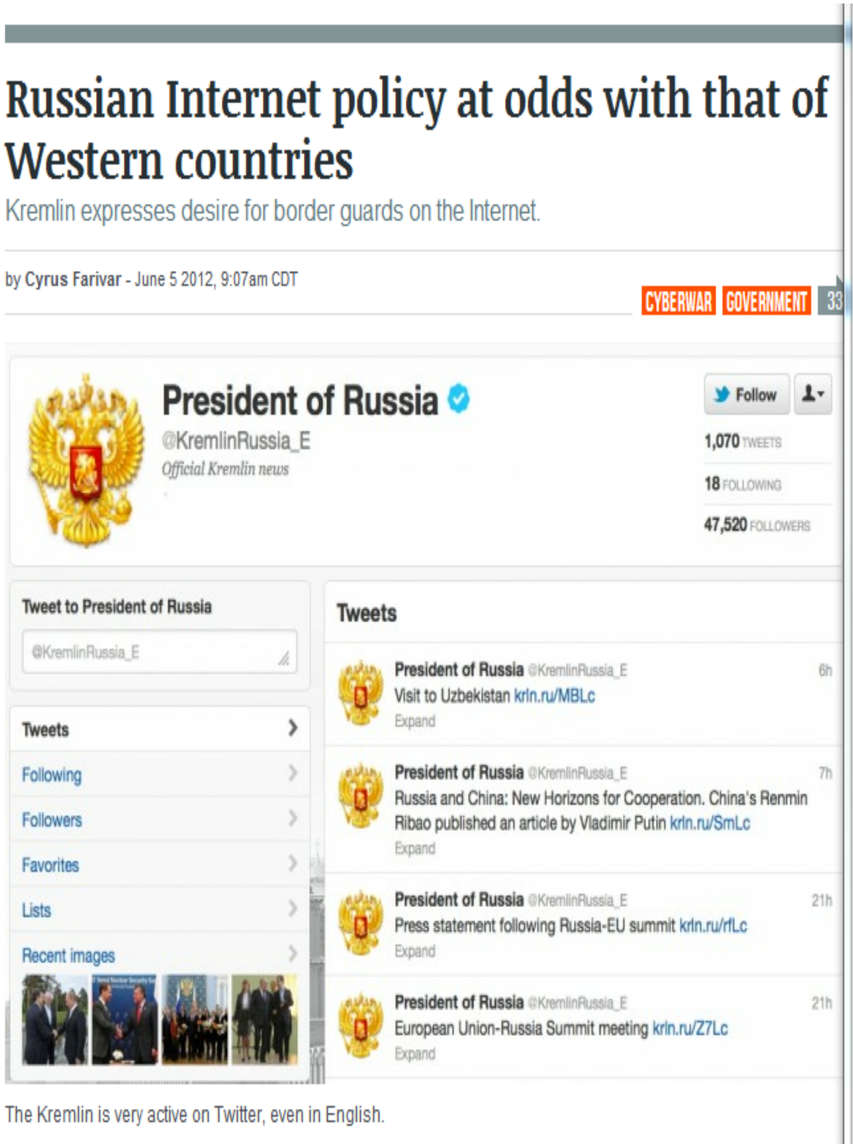
FSB (ФСБ)



ЕДИНАЯ
РОССИЯ

Red-DragonRising.com©

Official Statement of Russian Federation



Russian Internet policy at odds with that of Western countries

Kremlin expresses desire for border guards on the Internet.

by **Cyrus Farivar** - June 5 2012, 9:07am CDT

President of Russia ✓
@KremlinRussia_E
Official Kremlin news

1,070 TWEETS
18 FOLLOWING
47,520 FOLLOWERS

Tweet to President of Russia
@KremlinRussia_E

Tweets

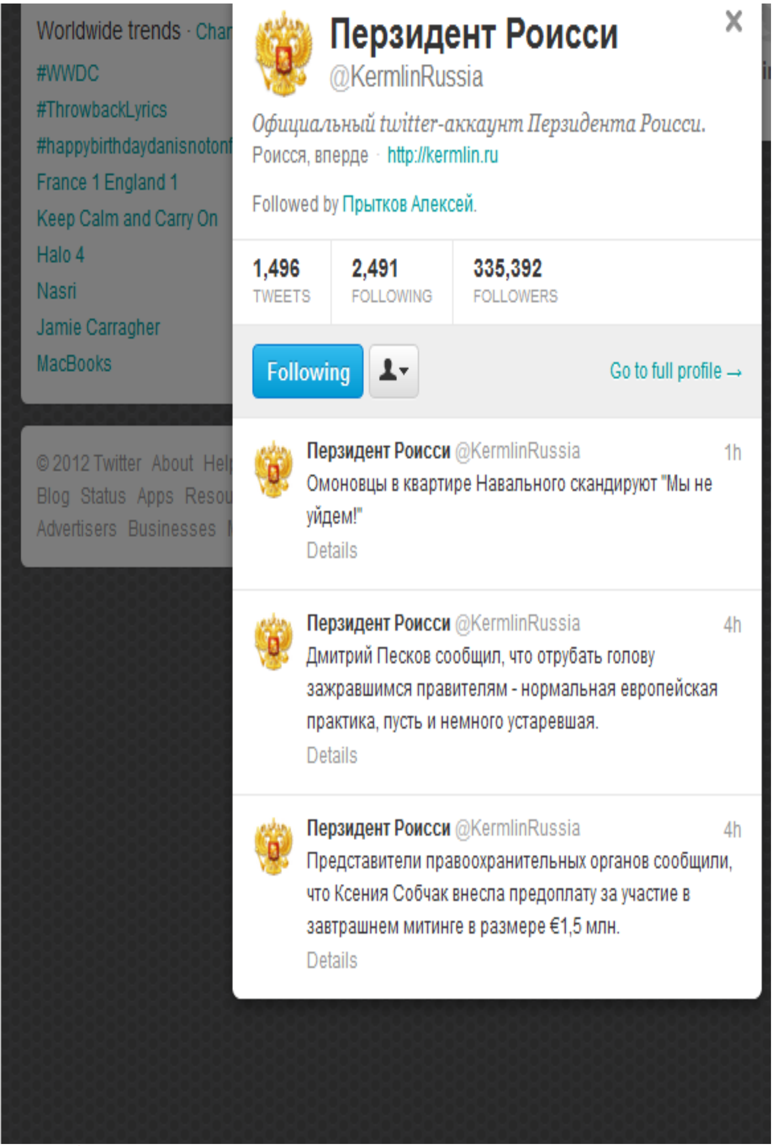
President of Russia @KremlinRussia_E 6h
Visit to Uzbekistan krln.ru/MBLc
Expand

President of Russia @KremlinRussia_E 7h
Russia and China: New Horizons for Cooperation. China's Renmin Ribao published an article by Vladimir Putin krln.ru/SmLc
Expand

President of Russia @KremlinRussia_E 21h
Press statement following Russia-EU summit krln.ru/rfLc
Expand

President of Russia @KremlinRussia_E 21h
European Union-Russia Summit meeting krln.ru/Z7Lc
Expand

The Kremlin is very active on Twitter, even in English.



Worldwide trends · Char
#WWDC
#ThrowbackLyrics
#happybirthdaydanisnotonf
France 1 England 1
Keep Calm and Carry On
Halo 4
Nasri
Jamie Carragher
MacBooks

© 2012 Twitter About Hel
Blog Status Apps Resou
Advertisers Businesses

Перзидент Роисси
@KermlinRussia
Официальный twitter-аккаунт Перзидента Роисси.
Роисся, вперде · http://kermlin.ru

Followed by Прытков Алексей.

1,496 TWEETS
2,491 FOLLOWING
335,392 FOLLOWERS

Перзидент Роисси @KermlinRussia 1h
Омоновцы в квартире Навального скандируют "Мы не уйдем!"
Details

Перзидент Роисси @KermlinRussia 4h
Дмитрий Песков сообщил, что отрубать голову зажравшимся правителям - нормальная европейская практика, пусть и немного устаревшая.
Details

Перзидент Роисси @KermlinRussia 4h
Представители правоохранительных органов сообщили, что Ксения Собчак внесла предоплату за участие в завтрашнем митинге в размере €1,5 млн.
Details

Russian Cyber Evolution…

- December 9th 1999 ~ Military Technical Information
  - Marshall Sergeyev
- 18 January 2000‘There are two wars going on – the actual hostilities and an information war.’

  - Maj Gen Boris Alekseyev

April 22nd 2000 ~ **Military Doctrine**

External Threats – Hostile Information Operations targeting military security
Internal Threats – Disruptive Operations targeting information infrastructure

September 9th 2000 - INFORMATION SECURITY DOCTRINE OF THE RUSSIAN FEDERATION …

Approved by President of the Russian Federation Vladimir Putin on September 9, 2000

Русская Доктрина информационной – Russkaya Doktrina informatsionnoĭ - Russian Information Doctrine

Focus of information weapons development:

Military Technical Information
December 9th 1999
Marshall Sergeyev

Cyber weapons

All-weather reconnaissance and accurate long-range weapons

Guided and electromagnetic energy weapons Stealth unmanned combat platforms (UAV)

Revolution of Military Affairs (RMA) appearance of new types of non- nuclear armaments whose significance… approaches the role of nuclear weapons

МИНИСТЕРСТВО ИНОСТРАННЫХ ДЕЛ
РОССИЙСКОЙ ФЕДЕРАЦИИ
Официальный сайт

29-12-2008

INFORMATION SECURITY DOCTRINE OF THE RUSSIAN FEDERATION

Approved by President of the Russian Federation Vladimir Putin on September 9, 2000

“The Information Security Doctrine of the Russian Federation represents a totality of official views on the goals, objectives, principles and basic guidelines for ensuring information security in the Russian Federation…”

Current Russian Doctrine serves as the basis for:

- shaping government policy on information security in the Russian Federation;
- preparing suggestions to improve the legal, procedural, scientific-technical and organizational framework for ensuring information security in the Russian Federation;
- devising targeted national information security programs.
The present Doctrine expounds the National Security Concept of the Russian Federation as applied to the information sphere…

The Military Doctrine of the Russian Federation
Approved by Russian
Federation Presidential Edict on 5 February 2010

http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b%21OpenDocument

http://kremlin.ru/

Evolution of Russian Cyber Military Doctrine

Federal Agency for Government Communications & Information (FAPSI)
Federal'naya Agenstvo Pravitel'stvennoy Svayazi i Informatsii….

March 2003, FAPSI was abolished by Presidential decree,
functions divided between the FSB and the Ministry of Defense…

ФСБ, Федеральная служба безопасности
Российской Федерации

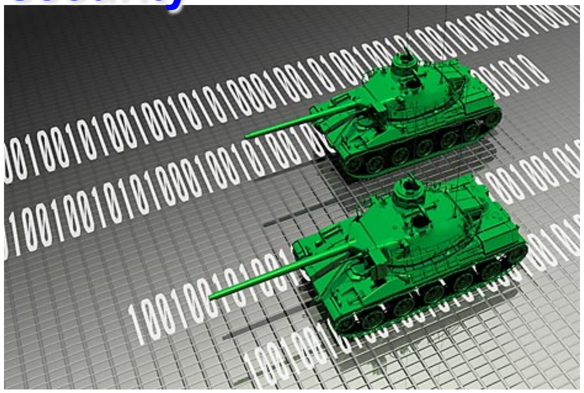
16 April 2010 Russia's Cyber Security Plans

Designed by Vladislav Sherstuyuk, retired general heads Institute of Information Security Issues at Moscow State University sits on Russia's National Security Council

21 March 2012 Russia Considering Cyber-Security Command
~ Deputy Prime Minister Dmitry Rogozin

29 March 2012 … Russian army to increase information security

Desire to keep up with United States
in Digital World Defense…and
respond rather than react…



http://www.technologyreview.com/view/418495/russias-cyber-security-plans/
http://fmso.leavenworth.army.mil/documents/Russianvuiw.htm
http://www.airpower.au.af.mil/airchronicles/apj/apj96/spec96/thomas.html

Official Statement of Russian Armed Forces IW

Russia Must Be Ready for Space, Cyber Wars

Chief of the General Staff of the Russian Armed Forces Nikolai Makarov on 28 January 2012

"As you see, warfare center has moved to aerospace and information spheres, including cyber security, from traditional war theatres on land and sea. Concepts of network-centric war have made great progress," Makarov told an Academy of Military Sciences meeting. "We appraise how ... this question is being solved in Western leading countries."

http://en.rian.ru/mlitary_news/20120128/171006069.html

"Cy-bear" Warfare: Russia's 21st Century Approach ~ Fusing Technology and Warfare

The Russian civilian, military intelligence & security services are increasingly using cyber-attacks, HUMINT, and other intelligence collection operations to ... acquire economic, financial, and propriety data & technology to directly support Russia's economic development and energy security…

Russian Cyber Attacks motivated by interesting factors:

- Chronic requirement to obtain the intelligence Russia desperately needs to drive economic diversification … necessary for long-term viability;
- Enduring Russian paranoia ~ global economic system continues biased against Russia…favoring US & other Western interests @ Russia's expense;
- Russia's continued dependence on natural resources, especially oil & gas….

http://www.foreignpolicydigest.org/cy-bear-warfare-russia-21st-century-approach-to-fusing-technology-and-warfare/
http://soufangroup.com/news/details/?Article_Id=203

The Russian Cyber Bear

Russian organizations responsible for

BOTH offensive & defensive cyber capabilities:

Federal Protective Service or FSO (Federal'naya Sluzhba Okhrani);

FSO has some 20,000 - 30,000 service personnel as well as several thousand civilian personnel …

- Conducting surveillance operations without warrant, responsible for maintaining Russian nuclear equivalent of the U.S. 'football‘…
- FSO also provides secure communications circuits for the Kremlin leadership and the military high command ...

Federal Security Service or FSB (Federal'naya Sluzhba Bezopasnosti);

Military Intelligence apparatus or GRU (Glavnoye Razvedyvatelnoye Upravleniye)

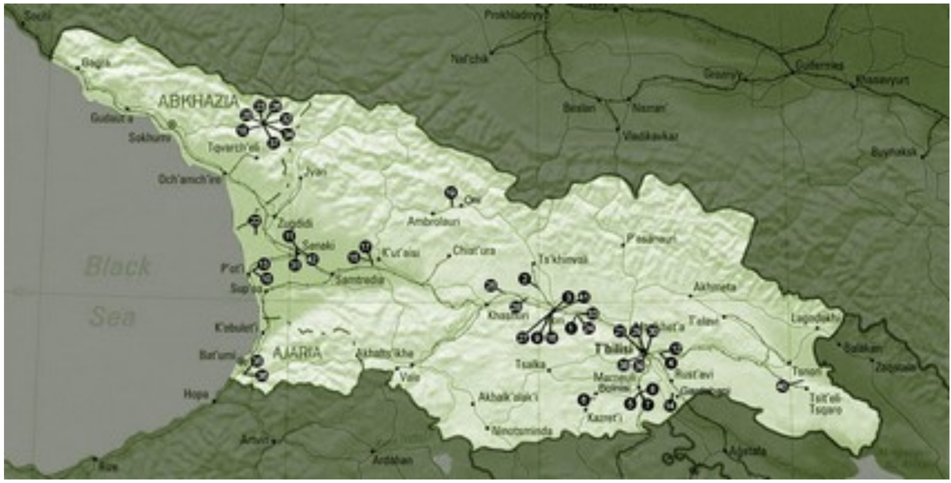
Russian LAW Enforcement & Military Capabilities to carry out Cyber Ops

Russian Invasions Included the First Real Use of "Cyber Warfare"

August 8th, 2008 **Russian troops crossed into South Ossetia vowing to defend what they called "Russian compatriots". As this was taking place, a multi-faceted cyber attack began against the Georgian infrastructure and key government web sites.**

Combined Cyber Arms attack included:

Defacing of Web Sites (Hacktivism), Web-based Psychological Operations (Psyc-Ops), a fierce propaganda campaign (PC) and of course a Distributed Denial of Service Attacks (DDoS)



http://www.acus.org/natosource/russian-intelligence-chief-accuses-west-over-cyber-security
http://defensetech.org/2008/08/13/cyber-war-2-0-russia-v-georgia/
http://www.nytimes.com/2008/08/13/technology/13cyber.html?_r=2&oref=slogin&
http://www.switched.com/2008/08/12/georgia-accuses-russia-of-conducting-cyber-warfare/

Russian Cyber War 2009

Russia engaged in cyber war with neighboring countries…

- January marked “the third successful cyber attack against a country” — when suspected Russian attackers distributed a denial of service attack that overwhelmed three of the four Internet service providers in Kyrgyzstan, disrupting Internet access…ZDNet.

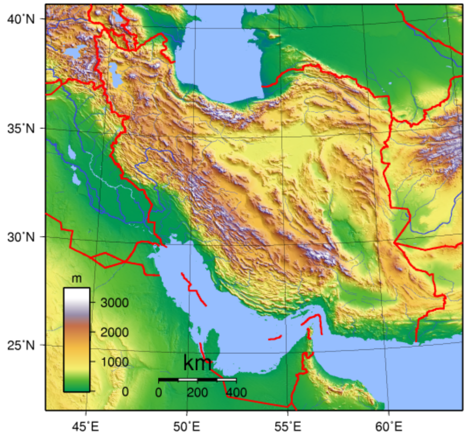
http://www.zdnet.com/blog/gadgetreviews/russia-engaged-in-cyber-war-with-neighboring-countries/1110

Red-DragonRising.com©

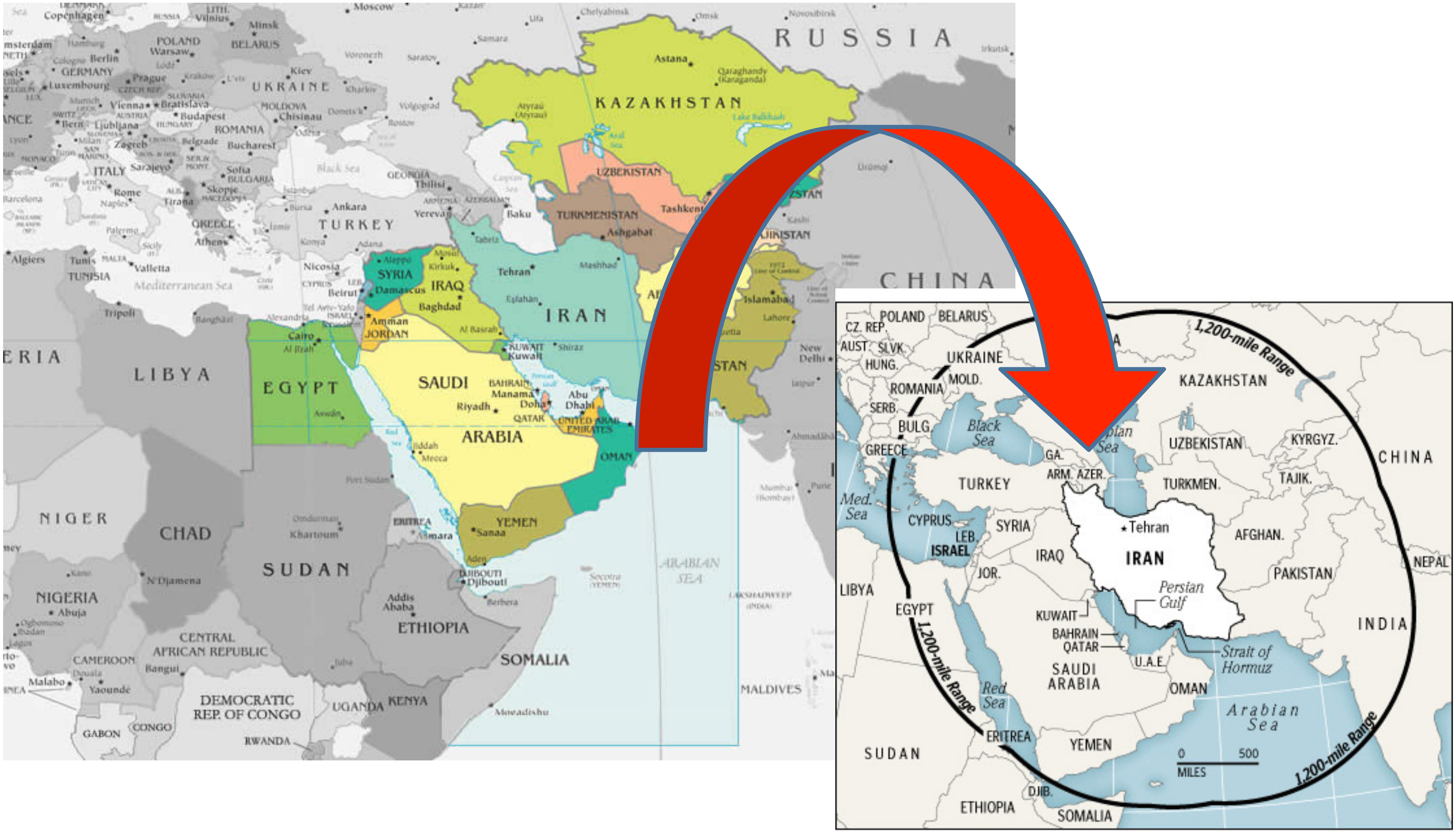
Cyber Initiative Comparison

Characteristics	Iran	Russia	China
Started IW/EW		**1999**	1995
Founding Father		**S.P. Rastorguev (Расторгуев С.П.) & Marshall Sergeyev (Маршалл Сергеев)**	Major General Wang Pu Feng (少將王浦峰)
Used as Combined Arms?		**Yes 2007 & 2008**	Yes - 2011
Use of Hacktivism as a Proxy?		**Yes – w/criminal intentions**	Yes
Official Military Command		**2010**	2010
External Motivators		**United States of America**	United States of America
Internet Controls?		**Yes**	Yes
Criminal Cyber Capability?		**Yes**	Yes
Impact on Commerce?		**Yes**	Yes

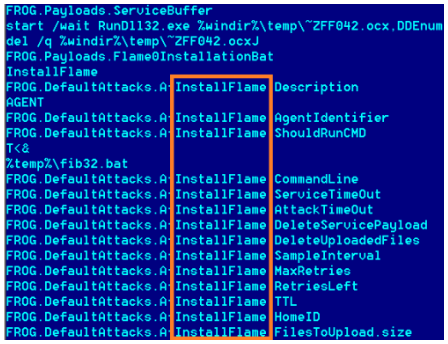
Islamic Republic of Iran



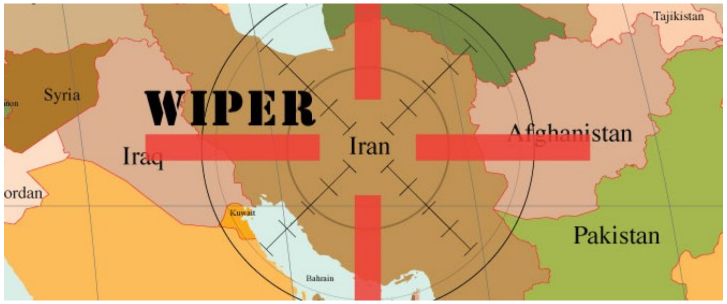
Where is Iran……

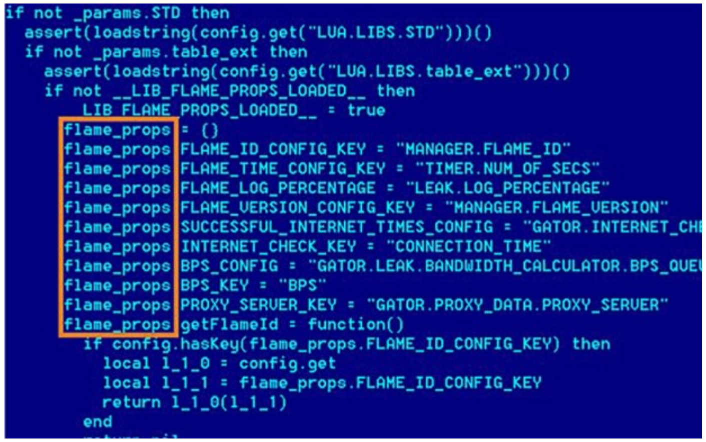


- ○ STUXNET
- ○ DUQU
- ○ FLAME
- ○ WIPER….

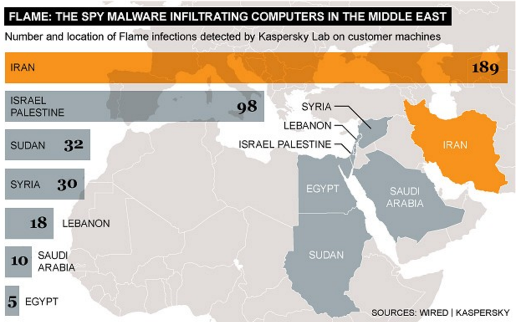


```
FROG.Payloads.ServiceBuffer
start /wait RunDll32.exe %windir%\temp\~ZFF042.ocx,DDEnum
del /q %windir%\temp\~ZFF042.ocxJ
FROG.Payloads.Flame0InstallationBat
InstallFlame
FROG.DefaultAttacks.A InstallFlame Description
AGENT
FROG.DefaultAttacks.A InstallFlame AgentIdentifier
FROG.DefaultAttacks.A InstallFlame ShouldRunCMD
T<&
%temp%\fib32.bat
FROG.DefaultAttacks.A InstallFlame CommandLine
FROG.DefaultAttacks.A InstallFlame ServiceTimeOut
FROG.DefaultAttacks.A InstallFlame AttackTimeOut
FROG.DefaultAttacks.A InstallFlame DeleteServicePayload
FROG.DefaultAttacks.A InstallFlame DeleteUploadedFiles
FROG.DefaultAttacks.A InstallFlame SampleInterval
FROG.DefaultAttacks.A InstallFlame MaxRetries
FROG.DefaultAttacks.A InstallFlame RetriesLeft
FROG.DefaultAttacks.A InstallFlame TTL
FROG.DefaultAttacks.A InstallFlame HomeID
FROG.DefaultAttacks.A InstallFlame FilesToUpload.size
```





```
if not _params.STD then
  assert(loadstring(config.get("LUA.LIBS.STD")))()
  if not _params.table_ext then
    assert(loadstring(config.get("LUA.LIBS.table_ext")))()
    if not __LIB_FLAME_PROPS_LOADED__ then
        LIB FLAME PROPS_LOADED__ = true
      flame_props = {}
      flame_props FLAME_ID_CONFIG_KEY = "MANAGER.FLAME_ID"
      flame_props FLAME_TIME_CONFIG_KEY = "TIMER.NUM_OF_SECS"
      flame_props FLAME_LOG_PERCENTAGE = "LEAK.LOG_PERCENTAGE"
      flame_props FLAME_VERSION_CONFIG_KEY = "MANAGER.FLAME_VERSION"
      flame_props SUCCESSFUL_INTERNET_TIMES_CONFIG = "GATOR.INTERNET_CHE
      flame_props INTERNET_CHECK_KEY = "CONNECTION_TIME"
      flame_props BPS_CONFIG = "GATOR.LEAK.BANDWIDTH_CALCULATOR.BPS_QUEU
      flame_props BPS_KEY = "BPS"
      flame_props PROXY_SERVER_KEY = "GATOR.PROXY_DATA.PROXY_SERVER"
      flame_props getFlameId = function()
        if config.hasKey(flame_props.FLAME_ID_CONFIG_KEY) then
          local l_1_0 = config.get
          local l_1_1 = flame_props.FLAME_ID_CONFIG_KEY
          return l_1_0(l_1_1)
        end
```

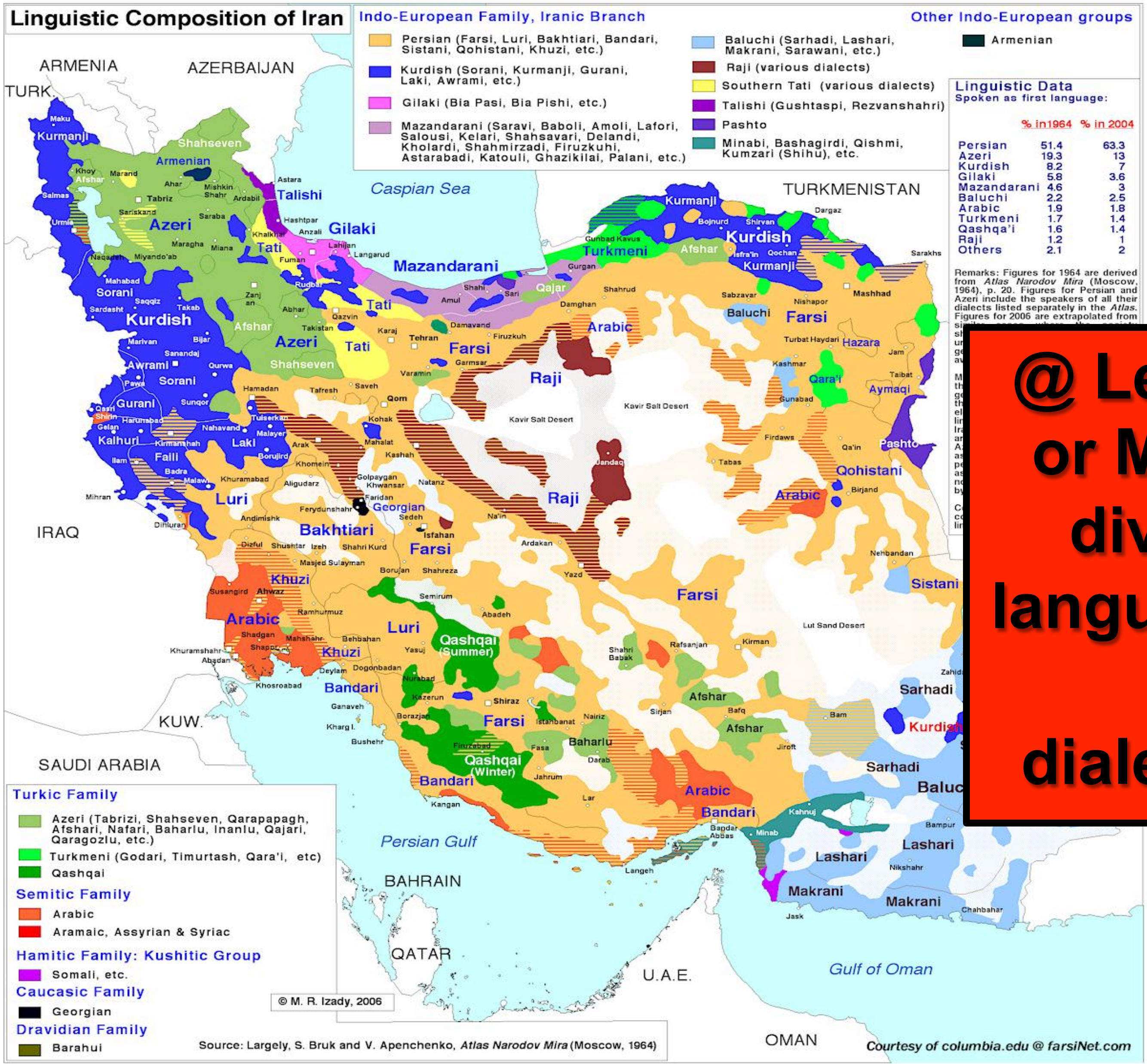


FLAME: THE SPY MALWARE INFILTRATING COMPUTERS IN THE MIDDLE EAST

Number and location of Flame infections detected by Kaspersky Lab on customer machines

SOURCES: WIRED | KASPERSKY

زبان های گوناگون



Linguistic Composition of Iran

Indo-European Family, Iranic Branch

- 🟧 Persian (Farsi, Luri, Bakhtiari, Bandari, Sistani, Qohistani, Khuzi, etc.)
- 🟦 Kurdish (Sorani, Kurmanji, Gurani, Laki, Awrami, etc.)
- 🟪 Gilaki (Bia Pasi, Bia Pishi, etc.)
- 🟪 Mazandarani (Saravi, Baboli, Amoli, Lafori, Salousi, Kelari, Shahsavari, Delandi, Kholardi, Shahmirzadi, Firuzkuhi, Astarabadi, Katouli, Ghazikilai, Palani, etc.)
- 🟦 Baluchi (Sarhadi, Lashari, Makrani, Sarawani, etc.)
- 🟫 Raji (various dialects)
- 🟨 Southern Tati (various dialects)
- 🟪 Talishi (Gushtaspi, Rezvanshahri)
- 🟪 Pashto
- 🟩 Minabi, Bashagirdi, Qishmi, Kumzari (Shihu), etc.

Other Indo-European groups

- ⬛ Armenian

Linguistic Data
Spoken as first language:

	% in1964	% in 2004
Persian	51.4	63.3
Azeri	19.3	13
Kurdish	8.2	7
Gilaki	5.8	3.6
Mazandarani	4.6	3
Baluchi	2.2	2.5
Arabic	1.9	1.8
Turkmeni	1.7	1.4
Qashqa'i	1.6	1.4
Raji	1.2	1
Others	2.1	2

Remarks: Figures for 1964 are derived from *Atlas Narodov Mira* (Moscow, 1964), p. 20. Figures for Persian and Azeri include the speakers of all their dialects listed separately in the *Atlas*. Figures for 2006 are extrapolated from

Turkic Family

- 🟩 Azeri (Tabrizi, Shahseven, Qarapapagh, Afshari, Nafari, Baharlu, Inanlu, Qajari, Qaragozlu, etc.)
- 🟩 Turkmeni (Godari, Timurtash, Qara'i, etc)
- 🟩 Qashqai

Semitic Family

- 🟧 Arabic
- 🟥 Aramaic, Assyrian & Syriac

Hamitic Family: Kushitic Group

- 🟪 Somali, etc.

Caucasic Family

- ⬛ Georgian

Dravidian Family

- 🟫 Barahui

© M. R. Izady, 2006

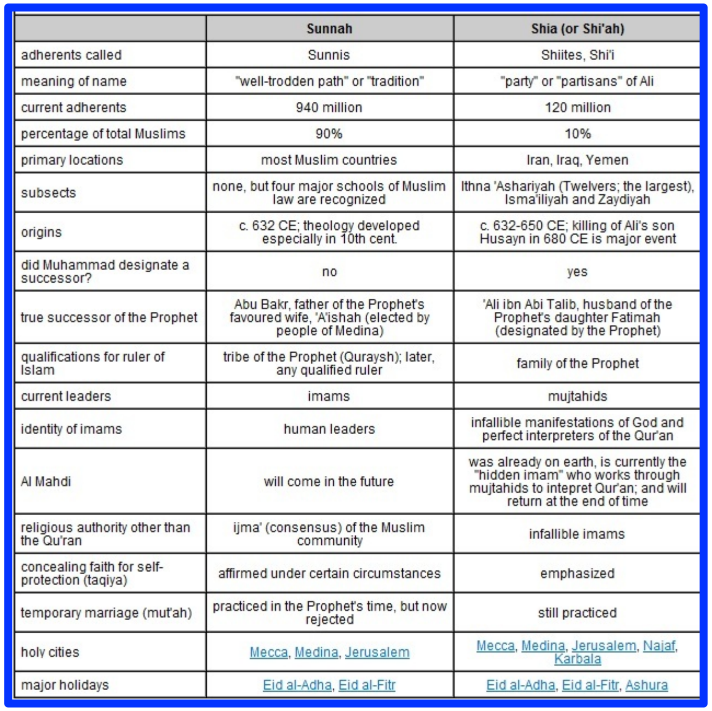
Source: Largely, S. Bruk and V. Apenchenko, *Atlas Narodov Mira* (Moscow, 1964)

Courtesy of columbia.edu @ farsiNet.com

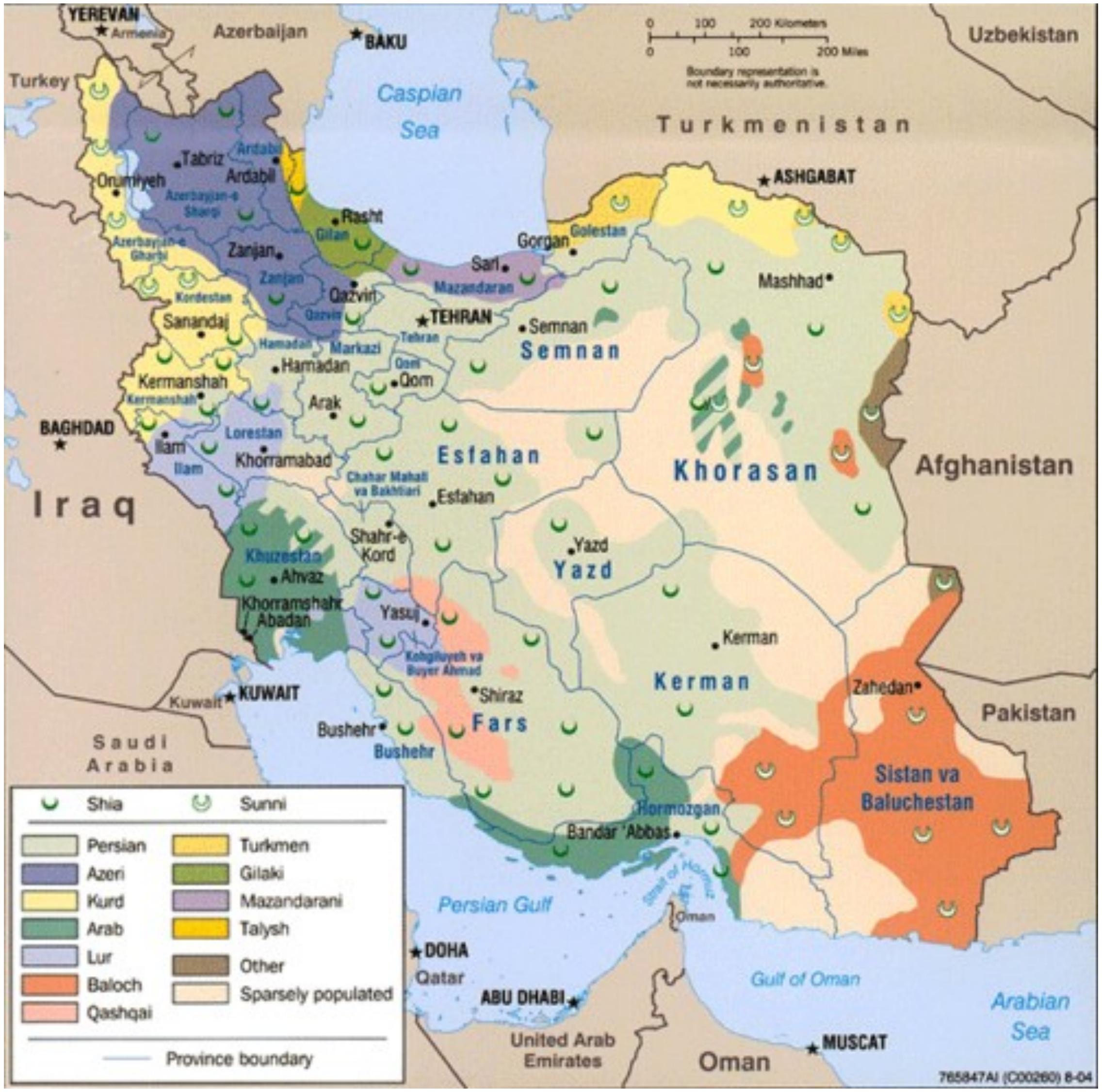
@ Least 18 or More… diverse languages… or dialects….

Shi'ah…Sunnah…BOTH!

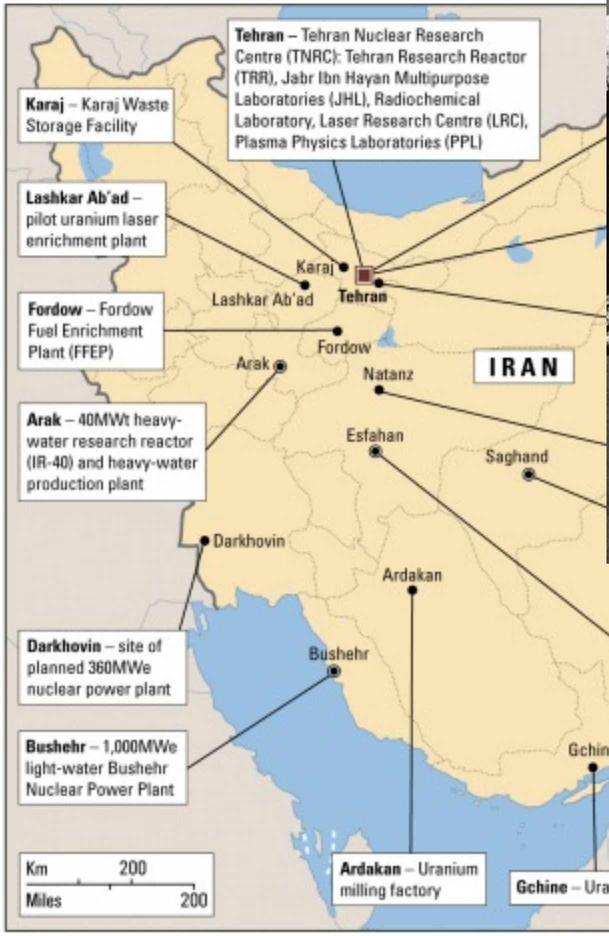
@ Least 12 or More…diverse ethnicities…. & Yet 2 Religions….

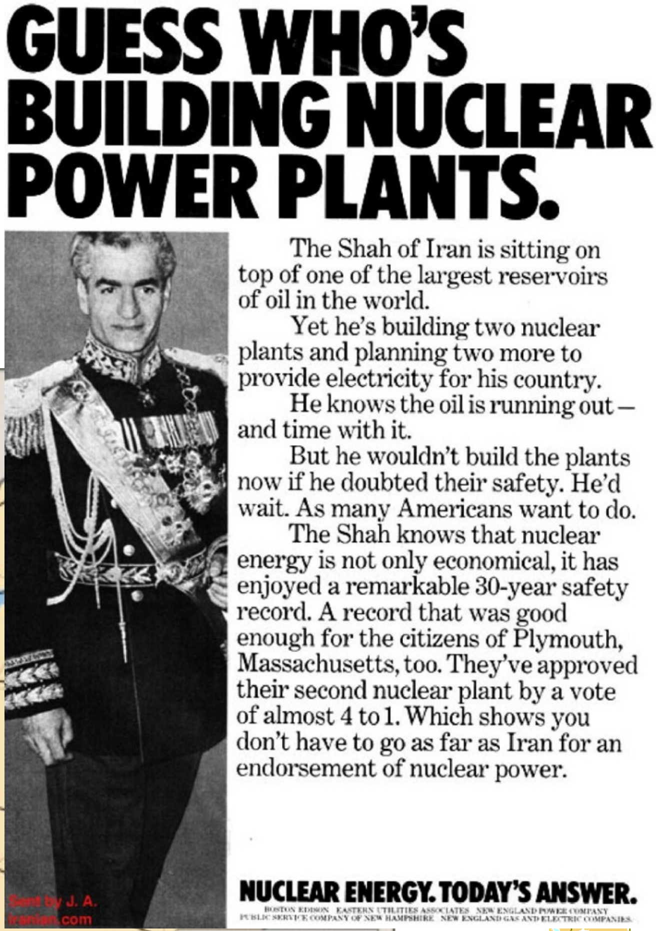


	Sunnah	Shia (or Shi'ah)
adherents called	Sunnis	Shiites, Shi'i
meaning of name	"well-trodden path" or "tradition"	"party" or "partisans" of Ali
current adherents	940 million	120 million
percentage of total Muslims	90%	10%
primary locations	most Muslim countries	Iran, Iraq, Yemen
subsects	none, but four major schools of Muslim law are recognized	Ithna 'Ashariyah (Twelvers; the largest), Isma'iliyah and Zaydiyah
origins	c. 632 CE; theology developed especially in 10th cent.	c. 632-650 CE; killing of Ali's son Husayn in 680 CE is major event
did Muhammad designate a successor?	no	yes
true successor of the Prophet	Abu Bakr, father of the Prophet's favoured wife, 'A'ishah (elected by people of Medina)	'Ali ibn Abi Talib, husband of the Prophet's daughter Fatimah (designated by the Prophet)
qualifications for ruler of Islam	tribe of the Prophet (Quraysh); later, any qualified ruler	family of the Prophet
current leaders	imams	mujtahids
identity of imams	human leaders	infallible manifestations of God and perfect interpreters of the Qur'an
Al Mahdi	will come in the future	was already on earth, is currently the "hidden imam" who works through mujtahids to intepret Qur'an; and will return at the end of time
religious authority other than the Qu'ran	ijma' (consensus) of the Muslim community	infallible imams
concealing faith for self-protection (taqiya)	affirmed under certain circumstances	emphasized
temporary marriage (mut'ah)	practiced in the Prophet's time, but now rejected	still practiced
holy cities	Mecca, Medina, Jerusalem	Mecca, Medina, Jerusalem, Najaf, Karbala
major holidays	Eid al-Adha, Eid al-Fitr	Eid al-Adha, Eid al-Fitr, Ashura



Red-DragonRising.com©


Tehran – Tehran Nuclear Research Centre (TNRC): Tehran Research Reactor (TRR), Jabr Ibn Hayan Multipurpose Laboratories (JHL), Radiochemical Laboratory, Laser Research Centre (LRC), Plasma Physics Laboratories (PPL)
Karaj – Karaj Waste Storage Facility
Lashkar Ab'ad – pilot uranium laser enrichment plant
Fordow – Fordow Fuel Enrichment Plant (FFEP)
Arak – 40MWt heavy-water research reactor (IR-40) and heavy-water production plant
Darkhovin – site of planned 360MWe nuclear power plant
Bushehr – 1,000MWe light-water Bushehr Nuclear Power Plant
Ardakan – Uranium milling factory
Gchine – Uranium mine
Saghand – Uranium mine
Esfahan – Esfahan Nuclear Technology Centre (ENTC): Uranium Conversion Facility (UCF); Fuel Manufacturing Plant (FMP), Fuel Fabrication Laboratory, Zirconium Production Plant, four small research reactors
Karaj
Tehran
Lashkar Ab'ad
Fordow
Arak
Natanz
IRAN
Esfahan
Saghand
Darkhovin
Ardakan
Bushehr
Gchine
Km 200
Miles 200
© IISS



GUESS WHO'S BUILDING NUCLEAR POWER PLANTS.

The Shah of Iran is sitting on top of one of the largest reservoirs of oil in the world.

Yet he's building two nuclear plants and planning two more to provide electricity for his country.

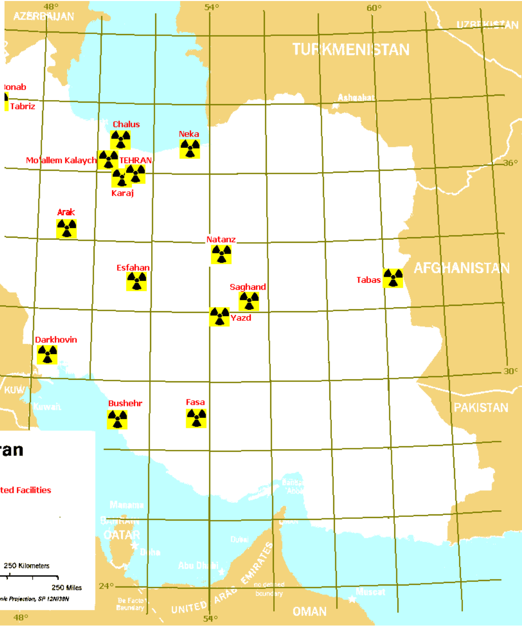
He knows the oil is running out – and time with it.

But he wouldn't build the plants now if he doubted their safety. He'd wait. As many Americans want to do.

The Shah knows that nuclear energy is not only economical, it has enjoyed a remarkable 30-year safety record. A record that was good enough for the citizens of Plymouth, Massachusetts, too. They've approved their second nuclear plant by a vote of almost 4 to 1. Which shows you don't have to go as far as Iran for an endorsement of nuclear power.

NUCLEAR ENERGY. TODAY'S ANSWER.

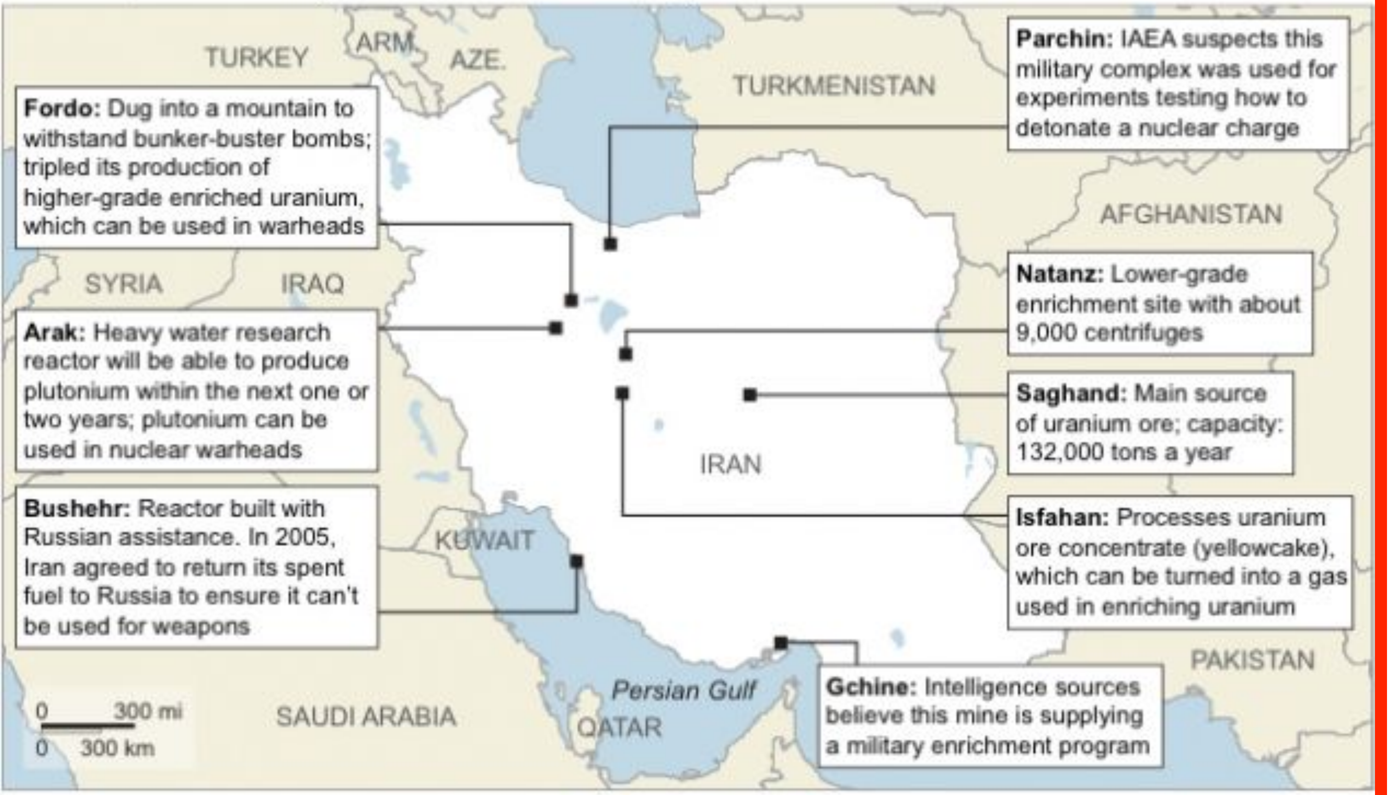
BOSTON EDISON EASTERN UTILITIES ASSOCIATES NEW ENGLAND POWER COMPANY
PUBLIC SERVICE COMPANY OF NEW HAMPSHIRE NEW ENGLAND GAS AND ELECTRIC COMPANIES.



Iranian Infrastructure… Cyber Target

Iran's nuclear sites

Iran is suspected of having a secret military nuclear program. Some of Iran's known nuclear sites:



Fordo: Dug into a mountain to withstand bunker-buster bombs; tripled its production of higher-grade enriched uranium, which can be used in warheads

Arak: Heavy water research reactor will be able to produce plutonium within the next one or two years; plutonium can be used in nuclear warheads

Bushehr: Reactor built with Russian assistance. In 2005, Iran agreed to return its spent fuel to Russia to ensure it can't be used for weapons

Parchin: IAEA suspects this military complex was used for experiments testing how to detonate a nuclear charge

Natanz: Lower-grade enrichment site with about 9,000 centrifuges

Saghand: Main source of uranium ore; capacity: 132,000 tons a year

Isfahan: Processes uranium ore concentrate (yellowcake), which can be turned into a gas used in enriching uranium

Gchine: Intelligence sources believe this mine is supplying a military enrichment program

SOURCE: ESRI

AP

Red-DragonRising.com©

Operation Olympic Games

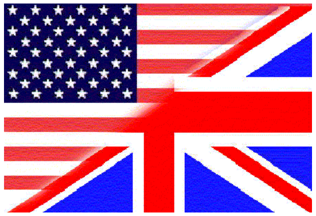
Target: Iranian Critical Infrastructure

Key Players: United States, Israel, United Kingdom

Objective: Destroy & degrade Iran’s Nuclear Plutonium Enrichment

Intelligence Estimate: **likening the cyber sabotage of Iran’s plants in some senses to the August 1945 atomic bombing of Hiroshima”**

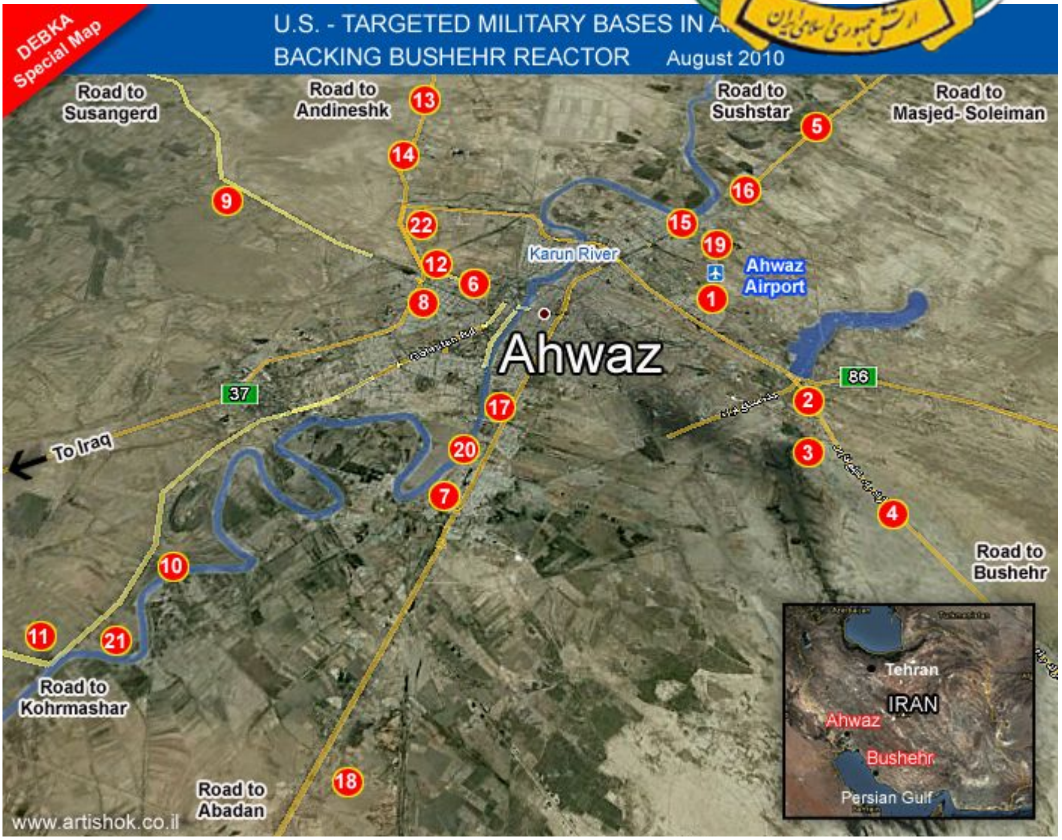
http://thediplomat.com/2012/06/26/is-u-s-in-iran-cyber-war/?all=true
http://collectinghats.blogspot.com/2009/08/im-not-slow-im-just-american-part-2.html
http://theriskyshift.com/2012/03/israeli-lobby-in-uk-conspiracy-or-anti-html/
http://finchin.com/stuxnet-flame-shape-cyberwars-to-come/



Red-DragonRising.com©

Iranian Military…
& Nuke Facilities…..

- 11. Ahwaz 92nd Division commando companies, which operate independently under their own command are better known as “independent companies.”
- Site above is also used by elements of the division’s 2nd Armored Brigade.
- 12. IRGC 92nd Armored Division’s 3rd Armored Brigade.
- 13. The IRGC’s Isfahan Artillery Brigade.
- 15. The Zargan power station for the military camps in the region which runs on gas.
- 18. A yacht and speedboat marina, recently renovated, for the private use of Revolutionary Guards commanders based in the region.
- 20. A light aircraft airport for ferrying farm produce..
- 21. A 500-meter-wide canal, which links the Karun River to the Majnoun islands in Iraq. Huge barges stand by there in case of an emergency calling for troops to be moved quickly inside the Khuzestan province.
- 22. A missile-anti-aircraft gun cluster for defending Ahwaz and its environs.



Quds – Iranian Intelligence

mme

نیروی قدس

… Niru-ye Qods…

News › World news › Iran

IRANBLOG
INSIDETHECRISIS

Previous   Blog home

Head of Iran's Quds force warns enemies of the regime

In rare comments, Qassem Suleimani says his forces 'will show Iranian zeal in the face of any possible aggression'

The head of Iran's Quds force, commander Qassem Suleimani.

The head of Iran's Quds force, Qassem Suleimani, ke
the media. Unlike other Iranian commanders who make
statements in the face of foreign threats to the Islamic
usually remains quiet.

Mounting pressure on Iran from Israel, however, has le
the man who heads the external arm of the Iranian rev
tasked with its overseas operations, but to issue a war
military strike against the country.

The semi-official Mehr news agency today quoted Sule
that his armed forces "will show Iranian zeal in the face
aggression against the country".

AL-QUDS DAY 2012
washington dc
FRIDAY AUGUST 17

THE PEOPLE UNITED WILL NEVER BE DEFEATED
alqudsday.org

WORLD PEACE RALLY
Dupont Circle
4PM - 6PM

COMMUNITY DINNER (IFTAR)
St. Stephens Church
1525 Newton Street NW
7PM - 10PM

- **Founded after 1979…Iran's Revolution…**

Sepāh-e Pāsdārān- / سپاه پاسداران انقلاب اسلامی
…Enqelāb-e Eslāmi

- **Army of the Guardians of the Islamic Revolution (IGRC)**
- **Commanded by Major General Qassem Suleimani**
- **Experience in Soviet Afghanistan, Bosnia….Iraq…'Stan's Redux…**
- **Iranian Military Support regionally…Syria…**
- **Reports directly to Supreme Leader of Iran Ayatollah Ali Khamenei**

نیروی قدس

…..to organize, train, equip, and finance foreign Islamic revolutionary movements. Quds Force maintains and builds contacts with underground Islamic militant organizations throughout the Islamic world….

http://www.guardian.co.uk/world/iran-blog/2012/mar/13/qassem-suleimani-issues-warning

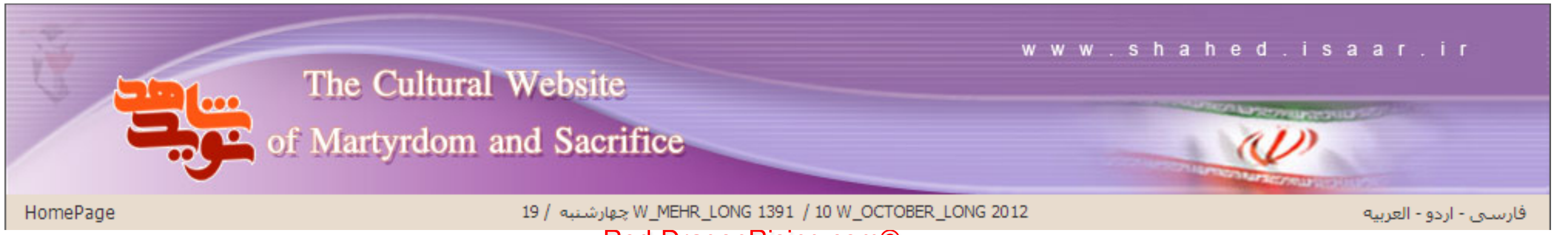
High Council of Cyberspace (Shoray-e Aali-e Fazaye Majazi).

- March 2012 – Order established by Ayatollah Khamenei
- Mission of instituting high-level policies on the cyberspace
- Includes….
  - President of Iran
  - Judicial Power Leader
  - Parliamentary Leader
  - IGRC CINC's
  - Police
  - Minister of Intelligence
  - Telecommunications, Culture & Science Ministers

All other Iranian organizations in charge of cyber operations are committed to implement the policies instituted by this new government body

http://www.cyberstrategie.org/?q=grands-dossiers/conflits-r%C3%A9gionaux-et-cyberterrorisme/structure-of-iran%E2%80%99s-cyber-

ارتش



19 / چهارشنبه W_MEHR_LONG 1391 / 10 W_OCTOBER_LONG 2012

The Cyber Defense Command (Gharargah-e Defa-e Saiberi)

November 2010 – Order established by Ayatollah Khamenei

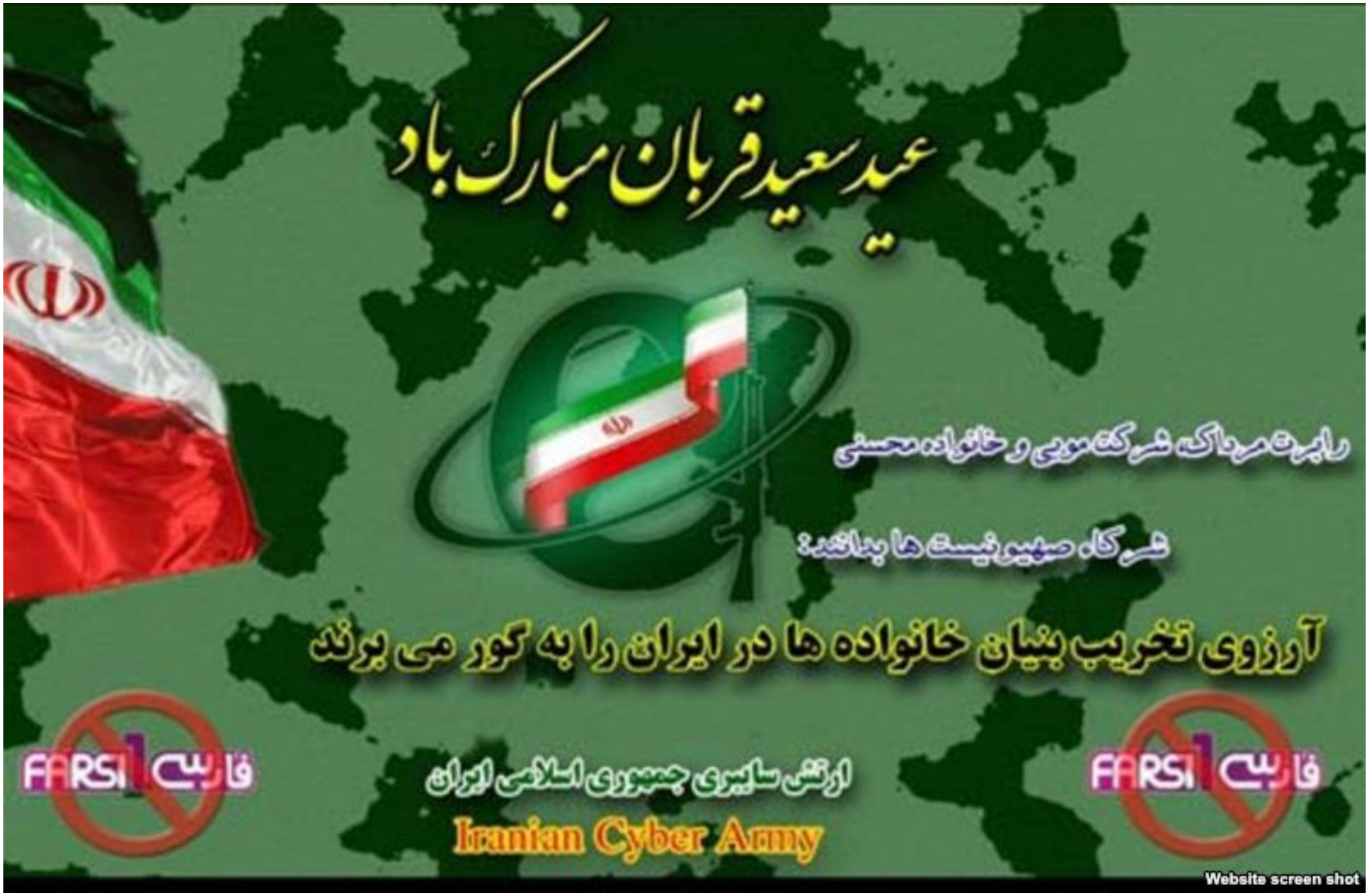
- Mission of responding to NCI effects brought upon by Stuxnet
- Supervised by :
- Joint Staff of the Armed Forces (Setad-e Kol-e Niruhay-e Mosalah)
- Operationally via Passive Civil Defense Organization (Sazeman-e Padafand-e Gheyr-e Amel)

Motivation to establish…..

Coordinating numerous government organizations and agencies to non-militarily respond to a military attack on the country with the goal of minimizing damage to the country's infrastructure and facilities in the event of a probable war…

http://www.cyberstrategie.org/?q=grands-dossiers/conflits-r%C3%A9gionaux-et-cyberterrorisme/structure-of-iran%E2%80%99s-cyber-warfare

ارتش سایبری ایران



عید سعید قربان مبارک باد

رابرت مرداک، شرکت مویی و خانواده محسنی

شرکاء صهیونیست ها بدانند:

آرزوی تخریب بنیان خانواده ها در ایران را به گور می برند

ارتش سایبری جمهوری اسلامی ایران

Iranian Cyber Army

http://www.rferl.org/content/Iranian_Cyber_Army_Hacks_Website_Of_Farsi1/2223708.html

Iran’s Cyber Army (UNOFFICIAL)

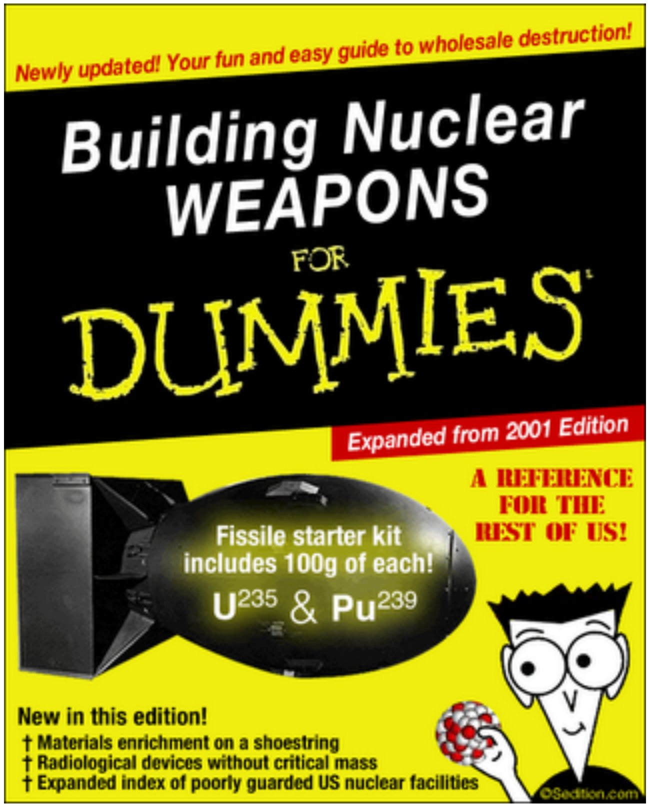
- Highly skilled information technology specialists & professional hackers who obfuscate their identities…
- No one claims responsibility…

  And yet…
- Unassailable evidence suggests that the group is affiliated with the IRGC…

http://www.cyberstrategie.org/?q=grands-dossiers/conflits-r%C3%A9gionaux-et-cyberterrorisme/structure-of-iran%E2%80%99s-cyber-warfare

Red-DragonRising.com©

Basij Paramilitary Force – Cyber Militias … (Rogue…Effective)


Newly updated! Your fun and easy guide to wholesale destruction!
Building Nuclear WEAPONS FOR DUMMIES
Expanded from 2001 Edition
A REFERENCE FOR THE REST OF US!
Fissile starter kit includes 100g of each!
U235 & Pu239
New in this edition!
† Materials enrichment on a shoestring
† Radiological devices without critical mass
† Expanded index of poorly guarded US nuclear facilities
©Sedition.com

Iran's paramilitary militia helping maintain internal security…

Primary Goal is:
Defeat of "Westoxification," Iranian term for the harming of Persian culture by Western influences present in the cyber realm...

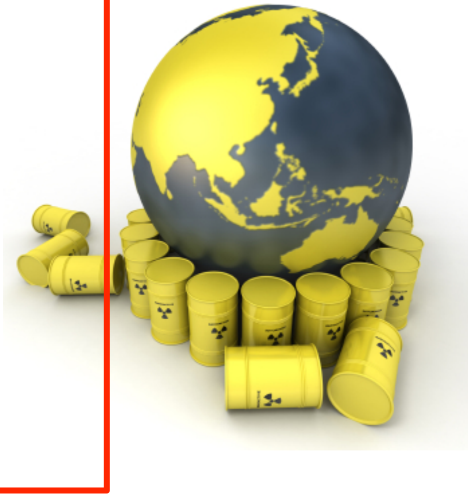
http://iranbriefing.net/?p=2682
http://www.foxnews.com/story/0,2933,534116,00.html

Red-DragonRising.com©

Iranian Cyber Police….

Iran: website filtering policy:

- ❑ Google Plus network blocked;
- ❑ Plan to unblock Facebook denied and/or
- ❑ Iranian top cyber police official:
- ❑ ….Facebook may be unblocked in the future….



http://www.darkgovernment.com/news/iran-ceating-its-own-internet/
http://www.hotforsecurity.com/blog/iran-allegedly-detected-massive-western-cyber-attack-2479.html

Red-DragonRising.com©

Committee to Identify Unauthorized Sites

Iran squeezes Web surfers, prepares censored national intranet

Iranians have lost the right to surf the Web anonymously at Internet cafes as the government reportedly moves closer to its ultimate goal of replacing the global network with a censored national intranet.

Iranian Government officials claim they need to control access to the Internet to counter what they say is a “soft” cultural war being waged by Western countries to influence the morals of Iranians.

Red-DragonRising.com©

http://privacy.cytalk.com/2012/01/iran-squeezes-web-surfers-prepares-censored-national-intranet/

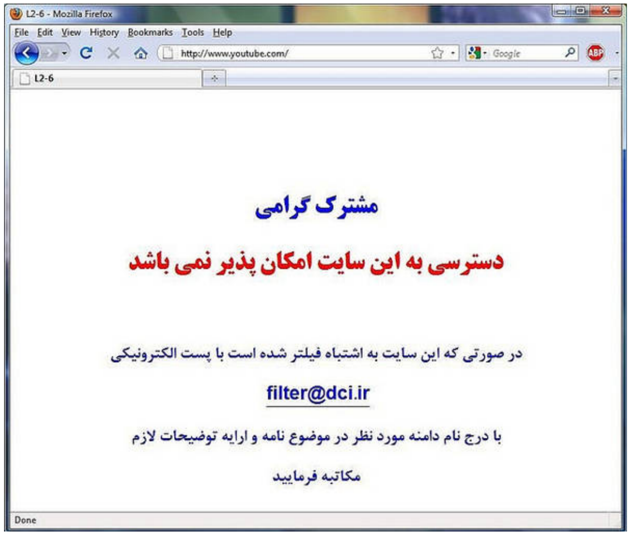
IRAN’s National Internet Project

Google, Gmail blocked as Iran pushes 'national Internet'

Reza Taghipour, Iran's information and communications minister, first phase of Iran’s nationwide project, covering governmental institutions in 29 provinces launched September 21.

Taghipour said all Iranian universities would become part of this network by early 2013, putting Iran a step closer to disconnecting itself entirely from the global Internet.

حلال
HALAL
Access
to this site is Denied
برابر قوانین جمهوری اسلامی ایران و دستور مقامات قضایی
دسترسی به این سایت مجاز نمی باشد



مشترک گرامی

دسترسی به این سایت امکان پذیر نمی باشد

در صورتی که این سایت به اشتباه فیلتر شده است با پست الکترونیکی

filter@dci.ir

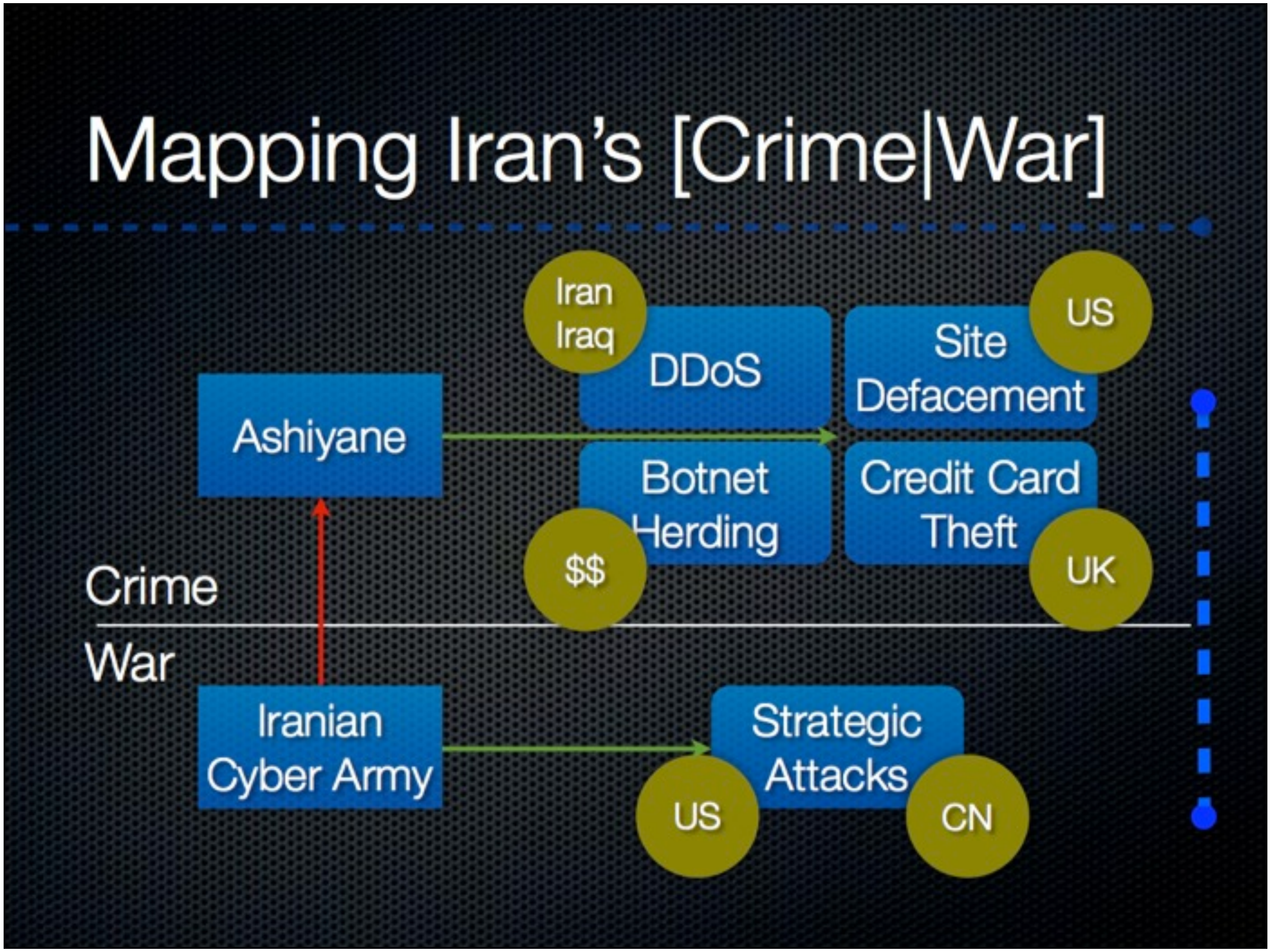
با درج نام دامنه مورد نظر در موضوع نامه و ارایه توضیحات لازم

مکاتبه فرمایید

Red-DragonRising.com©

http://www.huffingtonpost.com/huff-wires/20121010/ml-iran-spies-online/
http://www.abna.ir/data.asp?lang=3&Id=351147

Crime Pays…Not War… in Iran…



Mapping Iran's [Crime|War]

http://forum.internet-haganah.com/showthread.php?876-Behrouz-Kamalian-IRGC-cyber-operative-and-EU-designated-human-rights-abuser

Cyber Initiative Comparison

Characteristics	Iran	Russia	China
Started IW/EW	**2005**	1999	1995
Founding Father	**Major General Yahya Rahim Safavi**) رحیم صفوی (	S.P. Rastorguev (Расторгуев С.П.) & Marshall Sergeyev (Маршалл Сергеев)	Major General Wang Pu Feng (少將王浦峰)
Used as Combined Arms?	**Yes - 2011**	Yes 2007 & 2008	Yes - 2011
Use of Hacktivism as a Proxy?	**Yes**	Yes – w/criminal intentions	Yes
Official Military Command	**2010**	2010	2010
External Motivators	**United States of America, UK & Israel**	United States of America	United States of America
Internet Controls?	**Yes**	Yes	Yes
Criminal Cyber Capability?	**Yes**	Yes	Yes
Impact on Commerce?	**No**	Yes	Yes

Conclusions

1) Iran, Russia & 中國 plan cyber-espionage – defensively & offensively;
2) Each Nation State has separate & distinct reasons…
3) All Three Countries started their military cyber commands in 2010;
4) As US Militarized Cyber Domain Circa 2010… Iran, China & Russian did so in kind…
5) Cultural, economic, historical & linguistic threads for Iranian, Russian & Chinese cyber-espionage;
6) Citizen hacking an unofficial proxy cyber force multiplier;
7) Commercial enterprises & all organizations worldwide are permeable to cyber hacking in all form & methods;
8) Foreign language malware, RATs, Botnets are undiscoverable….

Conclusions

10) Iranian (Persian), Russian & Mandarin languages are an exceptional forms of cryptography…

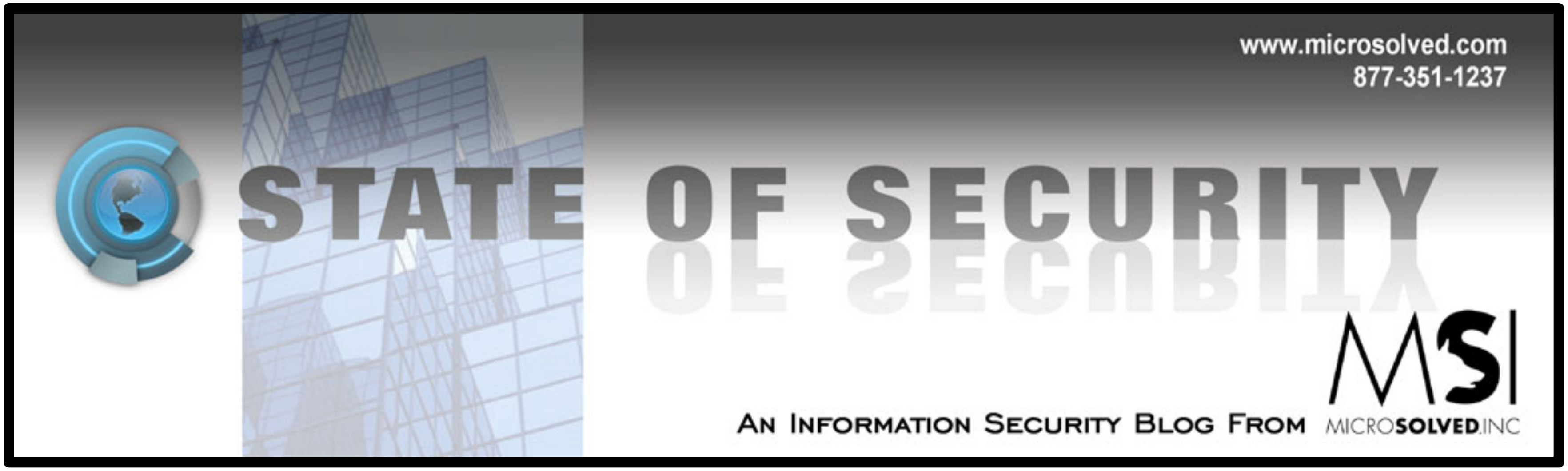
11) All Western InfoSec Technology are ineffective against Foreign cyber attacks…

12) Organizations cannot defend against various alleged Iranian, Russian & Chinese information warfare threats

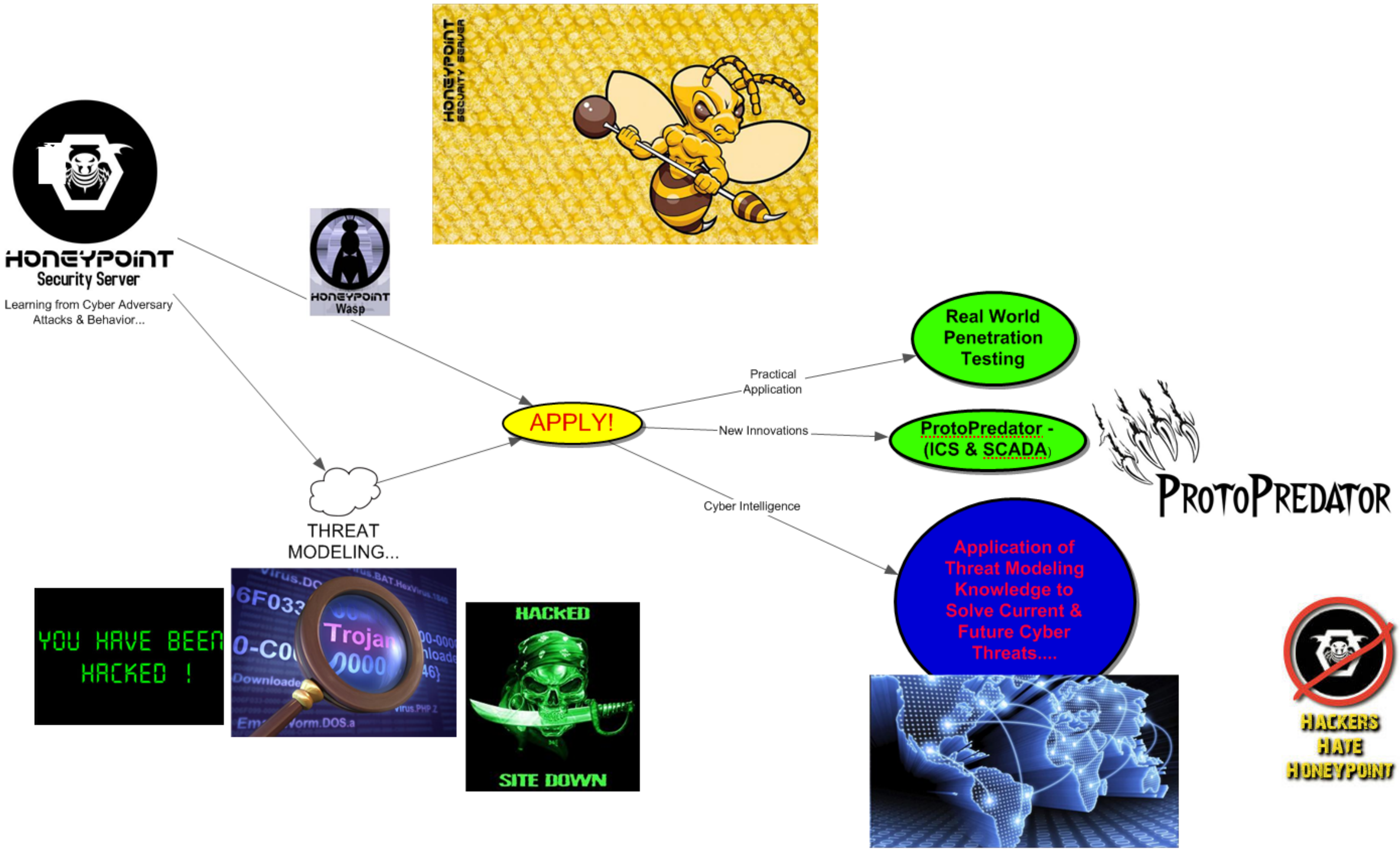
13) Offensive Cyber Capabilities must be developed…..protect your IP & Network

14)Nation State cyber-espionage threats are very serious & will only become much, much worse…..

Stateofsecurity.com



MicroSolved's HONEYPOINT Capabilities....



HONEYPOINT Security Server

Learning from Cyber Adversary Attacks & Behavior...

HONEYPOINT Wasp

THREAT MODELING...

APPLY!

Practical Application

Real World Penetration Testing

New Innovations

ProtoPredator - (ICS & SCADA)

Cyber Intelligence

Application of Threat Modeling Knowledge to Solve Current & Future Cyber Threats....

**MICROSOLVED TELLS YOU WHAT YOUR ADVERSARY IS LOOKING FOR…
TARGETED HONEYPOINT TOOLS OF ENGAGEMENT**

Russian References…

- http://www.mid.ru/bdomp/ns-osndoc.nsf/1e5f0de28fe77fdcc32575d900298676/2deaa9ee15ddd24bc32575d9002c442b%21OpenDocument
- http://kremlin.ru/
- http://www.technologyreview.com/view/418495/russias-cyber-security-plans/
- http://fmso.leavenworth.army.mil/documents/Russianvuiw.htm
- http://www.airpower.au.af.mil/airchronicles/apj/apj96/spec96/thomas.html
- http://www.ewdn.com/2013/01/25/fsb-to-forge-it-shield-against-global-cyber-attacks/
- http://www.ewdn.com/2012/02/02/report-russia-still-a-threat-to-global-cyber-security-but-less-exposed-to-attacks/
- http://www.techweekeurope.co.uk/news/report-super-dangerous-russian-cyber-gang-arrested-68222
- http://www.ewdn.com/2013/02/28/russian-army-develops-cyberattack-defenses/
- http://computer-forensics.sans.org/blog/2011/12/16/digital-forensics-sifting-cheating-timelines-with-log2timeline
- http://eastofcenter.tol.org/2012/06/russian-team-uncovers-stuxnet-on-steroids
- http://rt.com/politics/orders-fsb-sites-attacks-402/
- http://www.defencetalk.com/cyber-superweapon-virus-uncovered-russian-firm-42876/
- http://www.ibtimes.co.uk/articles/453233/20130403/flashback-creator-unmasked-russian-cyber-criminal-maxim.htm?

Iranian References…

- http://www.iranwatch.org/suspect/records/Maj-Gen-Yahya-Rahim-Safavi.html
- http://iranpulse.al-monitor.com/index.php/tag/yahya-rahim-safavi/
- http://www.rferl.org/content/article/1060431.html
- http://www.aljazeera.com/category/person/yahya-rahim-safavi
- http://www.jpost.com/IranianThreat/News/Article.aspx?id=286238
- http://www.reuters.com/article/2012/10/03/us-iran-cyber-idUSBRE8920MO20121003
- http://www.eurasiareview.com/03102012-us-israeli-cyber-attacks-against-iran-continue-with-assault-on-internet-oped/?
- http://www.csoonline.com/article/718068/iran-s-cyberattack-claims-difficult-to-judge-experts-say?source=rss_cso_exclude_net_net
- http://www.cyberstrategie.org/?q=grands-dossiers/conflits-r%C3%A9gionaux-et-cyberterrorisme/structure-of-iran%E2%80%99s-cyber-warfare
- http://thediplomat.com/2012/06/26/is-u-s-in-iran-cyber-war/
- http://iranpulse.al-monitor.com/index.php/2013/02/1323/former-head-of-the-revolutionary-guards-we-will-enter-the-area-if-we-sense-a-threat/#more-1323
- http://thediplomat.com/2012/06/26/is-u-s-in-iran-cyber-war/?all=true
- http://collectinghats.blogspot.com/2009/08/im-not-slow-im-just-american-part-2.html
- http://theriskyshift.com/2012/03/israeli-lobby-in-uk-conspiracy-or-anti-html/
- http://finchin.com/stuxnet-flame-shape-cyberwars-to-come/

People's Republic of China References…

- http://thediplomat.com/2013/04/19/is-cyber-war-the-new-cold-war/?all=true
- http://chinadigitaltimes.net/2013/04/cybersecurity-and-the-new-cold-war/?
- http://thediplomat.com/2011/08/25/did-china-tip-cyber-war-hand/
- http://thediplomat.com/2009/08/13/on-the-cyber-warpath/
- http://thediplomat.com/2011/11/09/china%E2%80%99s-cyber-moves-hurt-beijing/?all=true
- William J. Lynn III W. Defending a New Domain: The Pentagon's Cyberstrategy.// Foreign Affairs. September/October 2010.
- http://www.foreignaffairs.com/articles/66552/william-j-lynn-iii/defending-a-new-domain(29.08.2010)
- http://www.rawstory.com/rs/2010/0829/pentagon-weighs-applying-preemptive-warfare-tactics-internet/ (30.08.2010)
- http://thediplomat.com/2013/04/19/is-cyber-war-the-new-cold-war/?all=true
- http://www.nccgroup.com/en/our-services/security-testing-audit-compliance/technical-security-assessment-penetration-testing/the-latest-origin-of-hacks/

Image References:
http://techandscience.com/
http://www.website-guardian.com/
http://mashable.com/2013/04/23/global-malware-report/